



Concepts et procédures avancés AMS

Guide de l'utilisateur avancé d'AMS



Version October 3, 2025

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

Guide de l'utilisateur avancé d'AMS: Concepts et procédures avancés AMS

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 appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Qu'est-ce qu'AWS Managed Services ?	1
A propos de ce manuel	2
Plans d'opérations	2
Accélérez le plan des opérations	3
Plan d'opérations avancé	3
Mise en route	4
Termes clés	4
Service description (Description du service)	11
Fonctionnalités du plan d'exploitation avancé d'AWS Managed Services (AMS) AMS	11
Ce que nous faisons, ce que nous ne faisons pas	17
Matrice de responsabilité AMS (RACI)	18
Composants de base de l'environnement AMS	42
Limites du compte AMS	45
Objectifs de niveau de service AMS (SLOs)	48
AWS Services pris en charge	49
Configurations prises en charge	52
Systèmes d'exploitation non pris en charge	55
Interfaces avancées AMS	56
Points de terminaison d'un VPC	57
Espaces de noms protégés par AMS	58
Préfixes réservés AMS	60
Fenêtre de maintenance AMS	61
Ressources d'information AMS	61
Conformité avec AMS	62
Normes de conformité prises en charge par AMS	62
Responsabilité partagée	68
Images de machines AMS Amazon (AMIs)	68
Sécurité améliorée AMIs	71
Comment fonctionne l'intégration entre AD FS et AMS	71
Active Directory géré par AMS	73
Déploiements d'applications	76
Gestion des services	78
Gouvernance des comptes	78
Début du service	79

Gestion de la relation client (CRM)	79
Processus CRM	80
Réunions CRM	81
Arrangements de réunions CRM	82
Rapports mensuels du CRM	83
Optimisation des coûts	84
Cadre d'optimisation des coûts	84
Matrice de responsabilité pour l'optimisation des coûts	87
Heures de service	89
Obtenir de l'aide	90
Gestion des événements planifiés	91
Critères AMS PEM	91
Types de PEM	91
Le processus AMS PEM	92
PEM FAQs	92
Architecture réseau	94
Architecture réseau MALZ	94
À propos de l'architecture du réseau de zones d'atterrissage multi-comptes	94
Choisir un seul MALZ ou plusieurs MALZs	97
Comptes multi-comptes Landing Zone	103
Architecture du réseau SALZ	139
Services partagés de zone d'atterrissage à compte unique AMS	140
Configuration d'AMS	142
Paramètres par défaut d'AMS	143
Paramètres de résolution DNS par défaut (MALZ)	143
EC2 Profil d'instance IAM	144
Alertes issues de la surveillance de base dans AMS	152
Valeurs par défaut de conservation et de rotation des journaux	171
Utilisation des consoles AMS	172
Utilisation de l'API et de la CLI AMS	174
Points de terminaison HTTP de l'API AMS pour les appels REST	174
Installation ou mise à niveau de l'AMS CLI	175
Utilisation de l'API AMS en CLI, Ruby, Python et Java	177
AMS : apportez votre propre EPS	186
Activez BYOEPS pour votre compte	188
Réception de notifications AMS	191

Notifications AMI AMS avec SNS	192
Notifications de service	196
Notifications de changement d'état RFC	197
Configuration de DNS privés et publics	201
Gestion du trafic de sortie AMS	202
Déploiement de ressources IAM	204
Provisionnement IAM automatisé	204
Configuration des autorisations avec les rôles et profils IAM	229
Demande d'un nouveau rôle d'utilisateur IAM ou d'un nouveau profil d'instance	229
Limitez les autorisations avec des déclarations de politique de rôle IAM	230
Restreindre les autorisations avec les profils d'instance Amazon EC2 IAM	231
Règle de réclamation AD FS et paramètres SAML	232
Configurations des règles de réclamation ADFS	232
console Web	233
Accès à l'API et à la CLI avec SAML	233
Restreindre avec l'ACL réseau	237
AMS sur Outposts	238
AWS Outposts gestion de l'installation et des opérations	238
Provisionnement de ressources gérées par AMS sur AWS Outposts	241
Limitations d'AMS sur AWS Outposts	241
AMS sur la AWS Outposts conformité	243
AMS activé AWS Outposts FAQs	244
Utilisation d'étiquettes	246
Marquage automatique de l'infrastructure AMS	247
Tags recommandés par AMS	249
Étiqueter les notes de mise à jour	253
Planificateur de ressources	255
Déploiement du planificateur de ressources	256
Personnalisation du planificateur de ressources	256
Utilisation du planificateur de ressources	257
Estimateur de coûts AMS Resource Scheduler	258
Bonnes pratiques du planificateur de ressources AMS	259
AWS Systems Manager dans AMS Advanced	261
Documents AMS Advanced SSM disponibles	262
Versions des documents AMS Advanced SSM	262
Tarification Systems Manager	263

Comptes AMS externes	263
Déconnectez-vous des comptes de zone d'atterrissage à compte unique	264
Déconnectez-vous des comptes de zone d'atterrissage multi-comptes	268
Modes de gestion des modifications	290
Vue d'ensemble des modes	291
Types de modes et de comptes dans AMS	292
Modes AMS et applications ou charges de travail	295
Cas d'utilisation réels des modes AMS	303
Mode RFC	307
En savoir plus sur RFCs	308
Quels sont les types de modifications ?	349
Résolution des erreurs RFC	362
Mode de changement direct	373
Commencer à utiliser le mode Direct Change	374
Sécurité et conformité	376
Gestion du changement en mode Direct Change	382
Création de piles à l'aide du mode Direct Change	384
Cas d'utilisation du mode de changement direct	388
Mode développeur	388
Commencer à utiliser le mode développeur	390
Sécurité et conformité	392
Gestion des modifications	394
Provisionnement de l'infrastructure	399
Contrôles de détection	400
Journalisation, surveillance et gestion des événements	400
Gestion des incidents	400
Gestion des correctifs	401
Gestion de la continuité	401
Gestion de la sécurité et des accès	401
Mode de provisionnement en libre-service dans AMS	402
Commencer à utiliser le mode SSP dans AMS	403
Amazon API Gateway	403
Alexa for Business	404
Amazon AppStream 2.0	406
Amazon Athena	409
Amazon Bedrock	410

Amazon CloudSearch	411
Amazon CloudWatch Synthetics	413
Amazon Cognito	414
Amazon Comprehend	416
Amazon Connect	417
Amazon Data Firehose	419
Amazon DevOps Guru	420
Amazon DocumentDB (compatible avec MongoDB)	421
Amazon DynamoDB	422
Amazon Elastic Container Registry	424
EC2 Image Builder	425
Amazon ECS sur AWS Fargate	427
Amazon EKS sur AWS Fargate	429
Amazon EMR	433
Amazon EventBridge	436
Amazon Forecast	438
Amazon FSx	441
Amazon FSx pour OpenZFS	442
Amazon FSx pour NetApp ONTAP	444
Amazon Inspector Classic	446
Amazon Kendra	447
Amazon Kinesis Data Streams	448
Amazon Kinesis Video Streams	449
Amazon Lex	450
Amazon MQ	451
Service géré Amazon pour Apache Flink	452
Amazon Managed Streaming for Apache Kafka	453
Amazon Managed Service for Prometheus	454
Amazon Personalize	456
Amazon QuickSight	458
Amazon Rekognition	460
Amazon SageMaker AI	461
Amazon Simple Email Service	465
Amazon Simple Workflow Service	466
Amazon Textract	467
Amazon Transcribe	468

Amazon WorkSpaces	469
Services liés au code AMS	471
AWS Amplify	475
AWS AppSync	476
AWS App Mesh	477
AWS Audit Manager	478
AWS Batch	479
AWS Certificate Manager	480
AWS Private Certificate Authority	482
AWS CloudEndure	485
AWS CloudHSM	486
AWS CodeBuild	488
AWS CodeCommit	489
AWS CodeDeploy	491
AWS CodePipeline	492
AWS Compute Optimizer	494
AWS DataSync	495
AWS Device Farm	497
AWS Elastic Disaster Recovery	498
AWS Elemental MediaConvert	499
AWS Elemental MediaLive	500
AWS Elemental MediaPackage	501
AWS Elemental MediaStore	502
AWS Elemental MediaTailor	503
AWS Global Accelerator	504
AWS Glue	505
AWS Lake Formation	507
AWS Lambda	508
AWS License Manager	510
AWS Migration Hub	511
AWS Outposts	512
AWS Resilience Hub	512
AWS Secrets Manager	514
AWS Security Hub	517
AWS Service Catalog AppRegistry	518
AWS Shield	519

AWS Snowball Edge	520
AWS Step Functions	522
AWS Systems Manager Magasin de paramètres	523
AWS Systems Manager Automatisation	524
AWS Transfer Family	528
AWS Transit Gateway	529
AWS WAF	530
AWS Well-Architected Tool	531
AWS X-Ray	532
VM Import/Export	534
Mode géré par le client	535
Commencer à utiliser le mode géré par le client	536
AMS et AWS Service Catalog	536
Commencer à utiliser Service Catalog	536
Service Catalog dans AMS avant de commencer	537
Trouver les données dont vous avez besoin (SKMS)	541
Qu'est-ce que la gestion des connaissances liées aux services ?	541
Trouvez un VPC IDs	542
Rechercher un sous-réseau IDs	544
Trouvez l'AMI IDs	547
Rechercher un groupe de sécurité (SG) IDs	548
Rechercher des entités IAM	549
Trouver une pile IDs	549
Rechercher une instance IDs ou une adresse IP	551
Trouvez ARNs	554
Rechercher des ressources par ARN	556
Rechercher les paramètres du compte	557
Trouvez FQDNs	559
Trouver les zones de disponibilité (AZs)	560
Rechercher des sujets sur les réseaux sociaux	560
Rechercher les paramètres de sauvegarde	561
Gestion de l'accès	562
Qu'est-ce que la gestion des accès ?	562
Pourquoi et quand accédons-nous à votre compte	563
Comment et quand utiliser root	568
Console AMS Advanced et Amazon EC2 Access	569

Accès à la console AWS de gestion et à la console AMS	570
Accès temporaire à la console AMS	570
Accès aux instances à l'aide de bastions	571
Noms de bastion compatibles avec le DNS	573
Réduction des coûts sur les bastions de la zone d'atterrissage à compte unique (SALZ)	574
Utilisation des adresses IP bastions	575
Exemples d'accès aux instances	576
Contrôle d'accès basé sur l'équipe ou le rôle dans un compte AMS	587
Configuration d' EC2 instance automatisée	588
Conditions préalables à la configuration automatique des instances	588
Installation automatique de l'agent SSM	589
Prérequis	589
Demander l'installation automatique de l'agent SSM	590
Comment fonctionne l'installation automatique de l'agent SSM	590
Modifications automatisées	591
Mettre à jour automatiquement le code sur les instances Linux	591
Mettre à jour automatiquement le PBIS sur les instances Linux	592
Mettre à jour automatiquement la version minimale de SSM et des agents CloudWatch	593
CloudWatch fichiers de configuration, détails des mises à jour	594
Logs configurés automatiquement	595
Surveillance et gestion des événements	596
Qu'est-ce que le monitoring ?	597
Qu'est-ce que le système de surveillance AMS surveille ?	598
Surveillance proactive d'Active Directory Trust par zone d'atterrissage à compte unique	599
Fonctionnement de la surveillance	599
EC2 notifications groupées par instances	601
Notification d'alerte basée sur des balises	602
Afficher la configuration de surveillance d'un compte	603
Modification de la configuration de surveillance d'un compte	604
Notifications d'incidents liées aux applications dans AMS	604
Fournissez AppRegistry des informations sur votre compte AMS et créez des applications .	605
Créez des balises pour permettre l'enrichissement des dossiers	605
Personnalisez la gravité des demandes de support AMS en fonction de vos applications	605
Vérifiez les autorisations requises	606
En utilisant OpsCenter	607
Notifications d'alerte	608

Réception d'alertes	608
Notifications d'alerte basées sur des balises	609
Correction automatique des alertes par AMS	610
Création d' CloudWatch alarmes supplémentaires	618
Création de CloudWatch métriques et d'alarmes personnalisées	620
Utilisation d' CloudWatch Application Insights pour .Net et SQL Server	621
Routeur d'événements AMS	622
Amazon EventBridge Managed Rules déployées par AMS	622
Création de règles gérées pour AMS	623
Modification des règles gérées pour AMS	623
Suppression de règles gérées pour AMS	623
Correcteur fiable	623
Principaux avantages	624
Comment fonctionne Trusted Remediator	624
Termes clés	625
Commencez avec Trusted Remediator	626
Recommandations de Compute Optimizer prises en charge	630
Trusted Advisor Chèques pris en charge	635
Configuration de la correction des chèques	695
Flux de décision concernant le mode d'exécution	700
Configurer les didacticiels de correction	700
Travailler avec des mesures correctives	702
Journaux de correction	707
Bonnes pratiques	710
FAQs	710
Gestion des journaux	713
Qu'est-ce que la gestion des journaux ?	713
Comment fonctionne la journalisation AMS	713
Accès à vos journaux	714
Journaux de service agrégés AMS	714
Journaux des services partagés AMS	731
Amazon Elastic Compute Cloud (Amazon EC2) : journaux au niveau du système	734
Intégration à Splunk	736
Personnalisation de la configuration de votre journal	736
Modification de la conservation des CloudWatch journaux	736
Activer la journalisation pour les services pris en charge	737

Gestion de la sécurité	738
Protection des données dans AMS	738
Amazon Macie	739
GuardDuty	741
Pare-feu DNS Amazon Route 53 Resolver	744
AWS Certificate Manager certificat (ACM)	746
Chiffrement des données dans AMS	746
Identity and Access Management	748
Mesures de protection IAM pour les zones d'atterrissage multicomptes (MALZ)	748
Authentification par des identités	749
Enregistrement et surveillance des événements de sécurité	771
Sécurité des terminaux (EPS)	771
Processus d'atténuation des malwares	776
Sécurité d'Amazon Inspector	778
Réponse aux incidents AMS	780
Validation de conformité	781
Zone d'atterrissage multi-comptes affichant l'état de conformité de votre AWS Config	
Rules	781
Restrictions relatives à la politique de contrôle du service de zone d'atterrissage multi-	
comptes AMS	782
Résilience	783
Sécurité de l'infrastructure	783
Bonnes pratiques de sécurité	816
Zone d'atterrissage multi-comptes AMS (paramètres EPS autres que ceux par défaut)	816
Rambardes AMS	816
Politiques de contrôle des services MALZ	816
Réponse aux incidents de sécurité	816
Fonctionnement	817
Préparation	818
Détection	819
Analyser	820
Contenir	821
Éradiquer	823
Récupération	824
Rapport post-incident	824
Runbooks de réponse aux incidents de sécurité	825

Examens de sécurité des demandes de modification dans AMS Advanced	831
Processus de gestion des risques liés à la sécurité des clients	832
Normes techniques AMS Advanced	832
Commandes standard dans AMS Advanced	833
Changements qui introduisent des risques de sécurité élevés ou très élevés dans votre environnement	861
Gestion de la continuité	864
Qu'est-ce que la gestion de la continuité ?	864
Comment fonctionne la gestion de la continuité	864
Plans de sauvegarde	865
Coffres-forts de sauvegarde	868
Backup : types de modifications	870
Surveillance et génération de rapports pour les sauvegardes	870
Réponse à la reprise après sinistre	871
Planification de la reprise après sinistre	872
Multisite ou haute disponibilité (HA)	872
Secours semi-automatique	873
Veilleuse	874
Sauvegarde et restauration	875
Gestion des correctifs	881
AMS Patch Orchestrator : un modèle de patching basé sur des balises	883
Utilisation de Patch Orchestrator	884
Conditions préalables requises pour Patch Orchestrator	888
Fenêtres de correctifs	889
Notifications de correctifs	890
Références de correctifs	893
Balises réservées à Patch Orchestrator	893
Correctifs à la demande	894
Correctif standard AMS	894
Systèmes d'exploitation pris en charge	896
Patches pris en charge	896
Conception des correctifs et de l'infrastructure	899
Comment fonctionne l'application de correctifs standard AMS	900
Défaillances des correctifs standard AMS	905
Actions que vous pouvez effectuer dans le cadre de l'application de correctifs standard AMS	906

Correctif standard AMS FAQs	910
Engagements relatifs aux services de correction	912
Correctifs standard	912
Correctifs critiques	914
Rapports et options	918
Rapports sur demande	918
Rapports de patch AMS	919
Rapports AMS Backup	928
Incidents évités et suivi des rapports Top Talkers	930
Rapport détaillé sur les frais de facturation	932
Rapports Trusted Remediator	934
Rapports en libre-service	937
Opérations internes de l'API	938
Rapport de patch (quotidien)	942
Rapport de sauvegarde (quotidien)	952
Rapport d'incident (hebdomadaire)	957
Rapport de facturation (mensuel)	960
Rapports agrégés	963
Tableaux de bord de rapports en libre-service AMS	965
Stratégie de conservation des données	973
Débarquer de la SSR	974
Obtenez de l'aide	975
Gestion des incidents	975
Qu'est-ce que la gestion des incidents ?	977
Engagements relatifs aux services de gestion des incidents	978
Exemples de gestion des incidents	981
Gestion des demandes de service	987
Quand utiliser une demande de service	988
Comment fonctionne la gestion des demandes de service	989
Tester une demande de service	990
Création d'une demande de service	990
Surveillance et mise à jour des demandes de service	993
Répondre à une demande de service générée par AMS	994
Questions relatives à la facturation	995
Opérations à la demande	996
Demande d'opérations AMS à la demande	1006

Apporter des modifications aux offres d'opérations à la demande 1007

Historique du document 1008

 Mises à jour antérieures 1027

..... mlx

Qu'est-ce qu'AWS Managed Services ?

Bienvenue sur AWS Managed Services (AMS), la gestion des opérations d'infrastructure pour Amazon Web Services (AWS). AMS est un service d'entreprise qui assure la gestion continue de votre AWS infrastructure.

Ce guide de l'utilisateur est destiné aux professionnels de l'informatique et des développeurs d'applications. Une compréhension de base des termes et pratiques relatifs aux fonctionnalités informatiques, à la mise en réseau et au déploiement d'applications est supposée.

AMS met en œuvre les meilleures pratiques et assure la maintenance de votre infrastructure afin de réduire vos frais d'exploitation et vos risques. AMS fournit des services de cycle de vie complet pour fournir, exécuter et soutenir votre infrastructure, et automatise les activités courantes telles que les demandes de modification, la surveillance, la gestion des correctifs, la sécurité et les services de sauvegarde. AMS applique les politiques de votre entreprise et de votre infrastructure de sécurité, et vous permet de développer des solutions et des applications en utilisant votre approche de développement préférée.

Pour mieux comprendre l'architecture AMS, consultez [ces diagrammes](#).

Rubriques

- [À propos de ce guide de l'utilisateur AMS](#)
- [Plans d'opérations AMS](#)
- [Commencer à utiliser AWS Managed Services](#)
- [Termes clés d'AMS](#)
- [Service description \(Description du service\)](#)
- [Ressources d'information AMS](#)
- [Conformité avec AMS](#)
- [Images de machines AMS Amazon \(AMIs\)](#)
- [Comment fonctionne l'intégration entre AD FS et AMS](#)
- [Active Directory géré par AMS](#)
- [Déploiements d'applications AMS](#)

 Note

De nouveaux Régions AWS sont ajoutés fréquemment. Pour les systèmes d'exploitation les plus récents compatibles avec Régions AWS AMS et les plus récents compatibles avec AMS, voir. [Configurations prises en charge](#)

Pour en savoir plus Régions AWS, consultez [la section Gestion Régions AWS](#).

AMS cherche à améliorer continuellement ses services en fonction de vos commentaires. Nous utilisons plusieurs mécanismes pour activer votre libre-service, automatiser les tâches répétitives et implémenter les nouvelles fonctionnalités au fur Services AWS et à mesure de leur sortie. Vous pouvez soumettre une demande de service AMS à tout moment pour suggérer de nouvelles fonctionnalités ou des améliorations de fonctionnalités.

Les heures d'ouverture d'AMS sont 24 heures par jour, 7 jours par semaine, 365 jours par an.

AMS suit un ensemble de pratiques de gestion des services informatiques (ITSM) qui visent à aligner les services informatiques sur les besoins de votre entreprise.

À propos de ce guide de l'utilisateur AMS

Ce guide de l'utilisateur est destiné aux clients AMS Advanced disposant d'une zone d'atterrissage multi-comptes ou monocomptes. Pour plus de détails sur les offres de zones d'atterrissage AMS, consultez les [termes clés d'AMS](#) ; voir également Architecture de [zones d'atterrissage multicomptes et architecture de zones d'atterrissage à compte unique](#).

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-day infrastructure 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.

AMS Advanced propose également différents SLAs. Pour plus d'informations, consultez la [description du service AWS Managed Services AMS Advanced](#).

Commencer à utiliser AWS Managed Services

Pour en savoir plus sur la prise en main du service AMS de zone d'atterrissage multi-comptes, consultez l'introduction à l'[intégration d'AWS Managed Services](#). Les deux guides d'intégration fournissent des descriptions du service et des questions à prendre en compte pour vous aider à démarrer. Consultez l'ensemble des [fonctionnalités d'AWS Managed Services](#) Features et les ressources actuelles sur [AWS Managed Services Resources](#).

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 Advanced (AMS) est un plan d'exploitation du service AWS Managed Services destiné à gérer les opérations de votre AWS infrastructure. AMS Advanced fournit des opérations d'infrastructure de routine telles que les correctifs, la gestion de la continuité, la gestion de la sécurité et les processus de gestion informatique tels que la gestion des incidents, des modifications et des demandes de service. Pour obtenir la liste des services pris en charge, consultez [AWS Services pris en charge](#).

YouTube Vidéo : [Comment AMS peut-il m'aider à atteindre l'excellence opérationnelle dans le cloud ?](#)

Rubriques

- [Fonctionnalités du plan d'exploitation avancé d'AWS Managed Services \(AMS\) AMS](#)
- [Ce que nous faisons, ce que nous ne faisons pas](#)
- [Matrice de responsabilité AMS \(RACI\)](#)
- [Composants de base de l'environnement AMS](#)
- [Limites du compte AMS](#)
- [Objectifs de niveau de service AMS \(SLOs\)](#)
- [AWS Services pris en charge](#)
- [Configurations prises en charge](#)
- [Fonctionnalités pour les systèmes d'exploitation non pris en charge dans AMS](#)
- [Interfaces avancées AMS](#)
- [Points de terminaison VPC AMS](#)
- [Espaces de noms protégés par AMS](#)
- [Préfixes réservés AMS](#)
- [Fenêtre de maintenance AMS](#)

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

AMS Advanced propose les fonctionnalités suivantes pour les AWS services pris en charge :

- Journalisation, surveillance, garde-fous et gestion des événements :

AMS configure et surveille votre environnement géré pour enregistrer les activités et définit les alertes en fonction de divers contrôles de santé. Les alertes sont examinées par AMS pour les

services AWS applicables, et celles qui ont un impact négatif sur votre utilisation de ces services entraînent la création d'incidents. AMS agrège et stocke tous les journaux générés à la suite de toutes les opérations et journaux système dans Amazon S3. CloudWatch CloudTrail Vous pouvez demander la mise en place d'alertes supplémentaires. Outre les contrôles préventifs d'AMS, AMS déploie des garde-fous de configuration et des contrôles de détection pour vous protéger en permanence contre les erreurs de configuration susceptibles de réduire l'intégrité opérationnelle et de sécurité des comptes gérés, afin de renforcer vos contrôles tels que le balisage et la conformité. Lorsqu'un contrôle surveillé est détecté, une alarme est générée qui entraîne la notification, la modification ou l'arrêt des ressources sur la base de valeurs AMS par défaut prédéfinies que vous pouvez modifier.

- Gestion de la continuité (Backup and Restore) :

AMS fournit des sauvegardes des ressources à l'aide de la fonctionnalité AWS Backup standard existante selon un intervalle planifié que vous avez déterminé. Les actions de restauration à partir de snapshots spécifiques peuvent être effectuées par AMS avec votre RFC. Il est de votre responsabilité de sauvegarder les modifications de données qui se produisent entre les intervalles de capture. Vous pouvez soumettre une RFC pour des demandes de sauvegarde ou de capture d'écran en dehors des intervalles planifiés. En cas d'indisponibilité de la zone de disponibilité (AZ) dans une AWS région, AMS restaure l'environnement géré avec votre autorisation en recréant de nouvelles piles sur la base de modèles et des instantanés EBS disponibles des piles concernées.

- Gestion de la sécurité et des accès :

AMS assure la sécurité des terminaux (EPS), notamment en configurant une protection antivirus et anti-malware. Vous pouvez également utiliser vos propres outils et processus EPS et ne pas utiliser AMS pour EPS en utilisant une fonctionnalité appelée « Bring your own EPS » (BYOEPS). AMS configure également les fonctionnalités de AWS sécurité par défaut que vous avez approuvées lors de l'intégration, telles que les rôles AWS Identity and Access Management (IAM) et les groupes de EC2 sécurité Amazon, et utilise des AWS outils standard (par exemple, Amazon AWS Security Hub Macie, Amazon GuardDuty) pour surveiller les problèmes de sécurité et y répondre. Vous gérez vos utilisateurs par le biais d'un service d'annuaire approuvé que vous fournissez. Pour obtenir la liste des services d'annuaire approuvés, voir [Configurations prises en charge](#).

AMS inclut la sécurité des terminaux (EPS), qui inclut un antivirus (AV), et une protection contre les programmes malveillants, la détection des malwares et des intrusions (Trend Micro). Les groupes de sécurité sont définis par modèle de pile et sont modifiés au lancement en fonction de la visibilité des groupes de sécurité (publics/privés) de l'application.

L'accès aux systèmes est demandé par le biais de demandes de modification (RFCs) relatives à la gestion des modifications. La gestion des accès permet d'accéder à des ressources distinctes, telles que les EC2 instances Amazon AWS Management Console, et APIs. Après avoir établi une relation de confiance unidirectionnelle avec un déploiement d'AMS Microsoft Active Directory lors de l'intégration et de la fédération à AWS, vous pouvez utiliser vos informations d'identification d'entreprise existantes pour toutes les interactions.

- Gestion des correctifs :

AMS applique et installe des mises à jour aux EC2 instances des systèmes d'exploitation pris en charge (OSs) et aux logiciels préinstallés avec les systèmes d'exploitation pris en charge. Pour obtenir la liste des systèmes d'exploitation pris en charge, consultez [Configurations prises en charge](#).

AMS propose deux modèles de patching :

- correctif standard AMS pour les correctifs traditionnels basés sur les comptes, et
- AMS Patch Orchestrator, pour l'application de correctifs basés sur des balises.

Dans le correctif standard d'AMS, vous choisissez une fenêtre de maintenance mensuelle pour qu'AMS effectue la plupart des activités de mise à jour. AMS applique les mises à jour de sécurité critiques en dehors de la fenêtre de maintenance sélectionnée (avec les notifications appropriées) et les mises à jour importantes pendant la fenêtre de maintenance sélectionnée. AMS applique également des mises à jour aux outils de gestion de l'infrastructure pendant la période de maintenance sélectionnée. Vous pouvez exclure les piles de la gestion des correctifs ou rejeter les mises à jour, si vous le souhaitez.

Avec AMS Patch Orchestrator, vous définissez une fenêtre de maintenance par défaut par compte pour permettre à AMS d'effectuer des activités d'application de correctifs. Vous pouvez planifier des fenêtres de maintenance personnalisées supplémentaires pour AMS afin de patcher un ensemble spécifique d'instances que vous avez défini à l'aide de balises. AMS applique toutes les mises à jour disponibles, mais vous pouvez filtrer ou rejeter les mises à jour en créant une ligne de base de correctifs personnalisée. Pour les deux modèles, si vous approuvez ou rejetez une mise à jour fournie dans le cadre de la gestion des correctifs, mais que vous changez d'avis par la suite, il vous incombe de lancer la mise à jour via une RFC. AMS suit l'état des correctifs des ressources et met en évidence les systèmes qui ne sont pas à jour dans la revue commerciale mensuelle. La gestion des correctifs est limitée aux piles de l'environnement géré, y compris toutes les applications gérées par AMS et les services AWS pris en charge dotés de fonctionnalités d'application de correctifs (par exemple, RDS). Afin de prendre en charge tous

les types de configurations d'infrastructure lors de la publication d'une mise à jour, AMS a) met à jour l' EC2 instance et b) fournit une AMI AMS mise à jour que vous pouvez utiliser. Il est de votre responsabilité d'installer, de configurer, de corriger et de surveiller toutes les applications supplémentaires qui ne sont pas spécifiquement abordées ci-dessus.

- Gestion du changement :

La gestion des modifications AMS est le mécanisme qui vous permet de contrôler les modifications dans votre environnement géré. AMS utilise une combinaison de contrôles préventifs et de détection pour faciliter ce processus et fournit différents niveaux de contrôle et de risque associé en fonction du mode AMS sélectionné.

Toutes les actions effectuées dans votre environnement AMS sont enregistrées AWS CloudTrail.

Pour plus d'informations sur la gestion des modifications AMS et les différents modes, consultez le [guide de gestion des modifications AMS](#) et les [modes AMS](#).

- Gestion automatisée et en libre-service du provisionnement :

Vous pouvez mettre en service des ressources AWS sur AMS Advanced de différentes manières :

- Soumettre des demandes de modification de provisionnement et de configuration () RFCs
- Déploiement via AWS Service Catalog
- Déploiement via le [mode Direct Change](#)
- Déployez via [le mode développeur](#). N'oubliez pas que les ressources créées via le mode développeur ne sont pas gérées par AMS.
- Configurez les services AWS directement à l'aide du provisionnement en libre-service pour select Services AWS (voir [AWS Services pris en charge](#)).

- Gestion des incidents :

AMS vous informe de manière proactive des incidents détectés par AMS. AMS répond aux incidents soumis par le client et générés par AMS et résout les incidents en fonction de la priorité de l'incident. Sauf indication contraire de votre part, les incidents considérés par AMS comme présentant un risque pour la sécurité de votre environnement géré, ainsi que les incidents liés à la disponibilité d'AMS et d'autres services AWS, sont traités de manière proactive. AMS prend des mesures pour tous les autres incidents une fois que vous avez reçu votre autorisation. Les incidents récurrents sont traités par le processus de gestion des problèmes.

- 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.

- Établissement de rapports :

AMS vous fournit un rapport de service mensuel qui résume les principaux indicateurs de performance d'AMS, y compris 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 gestionnaire de prestation de services cloud (CSDM) AMS qui vous est attribué.

- 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. 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.

- Centre de service :

AMS gère les opérations d'ingénierie avec des employés à plein temps d'Amazon pour répondre aux demandes non automatisées, notamment la gestion des incidents, la gestion des demandes de service et la gestion des modifications. Le Service Desk fonctionne 24 heures sur 24, 7 jours sur 7, 365 jours par an.

- Ressources désignées :

Chaque client se voit attribuer un responsable de prestation de services cloud (CSDM) et un architecte cloud (CA).

- CSDMs peuvent être contactés directement. Ils effectuent des examens des services, des rapports de livraison et des informations tout au long des phases de la mise en œuvre, de la migration et du cycle de vie opérationnel. CSDMs effectuer des examens commerciaux mensuels et détailler des éléments tels que les dépenses financières, les recommandations de réduction des coûts, l'utilisation des services et les rapports sur les risques. Ils étudient en profondeur les statistiques de performance opérationnelle et fournissent des recommandations sur les domaines à améliorer.

- CAs peuvent être contactés directement et fournir une expertise technique pour vous aider à optimiser votre utilisation du AWS cloud. Les activités de CA incluent par exemple la sélection des charges de travail à migrer, l'assistance à l'intégration de comptes et de charges de travail supplémentaires, le rôle de responsable technique des activités opérationnelles telles que les journées de jeu, les tests de reprise après sinistre, la gestion des problèmes et les conseils techniques pour tirer le meilleur parti d'AMS et. AWS CAs animez des discussions techniques à tous les niveaux de votre organisation et aidez à gérer les incidents, à faire des compromis, à établir les meilleures pratiques et à atténuer les risques techniques.
- Mode développeur :

Cette fonctionnalité vous permet d'itérer rapidement les conceptions et les déploiements d'infrastructure au sein de comptes configurés par AMS [1] en autorisant un accès direct au service AWS et à APIs la console AWS en plus de l'accès au processus de gestion des modifications AMS. Les ressources mises en service ou configurées avec les autorisations du mode développeur en dehors du processus de gestion des modifications sont de votre responsabilité (voir « Gestion du provisionnement automatique et en libre-service »). Les ressources mises à disposition via le processus de gestion des modifications AMS sont prises en charge comme les autres charges de travail allouées à la gestion des modifications sur AMS.

- Assistance AWS :

Les clients d'AMS peuvent choisir le niveau de support AWS dont ils ont besoin pour compléter leur plan d'opérations AMS. Les comptes inscrits à AMS peuvent être abonnés au Business Support ou au Enterprise Support. Pour en savoir plus sur les différences entre les plans de support, consultez les [plans de support AWS](#).

- Compte géré par le client :

Cette fonctionnalité vous permet de demander des comptes AWS dans le même environnement géré, mais vous êtes responsable du fonctionnement continu des charges de travail et des ressources AWS au sein de ces comptes. AMS fournit des comptes gérés par les clients, mais une fois les comptes créés, aucune autre fonctionnalité ou service AMS n'est fourni à ces comptes. AWS n'inscrira pas les comptes gérés par les clients au support premium destiné aux entreprises. Il sera de votre responsabilité d'inscrire les comptes gérés par les clients au support AWS au tarif de support que vous avez choisi.

- Gestion du pare-feu :

AMS fournit une solution de pare-feu géré en option pour les services de pare-feu pris en charge, qui permet de filtrer le trafic sortant vers Internet pour les réseaux de votre environnement géré.

Cela exclut les services destinés au public qui n'utilisent pas l'infrastructure réseau AWS et dont le trafic est directement dirigé vers Internet. La solution combine une technologie de pare-feu de pointe avec des fonctionnalités de gestion de l'infrastructure AMS pour déployer, surveiller, gérer, dimensionner et restaurer l'infrastructure de pare-feu.

Lorsque vous embarquez dans AMS, vous recevez une liste complète de votre infrastructure réseau AMS. Pour obtenir à tout moment une liste actualisée des services exécutés pour soutenir votre infrastructure AMS, déposez une demande de service avec des informations spécifiques sur les informations que vous souhaitez. Pour demander une modification de la conception de votre réseau, créez une demande de service décrivant les modifications que vous souhaitez apporter, par exemple en ajoutant un VPC ou en demandant la modification d'une règle de groupe de sécurité.

Ce que nous faisons, ce que nous ne faisons pas

AMS vous propose une approche standardisée pour déployer l'infrastructure AWS et fournit la gestion opérationnelle continue nécessaire. Pour une description complète des rôles, des responsabilités et des services pris en charge, consultez la section [Description du service](#).

Note

Pour demander à AMS de fournir un service AWS supplémentaire, déposez une demande de service. Pour plus d'informations, consultez la section [Faire des demandes de service](#).

- Ce que nous faisons :

Une fois l'intégration terminée, l'environnement AMS est disponible pour recevoir les demandes de modification (RFCs), les incidents et les demandes de service. Votre interaction avec le service AMS tourne autour du cycle de vie d'une pile d'applications. Les nouvelles piles sont commandées à partir d'une liste préconfigurée de modèles, lancées dans des sous-réseaux de cloud privé virtuel (VPC) spécifiques, modifiées au cours de leur durée de vie opérationnelle par le biais de demandes de modification (RFCs) et surveillées pour détecter les événements et les incidents 24 heures sur 24, 7 jours sur 7.

Les piles d'applications actives sont surveillées et maintenues par AMS, y compris en appliquant des correctifs, et ne nécessitent aucune autre action pendant toute la durée de vie de la pile, sauf si une modification est requise ou si la pile est mise hors service. Les incidents détectés par AMS qui affectent l'état et le fonctionnement de la pile génèrent une notification et peuvent nécessiter

ou non une action de votre part pour les résoudre ou les vérifier. Les questions pratiques et autres demandes de renseignements peuvent être posées en soumettant une demande de service.

En outre, AMS vous permet d'activer des services AWS compatibles qui ne sont pas gérés par AMS. Pour plus d'informations sur les services compatibles avec AWS-AMS, consultez la section [Mode de provisionnement en libre-service](#).

- **CE QUE NOUS NE FAISONS PAS :**

Bien qu'AMS simplifie le déploiement des applications en fournissant un certain nombre d'options manuelles et automatisées, vous êtes responsable du développement, des tests, de la mise à jour et de la gestion de votre application. AMS fournit une assistance pour résoudre les problèmes d'infrastructure qui ont un impact sur les applications, mais AMS ne peut pas accéder aux configurations de vos applications ni les valider.

Matrice de responsabilité AMS (RACI)

Note

Afin de remplir ses obligations en temps opportun, AWS Managed Services (AMS) peut avoir besoin de votre contribution pour décider de la marche à suivre appropriée. AMS contactera le contact client désigné pour toutes ces clarifications et informations. AMS s'attend à recevoir une réponse à ces demandes dans les 24 heures ouvrables. En cas d'absence de réponse dans les 24 heures ouvrables, AMS peut choisir une action en votre nom.

La matrice AMS responsable, responsable, consultée et informée, ou RACI, attribue la responsabilité principale soit au client, soit à AMS pour diverses activités.

AMS gère votre infrastructure AWS. Le tableau suivant fournit un aperçu des responsabilités du client et d'AMS en ce qui concerne les activités du cycle de vie d'une application exécutée dans un environnement géré par AMS.

AMS n'est responsable d'aucune des activités suivantes concernant les comptes gérés par le client ou l'infrastructure qui y est exécutée ; par conséquent, ce RACI n'est pas applicable.

- R représente la 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 signifie informé ; une partie qui est informée des progrès, souvent uniquement une fois la tâche ou le résultat livrable terminé.
- Le provisionnement en libre-service fait référence aux ressources mises à disposition par le client en libre-service via l' AWS API ou la console, y compris le mode développeur et les services provisionnés en libre-service.

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.

Pour fournir des fonctionnalités de provisionnement en libre-service, AMS a créé des rôles IAM élevés avec des limites d'autorisation afin de limiter les modifications involontaires liées à l'accès direct aux services. AWS Les rôles n'empêchent pas tous les changements et il vous incombe de respecter vos contrôles internes, de respecter la conformité et de vérifier que tous les AWS services utilisés répondent aux certifications requises. C'est ce que nous appelons le mode de provisionnement en libre-service. Pour plus de détails sur les exigences de AWS conformité, voir [AWS Conformité](#).

Pour les ressources que vous fournissez en libre-service, AMS fournit la gestion des incidents, les contrôles de détection et les garde-fous, les rapports, les ressources désignées (Cloud Service Delivery Manager et Cloud Architect), la sécurité et l'accès, ainsi que le support technique par le biais de demandes de service. En outre, le cas échéant, vous assumez la responsabilité de la gestion de la continuité, de la gestion des correctifs, de la surveillance de l'infrastructure et de la gestion des modifications pour les ressources fournies ou configurées en dehors du système de gestion des modifications AMS.

Activité	Client	AWS Managed Services (AMS)
Cycle de vie des applications		

Activité	Client	AWS Managed Services (AMS)
Développement d'applications	R	I
Analyse et conception des exigences de l'infrastructure des applications	R	C
Conception et optimisation pour les piles AMS non standard	R	C
Conception et optimisation de la pile standard AMS	I	R
Déploiement de l'application	R	C
Déploiement de l'infrastructure AWS	C	R
Surveillance des applications	R	I
Tests et optimisation des applications	R	I
Conseils d'optimisation de l'infrastructure AWS	I	R
Surveillance de l'infrastructure AWS	I	R
Résoudre les problèmes liés aux applications	R	C
Résoudre les problèmes liés au réseau AWS	C	R
Résoudre les problèmes liés au système d'exploitation et à l'infrastructure	C	R
	R	C
Provisionnement en libre-service		
Intégration des applications et de l'ITSM		
Intégration des applications aux offres de services AWS	R	C

Activité	Client	AWS Managed Services (AMS)
Intégration de l'ITSM à l'interface AWS Managed Services	R	C
Réseaux		
Configuration et configuration de VPC et de VPC dans un environnement géré	C	R
Allouer un espace d'adressage privé pour VPCs (par exemple /16)	R	C
Configuration et exploitation de services gérés non AWS, gérés par le client Firewalls/Proxy/Bastions/HOSTs	R	C
Configuration et exploitation de la sécurité AWS Groups/NAT/Customer Bastions/NACL dans l'environnement géré	I	R
Configuration et mise en œuvre du réseau (par exemple DirectConnect) au sein du réseau du client	R	C
Configuration et mise en œuvre du réseau dans l'environnement géré	C	R
Configuration de l'environnement géré		
Définir les paramètres Auto Scaling par défaut pour les modèles Stack de base	I	R
Recommander l'optimisation de l'IR	C	R
Acheter de la capacité RI et PIOP	R	C

Activité	Client	AWS Managed Services (AMS)
Supprimer la capacité lorsque la capacité est surprovisionnée (lorsqu'elle est prise en charge par l'application client)	C	R
Créer/mettre à jour des informations spécifiques aux clients AWS pour AWS Managed Services	C	R
Configuration du S3	C	R
Provisionnement en libre-service	R	C
Configuration du glacier	C	R
Définition de la politique d'archivage	R	C
Configuration de la politique d'archivage	C	R
Sélection de la fenêtre de maintenance client	R	I
Gestion d'AWS RDS		
Surveiller l'état source/replica/RO de la réplication	I	R
Identifiez le RCA du basculement de la source	I	R
Configuration automatique des instantanés (sauvegarde)	C	R
	R	C
Provisionnement en libre-service		
Coordonner et planifier la gestion des correctifs du moteur de base de données	C	R
	R	C
Provisionnement en libre-service		

Activité	Client	AWS Managed Services (AMS)
Recommandez le stockage de base de données et la capacité PIOP	C	R
Provisionnement en libre-service	R	C
Recommander le dimensionnement des instances pour exécuter des bases de données	C	R
Provisionnement en libre-service	R	C
Recommander l'optimisation du RI pour l'environnement géré	C	R
Provisionnement en libre-service	R	C
Surveillance des performances RDS () CloudWatch	C	R
Provisionnement en libre-service	R	C
Configuration de l'abonnement aux événements RDS (SNS)	C	R
Provisionnement en libre-service	R	C
Configuration du groupe de sécurité RDS	C	R
Provisionnement en libre-service	R	C
Configuration du moteur parameter/option RDS	R	C
Conception de table de base de données	R	I
Indexation de base de données	R	I
Analyse du journal de base de données	R	I
Gestion du changement AMS		

Activité	Client	AWS Managed Services (AMS)
Création de clients RFCs (par exemple, accès aux ressources, creating/creating/deleting managed stacks, deploying/creating applications, modifications de la configuration des offres de AWS services)	R	I
Client approbateur RFCs	I	R
Création d'AWS Managed Services RFCs (par exemple, accès aux ressources, création de ressources pour le compte du client, mise à jour du système d'exploitation dans le cadre de la gestion des correctifs)	I	R
Approbation non automatisée RFCs	R	I
Soumission d'une demande pour de nouveaux types de modifications	R	C
Création de nouveaux types de modifications	I	R
Maintenance du calendrier de modification des applications	R	C
Avis concernant la prochaine fenêtre de maintenance	I	R
AWS Service Catalog		
Créez des portefeuilles et des produits	R	I
Distribuer des produits aux utilisateurs finaux	R	I
Création de balises et d'une bibliothèque d'options de balises	R	C

Activité	Client	AWS Managed Services (AMS)
Partage de portefeuilles et de produits avec les utilisateurs finaux	R	I
Réviser/mettre à jour les portefeuilles et les produits	R	I
Création et attribution de contraintes aux portefeuilles et aux produits	R	C
Associer des actions de service à des produits	R	C
Mettre à jour les ressources allouées avec la nouvelle version du produit	R	I
Approvisionnement		
Ajouts spécifiques au client à l'AMI de base d'AWS Managed Services	R	C
Configurer des types de modification approuvés supplémentaires utilisés pour provisionner des modèles Stack	C	R
Lancez les Stacks gérés et les ressources AWS associées soumises via le processus de gestion des modifications AMS ou AWS Service Catalog.	I	R
	R	I
Provisionnement en libre-service		
Install/Update applications personnalisées et tierces sur des instances mises en service via le processus de gestion des modifications AMS ou AWS Service Catalog.	R	I
Provisionnement - Stack Architecture		

Activité	Client	AWS Managed Services (AMS)
Fourniture de licences de système d'exploitation (y compris les frais d'utilisation pour les services AWS applicables, par exemple EC2 et RDS)	I	R
Provisionnement en libre-service	R	I
Définissez des modèles d'infrastructure de base (Stacks) pour le déploiement d'applications via le système de gestion des modifications AMS.	I	R
Provisionnement en libre-service	R	I
Création d'une base de référence approuvée AMIs ⁸	I	R
Évaluez l'inventaire des applications clients et déterminez leur adéquation avec les modèles d'infrastructure disponibles (Stacks)	R	C
Définissez des Stacks uniques qui s'ajoutent aux offres de modèles de base	R	C
Journalisation, surveillance et gestion des événements		
Enregistrement des journaux des modifications de l'infrastructure AWS	I	R
Enregistrement de tous les journaux des modifications apportées aux applications	R	C

Activité	Client	AWS Managed Services (AMS)
Installation et configuration d'agents et de scripts pour l'application de correctifs, la sécurité, la surveillance, etc., de l'infrastructure AWS mise en service via le processus de gestion des modifications AMS.	I	R
	R	C
Provisionnement en libre-service		
Définir les exigences spécifiques du client en matière de surveillance et d'incident	R	C
Configuration des alertes pour l'environnement géré	I	R
Surveillance de toutes les alertes configurées par AMS	I	R
	R	C
Provisionnement en libre-service		
Enquête sur les alertes relatives à l'infrastructure pour la notification d'incidents	I	R
	R	C
Provisionnement en libre-service		
Examen des alarmes liées aux applications	R	C
Gestion des incidents		
Notifier de manière proactive les incidents sur l'infrastructure AWS en fonction de la surveillance	I	R
	R	C
Provisionnement en libre-service		
Gérez les problèmes de performance et les pannes des applications	R	I

Activité	Client	AWS Managed Services (AMS)
Catégoriser la priorité des incidents	I	R
Fournir une réponse aux incidents	I	R
Assurer la résolution des incidents et la restauration de l'infrastructure	C	R
Note SLAs ne s'appliquent pas aux ressources basées sur des instances fournies en dehors de la gestion des modifications d'AMS, y compris celles mises en service via le provisionnement en libre-service et le mode développeur.		
Gestion des problèmes		
Identifier les problèmes dans un environnement géré	C	R
Exécutez le RCA en cas de problème dans un environnement géré	C	R
Résolution des problèmes dans un environnement géré	C	R
Identifier et résoudre les problèmes liés aux applications	R	I
Gestion de la sécurité		

Activité	Client	AWS Managed Services (AMS)
Sécurité de l'infrastructure du client : and/or établissement d'une base de référence pour le processus de conformité en matière de sécurité tel que déterminé et convenu lors de l'intégration du client.	C	R
	R	C
Provisionnement en libre-service		
Maintien de licences valides pour Managed EPS	R	C
Configuration de l'EPS géré	I	R
Provisionnement en libre-service	R	C
Mettre à jour Managed EPS	I	R
Provisionnement en libre-service	R	C
Surveillance des malwares sur les instances provisionnées via le processus AMS CM.	I	R
	R	C
Provisionnement en libre-service		
Gestion et mise à jour des signatures de virus.	I	R
	R	C
Corriger les instances infectées par des logiciels malveillants.	C	R
	R	C
Provisionnement en libre-service		
Gestion des événements de sécurité	C	R
Sécurité - Gestion des accès		

Activité	Client	AWS Managed Services (AMS)
Gérez le cycle de vie des utilisateurs et leurs autorisations pour les services d'annuaire locaux, qui sont utilisés pour accéder à AWS Managed Services	R	I
Utiliser un ou plusieurs systèmes d'authentification fédérés pour l'accès des clients à AWS la console/ APIs	R	C
Accepter et maintenir la confiance d'Active Directory (AD) entre AWS Managed Services AD et AD géré par le client	R	C
Lors de l'intégration, créez des rôles d'administrateur IAM entre comptes au sein de chaque compte géré	R	C
Sécurisez les informations d'identification AWS root pour chaque compte	I	R
Définition des ressources IAM pour l'environnement géré	C	R
Gérez les informations d'identification privilégiées pour l'accès au système d'exploitation pour les ingénieurs AMS	I	R
Gérez les informations d'identification privilégiées pour l'accès au système d'exploitation fournies au client par AMS	R	I
Réponse aux incidents de sécurité - Préparation		
Communications		

Activité	Client	AWS Managed Services (AMS)
Fournir les coordonnées de sécurité du client à AMS à utiliser lors des notifications d'événements de sécurité et des 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	CI	R
Entraînement		
Fournir au client de la documentation pour soutenir AMS pendant le processus de réponse aux incidents	I	R
Pratiquez la responsabilité partagée lors des processus de réponse aux incidents grâce à des journées de jeu sur la sécurité	RI	RC
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 à jour l'inventaire des actifs (AWS ressources) et connaissez leur valeur et leur criticité. Ces informations sont utiles lors de la stratégie de maîtrise des incidents	R	CI
Utilisez des AWS balises pour identifier les ressources et les charges de travail	R	CI
Définition et configuration de la conservation et de l'archivage des journaux	CI	R

Activité	Client	AWS Managed Services (AMS)
Base de référence sécurisée, configurations Compte AWS, politiques et gestion des accès	CI	RC
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	CI	R
Moniteur pris en charge Services AWS pour les alertes de sécurité	I	R
Déployer et gérer les outils de sécurité des terminaux	CI	R
Surveillez la présence de malwares sur les instances à l'aide de l'outil de sécurité des terminaux compatible AMS	I	R
Informez le client des événements détectés par le biais de messages sortants	I	R
Notification d'itinéraire et toute mise à jour ultérieure aux décideurs pour des comptes et des charges de travail spécifiques afin d'améliorer le temps de réponse aux incidents	R	CI
Définissez, déployez et gérez les services de détection standard AMS (par exemple, Amazon GuardDuty et AWS Config)	CI	R
Enregistrer les journaux AWS des modifications de l'infrastructure	I	RC

Activité	Client	AWS Managed Services (AMS)
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	RCI	R
Signalement des événements de sécurité		
Signaler à AMS une activité suspecte ou une enquête de sécurité en cours	R	CI
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	CI
Réponse aux incidents de sécurité - Analyser		
Enquête 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	RC
Évaluez false/true les résultats positifs à l'aide des données disponibles	RI	RC
Générez un instantané des instances concernées à partager avec le client si nécessaire	I	R

Activité	Client	AWS Managed Services (AMS)
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	CI
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	RCI	RC
SMEs Participez Services AWS aux enquêtes de sécurité	CI	R
Engagez des fournisseurs tiers lors de l'investigation (par exemple, pour l'investigation anti-malware EPS et pour le dialogue avec l'équipe d' TrendMicro assistance)	RCI	I
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
Contactez 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

Décider de l'exécution de la stratégie de confinement convenue et accepter les conséquences susceptibles d'affecter la disponibilité des services pendant la période de confinement	R	CI
Effectuez une sauvegarde des systèmes concernés pour une analyse plus approfondie	CI	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	CI
Définissez la stratégie de confinement en fonction de l'incident de sécurité et de la ressource affectée	CI	R
Activez le chiffrement et le stockage sécurisé des sauvegardes ponctuelles des systèmes concernés	CI	R
Exécutez les actions de confinement prises en charge pour les AWS ressources, notamment EC2 les instances, le réseau et l'IAM	CI	R

Réponse aux incidents de sécurité - Eradiquer

Stratégie d'éradication et exécution

Activité	Client	AWS Managed Services (AMS)
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	R	CI
Décider de la stratégie d'éradication convenue, du calendrier d'exécution de l'éradication et des conséquences	R	CI
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	CI	R
Éradiquer et renforcer les AWS ressources, notamment les EC2 instances, le réseau et l'éradication de l'IAM	CI	R
Éradication et renforcement des applications et des 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	R	I
Passez en revue les plans de sauvegarde pour restaurer les charges de travail gérées par AMS	CI	R

Activité	Client	AWS Managed Services (AMS)
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
Restaurer les applications et les charges de travail des clients (via des étapes de restauration spécifiques aux applications)	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 correctifs⁹

Surveillez les mises à jour applicables aux systèmes d'exploitation pris en charge et les logiciels préinstallés avec le système d'exploitation pris en charge pour les EC2 instances.

I

R

R

C

Provisionnement en libre-service

Informez le client des mises à jour à venir (s'applique uniquement au patch standard AMS)

I

R

Activité	Client	AWS Managed Services (AMS)
Exclure certaines mises à jour, and/or certains Stacks, des activités d'application de correctifs	R	I
Définissez des calendriers de fenêtres de maintenance par défaut et personnalisés et d'autres paramètres (par exemple, la durée des fenêtres de maintenance) pour appliquer les correctifs (s'applique au patch AMS) (Orchestrateur uniquement)	R	I
Définissez des lignes de base de correctifs personnalisés pour filtrer et exclure des correctifs spécifiques (s'applique uniquement à AMS Patch Orchestrator)	R	I
Marquez les instances pour les associer à des fenêtres de maintenance personnalisées et à des lignes de base de correctifs (s'applique uniquement à AMS Patch Orchestrator)	R	I
Suivez l'état des correctifs des ressources et mettez en évidence les systèmes qui ne sont pas à jour dans la revue commerciale mensuelle.	C	R
Corrigez le système d'exploitation Windows et les packages Microsoft installés sur le système d'exploitation qui sont régis par Windows Update	I R	R -
Provisionnement en libre-service		

Activité	Client	AWS Managed Services (AMS)
Corrigez les applications installées, les logiciels ou les dépendances d'applications non gérés par Windows Update	R	I
Provisionnement en libre-service	R	-
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
Provisionnement en libre-service	R	-
Corrigez les applications installées, les logiciels ou les dépendances d'applications non gérés par le gestionnaire de packages natif du système d'exploitation Linux	R	I
Provisionnement en libre-service	R	-
Gestion de la continuité		
Spécifier les plannings de sauvegarde	R	I
Exécutez les sauvegardes selon le calendrier prévu.	I	R
Provisionnement en libre-service	R	C
Valider les sauvegardes	R	I
Demander des activités de restauration de sauvegarde	R	I

Activité	Client	AWS Managed Services (AMS)
Exécutez des activités de restauration de sauvegarde.	I	R
Provisionnement en libre-service	R	C
Restaurez les piles affectées et. VPCs	I	R
Provisionnement en libre-service	R	C
Restaurer l'application personnalisée/tierce affectée	R	C
Génération de rapports		
Préparer et fournir un rapport de service mensuel	I	R
AMS activé AWS Outposts	R	I
Configurez et récupérez l'historique des audits d'API à la demande (CloudTrail).	I	R
Provisionnement en libre-service	R	I
Fournir un accès à l'historique des incidents via l'interface AWS Managed Services	I	R
Donnez accès à l'historique des modifications via l'interface AWS Managed Services.	I	R
Provisionnement en libre-service	N/A	N/A
Gestion des demandes de service		
Demander des informations à l'aide de demandes de service	R	I
Répondre aux demandes de service	I	R

Activité	Client	AWS Managed Services (AMS)
Pare-feu géré		
Demander le déploiement d'un pare-feu géré par AMS	R	I
Conception et optimisation de l'architecture de pare-feu gérée par AMS	I	R
Déploiement de l'infrastructure AWS et du dispositif de pare-feu géré par AMS	I	R
Fourniture de licences de pare-feu (y compris les frais d'utilisation pour les services AWS applicables, par exemple EC2)	R	I
Définir la liste des domaines autorisés par défaut	I	R
Demande d'ajout, de modification et de suppression de listes d'autorisation et de politiques de sécurité personnalisées	R	I
Configuration des alertes pour le pare-feu géré par AMS	I	R
Surveillance de toutes les alertes configurées par le pare-feu géré par AMS	I	R
Exécuter des sauvegardes de la configuration du pare-feu	I	R
Demander des activités de restauration de sauvegarde	R	I
Mettre à jour les ressources allouées avec la nouvelle version du produit	I	R

Activité	Client	AWS Managed Services (AMS)
Enregistrement des journaux de pare-feu gérés par AMS	I	R
Transférer les journaux depuis le pare-feu géré par AMS vers CloudWatch	I	R
Demander des modifications de configuration dans le pare-feu géré par AMS	R	I
Approuver les modifications de configuration dans le pare-feu géré par AMS	I	R
Exécuter les modifications de configuration dans le pare-feu géré par AMS	I	R

⁸ AMS fournit EC2 uniquement AMIs pour Amazon

⁹ AMS n'est responsable de la fin de vie OSES que lorsque le client signe un accord de support étendu avec le fournisseur du système d'exploitation

Composants de base de l'environnement AMS

Multi-Account Landing Zone

Il s'agit d'une estimation des composants et des coûts potentiels de l'infrastructure dans les comptes principaux. Cela n'inclut pas les autres coûts tels que la bande passante, la surveillance CloudWatch détaillée, la journalisation, les alarmes, Route53, Amazon S3, le Simple Notification Service (Amazon SNS), les instantanés ou les instances Amazon réservées. EC2

Vous payez pour les composants requis par l'infrastructure de zone d'atterrissage AWS gérée par AMS. Selon les estimations, le coût d'un environnement de zone d'atterrissage multi-comptes AMS ordinaire est de 2 450 dollars par mois et de 50 dollars pour un compte d'application simple.

Pour plus d'informations sur les tarifs, consultez la section [Tarification AWS](#).

Composants de base de l'environnement

Composant	Est. Coût	Description
Compte de gestion	60\$	Un compte AWS Organizations Management ; crée et gère financièrement les comptes des membres. Il contient le framework AWS Landing Zone (ALZ), les ensembles de configurations de comptes et les politiques de contrôle des services AWS Organization (SCPs). • Directory Service : 35\$ • CloudTrail: 7\$ • CloudWatch: 6\$ • Autres : 12\$
Compte de services partagés	2 000 USD	Contient l'infrastructure et les ressources nécessaires à la gestion des accès (Active Directory), à la gestion de la sécurité des terminaux (Trend Micro) et à vos bastions (SSH/RDP) ; l'estimation est de 2 400\$ par mois. Cette estimation n'inclut pas le coût des licences Trend Micro. • EC2: 800\$ (avec le nombre minimum de bastions) • ROUGES : 300\$ (EPS) • VPC (points de terminaison) : 400\$ • Directory Service : 300\$ • CloudWatch: 100\$ • GuardDuty : 15\$ • Secrets Manager : 10\$ • Transfert de données : 10\$ • Config : 10\$ • Autres : 45\$
Compte réseau	350\$	Le hub central pour le routage réseau entre les comptes AMS, votre réseau sur site et le trafic de sortie

Composant	Est. Coût	Description
		vers Internet. Il contient également des bastions DMZ publics (point d'entrée permettant aux ingénieurs AMS d'accéder aux hôtes de votre environnement AMS). Le prix peut augmenter en fonction du trafic passant par le Transit Gateway et Direct Connect. • EC2: 250\$ (Bastions) • VPC : 80\$ • Autres : 20\$
Compte Log Archive	20\$	Un compartiment S3 contenant des copies des fichiers journaux AWS CloudTrail et AWS Config de chacun de vos comptes d'environnement AMS. Les coûts augmentent à mesure que de plus en plus de journaux sont collectés. • S3 : 10\$ • CloudWatch: 5\$ • Autres : 5\$
Compte de sécurité	20\$	Le hub central pour les opérations liées à la sécurité et le point principal pour acheminer les notifications et les alertes vers les services du plan de contrôle AMS. Il héberge également le compte de gestion Amazon Guard Duty. Les coûts augmentent à mesure que de plus en plus d'événements sont analysés à l'aide d'Amazon GuardDuty. • CloudWatch: 15\$ • Autres : 5\$

Single-Account Landing Zone

Le tableau suivant répertorie les composants d'un exemple d'infrastructure gérée par AMS.

Composants de base de l'environnement, dernière mise à jour le 09/07/2020

Name (Nom)	Type d'instance	Système d'exploitation	Nombre de composants	
mc-eps-dsm	m5.large	Linux	2	
mc-management	m5.large	Windows	2	
mc-bastion-dmz-ssh	m5.large	Linux	2	
mc-bastion-customer-rdp	m5.large	Windows	2	
mc-eps-relay	m5.large	Linux	2	
services d'annuaire	N/A	N/A		
composants supplémentaires	N/A	N/A		

Pour plus d'informations sur les tarifs, consultez la section [Tarification AWS](#).

Limites du compte AMS

Il existe trois types distincts de limites à prendre en compte dans la zone de destination multi-comptes AMS : les limites de l'API AMS, les limites des ressources AMS et les limites AWS.

Il existe deux types distincts de limites à prendre en compte dans la zone de landing compte unique AMS : les limites de l'API AMS et les limites AWS.

Limites de l'API du compte AMS

Cette section décrit les limites de niveau de compte au-delà desquelles AWS Managed Services (AMS) limite le service d'API AMS SKMS. Cela signifie que si vous appelez l'un des appels listés APIs plus de 10 fois par seconde, l'un des appels est « limité » (vous recevez un `ThrottlingException`). Dans de rares cas, une dépendance externe ou descendante peut limiter l'API AMS, puis AMS peut limiter vos appels d'API à un rythme éventuellement inférieur.

 Note

Pour plus d'informations sur l'API AMS SKMS, téléchargez la référence via l'onglet Rapports de la console AWS Artifact.

Pour chaque API AMS SKMS répertoriée, l'opération est limitée après 10 TPS (transactions par seconde) :

- GetStack
- GetSubnet
- GetVpc
- ListAmis
- ListStackSummaries
- ListSubnetSummaries
- ListVpcSummaries

Limites de ressources des comptes de zone de landing zone multi-comptes AMS

Les limites de ressources des comptes concernent les comptes et VPCs les sous-réseaux d'applications de zone d'atterrissage multi-comptes AMS.

Limites de ressources du compte d'application

Il existe une limite souple de 50 comptes d'applications par organisation. Si vous avez un cas d'utilisation pour plus de 50 comptes d'applications, contactez votre responsable de prestation de services cloud (CSDM) pour lui faire part de vos besoins.

VPCs limites de ressources des sous-réseaux et des sous-réseaux

Il existe une limite souple de 10 VPCs par compte d'application dans la région AWS prédéfinie pour l'organisation.

Chaque VPC peut comporter de 1 à 10 niveaux de sous-réseau privés répartis sur 2 à 3 zones de disponibilité. En outre, chaque VPC peut comporter de 0 à 5 niveaux de sous-réseau publics répartis sur 2 à 3 zones de disponibilité. Si vos exigences dépassent ces limites, informez-en votre CSDM ou votre architecte cloud pour qu'il examine votre cas d'utilisation.

Rapport entre l'application et le compte de la zone d'atterrissage multi-comptes AMS

Un compte par application est pris en charge dans la zone de landing multi-comptes AMS ; toutefois, chaque compte d'application a un faible coût, et vous êtes facturé en fonction du nombre de connexions au Transit Gateway par heure et du volume de trafic qui passe par AWS Transit Gateway. Ainsi, plus les applications sont séparées dans les comptes ou VPCs, plus les coûts sont élevés.

Pour réduire les coûts tout en garantissant une séparation appropriée des tâches, AMS vous recommande 1) de regrouper les applications par équipes dotées de processus métiers étroitement liés, et 2) de ne pas mélanger les applications qui en sont à différents stades (production ou non) ou gérées par différentes équipes. De cette façon, vous aurez moins de comptes, la gestion des accès et la séparation des tâches seront plus faciles, et les coûts de trafic pourraient être atténués.

Par exemple : une entreprise produit une application de trading et une application de gestion de portefeuille. Les deux applications sont gérées par l'équipe informatique des investissements et échangent beaucoup de trafic entre elles. Dans ce scénario, l'entreprise peut bénéficier du regroupement des deux applications dans le même compte et dans le même VPC, car l'équipe informatique des investissements n'aura pas à demander l'accès à plusieurs comptes d'applications et l'entreprise économisera sur les coûts de trafic. Dans ce cas, l'entreprise doit créer un autre compte pour les mêmes applications en phase de développement et fournir un accès à l'équipe de développement.

Dans un autre scénario, l'entreprise dispose en production d'une application de paie et d'une application de comptabilité, gérées respectivement par les équipes informatiques des ressources humaines et de comptabilité. Bien que l'application de paie doive échanger des informations avec l'application de comptabilité, nous recommandons de séparer les deux applications dans des comptes différents, un par équipe, et d'établir une connexion entre les deux applications VPCs utilisant le compte Networking. De cette façon, l'entreprise empêchera l'équipe informatique des ressources humaines de demander des modifications affectant l'infrastructure des applications comptables, dont elle n'aurait aucune connaissance.

Conseils sur la façon de regrouper les comptes en unités organisationnelles (OUs). Une unité d'organisation est un mécanisme de regroupement logique qui vous permet de classer (regrouper) les comptes et d'appliquer des politiques et des configurations en fonction de ces groupes. L'approche recommandée pour les créer OUs consiste à les baser sur des politiques qui doivent être appliquées à un groupe spécifique de comptes, et non sur la hiérarchie interne des équipes au sein de votre structure hiérarchique. Une unité d'organisation n'est pas équivalente à une unité d'organisation Active Directory, et toute tentative de réplique de la structure d'unité d'organisation

AD AWS Organizations est déconseillée et se traduit par une structure d' and/or exploitation difficile à gérer.

AWS limites du compte

AWS les limites de compte s'appliquent à vos comptes AWS Managed Services (AMS). La méthode la plus simple pour déterminer les limites par défaut et actuelles des AWS services consiste à utiliser les [Quotas AWS de Service](#). AMS recommande d'ajuster les limites de service individuelles à la taille appropriée pour exécuter le ou les services du compte. Les limites agissent comme des garde-fous pour protéger vos comptes en termes de sécurité et de réduction des coûts. Si vous souhaitez augmenter une limite spécifique, soumettez une demande de service auprès d'AMS, et AMS Operations augmentera la limite en votre nom. Par exemple, la limite (ou quota) par défaut pour les instances RDS est de 40 ; si votre charge de travail nécessite 50 instances RDS, soumettez une demande de service pour AMS Operations afin d'augmenter la limite à la valeur requise.

Objectifs de niveau de service AMS (SLOs)

Le tableau suivant décrit les objectifs du service AWS Managed Services (AMS). Les accords de niveau de service (SLAs) pour d'autres aspects du service AMS, y compris la gestion des incidents, sont couverts dans le document SLA partagé avec vous lors de votre inscription à AMS. Pour plus d'informations, adressez-vous à votre CSDM.

Objectifs de niveau de service AMS

Fonctionnalité	Indicateur de performance (PI)	De plus (Business Days, M-F 8AM to 6PM local time)	Prime (Calendar Days, 24 x 7)
Gestion des modifications	Temps nécessaire pour planifier ou rejeter automatiquement RFCs	<= 30 minutes	<= 30 minutes
	Heure de lancement de l'heure d'exécution planifiée RFCs par rapport à l'heure d'exécution planifiée	<= 1 minute	<= 1 minute

Fonctionnalité	Indicateur de performance (PI)	De plus (Business Days, M-F 8AM to 6PM local time)	Prime (Calendar Days, 24 x 7)
	Temps nécessaire pour approve/reject ne pas être automatisé RFCs, disponible dans le catalogue CT	<=48 heures	<=24 heures
	Le temps nécessaire pour ne pas approve/reject être automatisé RFCs n'est pas disponible dans le catalogue CT	<=5 jours	<=5 jours
Gestion des problèmes	Temps nécessaire pour terminer l'analyse des causes profondes (RCA)	<=10 jours	<=10 jours
Gestion des demandes de service	Temps de réponse pour la première réponse et pour toutes les réponses suivantes	<=8 heures	<=4 heures

AWS Services pris en charge

AWS Managed Services (AMS) fournit des services de support à la gestion opérationnelle pour les AWS services suivants. Chaque AWS service étant distinct, le niveau de gestion opérationnelle et de support d'AMS varie en fonction de la nature et des caractéristiques du AWS service sous-jacent. Les AWS services spécifiques sont regroupés en fonction de la complexité et de l'étendue du service de soutien à la gestion opérationnelle fourni par AMS.

Note

Les trois groupes, A, B et C, indiquent le prix en pourcentage des dépenses mensuelles totales par compte pour le service AMS, sur la base du plan de support (Plus ou Premium), pour les clients AMS avant le 16 mars 2021. Les clients AMS intégrés après le 16 mars 2021 doivent soumettre une demande de service pour obtenir des informations tarifaires supplémentaires. Le groupe A n'indique aucun frais supplémentaire. Le groupe B indique un supplément de 12 % (Plus) ou de 18 % (Premium). Le groupe C indique un supplément de 25 % (Plus) ou 42 % (Premium).

Une étoile (*) indique les services déployés dans un environnement géré par AMS par un client utilisant la AWS console et APIs. Consultez la section « Gestion automatisée et en libre-service du provisionnement » [Fonctionnalités du plan d'exploitation avancé d'AWS Managed Services \(AMS\) AMS](#) pour plus de détails sur les responsabilités des clients lorsqu'ils fournissent et configurent les services de cette manière.

Deux étoiles (**) indiquent qu'Amazon AWS Outposts sera facturé EC2 en tant que service du groupe B ; toutes les autres ressources hébergées sur Amazon AWS Outposts seront facturées au tarif standard.

AWS Services pris en charge

Groupe A	Groupe B	Groupe C
Amazon Alexa for Business* Amazon Managed Streaming for Apache Kafka* Amazon CloudFront Amazon Elastic File System Amazon Glacier Amazon Simple Storage Service AWS Amplify* AWS AppMesh* AWS Auto Scaling AWS Backup AWS CloudFormation AWS Compute Optimizer AWS Global Accelerator*	Amazon API Gateway* Amazon AppStream* Amazon Athena* Amazon Bedrock* Amazon CloudSearch* Amazon Cognito* Amazon Comprehend* Amazon Connect* Amazon Document DB (with MongoDB compatibility)* Amazon DynamoDB* Amazon EC2 Container Registry (ECR)* Amazon Elastic Container Service (ECS) on AWS Fargate*	Amazon Aurora Amazon CloudWatch Amazon Elastic Block Store (EBS) Amazon Elastic Compute Cloud** Amazon Elastic Load Balancing (classic, application, and network; not gateway) Amazon ElastiCache Amazon OpenSearch Service Amazon GuardDuty Amazon Macie Amazon Redshift

Groupe A	Groupe B	Groupe C
AWS Identity and Access Management AWS License Manager* AWS Management Console AWS Marketplace AWS Lake Formation* AWS Well Architected Tool* VM Import/ Export*	Amazon Elastic Kubernetes Service (EKS) on Fargate* Amazon Elemental MediaConvert* Amazon Elemental MediaPackage* Amazon Elemental MediaStore* Amazon Elemental MediaTailor* Amazon Elastic MapReduce* AmazonEventBridge* Amazon Forecast* Amazon FSx* Amazon Inspector* Amazon Kendra* Amazon Kinesis Analytics* Amazon Kinesis Data Stream* Amazon Kinesis Firehose* Amazon Kinesis Video Streams* Amazon Lex* Amazon Managed Service for Prometheus* Amazon MQ* Amazon Personalize** Amazon Quantum Ledger Database (QLDB)* Amazon QuickSight* Amazon Rekognition* Amazon SageMaker* Amazon SimpleDB* Amazon Simple Workflow* Amazon Textract* Amazon Transcribe* Amazon Translate* Amazon WorkSpaces*	Amazon Relational Database Service Amazon Route 53 Amazon Route 53 Resolver DNS Firewall Amazon Simple Email Service Amazon Simple Notification Service Amazon Simple Queue Service Amazon Virtual Private Cloud (VPC) AWS CloudTrail AWS Config AWS Database Migration Service AWS Data Transfer AWS Direct Connect AWS Directory Service AWS Key Management Service AWS Systems Manager (SSM)

Groupe A	Groupe B	Groupe C
	AWS AppSync* AWS Audit Manager* AWS Batch* AWS Certificate Manager* AWS CloudEndure* AWS CloudHSM* AWS CodeBuild* AWS CodeCommit* AWS CodeDeploy* AWS CodePipeline* AWS DataSync* AWS Elemental MediaLive* AWS Glue* AWS Lambda* AWS MigrationHub* AWS Outposts** AWS Resilience Hub* AWS Secrets Manager* AWS Security Hub* AWS Service Catalog AWS Service Catalog AppRegistry* AWS Transfer for SFTP* AWS Shield* AWS Snowball* AWS Step Functions* AWS Transit Gateway* AWS WAF* AWS X-Ray*	

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 ci-dessous, tout AWS Managed Services fourni pour ces configurations demandées par le client sera traité comme un « service bêta » conformément aux conditions de service.

Configurations prises en charge

Voici les configurations prises en charge par AWS Managed Services (AMS) :

- Langue : AMS est disponible en anglais.
- Services de pare-feu :
 - Pare-feu DNS Amazon Route 53 Resolver
 - Pare-feu de nouvelle génération Palo Alto série VM
- Logiciel de sécurité : Deep Security de Trend Micro (obligatoire). AWS Marketplace: [Trend Micro Deep Security](#)
- Services d'annuaire approuvés : Microsoft Active Directory (AD)
- [AWS Services pris en charge](#).
- AWS Régions prises en charge :

AMS opère dans un sous-ensemble de toutes les AWS régions ; toutefois, l'AMS API/CLI fonctionne uniquement dans la région « USA Est (Virginie du Nord) ». Si vous exécutez l'API de gestion des modifications AMS (amscm) ou l'API de gestion des connaissances du service AMS (amsskms), dans une région autre que l'est des États-Unis, vous devez ajouter des éléments --region us-east-1 à la commande.

- USA Est (Virginie)
- USA Ouest (Californie du Nord)
- US West (Oregon)
- USA Est (Ohio)
- Canada (Centre)
- Amérique du Sud (São Paulo)
- UE (Irlande)
- UE (Francfort)
- UE (Londres)
- UE Ouest (Paris)
- Asie-Pacifique (Mumbai)
- Asie-Pacifique (Séoul)
- Asie-Pacifique (Singapour)
- Asie-Pacifique (Sydney)
- Asia Pacific (Tokyo)
- Amazon machine images (AMIs) : AMS fournit des images renforcées en termes de sécurité (AMIs) basées sur le test CIS de niveau 1 pour un sous-ensemble de systèmes d'exploitation pris

en charge par AMS. Pour connaître les systèmes d'exploitation dotés d'une image de sécurité améliorée, consultez le guide de l'utilisateur d'AMS Security. Pour accéder à ce guide AWS Artifact, filtrez l'onglet Reports pour AWS Managed Services. Pour y accéder AWS Artifact, contactez votre CSDM ou consultez [Getting Started with AWS Artifact](#).

- Systèmes d'exploitation pris en charge :

Systèmes d'exploitation pris en charge (x86-64)

- 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 pris en charge (ARM64)

- Amazon Linux 2023
- Amazon Linux 2 (date de fin de support AMS prévue le 30 juin 2026)
- 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 sont soumises [aux contrôles de sécurité](#) spécifiés par AMS dans le Guide de l'utilisateur avancé, 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

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

Un système d'exploitation non pris en charge est un système d'exploitation non répertorié dans le [Configurations 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.
Demandes de modification (RFCs)	AMS évalue l' RFCs exécution. Les systèmes d'exploitation non pris en charge peuvent avoir un impact sur la capacité d'exécution RFCs.

Capacité	Remarques
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 résultats d'Amazon et y répond.
Gestion des sauvegardes	AMS assure la gestion de la continuité dans AMS Advanced pour EC2 l'utilisation de AWS Backup plans et de coffres-forts personnalisés par AMS.

Interfaces avancées AMS

- Console AMS Advanced : vous utilisez la console AMS Advanced pour créer des incidents RFCs, les signaler et y répondre, faire des demandes de service et trouver des informations sur les produits existants VPCs et les piles. En cas de doute sur la marche à suivre ou lorsque vous avez besoin d'aide avec AMS ou vos ressources gérées, créez une demande de service à l'aide de cette interface.
- AWS Management Console: De nombreuses AWS consoles peuvent être utiles pour consulter les informations AMS, par exemple :
 - EC2 Console Amazon : à utiliser pour consulter les informations sur les instances, notamment les adresses IP des bastions, les groupes Amazon EC2 Auto Scaling et les équilibres de charge.
 - Conformité aux AWS Config règles des zones d'atterrissage multicomptes : vous pouvez consulter l'état de conformité de vos comptes et identifier les ressources non conformes.

- AWS CloudFormation console : à utiliser pour afficher les informations relatives à la pile, y compris la pile IDs (vous pouvez trouver les piles Amazon RDS et l'instance Amazon RDS IDs ici, ainsi que les informations sur les événements).
- Console Amazon RDS : à utiliser pour afficher les informations relatives à un événement, telles qu'une publication publiée sur une WordPress application sur un site dans votre compte. Notez que vous devez disposer de l'ID d'instance Amazon RDS.

Selon le mode de votre rôle de connexion, vous disposez de différents niveaux d'accès à la console AWS de gestion. Pour plus d'informations sur les modes, consultez la section [Modes AMS](#).

- API de gestion avancée des modifications AMS — Lecture/écriture : utilisez l'API de gestion des modifications (API CM) pour demander des ajouts et des modifications spécifiques à votre infrastructure gérée, notamment les configurations de surveillance des ressources, de journalisation, de sauvegarde et de correctifs. Utilisez également cette API pour demander l'accès aux ressources, supprimer des ressources AMIs, créer et créer des profils d'instance IAM. Vous pouvez accéder à l'API CM via l'AMS CLI et SDKs.
- API AMS SKMS — En lecture seule : utilisez cette API pour répertorier les ressources gérées et obtenir les informations nécessaires au signalement ou à la préparation des demandes de modification.
- Support API : utilisez l' Support API standard pour créer des incidents et des demandes de service et y répondre par programmation. Pour en savoir plus, consultez [Getting Started with Support](#).
- AWS APIs— Lecture seule : votre administrateur informatique principal peut utiliser le AWS APIs pour voir toutes les ressources gérées, consulter les CloudTrail journaux, les informations de facturation et de nombreuses autres fonctions de lecture.

Points de terminaison VPC AMS

Un point de terminaison VPC vous permet de vous connecter de manière privée à votre VPC Services AWS sans avoir besoin d'une passerelle Internet. Les instances de votre VPC ne requièrent pas d'adresses IP publiques pour communiquer avec les ressources du service.

Les points de terminaison sont des périphériques virtuels. Ce sont des composants de VPC dimensionnés horizontalement, redondants et hautement disponibles qui permettent la communication entre des instances de votre VPC et les services sans créer des risques d'indisponibilité ni de contraintes de bande passante sur votre trafic réseau. Pour en savoir plus, consultez la section Points de [terminaison VPC](#).

Il existe deux types de point de terminaison VPC : les points de terminaison d'interface et les points de terminaison de passerelle.

- Points de terminaison de passerelle : le VPC du compte possède un point de terminaison Amazon S3 Gateway activé par défaut.
- Points de terminaison de l'interface : les instances de votre environnement AMS peuvent communiquer avec les services pris en charge sans quitter le réseau Amazon. Ceci est facultatif pour la zone d'atterrissage à compte unique et n'est pas activé dans le compte par défaut ; soumettez une demande de service aux opérations AMS pour que cela soit activé. Toutefois, pour les zones de landing zone multicomptes, les points de terminaison de l'interface sont activés par défaut dans le compte Shared Services.

Liste des points de terminaison d'interface pris en charge par AMS :

- AWS CloudFormation
- AWS CloudTrail
- AWS Config
- EC2 API Amazon
- AWS Key Management Service
- Amazon CloudWatch
- CloudWatch Événements Amazon
- Amazon CloudWatch Logs
- AWS Secrets Manager
- Amazon SNS
- AWS Systems Manager
- AWS Security Token Service

Espaces de noms protégés par AMS

Liste des espaces de noms protégés pour AWS Managed Services (AMS). Lorsque vous travaillez avec AWS des ressources, évitez les conflits avec AMS en n'utilisant pas ces espaces de noms.

Pour plus de détails sur les autres espaces de noms de AWS services, consultez [Amazon Resource Names \(ARNs\) et AWS Service Namespaces](#).

- `ams-*` (il s'agit de la norme de dénomination préférée pour les nouvelles ressources)

- /ams/*(il s'agit de la norme de dénomination préférée pour les ressources basées sur les chemins)
- AWSManagedServices*(il s'agit de la norme de dénomination préférée pour les ressources, CamelCase le cas échéant)
- ams* et AMS*et Ams*
- AWS_* and aws*
- */aws_reserved/*
- CloudTrail* and Cloudtrail*
- codedeploy_service_role
- customer-mc-*
- eps and EPS
- EPSMarketplaceSubscriptionRole
- EPSDB*
- IAMPolicy*
- INGEST*
- LandingZone*
- Managed_Services*
- managementhost
- mc* et MC*et Mc*
- MMS*
- ms-
- NewAMS*
- Root*
- sentinel* and Sentinel*
- sentinel.int.
- StateMachine*
- StackSet-ams*
- StackSet-AWS-Landing-Zone
- TemplateId*

- UnhealthyInServiceBastion
- VPC_*

Préfixes réservés AMS

Les attributs de ressources AMS doivent respecter certains modèles ; par exemple, les noms de profil d'instance IAM, les BackupVault noms, les noms de balises, etc., ne doivent pas commencer par des préfixes réservés AMS. Ces préfixes réservés sont les suivants :

```
*/aws_reserved/*
ams- *
/ams/*
ams*
AMS*
Ams*
aws*
AWS*
AWS_*
AWSManagedServices*
codedeploy_service_role
CloudTrail*
Cloudtrail*
customer-mc- *
eps
EPSDB*
IAMPolicy*
INGEST*
LandingZone*
Managed_Services*
managementhost
mc*
MC*
Mc*
MMS*
ms-
NewAMS*
Root*
sentinel*
Sentinel*
sentinel.int.
StackSet-ams*
StackSet-AWS-Landing-Zone
```

```
StateMachine*  
TemplateId*  
VPC_*  
UnhealthyInServiceBastion
```

Fenêtre de maintenance AMS

La fenêtre de maintenance (ou fenêtre de maintenance) AWS Managed Services (ou fenêtre de maintenance) exécute les activités de maintenance d'AWS Managed Services (AMS) et a lieu le deuxième jeudi de chaque mois de 15 h 00 à 16 h 00, heure du Pacifique. AMS peut modifier le créneau de maintenance avec un préavis de 48 heures. Il s'agit d'AWS Managed Services (AMS), pour effectuer des activités de maintenance pour les infrastructures gérées, telles que le déploiement de nouveaux AMS AMIs.

Votre fenêtre de maintenance est celle où AMS appliquera les correctifs et vous déterminerez votre fenêtre de maintenance lors de l'intégration. Vous pouvez également accepter la fenêtre de correction proposée dans votre notification de service de correctifs, ou suggérer une autre fenêtre.

Pour obtenir des conseils sur la création d'une fenêtre de maintenance, voir [Fenêtre de maintenance](#).

Ressources d'information AMS

AMS fournit plusieurs ressources d'information pour vous aider à réussir.

- Guide de l'utilisateur d'AMS Accelerate : vous aide à comprendre les composants et fonctionnalités fournis par AMS Accelerate et à savoir comment les utiliser. Vous trouverez ici des informations générales sur AMS Accelerate, des détails sur les paramètres par défaut, la recherche de ressources et des exemples pratiques. [Index HTML](#), [PDF](#)
- Guide de l'utilisateur d'AMS Advanced : vous aide à comprendre les composants et fonctionnalités fournis par AMS Advanced et à savoir comment les utiliser. Vous trouverez ici des informations générales sur AMS Advanced, des détails sur les paramètres par défaut, la recherche de ressources et des exemples pratiques. [Index HTML](#), [PDF](#)
- Guide des applications avancées AMS : décrit les étapes de déploiement d'applications sur l'infrastructure AWS Managed Services. Cliquez ici pour obtenir des informations sur les méthodologies et considérations relatives au déploiement et à la maintenance des applications. [Index HTML](#), [PDF](#).
- Guide d'intégration avancé d'AMS : décrit les étapes initiales de création de l'infrastructure de base de zone de landing zone multi-comptes ou monocomptes AWS Managed Services dans un

compte AMS. Cliquez ici pour obtenir des informations sur les principes de base du compte AMS, la validation et les questions pour vous préparer à l'intégration à AMS. [Index HTML](#), [PDF](#).

- AMS Advanced Change Type Reference : fournit des informations de référence sur les types de modifications actuellement proposés par AWS Managed Services, notamment des schémas de type de modification et des exemples de procédures pas à pas pour chaque type de modification, ainsi que des conseils. Comprend des informations générales sur les types de modifications. Elle vous aide à comprendre tous les aspects des demandes de modification (RFCs) et des types de modification AMS (CTs). Cliquez ici pour obtenir des informations spécifiques sur les types de modifications, y compris des liens vers des informations pertinentes. [Index HTML](#), [PDF](#).
- Référence de l'API AMS CM (gestion des modifications) : décrit l'API AWS Managed Services CM, qui fournit des opérations de création et de surveillance des demandes de modification et fournit des informations sur vos ressources gérées par Managed Services. [Index HTML](#).
- Guides de sécurité AMS : Décrivez les informations de sécurité propriétaires d'AMS.

Privé ; disponible dans l'onglet AMS Reports de la console AWS Artifact.

- Ressources pour développeurs AMS : accès à la CLI et au SDK AMS, à la fois pour amscm et amsskms. Consultez <https://console.aws.amazon.com/managedservices/>.
- YouTube Vidéos AMS : les principales opérations des clients expliquées en vidéo. Regardez les [vidéos YouTube pédagogiques d'AWS Managed Services](#).
- Articles du blog AMS : informations spécialisées sur AWS Managed Services. Consultez les [blogs AWS](#).

Conformité avec AMS

AMS a fait l'objet d'un audit pour les normes suivantes et peut être utilisé dans le cadre de solutions pour lesquelles vous devez obtenir une certification de conformité.

Normes de conformité prises en charge par AMS

AMS soutient les normes AWS de conformité. Pour en savoir plus sur les programmes de AWS conformité, consultez la section [AWS Conformité](#).

Il s'agit des normes de conformité actuelles prises en charge par AMS.

FedRAMP : Le gouvernement fédéral américain s'engage à fournir ses services au peuple américain de la manière la plus

innovante, la plus sûre et la plus rentable possible. Le cloud computing joue un rôle clé dans la manière dont le gouvernement fédéral peut atteindre l'efficacité opérationnelle et innover à la demande pour faire avancer sa mission à travers le pays. C'est pourquoi de nombreuses agences fédérales utilisent aujourd'hui les services cloud AWS pour traiter, stocker et transmettre les données du gouvernement fédéral.

Pour plus d'informations, consultez [FedRAMP](#).

HIPAA : [AWS a étendu son programme de conformité à la loi HIPAA \(Health Insurance Portability and Accountability Act\) pour inclure AMS en tant que service éligible à la loi HIPAA](#). Si vous avez conclu un accord de partenariat commercial (BAA) avec AWS, vous pouvez utiliser AMS pour créer vos applications conformes à la loi HIPAA.

Consultez le [livre blanc consacré à la loi HIPAA](#) pour savoir comment tirer parti de l'AMS pour le traitement et le stockage des informations de santé. Pour de plus amples informations, consultez [Conformité à la loi HIPAA](#).

HITRUST : Le cadre de sécurité commun de la Health Information Trust Alliance (HITRUST CSF) s'appuie sur les normes et réglementations reconnues au niveau national et international telles que le RGPD, l'ISO, le NIST, le PCI et l'HIPAA pour créer un ensemble complet de contrôles de sécurité et de confidentialité de base.

Pour plus d'informations, consultez [HITRUST CSF](#).

La norme ISO 27001 : ISO/IEC 27001:2013 est une norme de gestion de la sécurité qui spécifie les meilleures pratiques de gestion de la sécurité et les contrôles de sécurité complets conformément au guide des meilleures pratiques ISO/IEC 27002. La base de cette certification est le développement et la mise en œuvre d'un programme de sécurité rigoureux, qui inclut le développement et la mise en œuvre d'un système de gestion de la sécurité de l'information (ISMS) qui définit la manière dont AWS gère perpétuellement la sécurité de manière holistique et complète.

Pour plus d'informations, voir [ISO/IEC 27001:2013](#).

La norme ISO 27017 : ISO/IEC 27017:2015 fournit des conseils sur les aspects de sécurité de l'information liés au cloud computing, en recommandant la mise en œuvre de contrôles de sécurité des informations spécifiques au cloud qui complètent les directives des normes 27002 et 27001. ISO/IEC ISO/IEC Ce code de pratique fournit des conseils supplémentaires sur la mise en œuvre des contrôles de sécurité des informations spécifiques aux fournisseurs de services cloud.

Pour plus d'informations, consultez [ISO/IEC 27017:2015](#)
Conformité.

ISO 27018 : ISO/IEC 27018:2019 est un code de pratique qui met l'accent sur la protection des données personnelles dans le cloud. Il est basé sur la norme de sécurité de l'ISO/IEC information 27002 et fournit des conseils de mise en œuvre sur les contrôles ISO/IEC 27002 applicables aux informations personnelles identifiables (PII) dans le cloud public. Il fournit également un ensemble de contrôles supplémentaires et des conseils associés destinés à répondre aux exigences de protection des informations personnelles du cloud public non prises en compte par l'ensemble de contrôles ISO/IEC 27002 existant.

Pour plus d'informations, consultez [ISO/IEC 27018:2019](#) Conformité.

ISO 9001 : ISO 9001:2015 décrit une approche axée sur les processus pour documenter et examiner la structure, les responsabilités et les procédures nécessaires pour parvenir à une gestion de la qualité efficace au sein d'une organisation. Des sections spécifiques de la norme contiennent des informations sur des sujets tels que :

- Exigences relatives à un système de gestion de la qualité, y compris la documentation d'un manuel qualité, le contrôle des documents et la détermination des interactions entre les processus
- Responsabilités de la direction
- Gestion des ressources, y compris les ressources humaines et l'environnement de travail d'une organisation
- Développement des services, y compris les étapes de la conception à la livraison
- Satisfaction du client
- Mesure, analyse et amélioration du système de gestion de la qualité par le biais d'activités telles que des audits internes et des actions correctives et préventives

Pour plus d'informations, voir Conformité à la [norme ISO 9001:2015](#).

PCI : AMS dispose d'une attestation de conformité à la norme de sécurité des données (DSS) de l'industrie des cartes de paiement (PCI) version 3.2 au niveau 1 des fournisseurs de services. Les clients qui utilisent les produits et services AWS pour stocker, traiter ou transmettre les données des titulaires de cartes peuvent utiliser AMS pour gérer leur propre certification de conformité à la norme PCI DSS.

Pour de plus amples informations sur PCI DSS, et notamment sur la manière de demander une copie de l'AWS PCI Compliance Package, veuillez consulter [PCI DSS, niveau 1](#). Il est important de noter que vous devez configurer des politiques de mot de passe précises dans AMS afin qu'elles soient conformes aux normes PCI DSS version 3.2. Pour plus de détails sur les politiques qui doivent être appliquées, consultez [Activer la conformité PCI pour votre répertoire AWS Microsoft AD](#).

SOC : Les rapports de contrôle du système et de l'organisation (SOC) AMS sont des rapports d'examen indépendants réalisés par des tiers qui montrent comment AMS atteint les principaux contrôles et objectifs de conformité. L'objectif de ces rapports est de vous aider, ainsi que vos auditeurs, à comprendre les contrôles AMS établis pour soutenir les opérations et la conformité. Il existe trois types de rapports AMS SOC :

- Rapport AWS SOC 1 - [Télécharger avec AWS Artifact](#)
- AWS SOC 2 : rapport de sécurité, de disponibilité et de confidentialité à [télécharger avec AWS Artifact](#)
- [AWS SOC 3 : rapport sur la sécurité, la disponibilité et la confidentialité](#)

Pour plus d'informations, consultez la section [Conformité SOC](#).

Responsabilité partagée

La sécurité, y compris la conformité à la norme PCI, est une [responsabilité partagée](#). Il est important de comprendre que le statut de conformité AMS ne s'applique pas automatiquement aux applications que vous exécutez dans le AWS cloud. Vous devez vous assurer que votre utilisation des AWS services est conforme aux normes. Pour plus de détails sur la manière dont AMS travaille avec ses clients dans le cadre d'activités spécifiques, consultez l'AMS [Matrice de responsabilité AMS \(RACI\)](#).

Images de machines AMS Amazon (AMIs)

AMS produit des Amazon Machine Images (AMIs) mises à jour chaque mois pour les systèmes d'exploitation pris en charge par AMS. En outre, AMS produit également des images renforcées en matière de sécurité (AMIs) basées sur le benchmark CIS de niveau 1 pour un sous-ensemble des [systèmes d'exploitation pris en charge par AMS](#). Pour savoir quels systèmes d'exploitation disposent d'une image de sécurité améliorée, consultez le guide de l'utilisateur de sécurité AMS, disponible via la page AWS Artifact -> Reports (trouvez l'option Reports dans le volet de navigation de gauche) filtré pour AWS Managed Services. Pour accéder à AWS Artifact, vous pouvez contacter votre CSDM pour obtenir des instructions ou consulter Getting [Started with AWS](#) Artifact.

Pour recevoir des alertes lorsque de nouveaux AMS AMIs sont publiés, vous pouvez vous abonner à une rubrique de notification Amazon Simple Notification Service (Amazon SNS) appelée « AMI AMS ». Pour plus de détails, consultez la section [Notifications AMI AMS avec SNS](#).

La convention de dénomination de l'AMI AMS est :customer-ams-<operating system>-<release date> - <version>. (par exemple,customer-ams-rhel6-2018.11-3)

Utilisez uniquement les AMS AMIs qui commencent parcustomer.

AMS recommande de toujours utiliser l'AMI la plus récente. Vous pouvez trouver la version la plus récente de l'une AMIs des manières suivantes :

- Je regarde dans la console AMS, sur la AMIspage.
- Affichage du dernier fichier CSV AMI AMS, disponible depuis votre CSDM ou via ce fichier ZIP : [contenu de l'AMI AMS 11.2024 et fichier CSV dans](#) un ZIP.

Pour les anciens fichiers ZIP AMI, consultez l'[historique des documents](#).

- Exécution de cette SKMS commande AMS (SDK AMS SKMS requis) :

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?starts_with(Name,'customer')].[Name,AmiId,CreationTime]" --output table
```

Contenu AMI AMS ajouté à la base AWS AMIs, par système d'exploitation (OS)

- Linux AMIs :
 - [AWS Outils CLI](#)
 - [NTP](#)
 - [Agent du service de protection des terminaux de Trend Micro](#)
 - [Déploiement de code](#)
 - [PBIS//Beyond Trust AD Bridge](#)
 - [Agent SSM](#)
 - Yum Upgrade pour les correctifs critiques
 - Scripts personnalisés/logiciels de gestion AMS (contrôle du démarrage, de la jointure AD, de la surveillance, de la sécurité et de la journalisation)
- Serveur Windows AMIs :
 - [Microsoft .NET Framework 4.5](#)
 - [PowerShell 5,1](#)
 - [AWS Outils pour Windows PowerShell](#)
 - PowerShell Modules AMS contrôlant le démarrage, la jointure AD, la surveillance, la sécurité et la journalisation
 - [Agent du service de protection des terminaux de Trend Micro](#)
 - [Agent SSM](#)
 - [CloudWatch Agent](#)
 - EC2Service de configuration (via Windows Server 2012 R2)
 - EC2Lancement (Windows Server 2016 et Windows Server 2019)
 - EC2LaunchV2 (Windows Server 2022 et versions ultérieures)

Basé sur Linux AMIs :

- Amazon Linux 2023 (dernière version mineure) (AMI minimale non prise en charge)

- Amazon Linux 2 (dernière version mineure)
- Amazon Linux (2ARM64)
- Red Hat Enterprise 7 (dernière version mineure)
- Red Hat Enterprise 8 (dernière version mineure)
- Red Hat Enterprise 9 (dernière version mineure)
- Serveur SUSE Linux Enterprise 15 SP6
- Ubuntu Linux 18.04
- Ubuntu Linux 20.04
- Ubuntu Linux 22.04
- Ubuntu Linux 24.04
- Amazon Linux : pour une présentation du produit, des informations sur les prix, des informations d'utilisation et des informations de support, consultez [Amazon Linux AMI \(HVM/64 bits\)](#) et [Amazon Linux 2](#).

Pour plus d'informations, consultez [Amazon Linux 2 FAQs](#).

- RedHat Enterprise Linux (RHEL) : pour une présentation du produit, des informations sur les prix, des informations d'utilisation et des informations de support, consultez [Red Hat Enterprise Linux \(RHEL\) 7 \(HVM\)](#).
- Ubuntu Linux 18.04 : pour une présentation du produit, des informations sur les prix, des informations d'utilisation et des informations d'assistance, consultez [Ubuntu 18.04 LTS - Bionic](#).
- SUSE Linux Enterprise Server pour applications SAP 15 SP6 :
 - Exécutez les étapes suivantes une fois par compte :
 1. Accédez à AWS Marketplace.
 2. Recherchez le produit SAP SUSE 15.
 3. Choisissez Continuer pour vous abonner.
 4. Choisissez Accepter les conditions.
 - Procédez comme suit chaque fois que vous devez lancer une nouvelle SP6 instance de SUSE Linux Enterprise Server pour SAP Applications 15 :
 1. Notez l'ID d'AMI de l'AMI SUSE Linux Enterprise Server for SAP Applications 15 abonnée.
 2. Créer un déploiement | Composants de pile avancés | Pile | EC2 Créer un type de modification ct-14027q0sjyt1h RFC. *InstanceAmiId* Remplacez-le par l'ID AWS Marketplace AMI auquel vous vous êtes abonné.

Basé sur Windows AMIs :

Microsoft Windows Server (2016, 2019 et 2022), basé sur la dernière version de Windows AMIs.

Pour des exemples de création AMIs, consultez la section [Créer une AMI](#).

Débarquement d'AMS AMIs :

AMS ne vous en communique aucune lors AMIs de l'offboarding afin d'éviter toute répercussion sur vos dépendances. Si vous souhaitez supprimer AMS AMIs de votre compte, vous pouvez utiliser l'`cancel-image-launch-permissionAPI` pour masquer des informations spécifiques AMIs. Par exemple, vous pouvez utiliser le script ci-dessous pour masquer tous AMIs les AMS précédemment partagés avec votre compte :

```
for ami in $(aws ec2 describe-images --executable-users self --owners 027415890775 --
query 'Images[].ImageId' --output text) ;
do
    aws ec2 cancel-image-launch-permission --image-id $ami ;
done
```

L'AWS CLI v2 doit être installée pour que le script puisse s'exécuter sans erreur. Pour connaître les étapes d'installation de l'interface de ligne de commande AWS, consultez la section [Installation ou mise à jour de la dernière version de l'interface de ligne de commande AWS](#). Pour plus de détails sur la `cancel-image-launch-permission` commande, consultez [cancel-image-launch-permission](#).

Sécurité améliorée AMIs

AMS fournit des images de sécurité améliorées (AMIs) basées sur le benchmark CIS de niveau 1 pour un sous-ensemble des systèmes d'exploitation pris en charge par AMS. Pour savoir quels systèmes d'exploitation disposent d'une image de sécurité améliorée, consultez le guide de sécurité client AWS Managed Services (AMS). Pour accéder à ce guide, ouvrez AWS Artifact, sélectionnez Reports dans le volet de navigation de gauche, puis filtrez pour AWS Managed Services. Pour obtenir des instructions sur la façon d'y accéder AWS Artifact, contactez votre CSDM ou consultez [Getting Started with AWS Artifact](#) pour plus d'informations.

Comment fonctionne l'intégration entre AD FS et AMS

Une confiance unidirectionnelle entre votre réseau local et le domaine AMS est le moyen par défaut pour accéder aux piles et VPCs. Lorsqu'un VPC et une pile sont créés, l'accès est accordé via

des groupes de sécurité Active Directory préconfigurés. En outre, l'accès au AWS Management Console peut être configuré à l'aide d'Active Directory Federation Service (AD FS) ou de tout logiciel de fédération prenant en charge le protocole SAML, pour une connexion unique (SSO) à la AWS console de gestion.

 Note

AMS peut se fédérer vers de nombreux services de fédération, tels que Ping, Okta, etc. Vous n'êtes pas limité à AD FS ; nous vous proposons ici un exemple d'une technologie de fédération à votre disposition.

Les informations présentées ici sont reprises de ce billet de blog : [Activation de la fédération à AWS l'aide de Windows Active Directory, AD FS et SAML 2.0.](#)

1. Le flux est lancé lorsqu'un utilisateur (appelons-le Bob) accède au site d'exemple AD FS (<https://Fully.Qualified.Domain.Name>). [Here/adfs/ls/IdpInitiatedSignOn.aspx](https://Fully.Qualified.Domain.Name/Here/adfs/ls/IdpInitiatedSignOn.aspx)) dans son domaine. Lorsque vous installez AD FS, vous obtenez un nouveau répertoire virtuel nommé adfs pour votre site Web par défaut, qui inclut cette page.
2. La page de connexion authentifie Bob auprès d'AD. Selon le navigateur utilisé par Bob, il peut être invité à saisir son nom d'utilisateur et son mot de passe AD.
3. Le navigateur de Bob reçoit une assertion SAML sous la forme d'une réponse d'authentification d'AD FS.
4. Le navigateur de Bob publie l'assertion SAML sur le point de AWS connexion pour SAML (<https://signin.aws.amazon.com/saml>). Dans les coulisses, la connexion utilise l'API [AssumeRoleWithSAML](#) pour demander des informations d'identification de sécurité temporaires, puis crée une URL de connexion pour le. AWS Management Console
5. Le navigateur de Bob reçoit l'URL de connexion et est redirigé vers la console.

Du point de vue de Bob, le processus se déroule de manière transparente. Il commence sur un site Web interne et se retrouve sur le AWS Management Console, sans jamais avoir à fournir d'informations AWS d'identification.

 Note

Vous trouverez de plus amples informations sur la configuration de la fédération sur la console AMS dans :

- Zone d'accueil multi-comptes : [configuration de la fédération sur la console AMS](#)
- Zone d'accueil à compte unique : [configuration de la fédération sur la console AMS](#)

Consultez également l'[annexe : Règle de réclamation AD FS et paramètres SAML](#). Pour plus d'informations sur l'utilisation de AWS Microsoft AD pour prendre en charge vos applications compatibles Active Directory, dans le AWS cloud, qui sont soumises aux exigences de conformité, voir Gérer la conformité avec [Microsoft AD](#).

Active Directory géré par AMS

AMS propose désormais un nouveau service appelé Managed Active Directory (alias Managed AD) qui permet à AMS de prendre en charge les opérations de votre infrastructure Active Directory (AD), tout en vous permettant de garder le contrôle de votre administration Active Directory.

Le support AMS pour Managed AD est similaire au support AMS pour Amazon Relational Database Service (Amazon RDS). Dans les deux cas, AWS (y compris AMS) prend en charge la création et la gestion de l'infrastructure exécutant le service, tandis que vous effectuez le contrôle d'accès et toutes les fonctions d'administration. Ce modèle présente les avantages suivants :

- Limite les risques de sécurité : AWS AMS n'a pas besoin de privilèges administratifs pour accéder à votre domaine.
- Intégrations directes : vous pouvez utiliser votre modèle d'autorisation actuel et l'intégrer à AD sans avoir à vous interfacer avec AMS.

Remarques :

- Ni AMS ni vous n'aurez accès à vos contrôleurs de domaine Managed AD. Aucun logiciel ne peut donc être installé sur les contrôleurs de domaine. Cela est important car les solutions tierces qui nécessitent l'installation de logiciels sur les contrôleurs de domaine ne sont pas autorisées.

Access fonctionne comme suit :

- AWS Équipe du Directory Service : a accès aux contrôleurs de domaine.
- AMS : a accès au Directory Service APIs pour effectuer certaines actions sur le domaine. Ces actions incluent la prise de clichés AD, la modification du schéma AD et d'autres actions.
- Vous : avez accès au domaine (AD) pour créer des utilisateurs, des groupes, etc.
- Nous vous recommandons d'effectuer une validation de principe sur Managed AD avant de migrer votre AD d'entreprise, car toutes les fonctionnalités d'un environnement AD traditionnel ne sont pas disponibles dans un environnement AD géré.
- AMS ne gèrera ni ne fournira de conseils sur la gestion de vos annonces. Par exemple, AMS ne fournira pas de conseils sur la structure des unités organisationnelles, la structure des politiques de groupe, les conventions de dénomination des utilisateurs AD, etc.

Cela fonctionne comme suit :

1. AMS intègre un nouveau compte Compte AWS pour vous, distinct de votre compte AMS et fournit un environnement Active Directory (AD) via AWS Directory Service (voir également [Qu'est-ce qu'AWS Directory Service ?](#)).

Voici les informations qu'un intégrateur de systèmes devra recueillir auprès de vous pour qu'AMS intègre Managed AD :

- Informations relatives au compte
 - ID de compte créé pour votre AD géré par AMS : numéro Compte AWS Compte AWS
 - Région dans laquelle intégrer votre Managed AD pour : Région AWS
- Informations Active Directory gérées :
 - Édition Microsoft AD : Standard/Enterprise. AWS Microsoft AD (édition standard) inclut 1 Go de stockage d'objets d'annuaire. Cette capacité peut prendre en charge jusqu'à 5 000 utilisateurs ou 30 000 objets de répertoire, y compris des utilisateurs, des groupes et des ordinateurs. AWS Microsoft AD (Enterprise Edition) inclut 17 Go de stockage d'objets d'annuaire, qui peut prendre en charge jusqu'à 100 000 utilisateurs ou 500 000 objets.

Pour plus d'informations, consultez [AWS Directory Service FAQs](#).

- FQDN de domaine : le FQDN de votre domaine AMS Managed AD.
- Nom NetBIOS du domaine : nom NetBIOS de votre domaine AMS Managed AD.
- Numéros de compte des comptes standard AMS auxquels vous souhaitez intégrer Managed AD (AMS configure une confiance unidirectionnelle entre l'AD du compte AMS Standard et l'AD géré)

- Des modifications du schéma Active Directory sont-elles nécessaires et, dans l'affirmative, quelles modifications ?
- Par défaut, deux contrôleurs de domaine sont configurés. Il vous en faut plus ? Dans l'affirmative, de combien en avez-vous besoin et pour quelle raison ?
- Mise en réseau pour les informations relatives à la gestion d'Active Directory :
 - CIDR AD VPC géré pour les contrôleurs de domaine (un CIDR dans votre plage de sous-réseaux privés pour les contrôleurs de domaine AD gérés) :
 - Sous-réseau CIDR 1 pour les contrôleurs de domaine : [votre CIDR doit faire partie du CIDR AD VPC géré par AMS]
 - Sous-réseau CIDR 2 pour les contrôleurs de domaine : [votre CIDR doit faire partie du CIDR AD VPC géré par AMS]

Exemples :

- CIDR AD VPC géré : 192.168.0.0/16
- CIDR 1 pour les contrôleurs de domaine : 192.168.1.0/24
- CIDR 2 pour les contrôleurs de domaine : 192.168.2.0/24

Pour éviter les conflits d'adresses IP, assurez-vous que le CIDR AD VPC géré que vous spécifiez n'entre en conflit avec aucun autre CIDR de sous-réseau privé que vous utilisez dans votre réseau d'entreprise.

- Technologie VPN (en option) : [Direct Connect/Direct Connect et VPN]
 - Numéro de système autonome BGP (ASN) de votre passerelle : [ASN fourni par le client]
 - Adresse IP routable par Internet pour l'interface externe de votre passerelle, l'adresse doit être statique : [Adresse IP fournie par le client]
 - Si votre connexion VPN nécessite ou non des itinéraires statiques : [oui/non]
2. AMS vous fournit le mot de passe du compte administrateur pour l'environnement AD et vous demande de le réinitialiser afin que les ingénieurs AMS ne puissent plus accéder à votre environnement AD.
 3. Pour réinitialiser le mot de passe du compte administrateur, connectez-vous à votre environnement Active Directory à l'aide d'Active Directory Users and Computers (ADUC). L'ADUC et les autres outils d'administration de serveurs distants (RSAT) doivent être installés et exécutés sur des hôtes administratifs que vous avez fournis sur une infrastructure autre qu'AMS. Microsoft applique les meilleures pratiques pour sécuriser ces hôtes administratifs. Pour plus

d'informations, consultez la section [Implémentation d'hôtes administratifs sécurisés](#). Vous gérez votre environnement Active Directory à l'aide de ces hôtes administratifs.

4. Dans le Compte AWS cadre de ses opérations quotidiennes, AMS gère tout ce qui concerne les services d' AWS annuaire ; par exemple, la configuration des VPC, les sauvegardes AD, la création et la suppression d'AD Trust, etc. Vous utilisez et gérez votre environnement AD ; par exemple, la création d'utilisateurs, la création de groupes, la création de politiques de groupe, etc.

Pour le tableau RACI le plus récent, consultez la section « Rôles et responsabilités » dans la section Voir la [description du service](#).

Déploiements d'applications AMS

Le guide du développeur d'applications AMS fournit des descriptions détaillées et des procédures pas à pas pour les déploiements suivants :

- L'AMS workload ingest CT vous permet, à vous et à un partenaire de migration vers le cloud AMS, de déplacer facilement vos charges de travail existantes vers un VPC géré par AMS. À l'aide de l'ingestion de charge de travail AMS, vous pouvez créer une AMI AMS en soumettant une RFC avec le formulaire Deployment | Ingestion | Stack from migration partner migrated instance | Create CT (ct-257p9zjk14ija). Vous devez avoir une instance migrée depuis votre site vers un partenaire AWS de migration, ainsi qu'un VPC AMS cible et un sous-réseau, dans lesquels l'instance sera ingérée.

Pour plus de détails, consultez le guide du développeur d'applications AMS sur [Workload Ingest](#).

- La fonctionnalité AWS CloudFormation de modification du type d'ingestion (ct-36cn2avfrj9v) vous permet d'utiliser facilement un modèle CloudFormation existant pour déployer des piles personnalisées dans un VPC géré par AMS.

Pour plus de détails, consultez le guide du développeur d'applications AMS sur [CloudFormation Template Ingest](#).

- Vous pouvez importer votre base de données sur site dans une nouvelle base de données vers votre compartiment Amazon S3 géré par AMS ou votre instance Amazon RDS. Pour ce faire, vous utilisez un type de changement de déploiement | Composants de pile avancés | Service de migration de base de données (DMS), notamment créer une instance de réplication (ct-27apldkhqr0ol), créer un groupe de sous-réseaux de réplication (ct-2q5azjd8p1ag5), créer une

tâche de réplication (ct-1d2fml15b9eth), créer un point de terminaison source (ct-0attesnjqy2cx) ou Créez un point de terminaison source (S3) (ct-2oxl37nphsrjz) et créez un point de terminaison cible (ct-3gf8dolbo8x9p) ou Créez un point de terminaison cible (S3) (ct-05muqzievnxk5).

Pour plus de détails, consultez le guide du développeur d'applications AMS sur [Database Migration Service](#).

- Vous pouvez importer votre base de données MS SQL locale dans une nouvelle base de données sur votre instance SQL RDS gérée par AMS. Pour ce faire, vous pouvez utiliser différents types de modifications AMS, l'API Amazon RDS et des AWS consoles.

Pour plus de détails, consultez le guide d'application AMS sur [Importation de base de données \(DB\) vers MS SQL RDS](#).

Gestion des services dans AWS Managed Services

Rubriques

- [Gouvernance des comptes dans AWS Managed Services](#)
- [Début du service dans AWS Managed Services](#)
- [Gestion de la relation client \(CRM\)](#)
- [Optimisation des coûts dans AWS Managed Services](#)
- [Heures de service dans AWS Managed Services](#)
- [Obtenir de l'aide sur AWS Managed Services](#)

Comment le service AMS fonctionne pour vous.

Gouvernance des comptes dans AWS Managed Services

Cette section traite de la gouvernance des comptes AMS.

Vous êtes désigné comme responsable de la prestation de services cloud (CSDM) qui fournit une assistance consultative au sein d'AMS 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 formuler des recommandations sur les meilleures 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.
- 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.

Début du service dans AWS Managed Services

Début du service : La date de début du service pour un compte AWS Managed Services est le premier jour du premier mois civil après lequel AWS vous informe que les activités définies dans les exigences d'intégration pour ce compte AWS Managed Services sont terminées ; à condition que si AWS envoie une telle notification après le 20e jour d'un mois civil, la date de début du service soit le premier jour du deuxième mois civil suivant la date de cette notification.

Début du service

- R représente la partie responsable qui fait le travail pour accomplir la tâche.
- Je signifie informé ; une partie qui est informée des progrès, souvent uniquement une fois la tâche ou le résultat livrable terminé.

Début du service

Étape #	Titre de l'étape	Description	Client	AMS
1.	Transfert du compte AWS du client	Le client crée un nouveau compte AWS et le transmet à AWS Managed Services	R	I
2.	Compte AWS Managed Services : conception	Finalisation de la conception du compte AWS Managed Services	I	R
3.	Compte AWS Managed Services - création	Un compte AWS Managed Services est créé conformément à la conception de l'étape 2	I	R

Gestion de la relation client (CRM)

AWS Managed Services (AMS) fournit un processus de gestion de la relation client (CRM) pour garantir l'établissement et le maintien d'une relation bien définie avec vous. Le fondement de cette

relation repose sur la connaissance qu'AMS a de vos besoins commerciaux. Le processus CRM facilite une compréhension précise et complète de :

- Les besoins de votre entreprise et comment y répondre
- Vos capacités et vos contraintes
- AMS et vos différentes responsabilités et obligations

Le processus CRM permet à AMS d'utiliser des méthodes cohérentes pour vous fournir des services et assurer la gouvernance de votre relation avec AMS. Le processus CRM inclut :

- Identifier vos principales parties prenantes
- Création d'une équipe de gouvernance
- Conduite et documentation des réunions d'évaluation des services avec vous
- Mise en place d'une procédure officielle de traitement des plaintes relatives au service assortie d'une procédure d'escalade
- Mise en œuvre et suivi de votre processus de satisfaction et de feedback
- Gérer votre contrat

Processus CRM

Le processus CRM inclut les activités suivantes :

- Identifier et comprendre les processus et les besoins de votre entreprise. Votre accord avec AMS identifie vos parties prenantes.
- Définition des services à fournir pour répondre à vos besoins et exigences.
- Rencontre avec vous lors des réunions de révision des services pour discuter de toute modification de l'étendue du service AMS, du SLA, du contrat et des besoins de votre entreprise. Des réunions intérimaires peuvent avoir lieu avec vous pour discuter des performances, des réalisations, des problèmes et des plans d'action.
- Surveillez votre satisfaction en utilisant notre enquête de satisfaction client et les commentaires fournis lors des réunions.
- Rendre compte des performances sur des rapports de performance mensuels mesurés en interne.
- Passez en revue le service avec vous afin de déterminer les possibilités d'amélioration. Cela inclut des communications fréquentes avec vous concernant le niveau et la qualité du service AMS fourni.

Réunions CRM

Les responsables de la prestation de services cloud d'AMS (CSDMs) vous rencontrent régulièrement pour discuter des pistes de service (opérations, sécurité et innovations en matière de produits) et des pistes exécutives (rapports de niveau de service, mesures de satisfaction et évolution des besoins de votre entreprise).

Réunion	Objectif	Mode	Les participants
Révision hebdomadaire du statut (facultatif)	Problèmes ou incidents en suspens, correctifs, événements de sécurité, dossiers de problèmes Tendance opérationnelle sur 12 semaines (+/- 6) Préoccupations des opérateurs d'applications Horaire du week-end	Client sur site location/ Telecom/Chime	AMS : CSDM et architecte cloud (CA) Membres de l'équipe assignés par le client (ex : équipes Cloud/ Infrastructure, Support des applications, équipes d'architecture, etc.)
Bilan mensuel de l'activité	Examiner les performances des niveaux de service (rapports, analyses et tendances) Analyse financière Feuille de route du produit CSAT	Client sur site location/ Telecom/Chime	AMS : CSDM, architecte cloud (CA), équipe de compte AMS, chef de produit technique AMS (TPM) (facultatif), responsable AMS OPS (facultatif) Vous : représentant de l'opérateur

Réunion	Objectif	Mode	Les participants
			ur de l'applica tion
Revue d'activité trimestrielle	Performances et tendances du tableau de bord et des accords de niveau de service (SLA) (6 mois) Plans/migrations des prochains mois, du 3 au 9 septembre 2012 Risque et atténuation des risques Initiatives d'amélioration clés Eléments de la feuille de route Opportunités alignées sur l'orientation future Financiers Initiatives de réduction des coûts Optimisation commerciale	Localisation du client sur site	AMS : CSDM, architecte cloud, équipe chargée des comptes AMS, directeur du service AMS, responsable des opérations AMS Vous : représentant de l'opérateur de l'application, représentant du service, directeur du service

Arrangements de réunions CRM

L'AMS CSDM est chargé de documenter la réunion, notamment :

- Création de l'ordre du jour, y compris les mesures à prendre, les problèmes et la liste des participants.
- Création de la liste des mesures examinées lors de chaque réunion pour s'assurer que les mesures sont achevées et résolues dans les délais.
- Distribution du compte rendu de la réunion et de la liste des mesures à prendre aux participants par e-mail dans un délai d'un jour ouvrable après la réunion.
- Stockage des comptes rendus de réunion dans le référentiel de documents approprié.

En l'absence du CSDM, le représentant de l'AMS qui dirige la réunion crée et distribue les procès-verbaux.

 Note

Votre CSDM travaille avec vous pour établir la gouvernance de votre compte.

Rapports mensuels du CRM

Votre AMS CSDM prépare et envoie des présentations mensuelles sur les performances des services. Les présentations incluent des informations sur les points suivants :

- Date du rapport
- Résumé et aperçus :
 - Principaux appels : nombre total et actif, état de l'application des correctifs, statut d'intégration du compte (uniquement pendant l'intégration), résumés des problèmes spécifiques aux clients
 - Performances : statistiques sur la résolution des incidents, les alertes, les correctifs, les demandes de modification (RFCs), les demandes de service et la disponibilité des consoles et des API
 - Problèmes, défis, préoccupations et risques : état des problèmes spécifiques au client
 - Éléments à venir : plans d'intégration ou de résolution des incidents spécifiques au client
- Ressources gérées : graphiques et diagrammes à secteurs des piles
- Mesures AMS : mesures de surveillance et d'événements, mesures d'incidents, mesures de conformité aux accords de niveau de service AMS, mesures de demande de service, mesures de gestion du changement, mesures de stockage, mesures de continuité, mesures de Trusted Advisor et résumés des coûts (présentés de plusieurs manières). Demandes de fonctionnalités. Informations de contact.

 Note

Outre les informations décrites, votre CSDM vous informe également de tout changement important dans le champ d'application ou les termes, y compris le recours à des sous-traitants par AMS pour les activités opérationnelles.

AMS génère des rapports sur les correctifs et les sauvegardes que votre CSDM inclut dans votre rapport mensuel. Dans le cadre du système de génération de rapports, AMS ajoute à votre compte une infrastructure à laquelle vous n'avez pas accès :

- Un compartiment S3, avec les données brutes rapportées
- Une instance Athena, avec des définitions de requêtes pour interroger les données
- Un Glue Crawler pour lire les données brutes du compartiment S3

Optimisation des coûts dans AWS Managed Services

AWS Managed Services vous fournit des rapports détaillés sur l'utilisation des coûts et les économies chaque mois lors de vos évaluations commerciales mensuelles (MBRs).

AMS suit un ensemble standard de processus et de mécanismes pour identifier les moyens de réduire les coûts dans vos comptes gérés et vous aider à planifier et à mettre en œuvre les modifications afin d'optimiser vos dépenses AWS.

Note

AMS développe une vidéo pour aider à optimiser les coûts. La première étape consiste à vous fournir un PDF et une feuille de calcul Excel présentant les meilleures pratiques en matière d'optimisation des coûts. Pour accéder à ces ressources, ouvrez le fichier ZIP du [guide rapide d'optimisation des coûts](#).

Cadre d'optimisation des coûts

AMS suit une approche en trois étapes pour optimiser vos coûts AWS :

1. Identifiez les pistes d'optimisation des coûts dans votre environnement géré
2. Vous présenter un plan d'optimisation des coûts
3. Aider à optimiser les coûts de manière mesurable

Identifier les pistes d'optimisation des coûts dans l'environnement géré

AMS utilise des outils AWS natifs tels que Cost Explorer et Trusted Advisor tout en tirant parti de plus de 20 modèles de réduction des coûts grâce à l'optimisation de l'architecture, aux optimisations AWS

axées sur les EC2 instances et aux comptes pour élaborer des recommandations de réduction de coûts personnalisées pour vous.

Certaines des recommandations d'optimisation sont les suivantes.

Recommandations d'optimisation architecturale :

- Utilisation optimale des classes de stockage S3 : Amazon S3 propose une gamme de classes de stockage pour répondre aux différentes exigences de charge de travail en fonction de l'accès aux données, de la résilience et du coût. La hiérarchisation intelligente S3 et l'analyse des classes de stockage S3 basées sur les besoins de charge de travail vous permettent de gérer efficacement les coûts de S3.
- Utilisation d'architectures de mise en cache : l'utilisation des instances de cache, le cas échéant, peut vous aider à remplacer certaines instances de base de données, tout en répondant à vos exigences en matière d'IOPS.
- Économies liées à la mise à niveau d'EBS : la migration de vos volumes EBS de gp2 à gp3 permet de réaliser des économies allant jusqu'à 20 % et vous pouvez tirer parti de performances de base prévisibles de 3 000 IOPS et de 125 Mbits/s, quelle que soit la taille du volume.
- Utilisation de l'élasticité : les fonctionnalités d'auto-scaling qu'elle AWS fournit permettent une utilisation efficace des ressources et des pistes d'optimisation des coûts. La révision et la mise à jour régulières des politiques de dimensionnement des instances en fonction des besoins permettent de réaliser des économies supplémentaires.

EC2 recommandations axées sur les instances

- Redimensionnement des instances : recommandations axées sur le dimensionnement des instances et sur les configurations optimales en fonction de l'utilisation. Les recommandations incluent également l'utilisation de la fonctionnalité Amazon EC2 Auto Scaling et le remplacement des EC2 AWS Lambda instances, le cas échéant, par du contenu Web statique sur Amazon S3, etc.
- Planification des instances : l'utilisation d'AMS Resource Scheduler pour démarrer et arrêter automatiquement les instances en fonction d'un calendrier permet de limiter les coûts, en particulier pour les instances hors production qui ne sont pas utilisées en dehors des heures ouvrables.
- Abonnement à des plans d'épargne : le plan d'épargne est le moyen le plus simple d'économiser sur AWS l'utilisation. Les EC2 Instance Savings Plans offrent jusqu'à 72 % d'économies par rapport à la tarification à la demande sur l'utilisation de vos EC2 instances Amazon. Les Amazon SageMaker AI Savings Plans offrent jusqu'à 64 % d'économies sur votre utilisation des services

Amazon SageMaker AI. AMS fournit des recommandations appropriées sur les plans d'épargne en fonction de votre utilisation AWS des ressources.

- Conseils d'utilisation et de consommation des instances réservées (RI) : les instances EC2 réservées Amazon (RI) offrent une réduction significative (jusqu'à 75 %) par rapport à la tarification à la demande et fournissent une réservation de capacité lorsqu'elles sont utilisées dans une zone de disponibilité spécifique.
- Utilisation d'instances ponctuelles : les charges de travail tolérantes aux pannes peuvent utiliser des instances ponctuelles et réduire les prix jusqu'à 90 %.
- Résiliation des instances inactives : identification et signalement des instances inactives ou peu utilisées qui peuvent être résiliées.

Recommandations axées sur les comptes

- Nettoyage du compte : Au niveau du compte, AMS identifie également les volumes EBS inutilisés, les CloudTrail traces dupliquées, les comptes vides contenant des ressources inutilisées, etc., et fournit des recommandations pour le nettoyage.
- Recommandations relatives aux accords de niveau de service : AMS examine régulièrement vos comptes Plus et Premium et recommande de choisir le niveau de SLA approprié pour les comptes.
- Optimisation de l'automatisation AMS : AMS optimise en permanence l'automatisation AMS et l'infrastructure utilisée pour fournir les services AMS.

Présenter aux clients et aider à planifier

AMS réalise des revues commerciales mensuelles (MBRs) avec les principales parties prenantes du client et présente les pistes, mécanismes et recommandations de réduction des coûts identifiés, ainsi que les économies potentielles. Nous travaillons également avec vous pour planifier les changements nécessaires.

Aider à la mise en œuvre des recommandations et mesurer l'impact sur les coûts

AMS aide à atteindre et à mesurer les impacts sur les coûts et les changements d'optimisation.

Vous évaluez l'impact sur l'application, les critères de risque et de réussite des modifications recommandées, et vous soumettez les demandes de modification appropriées (RFCs) via la console AMS. AMS collabore avec vous et met en œuvre les modifications liées à l'optimisation des coûts dans vos comptes gérés. AMS mesure l'impact sur les coûts et inclut les économies réalisées dans les bilans d'activité mensuels (MBRs).

Matrice de responsabilité pour l'optimisation des coûts

Responsabilités en matière d'optimisation des coûts AMS.

Optimisation des coûts RACI

Activité	Client	AMS
Compilati on des recommanc ations de réduction des coûts et préparati on du rapport	I	R
Présentat ion d'un rapport sur les économies de coûts	C	R
Planifica tion des changemer ts associés à la réduction des coûts	R	C
Évaluatio n de l'impact du	R	C

Activité	Client	AMS
changemer t et des risques		
Récolter RFCs des fonds pour mettre en œuvre les changemer ts	R	C
Révision RFCs et mise en œuvre des modificat ions	C	R
Tester l'applica tion et valider la mise en œuvre des modificat ions	R	C

Activité	Client	AMS
Mesurer l'impact sur les coûts après le changement et le présenter au client	I	R

Heures de service dans AWS Managed Services

Fonctionnalité	AMS avancé
	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,
Demande de modification automatisée (RFC)	24 h/24,
Demande de modification non automatisée (RFC)	24 h/24,
Responsable de la prestation de services cloud (CSDM)	Du lundi au vendredi : de 8h00 à 17h00, heures d'ouverture locales

Obtenir de l'aide sur AWS Managed Services

AMS vous soutient en matière de gestion des incidents, de gestion des demandes de service et de gestion des modifications 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 rapport d'incident. Pour plus de détails, voir [Signaler un incident](#). Pour des informations générales sur la gestion des incidents AMS, consultez la section [Réponse aux incidents](#).

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 plus de détails, [voir](#) [Création d'une demande de service](#). Pour des informations générales sur les demandes de service AMS, consultez la section [Gestion des demandes de service](#).

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 de domaines connexes RFCs 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.
- BYOEPS : utilisez la fonction « bring your own endpoint security » (BYOEPS) d'AMS pour remplacer l'agent Trend Micro Deep Security par votre solution de sécurité des terminaux préférée ou par une licence Trend Micro personnalisée. Pour de plus amples informations, veuillez consulter [AMS : apportez votre propre EPS](#).
- Reprise après sinistre : lors des événements de reprise après sinistre, AMS vous assiste lors de vos activités de reprise après sinistre planifiées. Pour de plus amples informations, veuillez consulter [Planification de la reprise après sinistre](#).

- Événement lié à la sécurité du client : événements de sécurité planifiés. Par exemple, l'activité des utilisateurs root et 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 une exécution prioritaire de RFCs, il est recommandé d'utiliser l'engagement Operations on Demand (OOD). Pour de plus amples informations, veuillez consulter [Opérations à la demande](#).

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 faire participer AMS à une RFC/Service demande (SR) lors d'un événement PEM ?

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

- 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'une RFC liée au PEM est soumise ?

- 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.

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 (RFC/demande de service), elles sont définies par AMS. SLOs

Pour plus d'informations, consultez la section [Objectifs de niveau de service AMS \(SLOs\)](#).

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).

Architecture réseau

AWS Managed Services (AMS) propose deux architectures réseau :

- Zone de landing zone multi-comptes (MALZ) : fournit des services communs, tels que l'accès, la sécurité des points de terminaison, la mise en réseau, à partir de comptes partagés pour les charges de travail déployées sur des comptes membres distincts.
- Zone de landing zone à compte unique (SALZ) : fournit des comptes autonomes dans lesquels les services courants tels que l'accès, la sécurité des points de terminaison et le réseau sont déployés dans le même compte que la charge de travail. Il est recommandé pour les charges de travail qui nécessitent un niveau élevé d'isolation, car cela implique des coûts AWS plus élevés.

Architecture réseau MALZ

À propos de l'architecture du réseau de zones d'atterrissage multi-comptes

Avant de commencer le processus d'intégration à la zone d'accueil multi-comptes (MALZ) d'AWS Managed Services (AMS), il est important de comprendre l'architecture de base, ou zone de destination, qu'AMS crée en votre nom, ses composants et ses fonctions.

La zone de landing zone multi-comptes AMS est une architecture multi-comptes, préconfigurée avec l'infrastructure nécessaire pour faciliter l'authentification, la sécurité, la mise en réseau et la journalisation.

Note

Pour les estimations des coûts, voir les [composants de base de l'environnement de zone d'atterrissage multi-comptes AMS](#).

Rubriques

- [Région de service](#)
- [Unités d'organisation](#)
- [Politiques de contrôle des services et AWS Organization](#)

Le schéma suivant décrit de manière générale la structure des comptes et la manière dont l'infrastructure est séparée dans chacun des comptes :

Région de service

Toutes les ressources d'une zone de landing zone multi-comptes AMS sont déployées dans la seule région AWS de votre choix, en raison de la limitation interrégionale actuelle avec Active Directory et Transit Gateway.

Unités d'organisation

Une zone de landing zone multi-comptes AMS typique comprend quatre unités organisationnelles de haut niveau () OUs :

- L'unité organisationnelle (UO) principale (utilisée pour regrouper les comptes afin de les administrer en tant qu'unité unique)
- L'UO des applications
- L'unité d'organisation gérée par le client
- L'unité d'intégration accélérée

La zone de landing multi-comptes gérée par AMS vous permet également de créer des comptes AWS personnalisés OUs pour regrouper et organiser des comptes AWS et de les SCPs associer à des comptes personnalisés ; pour des exemples à ce sujet, voir respectivement [Compte de gestion | Créer un compte personnalisé OUs](#) et un [compte de gestion | Créer un SCP personnalisé \(révision requise\)](#). AMS propose quatre comptes existants OUs dans le cadre desquels OUs de nouveaux comptes peuvent être demandés : accélération, applications > gérées, applications > développement et gestion par le client.

- accélérer l'UO :

Il s'agit d'une unité d'organisation de haut niveau dans la zone d'atterrissage multi-comptes AMS (MALZ). Les comptes relevant de cette unité d'organisation sont approvisionnés par AMS à l'aide d'une RFC (déploiement | zone d'atterrissage gérée | Compte de gestion | Création d'un compte Accelerate, modification de l'ID de type : ct-2p93tyd5angmi). Dans ces comptes d'applications accélérés, vous pouvez bénéficier de services opérationnels accélérés tels que la surveillance et les alertes, la gestion des incidents, la gestion de la sécurité et la gestion des sauvegardes. Pour plus de détails, consultez la section [Comptes AMS Accelerate](#).

- applications > unité d'organisation gérée :

Dans cette sous-unité organisationnelle de l'UO de l'application, les comptes sont entièrement gérés par AMS, y compris toutes les tâches opérationnelles. Les tâches opérationnelles incluent la gestion des demandes de service, la gestion des incidents, la gestion de la sécurité, la gestion de la continuité, la gestion des correctifs, l'optimisation des coûts, la surveillance et la gestion des événements. Ces tâches sont effectuées dans le cadre de la gestion de votre infrastructure. Plusieurs enfants OUs peuvent être créés selon les besoins, jusqu'à ce qu'une limite maximale d'enfants imbriqués OUs soit atteinte pour les organisations AWS. Pour plus de détails, consultez la section [Quotas for AWS Organizations](#).

- applications > UO de développement :

Dans le cadre de cette sous-unité d'organisation de l'application dans la zone de landing zone gérée par AMS, les comptes sont des comptes [en mode développeur](#) qui vous fournissent des autorisations élevées pour fournir et mettre à jour des ressources AWS en dehors du processus de gestion des modifications d'AMS. Cette UO soutient également la création de nouvelles UO pour enfants selon les besoins.

- UO gérée par le client :

Il s'agit d'une unité d'organisation de haut niveau dans la zone de landing multi-comptes AMS. Les comptes relevant de cette UO sont approvisionnés par AMS à l'aide d'une RFC. Dans ces comptes, vous êtes responsable du fonctionnement des charges de travail et des ressources AWS. Cette UO soutient également la création de nouvelles UO pour enfants selon les besoins.

À titre de bonne pratique, nous recommandons de regrouper les comptes relevant de ces sous-catégories OUs et des sous-comptes personnalisés OUs en fonction de leurs fonctionnalités et de leurs politiques.

Politiques de contrôle des services et AWS Organization

AWS fournit des politiques de contrôle des services (SCPs) pour la gestion des autorisations dans une organisation AWS. SCPs sont utilisés pour définir des garde-fous supplémentaires indiquant les actions que les utilisateurs peuvent effectuer et dans lesquelles. OUs Par défaut, AMS fournit un ensemble de comptes de gestion SCPs déployés qui fournissent des protections à différents niveaux d'unité d'organisation par défaut. Pour les restrictions relatives au SCP, veuillez contacter votre CSDM.

Vous pouvez également créer des éléments personnalisés SCPs et les associer à des éléments spécifiques OUs. Ils peuvent être demandés depuis votre compte de gestion en utilisant le type de modification ct-33ste5yc7hprs. AMS examine ensuite les personnalisations SCPs demandées avant de les appliquer à la cible OUs. Pour des exemples, voir [Compte de gestion | Créer un compte personnalisé OUs](#) et un [compte de gestion | Créer un SCP personnalisé \(révision requise\)](#).

Choisir un seul MALZ ou plusieurs MALZs

Le tableau suivant fournit quelques considérations de haut niveau pour choisir entre une seule zone d'atterrissage multi-comptes (MALZ) ou plusieurs zones d'atterrissage multi-comptes (par exemple, deux zones d'atterrissage multi-comptes : Prod et non-PROD). En général, le choix dépend des besoins individuels, des exigences légales et des pratiques d'exploitation.

Zone d'atterrissage multi-comptes unique par rapport à plusieurs zones d'atterrissage multi-comptes

Entité	Zone d'atterrissage AMS unique	Plusieurs zones d'atterrissage (deux ou plus)
Coût de base	Moins élevé, optimisé à environ 3 000\$ par mois.	Plus élevé, un coût supplémentaire d'environ 3 000\$ par environnement.
Facturation	Facture unique, grâce à un seul compte de facturation/gestion.	Facture distincte pour chaque zone d'atterrissage multi-comptes. Actuellement, AWS Org ne prend pas en charge les comptes à gestion multiple avec une facture unique.
Portabilité des instances réservées existantes (RIs)	Faible. RIs Les AWS ne sont actuellement pas convertibles entre plusieurs comptes de facturation. Vous réutilisez l'existant RIs pour une zone de landing zone multi-comptes.	Plus bas. Vous réutiliseriez et distribueriez RIs sur toute la zone de landing multi-comptes.
Réductions sur la hiérarchisation des produits	Élevée. Consultez la section Réductions sur volume .	Faible. Consultez la section Réductions sur volume .

Entité	Zone d'atterrissage AMS unique	Plusieurs zones d'atterrissage (deux ou plus)
Frais de configuration initiale (dans le respect des project/migration délais)	Faible. Intégrations Active Directory , réseau et authentification unique (SSO) une seule fois.	Élevée. Vous effectueriez Active Directory, l'intégration réseau et les intégrations SSO pour chaque zone de landing zone. Cela peut entraîner des retards potentiels dans tout projet de migration.
Configurabilité des services communs	Peu d'efforts. Vous configurez common/shared des services tels que le DNS, la sauvegarde, la surveillance, la journalisation, etc.	Des efforts importants. Une planification supplémentaire est nécessaire pour déterminer où seront situés l'infrastructure ou les services communs. Le trafic passant par plusieurs passerelles de transit (TGWs) dans chaque zone d'atterrissage peut entraîner des coûts supplémentaires.

Entité	Zone d'atterrissage AMS unique	Plusieurs zones d'atterrissage (deux ou plus)
Évolutivité	Moyen. AMS a actuellement une limite pratique de 150 comptes par zone d'atterrissage multi-comptes. Plusieurs équipes ou fournisseurs exécutant des applications sur le même compte peuvent avoir accès à des piles appartenant à différentes équipes. Cette limitation peut être atténuée en contrôlant l'accès aux piles spécifiques à l'application au niveau de la ServiceNow couche (en intégrant l'application AMS ServiceNow Connector et en utilisant des balises). Demandez aux responsables des techniques de livraison (TDMs) ou aux architectes cloud (CAs) d'AMS comment implémenter cela.	Élevée. Possibilité de tirer parti de plusieurs zones de landing multi-comptes pour distribuer les comptes tout en atteignant le niveau de ségrégation des comptes ou des applications. La gestion d'un grand nombre de comptes peut entraîner des frais généraux d'exploitation ou de coûts.
Risque opérationnel	(Cela dépend) Faible. Intégration opérationnelle et disponibilité opérationnelle une seule fois. Moins de risques de dérives du processus.	(Cela dépend) Faible. Multiples activités d'intégration et opérationnelles. La dérive dans plusieurs zones d'atterrissage au cours de cette période pourrait entraîner des risques opérationnels.
Plusieurs régions AWS	Région AWS unique. La zone de landing multi-comptes AMS est limitée à une seule région AWS. Pour couvrir plusieurs régions AWS, utilisez plusieurs zones de landing zone multi-comptes.	Plusieurs régions AWS. Avec plusieurs zones d'atterrissage multi-comptes, vous pouvez déployer chaque MALZ dans une région et les interconnecter à l'aide de la passerelle de transit (TGW) peering.

Entité	Zone d'atterrissage AMS unique	Plusieurs zones d'atterrissage (deux ou plus)
Migration ou portabilité du compte	Oui. Il est possible de déplacer des comptes d'une unité organisationnelle à une autre au sein de la même organisation AWS.	Non AMS ne prend pas en charge la migration d'un compte entre les zones d'atterrissage, c'est-à-dire entre AWS Organizations. Les charges de travail peuvent atteindre plusieurs zones d'atterrissage grâce à la passerelle de transit (TGW) ou au peering VPC.
Gestion des modifications	Moyen. Les modifications destructives apportées à des composants courants tels que TGW, Active Directory (AD) ou sortants (sortie) peuvent avoir un impact sur toutes les charges de travail dans une zone de landing zone multi-comptes. Cependant, les modifications apportées aux composants gérés par AMS sont testées en interne et intégrées dans des mises à jour continues.	Faible. Les modifications destructives apportées à des composants courants tels que le TGW, l'AD ou l'outbound (sortie) ne peuvent avoir d'impact que sur les charges de travail dans cette zone de landing multi-comptes spécifique.
Contrôles des données et des accès	(Cela dépend) Peu de contrôle si vous souhaitez vous connecter à différents réseaux sur site et sur site pour les charges de travail Prod ADs et Non-Prod. La fédération SAML, les domaines TGW et les groupes de sécurité (SGs) peuvent également aider à mettre en œuvre les contrôles requis.	(Cela dépend) Contrôle élevé si vous souhaitez vous connecter à différents réseaux sur site et sur site pour les charges de travail Prod ADs et Non-Prod. Utilisez des zones d'atterrissage séparées pour des exigences de conformité strictes.

Entité	Zone d'atterrissage AMS unique	Plusieurs zones d'atterrissage (deux ou plus)
Conformité et sécurité	(Cela dépend) Faible s'il existe des exigences de conformité strictes pour séparer complètement les charges de travail matérielles des charges de travail non matérielles. Des contrôles préventifs et de détection conformes à la norme AMS sont en place.	(Cela dépend) Une zone d'atterrissage pouvant aller jusqu'à plusieurs comptes pourrait aider à respecter des exigences de conformité strictes en séparant complètement les charges de travail matérielles des charges de travail non matérielles. Des contrôles préventifs et de détection conformes à la norme AMS sont en place.

Recommandation : sans obligation stricte de conformité ou multirégionale, commencer par une seule zone d'atterrissage multi-comptes AMS permettrait de trouver un bon équilibre entre le coût, la sécurité, l'excellence opérationnelle et la complexité de la migration. Vous pouvez toujours configurer une zone de landing zone supplémentaire si des contraintes liées à votre compte ou à votre activité sont rencontrées.

Zone d'atterrissage multi-comptes unique contre zone d'atterrissage multi-comptes multiple FAQs

Voici quelques questions fréquemment posées lorsque vous choisissez de configurer une seule zone d'atterrissage multi-comptes ou plusieurs zones d'atterrissage multi-comptes :

Q1 : Puis-je commencer par une seule zone d'atterrissage multi-comptes et passer à une zone d'atterrissage multi-comptes, si des limites de comptes ou des contraintes commerciales sont rencontrées ?

R : Oui. Vous pouvez choisir de configurer une autre zone de landing zone multi-comptes à tout moment :

- Un nouveau compte payeur devra être configuré (actuellement, AWS ne prend pas en charge les comptes à payeurs multiples dans une seule organisation AWS).
- La création de la base d'une zone d'atterrissage multi-comptes prend jusqu'à 2 semaines une fois que le questionnaire de zone d'atterrissage multi-comptes est rempli.

- Chaque zone de landing zone multi-comptes représente un supplément d'environ 3 000 USD par mois de frais de fonctionnement.
- L'intégration N/W, AD, DNS et SSO sera nécessaire pour établir le nouveau MALZ.
- Toutes les instances réservées (RIs) et les plans de réduction des coûts devront être configurés pour la nouvelle zone d'atterrissage multi-comptes (RIs ils ne sont pas transférables).
- La zone de landing multi-comptes AMS ne prend pas en charge la migration d'un compte entre des comptes de zone d'atterrissage multi-comptes, par exemple, entre AWS Orgs. Cependant, il est possible de déplacer des applications d'un compte à un autre en utilisant les méthodes de migration standard.

Q2 : Quelle est l'approche d'AMS vis-à-vis du MALZ en matière updates/changes d' underlying/ shared infrastructure et de quantification des risques pour les clients ? Fournissez des détails sur les garanties incluses dans le processus. Comment les clients peuvent-ils être sûrs que MALZ n' updates/changes aura aucun impact sur les clients ? Le client doit-il prendre des mesures pour éviter toute interruption ?

R : AMS suit une méthodologie de changement stricte utilisant des outils internes qui nous permettent de définir, de revoir, de planifier et d'exécuter des modifications dans les environnements des clients.

Le processus de publication des mises à jour impose la révision du code, les tests d'intégration, le déploiement dans des environnements gamma et bêta, ainsi que des temps de cuisson et des tests supplémentaires dans les environnements bêta et gamma avant la mise à disposition des environnements clients. Toutes les versions incluent des procédures d'annulation et sont étroitement surveillées par l'équipe chargée des versions et par l'équipe qui a créé et demandé la modification. Le champ d'application des versions est limité aux piles détenues et approvisionnées par AMS. En moyenne, nous exécutons au moins une version par semaine.

En outre :

- Les accords de niveau de service AMS sont applicables. Conformément à la description du service AMS, tout incident signalé à la suite d'une activité de maintenance d'infrastructure partagée respectera le SLA en vigueur en matière de résolution ou de crédits.
- Aucune mesure préventive particulière n'est requise par les clients pour éviter toute perturbation de l'infrastructure commune. Les clients disposent d'autorisations en lecture seule sur les comptes AWS Org ou Core UO. Ils ne peuvent donc pas apporter de modifications destructives à l'environnement principal de MALZ. Toutes les demandes du client adressées à l'infrastructure principale doivent être examinées et approuvées par AMS.

- Les clients peuvent tester certaines modifications au niveau de l'organisation, par exemple SCPs/Roles au niveau des comptes individuels non liés à la production, avant de propager les modifications au niveau de l'unité d'organisation de l'application. Cela fait partie de la feuille de route de l'AMS visant à autoriser plusieurs applications OUs (deuxième trimestre 2020), ce qui réduirait encore les risques liés à certains changements au niveau de l'organisation. L'équipe MALZ a déjà publié une unité d'organisation distincte pour les comptes « Build Mode », afin de garantir une séparation claire de la propriété des clients et des contrôles séparés.
- La plupart de ces modifications permettent à AMS de gérer la charge de travail de manière efficace et efficiente et n'ont pas nécessairement d'impact sur la charge de travail des clients. Lorsque AMS estime qu'une modification de l'infrastructure partagée peut avoir un impact sur la charge de travail des clients, elle est alors alignée sur la fenêtre de modification des clients.

Recommandation de haut niveau, commencez par plusieurs zones d'atterrissage multi-comptes si :

- Si cela vous aide à atteindre une conformité spécifique.
- Si vous devez utiliser Multi-Region.
- Si vous avez des charges de travail sur site et des réseaux différents pour les charges de travail ADs et Prod/Material non, les charges Prod/Non-Material workloads, to clearly segregate b/w de travail.

Comptes multi-comptes Landing Zone

Rubriques

- [Compte de gestion](#)
- [Compte réseau](#)
- [Compte Shared Services](#)
- [Compte Log Archive](#)
- [Compte de sécurité](#)
- [Types de comptes d'applications](#)
- [Compte AMS Tools \(migration des charges de travail\)](#)

Compte de gestion

Le compte de gestion est votre compte AWS initial lorsque vous commencez à vous inscrire à AMS. Il utilise AWS Organizations comme compte de gestion (également connu sous le nom de compte payeur qui paie les frais de tous les comptes membres), ce qui permet au compte de créer et de gérer financièrement des comptes de membres. Il contient le framework AWS Landing Zone (ALZ), les ensembles de configurations de comptes, les politiques de contrôle des services d'AWS Organization (SCPs), etc.

Pour plus d'informations sur l'utilisation d'un compte de gestion, consultez la section [Meilleures pratiques relatives au compte de gestion](#).

Le schéma suivant fournit une vue d'ensemble des ressources contenues dans le compte de gestion.

Ressources du compte de gestion

Hormis les services standard ci-dessus, aucune ressource AWS supplémentaire n'est créée dans le compte de gestion lors de l'intégration. Les entrées suivantes sont requises lors de l'intégration à AMS :

- ID du compte de gestion : ID du compte AWS que vous avez créé initialement.
- E-mails des comptes principaux : indiquez les e-mails à associer à chacun des comptes principaux : réseau, services partagés, journalisation et compte de sécurité.
- Région de service : indiquez la région AWS dans laquelle toutes les ressources de votre zone d'atterrissage AMS seront déployées.

Compte réseau

Le compte réseau sert de hub central pour le routage réseau entre les comptes de zone de landing zone multi-comptes AMS, votre réseau local et le trafic de sortie vers Internet. En outre, ce compte contient des bastions DMZ publics qui constituent le point d'entrée permettant aux ingénieurs AMS d'accéder aux hôtes de l'environnement AMS. Pour plus de détails, consultez le schéma de haut niveau du compte réseau ci-dessous.

Architecture des comptes réseau

Le schéma suivant décrit l'environnement de la zone d'atterrissage multi-comptes AMS, en présentant les flux de trafic réseau entre les comptes, et constitue un exemple de configuration hautement disponible.

AMS configure pour vous tous les aspects du réseau sur la base de nos modèles standard et des options que vous avez sélectionnées lors de l'intégration. Une conception de réseau AWS standard est appliquée à votre compte AWS, et un VPC est créé pour vous et connecté à AMS par VPN ou Direct Connect. Pour plus d'informations sur Direct Connect, consultez [AWS Direct Connect](#). VPCs Les standards incluent la DMZ, les services partagés et un sous-réseau d'applications. Au cours du processus d'intégration, des informations supplémentaires VPCs peuvent être demandées et créées pour répondre à vos besoins (par exemple, divisions clients, partenaires). Après l'intégration, vous recevez un schéma de réseau : un document d'environnement qui explique comment votre réseau a été configuré.

Note

Pour plus d'informations sur les limites et les contraintes de service par défaut pour tous les services actifs, consultez la documentation relative [aux limites de service AWS](#).

La conception de notre réseau repose sur le [« principe du moindre privilège »](#) d'Amazon. Pour ce faire, nous acheminons tout le trafic entrant et sortant via une zone démilitarisée, à l'exception du trafic provenant d'un réseau fiable. Le seul réseau fiable est celui configuré entre votre environnement sur site et le VPC via l'utilisation d'un and/or VPN et d'AWS Direct Connect (DX). L'accès est accordé par le biais d'instances de bastion, empêchant ainsi l'accès direct aux ressources de production. Toutes vos applications et ressources résident dans des sous-réseaux privés accessibles via des équilibres de charge publics. Le trafic de sortie public passe par les passerelles NAT du VPC de sortie (dans le compte réseau) vers la passerelle Internet, puis vers Internet. Le trafic peut également passer par votre VPN ou Direct Connect vers votre environnement sur site.

Connectivité réseau privé à l'environnement de zone d'atterrissage multi-comptes AMS

AWS propose une connectivité privée via un réseau privé virtuel (VPN) ou des lignes dédiées avec AWS Direct Connect. La connectivité privée dans votre environnement multi-comptes est configurée à l'aide de l'une des méthodes décrites ci-dessous :

- Connectivité Edge centralisée à l'aide de Transit Gateway
- Connexion du and/or VPN Direct Connect (DX) aux clouds privés virtuels du compte () VPCs

Connectivité périphérique centralisée à l'aide d'une passerelle de transit

AWS Transit Gateway est un service qui vous permet de connecter votre réseau VPCs et celui de votre réseau sur site à une passerelle unique. La passerelle de transit (TGW) peut être utilisée pour consolider votre connectivité périphérique existante et l'acheminer via un ingress/egress point unique. La passerelle de transit est créée dans le compte réseau de votre environnement multi-comptes AMS. Pour plus d'informations sur la passerelle de transit, consultez [AWS Transit Gateway](#).

La passerelle AWS Direct Connect (DX) est utilisée pour connecter votre connexion DX via une interface virtuelle de transit à la VPCs ou aux passerelles VPNs connectées à votre passerelle de transit. Vous associez une passerelle Direct Connect à la passerelle de transit. Créez ensuite une interface virtuelle de transit pour votre connexion AWS Direct Connect à la passerelle Direct Connect. Pour plus d'informations sur les interfaces virtuelles DX, consultez la section [Interfaces virtuelles AWS Direct Connect](#).

Cette configuration offre les avantages suivants. Vous pouvez :

- Gérez une seule connexion pour plusieurs VPCs ou pour celles VPNs qui se trouvent dans la même région AWS.
- Faites connaître les préfixes sur site sur AWS, et d'AWS sur site.

Note

[Pour plus d'informations sur l'utilisation d'un DX avec les services AWS, consultez la section Resiliency Toolkit Classic.](#) Pour plus d'informations, consultez la section [Associations de Transit Gateway](#).

Pour augmenter la résilience de votre connectivité, nous vous recommandons d'associer au moins deux interfaces virtuelles de transit provenant de différents sites AWS Direct Connect à la passerelle Direct Connect. Pour plus d'informations, consultez la [recommandation de résilience d'AWS Direct Connect](#).

Connexion d'un DX ou d'un VPN au compte VPCs

Avec cette option, les environnements VPCs de zone d'atterrissage multi-comptes de votre AMS sont directement connectés à Direct Connect ou à un VPN. Le trafic circule directement depuis Direct Connect ou VPCs vers le VPN sans passer par la passerelle de transit.

Ressources du compte réseau

Comme le montre le schéma du compte réseau, les composants suivants sont créés dans le compte et nécessitent votre saisie.

Le compte réseau en contient deux VPCs : le VPC de sortie et le VPC DMZ, également connu sous le nom de VPC de périmètre.

Responsable du réseau AWS

AWS Network Manager est un service qui vous permet de visualiser vos réseaux de passerelles de transit (TGW) sans frais supplémentaires pour AMS. Il fournit une surveillance centralisée du réseau à la fois sur les ressources AWS et sur les réseaux sur site, une vue globale unique de leur réseau privé sous forme de diagramme topologique et de carte géographique, ainsi que des mesures d'utilisation, telles que l'état de in/out, packets in/out, packets dropped, and alerts for changes in the topology, routing, and up/down connexion en octets. Pour plus d'informations, consultez [AWS Network Manager](#).

Utilisez l'un des rôles suivants pour accéder à cette ressource :

- AWSManagedServicesCaseRole
- AWSManagedServicesReadOnlyRole
- AWSManagedServicesChangeManagementRole

VPC de sortie

Le VPC de sortie est principalement utilisé pour le trafic de sortie vers Internet et est composé de sous-réseaux répartis dans un maximum public/private de trois zones de disponibilité (). AZs Les passerelles de traduction d'adresses réseau (NAT) sont mises en service dans les sous-réseaux

publics, et les pièces jointes VPC de passerelle de transit (TGW) sont créées dans les sous-réseaux privés. Le trafic Internet sortant de tous les réseaux entre via le sous-réseau privé via TGW, où il est ensuite acheminé vers un NAT via des tables de routage VPC.

Pour ceux VPCs qui contiennent des applications destinées au public dans un sous-réseau public, le trafic provenant d'Internet est contenu dans ce VPC. Le trafic de retour n'est pas routé vers le TGW ou le VPC de sortie, mais renvoyé via la passerelle Internet (IGW) du VPC.

Note

Plage d'adresses CIDR VPC réseau : lorsque vous créez un VPC, vous devez spécifier une plage d'adresses IPv4 pour le VPC sous la forme d'un bloc de routage interdomaine sans classe (CIDR) ; par exemple, 10.0.16.0/24. Il s'agit du bloc CIDR principal pour votre VPC. L'équipe de la zone d'atterrissage multi-comptes d'AMS recommande une plage de 24 (avec plus d'adresses IP) afin de fournir une certaine mémoire tampon au cas où d'autres ressources/appareils seraient déployés à l'avenir.

Pare-feu de sortie Palo Alto géré

AMS fournit une solution de pare-feu de sortie gérée à Palo Alto, qui permet de filtrer le trafic sortant vers Internet pour tous les réseaux de l'environnement multicomptes Landing Zone (à l'exception des services destinés au public). Cette solution associe une technologie de pare-feu de pointe (Palo Alto VM-300) aux capacités de gestion de l'infrastructure d'AMS pour déployer, surveiller, gérer, dimensionner et restaurer l'infrastructure dans des environnements d'exploitation conformes. Les tiers, y compris Palo Alto Networks, n'ont pas accès aux pare-feux ; ils sont gérés uniquement par les ingénieurs d'AMS.

Contrôle du trafic

La solution de pare-feu sortant géré gère une liste d'autorisations de domaines composée des domaines requis par AMS pour des services tels que les sauvegardes et les correctifs, ainsi que des domaines que vous avez définis. Lorsque le trafic Internet sortant est acheminé vers le pare-feu, une session est ouverte, le trafic est évalué et, s'il correspond à un domaine autorisé, le trafic est transféré vers la destination.

Architecture

La solution de pare-feu de sortie géré suit un modèle de haute disponibilité, dans lequel deux à trois pare-feux sont déployés en fonction du nombre de zones de disponibilité (). AZs La solution utilise

une partie de l'espace IP du VPC de sortie par défaut, mais fournit également une extension VPC (/24) pour les ressources supplémentaires nécessaires à la gestion des pare-feux.

Flux réseau

À un niveau élevé, le routage du trafic de sortie public reste le même, à l'exception de la manière dont le trafic est acheminé vers Internet depuis le VPC de sortie :

1. Le trafic de sortie destiné à Internet est envoyé au Transit Gateway (TGW) via la table de routage VPC
2. TGW achemine le trafic vers le VPC de sortie via la table de routage TGW
3. Le VPC achemine le trafic vers Internet via les tables de routage du sous-réseau privé
 - a. Dans l'environnement Multi-Account Landing Zone par défaut, le trafic Internet est envoyé directement à une passerelle de traduction d'adresses réseau (NAT). La solution de pare-feu géré reconfigure les tables de routage du sous-réseau privé pour pointer plutôt la route par défaut (0.0.0.0/0) vers une interface de pare-feu.

Les pare-feux eux-mêmes contiennent trois interfaces :

1. Interface sécurisée : interface privée pour recevoir le trafic à traiter.
2. Interface non fiable : interface publique pour envoyer du trafic vers Internet. Comme les pare-feux exécutent le NAT, les serveurs externes acceptent les demandes provenant de ces adresses IP publiques.
3. Interface de gestion : interface privée pour l'API du pare-feu, les mises à jour, la console, etc.

Tout au long du routage, le trafic est maintenu dans la même zone de disponibilité (AZ) afin de réduire le trafic inter-AZ. Le trafic ne se croise qu'en AZs cas de basculement.

Modification de la liste d'autorisations

Après l'intégration, une liste d'autorisation par défaut nommée `ams-allowlist` est créée, contenant les points de terminaison publics requis par AMS ainsi que les points de terminaison publics pour appliquer des correctifs aux hôtes Windows et Linux. Une fois opérationnel, vous pouvez créer des RFC dans la console AMS sous la catégorie Management | Managed Firewall | Outbound (Palo Alto)

pour créer ou supprimer des listes d'autorisation, ou modifier les domaines. Sachez que cela `ams-allowlist` ne peut pas être modifié. Les RFC sont gérées de manière entièrement automatisée (elles ne sont pas manuelles).

Politique de sécurité personnalisée

Les politiques de sécurité déterminent s'il faut bloquer ou autoriser une session en fonction des attributs du trafic, tels que la zone de sécurité source et de destination, l'adresse IP source et de destination et le service. Les politiques de sécurité personnalisées sont prises en charge de manière entièrement automatisée RFCs. CTs pour créer ou supprimer une politique de sécurité se trouve dans la catégorie Gestion | Pare-feu géré | Outbound (Palo Alto), et le CT permettant de modifier une politique de sécurité existante se trouve dans la catégorie Déploiement | Pare-feu géré | Outbound (Palo Alto). Vous serez en mesure de créer de nouvelles politiques de sécurité, de modifier les politiques de sécurité ou de supprimer des politiques de sécurité.

 Note

La politique de sécurité par défaut `ams-allowlist` ne peut pas être modifiée

CloudWatch Tableaux de bord de sortie PA

Deux tableaux de bord fournissent une vue agrégée de Palo Alto (PA). Le tableau de bord AMS-MF-PA-egress-config-dashboard fournit un aperçu de la configuration PA, des liens vers des listes d'autorisation et une liste de toutes les politiques de sécurité, y compris leurs attributs. CloudWatch

Le tableau de bord AMS-MF-PA-Egress-Dashboard peut être personnalisé pour filtrer les journaux de trafic. Par exemple, pour créer un tableau de bord pour une politique de sécurité, vous pouvez créer une RFC avec un filtre tel que :

[illegible]

```
| display @timestamp, @rule, @action, @session_end_reason, @protocol, @source_ip,  
  @destination_ip, @source_port, @destination_port, @session_id, @from_zone,  
  @to_zone, @category, @bytes_sent, @bytes_recieved, @packets_sent, @packets_recieved,  
  @source_country, @destination_country
```

Modèle Failover

La solution de pare-feu inclut deux à trois hôtes Palo Alto (PA) (un par AZ). Les canaris Healthy Check suivent un horaire constant pour évaluer l'état de santé des hôtes. Si un hôte est identifié comme défaillant, AMS en est averti et le trafic correspondant à cette zone est automatiquement transféré vers un hôte sain situé dans une autre zone de disponibilité via une modification de la table de routage. Étant donné que le flux de travail de vérification de l'état s'exécute en permanence, si l'hôte redevient sain en raison de problèmes transitoires ou d'une correction manuelle, le trafic est redirigé vers la bonne zone de disponibilité avec l'hôte sain.

Dimensionnement

AMS surveille le pare-feu pour vérifier les limites de débit et d'évolutivité. Lorsque les limites de débit dépassent les seuils de filigrane inférieurs (CPU/réseau), AMS reçoit une alerte. Un seuil bas indique que les ressources approchent de la saturation, atteignant un point où AMS évaluera les indicateurs au fil du temps et proposera des solutions de mise à l'échelle.

Sauvegarde et restauration

Les sauvegardes sont créées lors du lancement initial, après toute modification de configuration et à intervalles réguliers. Les sauvegardes de lancement initiales sont créées par hôte, mais les modifications de configuration et les sauvegardes à intervalles réguliers sont effectuées sur tous les hôtes du pare-feu lorsque le flux de travail de sauvegarde est invoqué. Les ingénieurs d'AMS peuvent créer des sauvegardes supplémentaires en dehors de ces fenêtres ou fournir des informations de sauvegarde sur demande.

Les ingénieurs d'AMS peuvent effectuer la restauration des sauvegardes de configuration si nécessaire. Si une restauration est requise, elle aura lieu sur tous les hôtes afin de synchroniser la configuration entre les hôtes.

La restauration peut également avoir lieu lorsqu'un hôte a besoin du recyclage complet d'une instance. Une restauration automatique de la dernière sauvegarde a lieu lorsqu'une nouvelle EC2 instance est provisionnée. En général, les hôtes ne sont pas recyclés régulièrement et sont réservés en cas de panne grave ou de remplacement d'AMI requis. Les recyclages de l'hôte sont lancés manuellement et vous êtes averti avant qu'un recyclage ne soit effectué.

Outre les sauvegardes de configuration du pare-feu, vos règles de liste d'autorisation spécifiques sont sauvegardées séparément. Une sauvegarde est automatiquement créée lorsque les règles de liste d'autorisation que vous avez définies sont modifiées. La restauration de la sauvegarde de la liste d'autorisation peut être effectuée par un ingénieur AMS, si nécessaire.

Mises à jour

La solution AMS Managed Firewall nécessite plusieurs mises à jour au fil du temps pour apporter des améliorations au système, des fonctionnalités supplémentaires ou des mises à jour du système d'exploitation (OS) ou du logiciel du pare-feu.

La plupart des modifications n'affecteront pas l'environnement d'exécution, comme la mise à jour de l'infrastructure d'automatisation, mais d'autres modifications, telles que la rotation des instances de pare-feu ou la mise à jour du système d'exploitation, peuvent provoquer des perturbations. Lorsqu'une interruption de service potentielle due à des mises à jour est évaluée, AMS coordonnera ses efforts avec vous pour tenir compte des périodes de maintenance.

Accès de l'opérateur

Les opérateurs AMS utilisent leurs ActiveDirectory informations d'identification pour se connecter à l'appareil Palo Alto afin d'effectuer des opérations (par exemple, appliquer des correctifs, répondre à un événement, etc.). La solution conserve les journaux standard d'authentification des opérateurs AMS et de modification de configuration pour suivre les actions effectuées sur les hôtes Palo Alto.

Journaux par défaut

Par défaut, les journaux générés par le pare-feu résident dans le stockage local de chaque pare-feu. Au fil du temps, les journaux locaux seront supprimés en fonction de l'utilisation du stockage. La solution AMS permet l'envoi en temps réel des journaux des machines vers CloudWatch les journaux ; pour plus d'informations, voir [CloudWatch Intégration des journaux](#).

Les ingénieurs d'AMS ont toujours la possibilité d'interroger et d'exporter les journaux directement depuis les machines si nécessaire. En outre, les journaux peuvent être expédiés vers un Panorama appartenant au client ; pour plus d'informations, voir. [Intégration du Panorama](#)

Les journaux collectés par la solution sont les suivants :

Codes d'état RFC

Type de journal	Description
Trafic	Affiche une entrée pour le début et la fin de chaque session. Chaque entrée inclut la date et l'heure, les zones source et de destination, les adresses et les ports, le nom de l'application, le nom de la règle de sécurité appliquée au flux, l'action de la règle (autoriser, refuser ou supprimer), l'interface d'entrée et de sortie, le nombre d'octets et le motif de fin de session. La colonne Type indique si l'entrée concerne le début ou la fin de la session, ou si la session a été refusée ou abandonnée. Un « abandon » indique que la règle de sécurité qui a bloqué le trafic spécifiait « n'importe quelle » application, tandis qu'un « refus » indique que la règle a identifié une application spécifique. Si le trafic est supprimé avant que l'application ne soit identifiée, par exemple lorsqu'une règle supprime tout le trafic pour un service spécifique, l'application est indiquée comme « non applicable ».
Menace	Affiche une entrée pour chaque alarme de sécurité générée par le pare-feu. Chaque entrée inclut la date et l'heure, le nom ou l'URL de la menace, les zones source et de destination, les adresses et les ports, le nom de l'application, ainsi que l'action d'alarme (autoriser ou bloquer) et sa gravité. La colonne Type indique le type de menace, tel que « virus » ou « logiciel espion » ; la colonne Nom est la description ou l'URL de la menace ; et la colonne Catégorie représente la catégorie de menace (telle que « keylogger ») ou la catégorie d'URL.
Filtrage d'URL	Affiche les journaux des filtres d'URL, qui contrôlent l'accès aux sites Web et indiquent si les utilisateurs peuvent envoyer des informations d'identification aux sites Web.
Configuration	Affiche une entrée pour chaque modification de configuration. Chaque entrée inclut la date et l'heure, le nom d'utilisateur de l'administrateur, l'adresse IP à partir de laquelle la modification a été effectuée, le type

Type de journal	Description
	de client (interface Web ou CLI), le type de commande exécutée, si la commande a réussi ou échoué, le chemin de configuration et les valeurs avant et après la modification.
Système	Affiche une entrée pour chaque événement du système. Chaque entrée inclut la date et l'heure, la gravité de l'événement et une description de l'événement.
Alarmes	Le journal des alarmes enregistre des informations détaillées sur les alarmes générées par le système. Les informations contenues dans ce journal sont également signalées dans Alarmes. Reportez-vous à la section « Définir les paramètres d'alarme ».
Authentification	Affiche des informations sur les événements d'authentification qui se produisent lorsque les utilisateurs finaux tentent d'accéder aux ressources réseau dont l'accès est contrôlé par les règles de politique d'authentification. Les utilisateurs peuvent utiliser ces informations pour résoudre les problèmes d'accès et pour ajuster la politique d'authentification utilisateur selon les besoins. En conjonction avec les objets de corrélation, les utilisateurs peuvent également utiliser les journaux d'authentification pour identifier les activités suspectes sur le réseau des utilisateurs, telles que les attaques par force brute. Les utilisateurs peuvent éventuellement configurer des règles d'authentification pour enregistrer les délais d'authentification. Ces délais concernent la période pendant laquelle un utilisateur ne doit s'authentifier qu'une seule fois pour une ressource, mais peut y accéder à plusieurs reprises. Le fait de consulter les informations relatives aux délais d'expiration aide les utilisateurs à décider s'il convient de les ajuster et de quelle manière.

Type de journal	Description
Unifié	Affiche les dernières entrées du journal relatives au trafic, aux menaces, au filtrage des URL, aux WildFire soumissions et au filtrage des données dans une seule vue. La vue collective des journaux permet aux utilisateurs d'examiner et de filtrer ces différents types de journaux ensemble (au lieu de rechercher chaque ensemble de journaux séparément). Les utilisateurs peuvent également choisir les types de journaux à afficher : cliquez sur la flèche située à gauche du champ de filtre et sélectionnez trafic, menace, URL, données, and/or incendie de forêt pour afficher uniquement les types de journaux sélectionnés.

Gestion d'événements

AMS surveille en permanence la capacité, l'état de santé et la disponibilité du pare-feu. Les métriques générées par le pare-feu, ainsi que les métriques AWS/AMS générées, sont utilisées pour créer des alarmes qui sont reçues par les ingénieurs d'exploitation d'AMS, qui étudieront et résoudront le problème. Les alarmes actuelles concernent les cas suivants :

Alarmes liées aux événements :

- Utilisation du processeur Firewall Dataplane
 - Utilisation du processeur - Processeur du plan de données (traitement du trafic)
- L'utilisation des paquets du plan de données du pare-feu est supérieure à 80 %
 - Utilisation des paquets - Plan de données (traitement du trafic)
- Utilisation des sessions du plan de données du pare-feu
- Session de plan de données du pare-feu active
- Utilisation agrégée du processeur du pare-feu
 - Utilisation du processeur dans l'ensemble CPUs
- Failover par AZ
 - Alarmes en cas de basculement dans un AZ
- Hôte Syslog défaillant
 - L'hôte Syslog échoue à la vérification de santé

Alarmes de gestion :

- Alarme de défaillance du moniteur Health Check
 - Lorsque le flux de travail de contrôle de santé échoue de façon inattendue
 - Cela concerne le flux de travail lui-même, et non en cas d'échec de la vérification de l'état du pare-feu
- Alarme d'échec de rotation des mots
 - Lorsque la rotation des mots de passe échoue
 - Le mot de passe utilisateur de l'API/du service est modifié tous les 90 jours

Métriques

Toutes les mesures sont capturées et stockées CloudWatch dans le compte réseau. Vous pouvez les consulter en accédant à la console au compte réseau et en accédant à la CloudWatch console. Les mesures individuelles peuvent être consultées sous l'onglet des métriques ou un tableau de bord à volet unique contenant certaines mesures et les métriques agrégées peuvent être consultées en accédant à l'onglet Tableau de bord et en sélectionnant AMS-MF-PA-Egress-Dashboard.

Métriques personnalisées :

- Vérification de l'état
 - Espace de nom : AMS/MF/PA/Egress
 - PARouteTableConnectionsByAZ
 - PAUnhealthyByInstance
 - PAUnhealthyAggregatedByAZ
 - PAHealthCheckLockState
- Pare-feu généré
 - Espace de noms : /AMS/MF/PA/Egress<instance-id>
 - DataPlaneCPUUtilizationPCT
 - DataPlanePacketBufferUtilization
 - poêle GPGateway UtilizationPct
 - panSessionActive
 - panSessionUtilization

CloudWatch Intégration des journaux

CloudWatch L'intégration des journaux transfère les journaux des pare-feux vers les CloudWatch journaux, ce qui réduit le risque de perte de journaux en raison de l'utilisation du stockage local. Les journaux sont remplis en temps réel au fur et à mesure que les pare-feux les génèrent et peuvent être consultés à la demande via la console ou l'API.

Des requêtes complexes peuvent être créées pour l'analyse des journaux ou exportées au format CSV à l'aide d' CloudWatch Insights. En outre, le tableau de CloudWatch bord personnalisé du pare-feu géré par AMS affichera également un aperçu rapide des requêtes spécifiques du journal de trafic et une visualisation graphique du trafic et des atteintes aux politiques au fil du temps. L'utilisation de CloudWatch journaux permet également une intégration native à d'autres services AWS tels qu'AWS Kinesis.

Note

Les journaux PA ne peuvent pas être directement transférés vers un collecteur Syslog existant sur site ou tiers. La solution AMS Managed Firewall permet l'envoi en temps réel des journaux des machines PA vers AWS CloudWatch Logs. Vous pouvez utiliser la fonctionnalité CloudWatch Logs Insight pour exécuter des requêtes ad hoc. De plus, les journaux peuvent être expédiés vers la solution de gestion Panorama de votre Palo Alto. CloudWatch les journaux peuvent également être transférés vers d'autres destinations à l'aide des filtres CloudWatch d'abonnement. Pour en savoir plus sur Panorama, consultez la section suivante. Pour en savoir plus sur Splunk, consultez la section [Intégration à Splunk](#).

Intégration du Panorama

AMS Managed Firewall peut, en option, être intégré à votre Panorama existant. Cela vous permet de visualiser les configurations du pare-feu depuis Panorama ou de transférer les journaux du pare-feu vers le Panorama. L'intégration de Panorama à AMS Managed Firewall est en lecture seule et les modifications de configuration des pare-feux depuis Panorama ne sont pas autorisées. Panorama est entièrement géré et configuré par vous, AMS se chargera uniquement de configurer les pare-feux pour communiquer avec lui.

Licences

Le prix du pare-feu géré AMS dépend du type de licence utilisée (licence horaire ou licence BYOL) et de la taille de l'instance dans laquelle l'appliance s'exécute. Vous devez commander la taille des instances et les licences du pare-feu Palo Alto que vous préférez via AWS Marketplace.

- Licences Marketplace : acceptez les termes et conditions du pack 1 de pare-feu de nouvelle génération de la série VM depuis le compte réseau de MALZ.
- Licences BYOL : acceptez les termes et conditions du pare-feu de nouvelle génération de série VM (BYOL) depuis le compte réseau de MALZ et partagez le « code d'authentification BYOL » obtenu après l'achat de la licence à AMS.

Limites

À l'heure actuelle, AMS prend en charge les pare-feux des séries VM-300 ou VM-500. Les configurations peuvent être trouvées ici : [Modèles de la série VM sur des instances AWS EC2](#),

Note

La solution AMS s'exécute en mode actif-actif, chaque instance PA de sa zone de zone de disponibilité gérant le trafic de sortie pour sa zone de disponibilité respective. Ainsi, avec deux AZs, chaque instance PA gère le trafic de sortie jusqu'à 5 Gbit/s et fournit efficacement un débit global de 10 Gbit/s sur deux instances. AZs II en va de même pour toutes les limites de chaque AZ. Si le bilan de santé de l'AMS échoue, nous transférons le trafic de l'AZ présentant le mauvais PA vers une autre AZ, et pendant le remplacement de l'instance, la capacité est réduite aux AZs limites restantes.

AMS ne prend actuellement pas en charge les autres offres Palo Alto disponibles sur AWS Marketplace ; par exemple, vous ne pouvez pas demander le « pack de pare-feu de nouvelle génération de la série VM 2 ». Notez que la solution AMS Managed Firewall utilisant Palo Alto ne fournit actuellement qu'une offre de filtrage du trafic sortant, de sorte que l'utilisation de packs avancés de la série VM n'apporterait aucune fonctionnalité ou avantage supplémentaire.

Exigences relatives à l'intégration

- Vous devez consulter et accepter les conditions générales du pare-feu de nouvelle génération de la série VM de Palo Alto sur AWS Marketplace.

- Vous devez confirmer la taille de l'instance que vous souhaitez utiliser en fonction de votre charge de travail attendue.
- Vous devez fournir un bloc CIDR /24 qui n'entre pas en conflit avec les réseaux de votre environnement Multi-Account Landing Zone ou On-Prem. Il doit être de la même classe que le VPC de sortie (la solution fournit une extension VPC /24 au VPC de sortie).

Tarification

Les coûts d'infrastructure de base d'AMS Managed Firewall sont divisés en trois facteurs principaux : l' EC2 instance qui héberge le pare-feu Palo Alto, la licence logicielle, les licences de la série Palo Alto VM et les intégrations. CloudWatch

Les prix suivants sont basés sur le pare-feu de la gamme VM-300.

- EC2 Instances : le pare-feu Palo Alto fonctionne selon un modèle de haute disponibilité de 2 à 3 EC2 instances, l'instance étant basée sur les charges de travail attendues. Le coût de l'instance dépend de la région et du nombre de AZs
 - Par exemple us-east-1, m5.xlarge, 3 AZs
 - $0,192\$ * 24 * 30 * 3 = 414,72\$$
 - <https://aws.amazon.com/ec2/tarification/à la demande/>
 - Licences Palo Alto : Le coût de la licence logicielle d'un pare-feu de nouvelle génération Palo Alto VM-300 dépend du nombre d'AZ ainsi que du type d'instance.
 - Par exemple us-east-1, m5.xlarge, 3 AZs
 - $0,87\$ * 24 * 30 * 3 = 1879,20\$$
 - https://aws.amazon.com/marketplace/PP/B083M7JPKB ? ref_=srh_res_product_title #pdp - pricing
 - CloudWatch Intégration des journaux : l'intégration CloudWatch des journaux utilise des SysLog serveurs (EC2 - t3.medium), le NLB et les journaux. CloudWatch Le coût des serveurs est basé sur la région et le nombre de serveurs AZs, et le coût des NLB/CloudWatch journaux varie en fonction de l'utilisation du trafic.
 - Par exemple us-east-1, t3.medium, 3AZ
 - $0,0416\$ * 24 * 30 * 3 = 89,86\$$
 - <https://aws.amazon.com/ec2/tarification/à la demande/>
 - <https://aws.amazon.com/cloudwatch/tarification/>

Périmètre (DMZ) VPC

Le VPC Perimeter, ou DMZ, contient les ressources nécessaires aux ingénieurs des opérations AMS pour accéder aux réseaux AMS. Il contient 2 ou 3 sous-réseaux publics AZs, avec des hôtes SSH Bastions dans un groupe Auto Scaling (ASG) auquel les ingénieurs d'AMS Operations peuvent se connecter ou par tunnel. Les groupes de sécurité attachés aux bastions de la zone démilitarisée contiennent des règles relatives au port 22 en provenance d'Amazon Corp Networks.

Plage d'adresses CIDR VPC DMZ : lorsque vous créez un VPC, vous devez spécifier une plage d'IPv4 adresses pour le VPC sous la forme d'un bloc de routage interdomaine sans classe (CIDR) ; par exemple, 10.0.16.0/24. Il s'agit du bloc CIDR principal pour votre VPC.

Note

L'équipe AMS recommande une plage de 24 (avec plus d'adresses IP) pour fournir une certaine mémoire tampon au cas où d'autres ressources, telles qu'un pare-feu, seraient déployées à l'avenir.

AWS Transit Gateway

AWS Transit Gateway (TGW) est un service qui vous permet de connecter vos Amazon Virtual Private Clouds (VPCs) et vos réseaux sur site à une passerelle unique. La passerelle de transit est l'épine dorsale du réseau qui gère le routage entre les réseaux de comptes AMS et les réseaux externes. Pour plus d'informations sur Transit Gateway, consultez [AWS Transit Gateway](#).

Fournissez les informations suivantes pour créer cette ressource :

- Numéro ASN de la passerelle de transit * : indiquez le numéro de système autonome (ASN) privé de votre passerelle de transit. Cela devrait être l'ASN pour le côté AWS d'une session Border Gateway Protocol (BGP). La plage est comprise entre 64512 et 65534 pour 16 bits. ASNs

Compte Shared Services

Le compte Shared Services sert de hub central pour la plupart des services de plan de données AMS. Le compte contient l'infrastructure et les ressources nécessaires à la gestion des accès (AD), à la gestion de la sécurité des terminaux (Trend Micro), ainsi que les bastions des clients (SSH/RDP). Le graphique suivant présente un aperçu général des ressources contenues dans le compte Shared Services.

Le VPC Shared Services est composé du sous-réseau AD, du sous-réseau EPS et du sous-réseau Customer Bastions dans les trois zones de disponibilité (). AZs Les ressources créées dans le VPC Shared Services sont répertoriées ci-dessous et nécessitent votre contribution.

- Plage d'adresses CIDR VPC Shared Services : lorsque vous créez un VPC, vous devez spécifier une plage d'adresses IPv4 pour le VPC sous la forme d'un bloc de routage interdomaine sans classe (CIDR) ; par exemple, 10.0.1.0/24. Il s'agit du bloc CIDR principal pour votre VPC.

 Note

L'équipe AMS recommande la plage de /23.

- Détails d'Active Directory : Microsoft Active Directory (AD) est utilisé pour la user/resource gestion, l'authentification/l'autorisation et le DNS sur tous vos comptes de zone de landing zone multi-comptes AMS. AMS AD est également configuré avec une confiance unidirectionnelle à votre Active Directory pour une authentification basée sur la confiance. Les entrées suivantes sont requises pour créer l'AD :
 - Nom de domaine complet (FQDN) : nom de domaine complet pour le répertoire Microsoft AD géré par AWS. Le domaine ne doit pas être un domaine existant ou un domaine enfant d'un domaine existant de votre réseau.
 - Nom NetBIOS du domaine : si vous ne spécifiez pas de nom NetBIOS, AMS utilise par défaut le nom de la première partie du DNS de votre répertoire. Par exemple, corp pour le répertoire DNS corp.example.com.
- Trend Micro — Sécurité de la protection des terminaux (EPS) : Trend Micro Endpoint Protection (EPS) est le principal composant d'AMS pour la sécurité du système d'exploitation. Le système comprend Deep Security Manager (DSM), des EC2 instances, des EC2 instances relais et un agent présent dans tous les plans de données et les EC2 instances du client.

Vous devez utiliser le `EPSTMarketplaceSubscriptionRole` compte Shared Services et vous abonner soit à l'AMI Trend Micro Deep Security (BYOL), soit à Trend Micro Deep Security (Marketplace).

Les entrées par défaut suivantes sont requises pour créer un EPS (si vous souhaitez modifier les valeurs par défaut) :

- Type d'instance de relais : valeur par défaut - m5.large
 - Type d'instance DSM : valeur par défaut : m5.xlarge
 - Taille de l'instance de base de données : valeur par défaut : 200 Go
 - Type d'instance RDS : valeur par défaut - db.m5.large
- Bastions du client : vous disposez de bastions SSH ou RDP (ou les deux) dans le compte Shared Services, pour accéder à d'autres hôtes de votre environnement AMS. Afin d'accéder au réseau AMS en tant qu'utilisateur (SSH/RDP), you must use "customer" Bastions as the entry point. The network path originates from the on-premise network, goes through DX/VPN à la passerelle de transit (TGW), puis d'être acheminé vers le VPC Shared Services. Une fois que vous êtes en mesure d'accéder au bastion, vous pouvez accéder à d'autres hôtes dans l'environnement AMS, à condition que la demande d'accès ait été accordée.
- Les entrées suivantes sont requises pour les bastions SSH.
 - Capacité d'instance souhaitée de SSH Bastion : valeur par défaut : 2.
 - Nombre maximal d'instances SSH Bastion : valeur par défaut : 4.
 - Instances minimales de SSH Bastion : valeur par défaut -2.
 - Type d'instance SSH Bastion : valeur par défaut : m5.large (peut être modifiée pour réduire les coûts, par exemple un t3.medium).
 - SSH Bastion Ingress CIDRs : plages d'adresses IP à partir desquelles les utilisateurs de votre réseau accèdent à SSH Bastions.
 - Les entrées suivantes sont requises pour les bastions Windows RDP.
 - Type d'instance RDP Bastion : valeur par défaut : t3.medium.
 - Sessions minimales souhaitées par RDP Bastion : valeur par défaut : 2.
 - Nombre maximal de sessions RDP : valeur par défaut -10.
 - Type de configuration RDP Bastion : vous pouvez choisir l'une des configurations ci-dessous
 - SecureStandard = Un utilisateur reçoit un bastion et un seul utilisateur peut se connecter au bastion.
 - SecureHA = Un utilisateur reçoit deux bastions dans deux AZ différentes auxquels il peut se connecter et un seul utilisateur peut se connecter au bastion.
 - SharedStandard = Un utilisateur reçoit un bastion auquel se connecter et deux utilisateurs peuvent se connecter au même bastion en même temps.

- SharedHA = Un utilisateur reçoit deux bastions dans deux AZ différentes auxquels se connecter et deux utilisateurs peuvent se connecter au même bastion en même temps.
- Entrée RDP du client CIDRs : plages d'adresses IP à partir desquelles les utilisateurs de votre réseau accèderont aux bastions RDP.

Mises à jour des services partagés : zone d'accueil multi-comptes

AMS applique les versions des plans de données aux comptes gérés sur une base mensuelle, sans préavis.

AMS utilise l'unité d'organisation principale pour fournir des services partagés tels que l'accès, le réseau, l'EPS, le stockage des journaux, l'agrégation d'alertes dans votre zone d'accueil multicomptes. AMS est chargé de remédier aux vulnérabilités, d'appliquer des correctifs et de déployer ces services partagés. AMS met régulièrement à jour les ressources utilisées pour fournir ces services partagés afin que les utilisateurs aient accès aux dernières fonctionnalités et aux mises à jour de sécurité. Les mises à jour ont généralement lieu sur une base mensuelle. Les ressources incluses dans ces mises à jour sont les suivantes :

- Comptes faisant partie de l'unité d'organisation principale.

Le compte de gestion, le compte de services partagés, le compte réseau, le compte de sécurité et le compte d'archivage des journaux contiennent des ressources pour les bastions RDP et SSH, les proxys, les hôtes de gestion et la sécurité des terminaux (EPS), qui sont généralement mises à jour tous les mois. AMS utilise des EC2 déploiements immuables dans le cadre de l'infrastructure de services partagés.

- Nouvel AMS AMIs intégrant les dernières mises à jour.

Note

Les opérateurs AMS utilisent un type de modification de suppression d'alarme (CT) interne lorsqu'ils exécutent des modifications du plan de données et le RFC correspondant à ce CT apparaît dans votre liste de RFC. En effet, au fur et à mesure que la version du plan de données est déployée, diverses infrastructures peuvent être arrêtées, redémarrées, mises hors ligne, ou le déploiement peut entraîner des pics de processeur ou d'autres effets déclenchant des alarmes qui, lors du déploiement du plan de données, ne sont pas

pertinentes. Une fois le déploiement terminé, le bon fonctionnement de toute l'infrastructure est vérifié et les alarmes sont réactivées.

Compte Log Archive

Le compte Log Archive sert de plateforme centrale pour l'archivage des journaux dans votre environnement de zone de landing zone multi-comptes AMS. Le compte contient un compartiment S3 qui contient des copies des fichiers journaux AWS CloudTrail et AWS Config de chacun des comptes d'environnement de zone de landing zone multi-comptes AMS. Vous pouvez utiliser ce compte pour votre solution de journalisation centralisée avec AWS Firehose ou Splunk, etc. L'accès d'AMS à ce compte est limité à quelques utilisateurs ; réservé aux auditeurs et aux équipes de sécurité pour les enquêtes de conformité et d'investigation liées à l'activité du compte.

Compte de sécurité

Le compte Security est le point central pour les opérations liées à la sécurité du logement et le principal point de transmission des notifications et des alertes vers les services du plan de contrôle AMS. En outre, le compte Security héberge le compte de gestion Amazon Guard Duty et l'agrégateur AWS Config.

Types de comptes d'applications

Les comptes d'application sont des comptes AWS intégrés à l'architecture de zone d'atterrissage gérée par AMS que vous utilisez pour héberger vos charges de travail. AMS propose trois types de comptes d'application :

- [Comptes d'applications gérés par AMS](#)
- [Comptes AMS Accelerate](#)
- [Comptes d'applications gérés par le client](#)

Les comptes d'applications sont regroupés différemment OUs dans AWS Organizations en fonction du type de compte d'application :

- Root OU :
 1. UO d'applications

- UO gérée : comptes gérés par AMS
 - UO de développement : comptes gérés par AMS avec le mode développeur activé
2. Accélérer l'unité d'exploitation : AMS accélère les comptes d'applications
 3. UO gérée par le client : comptes d'applications gérés par le client

Les comptes d'applications sont approvisionnés via un RFC soumis depuis le compte de gestion :

- [Créer un compte d'application avec le VPC ct-1zdasmc2ewzrs](#)
- Créer un compte Accelerate [ct-2p93tyd5angmi](#)
- [Créer un compte d'application géré par le client ct-3pwbixz27n3tn](#)

Comptes d'applications gérés par AMS

Les comptes d'applications entièrement gérés par AMS sont appelés comptes d'applications gérés par AMS, dans lesquels certaines ou toutes les tâches opérationnelles, telles que la gestion des demandes de service, la gestion des incidents, la gestion de la sécurité, la gestion de la continuité (sauvegarde), la gestion des correctifs, l'optimisation des coûts ou la surveillance et la gestion des événements de l'infrastructure, sont effectuées par AMS.

Le nombre de tâches effectuées par AMS dépend du mode de gestion des modifications que vous sélectionnez. Les comptes gérés par AMS prennent en charge différents modes de gestion du changement :

- [Mode RFC](#)
- [Mode de changement direct dans AMS](#)
- [AMS et AWS Service Catalog](#)
- [Mode développeur avancé AMS](#)
- [Mode de provisionnement en libre-service dans AMS](#)

Pour plus d'informations sur la gestion des modifications et les différents modes, consultez [Modes de gestion des modifications](#).

Certains services AWS peuvent être utilisés dans votre compte géré par AMS sans gestion AMS. La liste de ces services AWS et la procédure à suivre pour les ajouter à votre compte AMS sont décrites dans la section [Provisionnement en libre-service](#).

Comptes AMS Accelerate

AMS Accelerate est le plan d'exploitation AMS qui permet d'exploiter l'infrastructure AWS supportant les charges de travail. 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 qui nécessitent 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 utiliserez vos mécanismes d'accès et de changement préférés, 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.

Note

Les comptes AMS Accelerate dans AMS Advanced ne disposent pas de la gestion des modifications AMS (RFCs) ou de la console AMS Advanced. Ils disposent plutôt de la console et de la fonctionnalité AMS Accelerate.

Les comptes Accelerate ne peuvent être approvisionnés qu'à partir de votre compte AMS multi-comptes landing zone Management. Accelerate propose différentes fonctionnalités opérationnelles. Pour en savoir plus, consultez la [description du service Accelerate](#).

- Vous continuerez à profiter de certaines fonctionnalités des comptes principaux de la zone d'atterrissage multi-comptes (MALZ), telles que la journalisation centralisée, la facturation unique, l'agrégateur de configuration dans le compte de sécurité et. SCPs
- AMS Accelerate ne fournit pas certains services AMS Advanced tels que l'EPS, la gestion des accès, la gestion des modifications et le provisionnement. Nous vous recommandons de suivre les étapes suivantes pour accéder à la passerelle de transit (TGW) et la configurer.

Pour plus de détails sur Accelerate, voir [Qu'est-ce qu'Accelerate ?](#)

Création de votre compte Accelerate

Pour créer un compte Accelerate, suivez les étapes décrites ici [Créer un compte Accelerate](#).

Accès à votre compte Accelerate

Une fois que vous avez créé un compte Accelerate sur votre compte de zone de landing zone multi-comptes (MALZ), un rôle avec des autorisations [d'accès administratives](#) est `AccelerateDefaultAdminRole` inscrit dans le compte et vous pouvez l'assumer.

Pour accéder au nouveau compte Accelerate :

1. Connectez-vous à la console IAM pour le compte de gestion doté du `CustomerDefaultAssumeRole` rôle.
2. Dans la console IAM, dans la barre de navigation, choisissez votre nom d'utilisateur.
3. Choisissez Changer de rôle. Si vous choisissez cette option pour la première fois, une page contenant plus d'informations s'affiche. Après l'avoir lue, choisissez Switch Role (Changer de rôle). Si vous désactivez les cookies de votre navigateur, cette page peut s'afficher de nouveau.
4. Sur la page Switch Role, tapez l'ID du compte Accelerate et le nom du rôle à assumer : `AccelerateDefaultAdminRole`.

Maintenant que vous y avez accès, vous pouvez créer de nouveaux rôles IAM pour continuer à accéder à votre environnement. Si vous souhaitez tirer parti de la fédération SAML pour votre compte Accelerate, consultez la section [Permettre aux utilisateurs fédérés SAML 2.0 d'accéder à la console de gestion AWS](#).

Connexion de votre compte Accelerate à Transit Gateway

AMS ne gère pas la configuration réseau d'un compte Accelerate. Vous avez la possibilité de gérer votre propre réseau à l'aide d'AWS APIs (voir [Networking Solutions](#)) ou de vous connecter au réseau MALZ géré par AMS, en utilisant le Transit Gateway (TGW) existant déployé dans AMS MALZ.

Note

Vous ne pouvez associer un VPC au TGW que si le compte Accelerate se trouve dans la même région AWS. Pour plus d'informations, consultez la section [Passerelles de transport en commun](#).

Pour ajouter votre compte Accelerate à Transit Gateway, demandez un nouvel itinéraire en utilisant le type de changement [Deployment | Managed landing zone | Networking account | Add static route](#) (ct-3r2ckznmt0a59), en incluant les informations suivantes :

- **Blackhole** : True pour indiquer que la cible de l'itinéraire n'est pas disponible. Procédez ainsi lorsque le trafic de l'itinéraire statique doit être supprimé par le Transit Gateway. False pour acheminer le trafic vers l'ID de pièce jointe TGW spécifié. La valeur par défaut est false.
- **DestinationCidrBlock**: plage d' IPv4 adresses CIDR utilisée pour les correspondances de destination. Les décisions de routage sont basées sur la correspondance la plus spécifique. Exemple : 10.0.2.0/24.
- **TransitGatewayAttachmentId**: ID de pièce jointe TGW qui servira de cible à la table de routage. Si Blackhole est faux, ce paramètre est obligatoire, sinon laissez ce paramètre vide. Exemple : tgw-attach-04eb40d1e14ec7272.
- **TransitGatewayRouteTableId**: ID de la table de routage TGW. Exemple : tgw-rtb-06ddc751c0c0c881c.

Créez des itinéraires dans les tables de routage TGW pour vous connecter à ce VPC :

1. Par défaut, ce VPC ne pourra communiquer avec aucun autre VPCs VPC de votre réseau MALZ.
2. Décidez avec votre architecte de solutions avec quoi VPCs vous souhaitez que ce VPC Accelerate communique.
3. Soumettre un [déploiement | Zone d'atterrissage gérée | Compte réseau | Ajouter un type de changement de route statique](#) (ct-3r2ckznmt0a59), incluez les informations suivantes :
 - **Blackhole** : True pour indiquer que la cible de l'itinéraire n'est pas disponible. Procédez ainsi lorsque le trafic de l'itinéraire statique doit être supprimé par le Transit Gateway. False pour acheminer le trafic vers l'ID de pièce jointe TGW spécifié. La valeur par défaut est false.
 - **DestinationCidrBlock**: plage d' IPv4 adresses CIDR utilisée pour les correspondances de destination. Les décisions de routage sont basées sur la correspondance la plus spécifique. Exemple : 10.0.2.0/24.
 - **TransitGatewayAttachmentId**: ID de pièce jointe TGW qui servira de cible à la table de routage. Si Blackhole est faux, ce paramètre est obligatoire, sinon laissez ce paramètre vide. Exemple : tgw-attach-04eb40d1e14ec7272.
 - **TransitGatewayRouteTableId**: ID de la table de routage TGW. Exemple : tgw-rtb-06ddc751c0c0c881c.

Connexion d'un nouveau compte Accelerate VPC au réseau AMS Multi-Account Landing Zone (création d'une pièce jointe VPC TGW) :

1. Dans votre compte réseau de zone de landing zone multi-comptes, ouvrez la console [Amazon VPC](#).
2. Dans le volet de navigation, choisissez Passerelles de transit. Enregistrez l'ID TGW de la passerelle de transit que vous voyez.
3. Dans votre compte Accelerate, ouvrez la [console Amazon VPC](#).
4. Dans le volet de navigation, choisissez Transit Gateway Attachments > Create Transit Gateway Attachment. Faites les choix suivants :
 - Pour le Transit Gateway ID, choisissez l'ID de passerelle de transit que vous avez enregistré à l'étape 2.
 - Pour Attachment type (Type d'attachement), choisissez VPC.
 - Sous Attachement de VPC, saisissez un nom pour la Balise de nom d'attachement (facultatif).
 - Choisissez d'activer ou non le IPv6 support DNS.
 - Pour VPC ID (ID de VPC), choisissez le VPC à attacher à la passerelle de transit. Ce VPC doit avoir au moins un sous-réseau associé.
 - Pour Sous-réseau IDs, sélectionnez un sous-réseau pour chaque zone de disponibilité à utiliser par la passerelle de transit pour acheminer le trafic. Vous devez sélectionner au moins un sous-réseau. Vous pouvez sélectionner un seul sous-réseau par zone de disponibilité.
5. Choisissez Créer un attachement. Enregistrez l'ID de la pièce jointe TGW nouvellement créée.

Associer la pièce jointe TGW à une table de routage :

1. Décidez à quelle table de routage TGW vous souhaitez associer le VPC. Nous vous recommandons de créer une nouvelle table de routage d'application pour le compte Accelerate VPCs en utilisant le type de changement Deployment | Managed landing zone | Networking account | Create transit gateway route table (ct-3dscwaeyi6cup).
2. Soumettez une RFC [de gestion | Zone d'atterrissage gérée | Compte réseau | Associer une pièce jointe TGW](#) (ct-3nmhh0qr338q6) sur le compte réseau pour associer la pièce jointe VPC ou TGW à la table de routage que vous sélectionnez.

Créez des itinéraires dans les tables de routage TGW pour vous connecter à ce VPC :

1. Par défaut, ce VPC ne pourra communiquer avec aucun autre VPC de votre réseau de zone VPCs d'atterrissage multi-comptes.

2. Décidez avec votre architecte de solutions avec quoi VPCs vous souhaitez que ce VPC de compte Accelerate communique.
3. Soumettez une RFC de [déploiement](#) | [Zone d'atterrissage gérée](#) | [Compte réseau](#) | [Ajoutez une route statique](#) (ct-3r2ckznmt0a59) au compte réseau pour créer les itinéraires TGW dont vous avez besoin.

Configuration de vos tables de routage VPC pour qu'elles pointent vers la passerelle de transit multi-comptes AMS pour la zone d'atterrissage :

1. Décidez avec votre architecte de solutions quel trafic vous souhaitez envoyer vers la passerelle de transit AMS Multi-Account Landing Zone.
2. Soumettez une RFC de [déploiement](#) | [Zone d'atterrissage gérée](#) | [Compte réseau](#) | [Ajoutez une route statique](#) (ct-3r2ckznmt0a59) au compte réseau pour créer les itinéraires TGW dont vous avez besoin.

Comptes d'applications gérés par le client

Vous pouvez créer des comptes qu'AMS ne gère pas de manière standard. Ces comptes sont appelés comptes gérés par le client et vous permettent de contrôler totalement l'infrastructure au sein des comptes tout en profitant des avantages de l'architecture centralisée gérée par AMS.

Les comptes gérés par le client n'ont pas accès à la console AMS ni à aucun des services que nous fournissons (correctif, sauvegarde, etc.).

Les comptes gérés par le client ne peuvent être approvisionnés qu'à partir de votre compte de gestion de zone d'atterrissage multi-comptes AMS.

Les différents modes AMS fonctionnent différemment avec les comptes d'application ; pour en savoir plus sur les modes, consultez les [modes AWS Managed Services](#).

Pour créer votre compte d'application géré par le client, voir [Compte de gestion](#) | [Créer un compte d'application géré par le client](#).

Pour supprimer un compte d'application géré par le client, utilisez [Compte de gestion](#) | [Compte d'application externe](#). (Le CT de [confirmation de l'offboarding](#) ne s'applique pas aux comptes d'applications gérés par le client.)

Accès à votre compte géré par le client

Une fois que vous avez créé un compte géré par le client (CMA) dans une zone de landing zone multi-comptes, un rôle d'administrateur (MALZ) est `CustomerDefaultAdminRole` intégré au compte et vous pouvez assumer, par le biais de la fédération SAML, pour configurer le compte.

Pour accéder au CMA :

1. Connectez-vous à la console IAM pour le compte de gestion doté du `CustomerDefaultAssumeRole`.
2. Dans la console IAM, dans la barre de navigation, choisissez votre nom d'utilisateur.
3. Choisissez **Changer de rôle**. Si vous choisissez cette option pour la première fois, une page contenant plus d'informations s'affiche. Après l'avoir lue, choisissez **Switch Role (Changer de rôle)**. Si vous désactivez les cookies de votre navigateur, cette page peut s'afficher de nouveau.
4. Sur la page **Changer de rôle**, tapez l'ID du compte géré par le client et le nom du rôle à assumer : `CustomerDefaultAdminRole`.

Maintenant que vous y avez accès, vous pouvez créer de nouveaux rôles IAM pour continuer à accéder à votre environnement. Si vous souhaitez tirer parti de la fédération SAML pour votre compte CMA, consultez la section [Permettre aux utilisateurs fédérés SAML 2.0 d'accéder à la console de gestion AWS](#).

Connecter votre CMA à Transit Gateway

AMS ne gère pas la configuration réseau des comptes gérés par le client (CMAs). Vous avez la possibilité de gérer votre propre réseau à l'aide d'AWS APIs (voir [Networking Solutions](#)) ou de vous connecter au réseau de zones d'atterrissage multi-comptes géré par AMS, en utilisant le Transit Gateway (TGW) existant déployé dans AMS MALZ.

Note

Un VPC ne peut être rattaché au TGW que si le CMA se trouve dans la même région AWS. Pour plus d'informations, consultez la section [Passerelles de transport en commun](#).

Pour ajouter votre CMA à Transit Gateway, demandez un nouvel itinéraire avec le type de changement de [compte Networking | Add static route \(ct-3r2ckznmt0a59\)](#) et incluez les informations suivantes :

- **Blackhole** : True pour indiquer que la cible de l'itinéraire n'est pas disponible. Procédez ainsi lorsque le trafic de l'itinéraire statique doit être supprimé par le Transit Gateway. False pour acheminer le trafic vers l'ID de pièce jointe TGW spécifié. La valeur par défaut est false.
- **DestinationCidrBlock**: plage IPV4 CIDR utilisée pour les correspondances de destination. Les décisions de routage sont basées sur la correspondance la plus spécifique. Exemple : `10.0.2.0/24`.
- **TransitGatewayAttachmentId**: ID de pièce jointe TGW qui servira de cible à la table de routage. Si Blackhole est faux, ce paramètre est obligatoire, sinon laissez ce paramètre vide. Exemple : `tgw-attach-04eb40d1e14ec7272`.
- **TransitGatewayRouteTableId**: ID de la table de routage TGW. Exemple : `tgw-rtb-06ddc751c0c0c881c`.

Connexion d'un nouveau VPC géré par le client au réseau AMS Multi-Account Landing Zone (création d'une pièce jointe VPC TGW) :

1. Dans votre compte réseau de zone de landing zone multi-comptes, ouvrez la console [Amazon VPC](#).
2. Dans le volet de navigation, choisissez Transit Gateways. Enregistrez l'ID TGW de la passerelle de transit que vous voyez.
3. Dans votre compte géré par le client, ouvrez la [console Amazon VPC](#).
4. Dans le volet de navigation, choisissez Transit Gateway Attachments > Create Transit Gateway Attachment. Faites les choix suivants :
 - a. Pour le Transit Gateway ID, choisissez l'ID de passerelle de transit que vous avez enregistré à l'étape 2.
 - b. Pour Attachment type (Type d'attachement), choisissez VPC.
 - c. Sous Attachement de VPC, saisissez un nom pour la Balise de nom d'attachement (facultatif).
 - d. Choisissez d'activer ou non le IPv6 support DNS.
 - e. Pour VPC ID (ID de VPC), choisissez le VPC à attacher à la passerelle de transit. Ce VPC doit avoir au moins un sous-réseau associé.
 - f. Pour Sous-réseau IDs, sélectionnez un sous-réseau pour chaque zone de disponibilité à utiliser par la passerelle de transit pour acheminer le trafic. Vous devez sélectionner au moins un sous-réseau. Vous pouvez sélectionner un seul sous-réseau par zone de disponibilité.

5. Choisissez Créer un attachement. Enregistrez l'ID de la pièce jointe TGW nouvellement créée.

Associer la pièce jointe TGW à une table de routage :

Décidez à quelle table de routage TGW vous souhaitez associer le VPC. Nous vous recommandons de créer une nouvelle table de routage d'applications pour Customer Managed VPCs en soumettant une RFC de déploiement | Zone d'atterrissage gérée | Compte réseau | Création d'une table de routage de passerelle de transit (ct-3dscwaeyi6cup). Pour associer la pièce jointe VPC ou TGW à la table de routage que vous sélectionnez, soumettez une RFC Déploiement | Zone d'atterrissage gérée | Compte réseau | Pièce jointe TGW associée (ct-3nmhh0qr338q6) sur le compte réseau.

Créez des itinéraires dans les tables de routage TGW pour vous connecter à ce VPC :

1. Par défaut, ce VPC ne pourra communiquer avec aucun autre VPCs VPC de votre réseau Multi-Account Landing Zone.
2. Décidez avec votre architecte de solutions avec quoi VPCs vous souhaitez que ce VPC géré par le client communique. Soumettez une RFC de déploiement | Zone d'atterrissage gérée | Compte réseau | Ajoutez une route statique (ct-3r2ckznmt0a59) au compte réseau pour créer les itinéraires TGW dont vous avez besoin.

Note

Ce CT (ct-3r2ckznmt0a59) n'autorise pas l'ajout de routes statiques à la table de routage principale EgressRouteDomain ; si votre CMA doit autoriser le trafic de sortie, soumettez une RFC de gestion | Autre | Autre (MOO) avec ct-0xdawir96cy7k.

Configuration de vos tables de routage VPC pour qu'elles pointent vers la passerelle de transit AMS Multi-Account Landing Zone :

Décidez avec votre architecte de solutions quel trafic vous souhaitez envoyer vers la passerelle de transit AMS Multi-Account Landing Zone. Mettez à jour vos tables de routage VPC pour envoyer le trafic vers la pièce jointe TGW créée précédemment

Obtenir de l'aide opérationnelle avec vos comptes gérés par le client

AMS peut vous aider à gérer les charges de travail que vous avez déployées dans vos comptes gérés par le client en intégrant le compte à AMS Accelerate. Avec AMS Accelerate, vous pouvez bénéficier de services opérationnels 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 votre mode d'utilisation AWS. AMS Accelerate propose également un module complémentaire de correctif en option pour les charges de travail EC2 basées qui nécessitent des correctifs réguliers. Avec AMS Accelerate, vous continuez à utiliser, configurer et déployer tous les AWS services de manière native ou avec vos outils préférés, comme vous le faites avec les comptes gérés par les clients AMS Advanced. Vous utilisez vos mécanismes d'accès et de changement préférés, tandis qu'AMS applique des pratiques éprouvées qui permettent de faire évoluer votre équipe, d'optimiser les coûts, d'accroître la sécurité et l'efficacité et d'améliorer la résilience. Pour en savoir plus, consultez la [description du service Accelerate](#).

Pour intégrer votre compte géré par le client à Accelerate, contactez votre CSDM et suivez les étapes décrites dans [Getting Started with AMS Accelerate](#).

Note

Les comptes AMS Accelerate dans AMS Advanced ne disposent pas de la gestion des modifications AMS (demandes de modification ou RFCs) ni de la console AMS Advanced. Ils disposent plutôt de la console et de la fonctionnalité AMS Accelerate.

Compte AMS Tools (migration des charges de travail)

Votre compte Multi-Account Landing Zone Tools (avec VPC) permet d'accélérer les efforts de migration, d'améliorer votre position en matière de sécurité, de réduire les coûts et la complexité et de normaliser votre modèle d'utilisation.

Un compte d'outils fournit les éléments suivants :

- Une limite bien définie pour l'accès aux instances de réplication pour les intégrateurs de systèmes en dehors de vos charges de travail de production.
- Vous permet de créer une chambre isolée pour vérifier la présence de logiciels malveillants ou de routes réseau inconnues dans une charge de travail avant de la placer dans un compte associé à d'autres charges de travail.

- En tant que configuration de compte définie, elle permet d'accélérer l'intégration et la configuration pour la migration des charges de travail.
- Routes réseau isolées pour sécuriser le trafic depuis un compte sur site CloudEndure -> -> Outils -> Image ingérée AMS. Une fois qu'une image a été ingérée, vous pouvez la partager sur le compte de destination via une RFC AMS Management | Advanced stack components | AMI | Share (ct-1eiczxw8ihc18).

Schéma d'architecture de haut niveau :

Utilisez le type de changement de type Déploiement | Zone d'atterrissage gérée | Compte de gestion | Créer un compte d'outils (avec VPC) (ct-2j7q1hgf26x5c) pour déployer rapidement un compte d'outils et instancier un processus d'ingestion de charge de travail dans un environnement de zone d'atterrissage multicompte. Voir [Compte de gestion, compte Outils : création \(avec VPC\)](#).

Note

Nous recommandons d'avoir deux zones de disponibilité (AZs), car il s'agit d'un hub de migration.

Par défaut, AMS crée les deux groupes de sécurité suivants (SGs) dans chaque compte. Confirmez que ces deux SGs éléments sont présents. S'ils ne sont pas présents, veuillez ouvrir une nouvelle demande de service auprès de l'équipe AMS pour en faire la demande.

- SentinelDefaultSecurityGroupPrivateOnlyEgressAll
- InitialGarden-SentinelDefaultSecurityGroupPrivateOnly

Assurez-vous que les instances de CloudEndure réplication sont créées dans le sous-réseau privé où se trouvent des itinéraires permettant de revenir sur site. Vous pouvez le confirmer en vous assurant que les tables de routage du sous-réseau privé disposent d'une route par défaut vers TGW. Cependant, l'exécution d'une coupure de CloudEndure machine doit se faire dans le sous-réseau privé « isolé » où il n'y a pas de route de retour vers le réseau local, seul le trafic sortant d'Internet est autorisé. Il est essentiel de s'assurer que le transfert a lieu dans le sous-réseau isolé afin d'éviter d'éventuels problèmes avec les ressources sur site.

Prérequis :

1. Niveau de support Plus ou Premium.
2. Le compte d'application IDs pour la clé KMS sur laquelle AMIs ils sont déployés.
3. Le compte d'outils, créé comme décrit précédemment.

AWS Service de migration d'applications (AWS MGN)

[AWS Le service de migration d'applications](#) (AWS MGN) peut être utilisé dans votre compte MALZ Tools via le rôle `AWSToolsManagedServicesMigrationRole` IAM créé automatiquement lors du provisionnement du compte Tools. Vous pouvez utiliser AWS MGN pour migrer des applications et des bases de données qui s'exécutent sur des versions prises en charge des [systèmes d'exploitation](#) Windows et Linux.

Pour plus d' up-to-date informations sur le Région AWS support, consultez [la liste des services AWS régionaux](#).

Si votre système préféré n' Région AWS est pas actuellement pris en charge par AWS MGN, ou si le système d'exploitation sur lequel vos applications s'exécutent n'est pas actuellement pris en charge par AWS MGN, envisagez plutôt d'utiliser la [CloudEndure migration](#) dans votre compte Tools.

Demande d' AWS initialisation de MGN

AWS MGN doit être [initialisé](#) par AMS avant la première utilisation. Pour en faire la demande pour un nouveau compte Tools, soumettez une RFC Management | Other | Other depuis le compte Tools avec les informations suivantes :

RFC Subject=Please initialize AWS MGN in this account

RFC Comment=Please click 'Get started' on the MGN welcome page here:

https://console.aws.amazon.com/mgn/home?region=MALZ_PRIMARY_REGION#/welcome using all default values to 'Create template' and complete the initialization process.

Une fois qu'AMS a terminé avec succès le RFC et initialisé AWS MGN dans votre compte Tools, vous pouvez l'utiliser `AWSToolsManagedServicesMigrationRole` pour modifier le modèle par défaut en fonction de vos besoins.

Activer l'accès au nouveau compte AMS Tools

Une fois le compte Tools créé, AMS vous fournit un identifiant de compte. L'étape suivante consiste à configurer l'accès au nouveau compte. Procédez comme suit :

1. Mettez à jour les groupes Active Directory appropriés vers le compte approprié IDs.

Les nouveaux comptes créés par AMS sont dotés de la politique de ReadOnly rôle ainsi que d'un rôle permettant aux utilisateurs de déposer des dossiers. RFCs

Le compte Tools dispose également d'un rôle et d'un utilisateur IAM supplémentaires :

- Rôle IAM : `AWSToolsMigrationRole`
 - Utilisateur IAM : `customer_cloud_endure_user`
2. Demandez des politiques et des rôles pour permettre aux membres de l'équipe d'intégration des services de configurer le niveau d'outils suivant.

Accédez à la console AMS et enregistrez les fichiers suivants RFCs :

- a. Créez une clé KMS. Utilisez [Create KMS Key \(auto\)](#) ou [Create KMS Key \(révision requise\)](#).

Lorsque vous utilisez KMS pour chiffrer les ressources ingérées, l'utilisation d'une clé KMS unique partagée avec les autres comptes de l'application Multi-Account Landing Zone permet de sécuriser les images ingérées afin qu'elles puissent être déchiffrées dans le compte de destination.

- b. Partagez la clé KMS.

Utilisez le type de modification Management | Advanced stack components | KMS key | Share (révision requise) (ct-05yb337abq3x5) pour demander que la nouvelle clé KMS soit partagée avec les comptes de votre application où résidera la clé ingérée. AMIs

Exemple graphique de la configuration finale d'un compte :

Exemple de politique CloudEndure IAM pré-approuvée par AMS

Pour consulter une CloudEndure politique IAM préapprouvée par AMS : décompressez le fichier d'[exemple de zone d'atterrissage WIGS Cloud Endure](#) et ouvrez le `customer_cloud_endure_policy.json`

Test de la connectivité et de la end-to-end configuration du compte AMS Tools

1. Commencez par configurer CloudEndure et installer l' CloudEndure agent sur un serveur qui sera répliqué sur AMS.
2. Créez un projet dans CloudEndure.
3. Entrez les AWS informations d'identification partagées lorsque vous avez effectué les prérequis, via le gestionnaire de secrets.
4. Dans les paramètres de réplication :
 - a. Sélectionnez les deux groupes de sécurité AMS « Sentinel » (privé uniquement EgressAll) pour l'option Choisissez les groupes de sécurité à appliquer aux serveurs de réplication.
 - b. Définissez les options de transfert pour les machines (instances). Pour plus d'informations, reportez-vous [à l'étape 5. Découper](#)
 - c. Sous-réseau : sous-réseau privé.
5. Groupe de sécurité :
 - a. Sélectionnez les deux groupes de sécurité AMS « Sentinel » (privé uniquement et EgressAll).
 - b. Les instances de transition doivent communiquer avec l'Active Directory (MAD) géré par AMS et avec les points de terminaison publics : AWS
 - i. IP élastique : aucune
 - ii. IP publique : non
 - iii. Rôle IAM : customer-mc-ec profil à 2 instances
 - c. Définissez les balises conformément à votre convention de balisage interne.
6. Installez l' CloudEndure agent sur la machine et recherchez l'instance de réplication qui apparaîtra dans votre compte AMS dans la EC2 console.

Le processus d'ingestion d'AMS :

Hygiène des comptes AMS Tools

Vous devrez procéder au nettoyage une fois que vous aurez terminé de partager l'AMI dans le compte et que vous n'aurez plus besoin des instances répliquées :

- Après l' WIGs ingestion de l'instance :
 - Instance de transition : au minimum, arrêtez ou mettez fin à cette instance, une fois le travail terminé, via la console AWS

- Sauvegardes d'AMI avant ingestion : supprimez une fois que l'instance a été ingérée et que l'instance sur site a été arrêtée
- Instances ingérées par AMS : désactivez la pile ou mettez-la hors service une fois que l'AMI a été partagée
- AMS-ingested AMIs : Supprimer une fois le partage avec le compte de destination terminé
- Nettoyage de fin de migration : documentez les ressources déployées via le mode développeur pour vous assurer que le nettoyage a lieu régulièrement, par exemple :
 - Groupes de sécurité
 - Ressources créées via Cloud-formation
 - Réseau ACK
 - Sous-réseau
 - VPC
 - Table de routage
 - Rôles
 - Utilisateurs et comptes

Migration à grande échelle - Migration Factory

Voir [Présentation de la solution AWS CloudEndure Migration Factory](#).

Architecture du réseau SALZ

Le schéma suivant décrit la configuration du réseau VPC de la zone d'atterrissage à compte unique (SALZ) d'AWS Managed Services (AMS) et constitue un exemple de configuration à haute disponibilité.

AMS configure pour vous tous les aspects de la mise en réseau sur la base de nos modèles standard et des options que vous avez sélectionnées lors de l'intégration. Une conception de réseau AWS standard est appliquée à votre compte AWS, et un cloud privé virtuel (VPC) est créé pour vous et connecté à AMS par VPN ou Direct Connect. Pour en savoir plus sur Direct Connect, rendez-vous sur [AWS Direct Connect](#). Les standards incluent la DMZ, les services partagés et un sous-réseau d'applications. Au cours du processus d'intégration, des informations supplémentaires VPCs peuvent être demandées et créées pour répondre à vos besoins (par exemple, divisions

clients, partenaires). Après l'intégration, vous recevez un diagramme de réseau, un document d'environnement qui explique comment votre réseau a été configuré.

Note

Pour en savoir plus sur les limites et les contraintes de service par défaut pour tous les services actifs, consultez la documentation relative [aux limites de service AWS](#).

La conception de notre réseau repose sur le « [principe du moindre privilège](#) » d'Amazon. Pour ce faire, nous acheminons tout le trafic, entrant et sortant, via des passerelles, à l'exception du trafic provenant d'un réseau fiable. Le seul réseau fiable est celui configuré entre votre environnement sur site et le VPC via l'utilisation d'un and/or VPN et d'AWS Direct Connect (DX). L'accès est accordé par le biais d'instances de bastion, empêchant ainsi l'accès direct aux ressources de production. Toutes vos applications et ressources se trouvent dans des sous-réseaux privés accessibles via des équilibreurs de charge publics. Le trafic de sortie public passe par nos proxys de transfert vers Internet Gateway, puis vers Internet. Le trafic peut également passer par votre VPN ou Direct Connect vers votre environnement sur site.

Services partagés de zone d'atterrissage à compte unique AMS

Les sous-réseaux de services partagés contiennent les services d'annuaire AMS, l'hôte de gestion qui automatise le provisionnement et les tâches courantes, le serveur de gestion antivirus (TrendMicro) et les hôtes bastions internes :

- AMS Directory Services = Contrôleur de domaine AD

Crée un Active Directory dans les comptes AMS, crée le domaine AMS, joint les piles gérées au domaine lors du lancement.

- Hôtes de gestion = AMS Management Host (automatisation du provisionnement et des tâches courantes)

Agissez en tant que point de terminaison d'API pour modifier AWS Directory Service et interagir avec les contrôleurs de AWS Directory Service domaine.

- Services de sécurité : serveur de gestion antivirus (TrendMicro) = EPS DSM + EPS Relay

Utilise le logiciel Trend Micro™ Deep Security (DSM), fonctionne selon un modèle client-serveur et dispose d'une base de données principale comprenant des gestionnaires, des agents et des relais Deep Security.

- Hôtes bastions internes = bastions des clients

Des serveurs spécialisés conçus pour être le point d'accès principal depuis Internet et servir de proxy à vos autres EC2 instances Amazon.

Configuration d'AMS

Rubriques

- [Comprendre les paramètres par défaut d'AMS](#)
- [Utilisation des consoles AMS](#)
- [Utilisation de l'API et de la CLI AMS](#)
- [AMS : apportez votre propre EPS](#)
- [Réception de notifications AMS](#)
- [Configuration de DNS privés et publics](#)
- [Gestion du trafic de sortie AMS](#)
- [Déploiement de ressources IAM dans AMS Advanced](#)
- [Configuration des autorisations dans AMS à l'aide de rôles et de profils IAM](#)
- [Règle de réclamation AD FS et paramètres SAML](#)
- [Restreindre avec l'ACL réseau](#)
- [AMS sur Outposts](#)
- [Utilisation de balises dans AMS](#)
- [Planificateur de ressources AWS Managed Services](#)
- [AWS Systems Manager dans AMS Advanced](#)
- [Comptes AMS externes](#)

Certaines tâches de configuration d'AMS peuvent être effectuées lors de l'intégration.

Pour une description complète des rôles et des responsabilités, y compris l'AMS [AWS Services pris en charge](#), voir [Matrice de responsabilité AMS \(RACI\)](#).

Note

Pour demander à AMS de fournir un AWS service supplémentaire, déposez une demande de service. Pour plus d'informations sur la procédure à suivre pour effectuer cette demande, consultez [Gestion des demandes de service](#).

Comprendre les paramètres par défaut d'AMS

Votre réseau AWS Managed Services (AMS) possède une configuration standardisée avec des valeurs par défaut pour la plupart des services.

Cette section décrit les paramètres par défaut utilisés par AMS pour l'accès, la surveillance, la journalisation et la gestion.

Pour un exemple des coûts d'infrastructure d'une zone d'atterrissage multicompte ou d'une zone d'atterrissage à compte unique, voir. [Composants de base de l'environnement AMS](#)

Rubriques

- [Paramètres de résolution DNS par défaut \(MALZ\)](#)
- [EC2 Profil d'instance IAM](#)
- [Alertes issues de la surveillance de base dans AMS](#)
- [Valeurs par défaut de conservation et de rotation des journaux](#)

Paramètres de résolution DNS par défaut (MALZ)

Zone de landing multi-comptes AWS Managed Services (AMS) : dans les environnements AWS, la résolution du système de noms de domaine (DNS) entre le résolveur Route 53 et les résolveurs DNS d'un VPC peut être intégrée en configurant les règles de transfert du résolveur. Avant que ces règles puissent être utilisées pour le transfert de requêtes DNS, il est nécessaire de configurer des points de terminaison de résolution entrants et sortants vers lesquels ces requêtes peuvent être transmises.

Par défaut, les requêtes DNS au sein du compte VPCs d'application dans les paramètres multi-comptes d'AMS sont transmises aux redirecteurs conditionnels du domaine AWS Directory Service for Microsoft Active Directory (également appelé Managed AD) présent dans le compte de services partagés. AMS vous permet éventuellement d'utiliser le AmazonProvided DNS ; par exemple, le AmazonProvided DNS pour transférer les requêtes DNS vers. Cela vous permet d'utiliser des points de terminaison VPC qui, aujourd'hui, ne prennent en charge que le DNS fourni par Amazon via Amazon Route 53. En conséquence, les règles de résolution sont également configurées automatiquement pour les points de terminaison VPC courants qui sont déployés par défaut dans le compte de services partagés. Pour plus d'informations sur ces points de terminaison VPC courants, consultez. [Points de terminaison VPC AMS](#)

Pour configurer les ensembles d'options DHCP (Dynamic Host Configuration Protocol) dans tous vos comptes d'application VPCs afin d'utiliser le DNS fourni par Amazon pour les points de terminaison

VPC, et pour que les règles du résolveur Route53 pointent vers les points de terminaison VPC communs de vos comptes de services partagés (avec une règle de résolution facultative pour le domaine local), créez une gestion | Autre | Autre | Création de demande de modification (RFC) spécifiant le compte de services partagés et demandant l'activation de le compte d'application, le DNS local du VPC et les règles du résolveur Route 53 pour les points de terminaison VPC.

EC2 Profil d'instance IAM

Un profil d'instance est un conteneur pour un rôle IAM que vous pouvez utiliser pour transmettre des informations de rôle à une EC2 instance lorsque celle-ci démarre.

MALZ

Il existe deux profils d'instance par défaut AMS, `customer-mc-ec2-instance-profile` et `customer-mc-ec2-instance-profile-s3`. Ces profils d'instance fournissent les autorisations décrites dans le tableau suivant.

Descriptions des politiques

Profil	Stratégies
customer-mc-ec2-in stance-profile	AmazonSSMManagedInstanceCore : Permet aux instances Ec2 d'utiliser l'agent SSM.
	AMSInstanceProfileLoggingPolicy : Permet aux instances Ec2 de transférer les journaux vers S3 et CloudWatch.
	AMSInstanceProfileManagementPolicy : Permet aux instances Ec2 d'effectuer des actions de démarrage, comme rejoindre Active Directory.
	AMSInstanceProfileMonitoringPolicy : Permet aux instances Ec2 de communiquer les résultats aux services de surveillance AMS.
	AMSInstanceProfilePatchPolicy : Permet aux instances Ec2 de recevoir des correctifs.

Profil	Stratégies
customer-mc-ec2-instance-profile-s3	AMSIInstanceProfileBY0EPSPolicy : Permet aux instances Ec2 d'utiliser AMS pour apporter votre propre EPS .
	AMSIInstanceProfileLoggingPolicy : Permet aux instances Ec2 de transférer les journaux vers S3 et CloudWatch.
	AMSIInstanceProfileManagementPolicy : Permet aux instances Ec2 d'effectuer des actions de démarrage, comme rejoindre Active Directory.
	AMSIInstanceProfileMonitoringPolicy : Permet aux instances Ec2 de communiquer les résultats aux services de surveillance AMS.
	AMSIInstanceProfilePatchPolicy : Permet aux instances Ec2 de recevoir des correctifs.
	AMSIInstanceProfileS3WritePolicy : Permet aux instances Ec2 d'accéder read/write aux compartiments S3 du client.

SALZ

Il existe un profil d'instance par défaut AMScustomer-mc-ec2-instance-profile, qui accorde des autorisations conformément à la politique customer_ec2_instance_profile_policy d'instance IAM. Ce profil d'instance fournit les autorisations décrites dans le tableau suivant. Le profil accorde des autorisations aux applications exécutées sur l'instance, et non aux utilisateurs qui se connectent à l'instance.

Les politiques incluent souvent plusieurs instructions, chaque instruction octroyant des autorisations à un ensemble différent de ressources ou octroyant des autorisations dans des conditions spécifiques.

CW = CloudWatch. ARN = nom de la ressource Amazon. * = caractère générique (n'importe lequel).

EC2 autorisations de profil d'instance IAM par défaut

CW = CloudWatch. ARN = nom de la ressource Amazon. * = caractère générique (n'importe lequel).

Déclaration de stratégie	Effet	Actions	Description et ressource (ARN)
Amazon Elastic Compute Cloud (Amazon EC2)			
EC2 Actions relatives aux messages	Autorisation	AcknowledgeMessage, DeleteMessage, FailMessage, GetEndpoint, GetMessages, SendReply	Autorise EC2 les actions de messagerie de Systems Manager sur votre compte.
Ec2 Décrire	Autorisation	* (Tous)	Permet à la console d'afficher les détails de configuration EC2 d'un compte.
Je reçois un identifiant de rôle	Autorisation	GetRole	Permet d' EC2 obtenir votre identifiant IAM à partir de <code>aws:iam::*:role/customer-*</code> et <code>aws:iam::*:role/customer_*</code> .
Instance pour télécharger les événements du journal	Autorisation	Créer un groupe de journaux	Permet de créer des journaux dans <code>:aws:logs::*:log-group:i-*</code>
		Créer un flux de journal	Permet de diffuser les journaux vers <code>:aws:logs::*:log-group:i-*</code>

CW = CloudWatch. ARN = nom de la ressource Amazon. * = caractère générique (n'importe lequel).

Déclaration de stratégie	Effet	Actions	Description et ressource (ARN)
CW pour MMS	Autorisation	DescribeAlarms, PutMetricAlarm, PutMetricData	Permet CloudWatch de récupérer les alarmes de votre compte. Permet à CW de créer ou de mettre à jour une alarme et de l'associer à la métrique spécifiée. Permet à CW de publier des points de données métriques sur votre compte.
Mots-clés Ec2	Autorisation	CreateTags, DescribeTags,	Permet d'ajouter, de remplacer et de décrire des balises sur les instances spécifiées dans votre compte.
Refuser explicitement les journaux CW	Refuser	DescribeLogStreams, FilterLogEvents, GetLogEvents	Interdit de répertorier, de filtrer ou d'obtenir les flux de journaux pour : <code>aws:logs:*:*:log-group:/mc/*</code>
Amazon EC2 Simple Systems Manager (SSM)			

CW = CloudWatch. ARN = nom de la ressource Amazon. * = caractère générique (n'importe lequel).

Déclaration de stratégie	Effet	Actions	Description et ressource (ARN)
Actions du SSM	Autorisation	DescribeAssociation, GetDocument, ListAssociations, UpdateAssociationStatus, UpdateInstanceInformation	Permet une variété de fonctions SSM dans votre compte.
Accès SSM dans S3	Autorisation	GetObject, PutObject, AbortMultipartUpload, ListMultipartUploadParts, ListBucketMultipartUploads	Permet au SSM d'entrer et de mettre EC2 à jour des objets, d'abandonner un téléchargement d'objets en plusieurs parties vers, et de répertorier les ports et les compartiments disponibles pour les téléchargements en plusieurs parties. <code>aws:s3:::mc-*-internal-*/aws/ssm*</code>

Amazon EC2 Simple Storage Service (S3)

Obtenir un objet dans S3	Autorisation	Get Liste	Permet aux EC2 applications de récupérer et de répertorier des objets dans des compartiments S3 de votre compte.
Accès chiffré au journal S3 par le client	Autorisation	PutObject	Permet aux EC2 applications de mettre à jour des objets dans <code>aws:s3:::mc-*-logs-*/encrypted/app/*</code>

CW = CloudWatch. ARN = nom de la ressource Amazon. * = caractère générique (n'importe lequel).

Déclaration de stratégie	Effet	Actions	Description et ressource (ARN)
Corrigez Data Put Object S3	Autorisation	PutObject	Permet aux EC2 applications de télécharger des données de correctif dans vos compartiments S3 à l'adresse <code>aws:s3:::awsms-a*-patch-data-*</code>
Téléchargement de vos propres journaux vers S3	Autorisation	PutObject	Permet aux EC2 applications de télécharger des journaux personnalisés vers : <code>aws:s3:::mc-a*-logs-*/aws/instances/*/\${aws:userid}/*</code>
Refuser explicitement les journaux S3 de MC Namespace	Refuser	GetObject* Mette*	Interdit aux EC2 applications d'obtenir ou de placer des objets depuis ou vers : <code>aws:s3:::mc-a*-logs-*/encrypted/mc*</code> , <code>aws:s3:::mc-a*-logs-*/mc/*</code> , <code>aws:s3:::mc-a*-logs-audit/*</code>

CW = CloudWatch. ARN = nom de la ressource Amazon. * = caractère générique (n'importe lequel).

Déclaration de stratégie	Effet	Actions	Description et ressource (ARN)
Refuser explicitement la suppression de S3	Refuser	* (tous)	Interdit aux EC2 applications d'effectuer des actions sur des objets dans : aws:s3:::mc-a*-logs-*/* , aws:s3:::mc-a*-internal-*/* ,
Refuser explicitement le compartiment CFN S3	Refuser	Supprimer*	Interdit aux EC2 applications de supprimer des objets dans : aws:s3:::cf-templates-*
Refuser explicitement le bucket de liste S3	Refuser	ListBucket	Vous interdit de répertorier les objets chiffrés, les objets du journal d'audit ou les objets réservés (mc) provenant de : aws:s3:::mc-*-logs-*
AWS Secrets Manager sur Amazon EC2			

CW = CloudWatch. ARN = nom de la ressource Amazon. * = caractère générique (n'importe lequel).			
Déclaration de stratégie	Effet	Actions	Description et ressource (ARN)
Accès aux secrets de Trend Cloud One	Autorisation	GetSecretValue	Permet EC2 à Amazon d'accéder aux secrets pour la migration vers Trend Cloud One : <pre>aws:secretsmanager :***:secret:/ams/eps/ cloud-one-agent-tenant- id* , arn:aws:secretsman ager:***:secret:/ams/ eps/cloud-one-agent- activation-token* , aws:secretsmanager :***:secret:/ams/eps/ cloud-one-agent-tenant- id* , aws:secretsmanager :***:secret:/ams/eps/ cloud-one-agent-tenant- guid*</pre>
AWS Key Management Service sur Amazon EC2			

CW = CloudWatch. ARN = nom de la ressource Amazon. * = caractère générique (n'importe lequel).

Déclaration de stratégie	Effet	Actions	Description et ressource (ARN)
Clé de déchiffrement Trend Cloud One	Autorisation	Decrypt	Autoriser Amazon EC2 à déchiffrer la AWS KMS clé avec le nom d'alias/-migration ams/eps/cloudone arn:aws:kms:*:*:alias/ams/eps/cloudone-migration

Si vous ne connaissez pas les politiques Amazon IAM, consultez la section [Présentation des politiques IAM](#) pour obtenir des informations importantes.

Note

Les politiques incluent souvent plusieurs instructions, chaque instruction octroyant des autorisations à un ensemble différent de ressources ou octroyant des autorisations dans des conditions spécifiques.

Alertes issues de la surveillance de base dans AMS

En savoir plus sur les paramètres de surveillance par défaut d'AMS. Pour de plus amples informations, veuillez consulter [Surveillance et gestion des événements dans AMS](#).

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'une RFC Management | Other | Other | Update (ct-0xdawir96cy7k) après avoir déterminé les modifications souhaitées et vous être abonné à la rubrique Amazon SNS correspondante. CloudWatch Pour plus d'informations sur la création et l'abonnement à des sujets, voir [S'abonner à un sujet](#). Pour obtenir des informations générales, consultez [Amazon SNS FAQs](#). Pour être averti directement lorsque les alarmes dépassent leur seuil, en plus du processus d'alerte standard d'AMS, suivez ces instructions sur la façon de remplacer les configurations d'alarme.

[Réception d'alertes générées par AMS](#)

Amazon CloudWatch assure une rétention prolongée des métriques. Pour plus d'informations, consultez [Limites CloudWatch](#).

Note

AMS étalonne 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 met régulièrement à jour la surveillance de base des comptes existants et il se peut que vous subissiez un certain décalage avant que les mises à jour ne soient mises en place. Pour de plus amples informations, veuillez consulter [Affichage de la configuration de surveillance pour un compte AMS](#).

Note

L'alerte d' EC2 instance Non-root volume usage est DÉSACTIVÉE par défaut. [Si vous avez besoin de générer une alerte basée sur cette alarme, vous devez l'activer à l'aide du type de modification RFC ct-0erload6uyvvg](#)

Alertes issues de la surveillance de base

Service	Alerte de sécurité	Nom de l'alerte et condition de déclenchement	Remarques

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, ces alertes peuvent être envoyées directement à votre adresse e-mail (si vous avez souscrit à la rubrique Direct-Customer-Alerts SNS).

Instance d'Application Load Balancer (ALB)	Non	RejectedConnectionCount somme > 0 pendant 1 min, 5 fois de suite.	CloudWatch alarme si le nombre de connexions rejetées parce que l'équilibreur de charge a atteint son maximum.

Service	Alerte de sécurité	Nom de l'alerte et condition de déclenchement	Remarques
Application Load Balancer (ALB) cible	Non	TargetConnectionErrorCount somme > 0 pendant 1 min, 5 fois de suite.	CloudWatch alarme si le nombre de connexions a été établi sans succès entre l'équilibreur de charge et les instances enregistrées.
EC2 Instance Amazon — Windows	Non	SecureChannelFailure > 0,0 pour 10 des 15 derniers points de données.	CloudWatch alarme sur les instances Windows pour avertir en cas d'échec de la connexion Secure a Channel.
Instance Aurora	Non	CPUUtilization > 85 % pendant 5 minutes, 2 fois de suite.	CloudWatch alarme.
AWS Backup	Oui	DeleteRecoveryPoint Un principal de rôle IAM ou un utilisateur principal IAM inattendu a supprimé un point de AWS Backup récupération.	CloudWatch événement. Émis lorsqu'un point de restauration de sauvegarde est supprimé.
AWS Outposts	Oui	AMSOupostsInstanceFamilyCapacityAvailability InstanceFamilyCapacityAvailability = 80 % pendant 5 minutes, 12 fois consécutives.	CloudWatch alarme sur la capacité de la famille d'instances, la disponibilité de la AWS Outposts ressource.

Service	Alerte de sécurité	Nom de l'alerte et condition de déclenchement	Remarques
EC2 instance - tout OSs	Non	AMSOupostsInstanceTypeCapacityAvailability TypeCapacityAvailability = 80 % pendant 5 minutes, 12 fois consécutives.	CloudWatch alarme sur le type d'instance (capacité, disponibilité de la AWS Outposts ressource).
		AMSOupostsConnectedStatusC onnectedStatus < 1 pendant 5 minutes, 1 fois de suite.	CloudWatch alarme lors AWS Outposts de la connexion au lien de service, moins d'un compte est altéré.
		AMSOupostsCapacityExceptio nCapacityExceptions 0 pendant 5 minutes, 1 fois de suite.	CloudWatch alarme en cas d'erreur de capacité insuffisante (par exemple, lancement d'une ressource AWS Outposts) .
	Non	CPUUtilization* >= 95 % pendant 5 minutes, 6 fois de suite.	CloudWatch alarme. L'utilisa tion élevée du processeur est un indicateur d'un changement d'état de l'application, tel qu'un blocage, des boucles infinies, des attaques malveillantes et d'autres anomalies.
		StatusCheckFailed > 0 pendant 5 minutes, 3 fois de suite.	CloudWatch alarme.

Service	Alerte de sécurité	Nom de l'alerte et condition de déclenchement	Remarques
		Utilisation du volume racine ≥ 95 % pendant 5 minutes, 6 fois de suite.	
		Utilisation d'un volume autre que le volume root > 85 % pendant 5 minutes, 2 fois de suite. Désactivé par défaut ; pour plus d'informations, consultez https://docs.aws.amazon.com/manage-dservices/latest/ctref/management-monitoring-cloudwatch-enable-non-root-volumes-monitoring.html#management-monitoring-cloud-watch-enable-non-root-volumes-monitoring-info.	
		Sans mémoire* MemoryFree < 5 % pendant 5 minutes, 6 fois de suite.	
	Oui	Logiciel malveillant EPS Un logiciel malveillant a été détecté sur l'instance.	CloudWatch événement.

Service	Alerte de sécurité	Nom de l'alerte et condition de déclenchement	Remarques
EC2 Instance Amazon - Linux	Non	Utilisation de l'inode du volume racine	CloudWatch alarme. Appliqué aux instances Linux uniquement.
		Moyenne ≥ 95 % pendant 5 minutes, 6 fois de suite.	
		Swap gratuit*	
ElastiCache Cluster	Non	Échange de mémoire < 5 % pendant 5 minutes, 6 fois de suite.	Cette alarme indique à AMS la limite de connexion maximale d'un ElastiCache hôte. CloudWatch Alarme. Si vous souhaitez mettre à jour ce seuil, contactez le support AMS.
		CurrConnections = 65000	

Service	Alerte de sécurité	Nom de l'alerte et condition de déclenchement	Remarques
ElastiCache Nœud	Non	CPUUtilization Moyenne > valeur prédéfinie pendant 15 minutes, 2 fois consécutives.	CloudWatch alarme. La valeur par défaut est 90. Si vous utilisez Redis, utilisez l'une des valeurs suivantes en fonction du type d'instance : • cache.t1.micro : 90 % • cache.m1.small : 90 % • cache.m1.medium : 90 % • cache.m1.large : 45 % • cache.m1.xlarge : 22,5 % • cache.m2.xlarge : 45 % • cache.m2.4xlarge : 11,25 % • cache.c1.xlarge : 11,25 % • cache.t2.micro : 90 % • cache.t2.small : 90 % • cache.t2.medium : 45 % • cache.m3.medium : 90 % • cache.m3.large : 45 % • cache.m3.xlarge : 22,5 % • cache.m3.2xlarge : 11,25 % • cache.r3.large : 45 % • cache.r3.xlarge : 22,5 % • cache.r3.2xlarge : 11,25 % • cache.r3.4xlarge : 5,625 % • cache.r3.8xlarge : 2,8125 %

Service	Alerte de sécurité	Nom de l'alerte et condition de déclenchement	Remarques
Elasticache Nœud - memcached	Non	SwapUsage maximum > 50 000 000 octets pendant 5 minutes, 5 fois de suite.	CloudWatch alarme. Appliqué à Memcached uniquement.
OpenSearch grappe	Non	ClusterStatus.rouge le maximum est >= 1 pendant 1 minute, 1 fois consécutive. AMS prend des mesures proactives pour réduire l'impact opérationnel lorsque cette alerte est déclenchée.	CloudWatch alarme. Au moins une partition principale et ses répliques ne sont pas allouées à un nœud. Pour en savoir plus, consultez la section État du cluster rouge .
OpenSearch domaine	Non	KMSKeyErreur >= 1 pendant 1 minute, 1 fois de suite.	CloudWatch alarme. La clé de chiffrement KMS qui est 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 Chiffrement des données au repos pour le OpenSearch service Service .
		ClusterStatus.jaune le maximum est >= 1 pendant 1 minute, 1 fois consécutive AMS prend des mesures proactives pour réduire l'impact opérationnel lorsque cette alerte est déclenchée.	Au moins une partition de réplique n'est pas allouée à un nœud. Pour en savoir plus, consultez la section État du cluster jaune .

Service	Alerte de sécurité	Nom de l'alerte et condition de déclenchement	Remarques
		FreeStorageSpace le minimum est ≤ 20480 pendant 1 minute, 1 fois consécutive AMS prend des mesures proactives pour réduire l'impact opérationnel lorsque cette alerte est déclenchée.	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.
		ClusterIndexWritesBlocked ≥ 1 pendant 5 minutes, 1 fois consécutive AMS prend des mesures proactives pour réduire l'impact opérationnel lorsque cette alerte est déclenchée.	Le cluster bloque les demandes d'écriture. Pour en savoir plus, consultez ClusterBlockException.
		Nœuds le minimum est $< x$ pendant 1 jour, 1 fois consécutive AMS prend des mesures proactives pour réduire l'impact opérationnel lorsque cette alerte est déclenchée.	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.
		CPUUtilization la moyenne est supérieure ou égale à 80 % pendant 15 minutes, 3 fois de suite AMS prend des mesures proactives pour réduire l'impact opérationnel lorsque cette alerte est déclenchée.	L'utilisation du processeur à 100 % est courante, mais le maintien de moyennes élevées pose problème. Envisagez d'utiliser des types d'instances plus grands ou d'ajouter des instances.

Service	Alerte de sécurité	Nom de l'alerte et condition de déclenchement	Remarques
		JVMMemoryPression le maximum est ≥ 80 % pendant 5 minutes, 3 fois consécutives AMS prend des mesures proactives pour réduire l'impact opérationnel lorsque cette alerte est déclenchée.	Le cluster peut rencontrer des erreurs de mémoire insuffisante si l'utilisation augmente. Envisagez une mise à l'échelle verticale. Amazon ES utilise la moitié de la RAM d'une instance pour la pile Java, pour une taille maximale 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.
		Maître CPUUtilization la moyenne est supérieure ou égale à 50 % pendant 15 minutes, 3 fois de suite AMS prend des mesures proactives pour réduire l'impact opérationnel lorsque cette alerte est déclenchée.	Envisagez d'utiliser des types d'instances plus grands pour vos nœuds maîtres dédiés. En raison de leur rôle dans la stabilité des clusters et blue/green les déploiements, les nœuds maîtres dédiés devraient avoir une utilisation moyenne du processeur inférieure à celle des nœuds de données.

Service	Alerte de sécurité	Nom de l'alerte et condition de déclenchement	Remarques
		JVMMemoryPression principale le maximum est ≥ 80 % pendant 15 minutes, 1 fois consécutive AMS prend des mesures proactives pour réduire l'impact opérationnel lorsque cette alerte est déclenchée.	Envisagez d'utiliser des types d'instances plus grands pour vos nœuds maîtres dédiés. En raison de leur rôle dans la stabilité des clusters et blue/green les déploiements, les nœuds maîtres dédiés devraient avoir une utilisation moyenne du processeur inférieure à celle des nœuds de données.
OpenSearch instance	Non	AutomatedSnapshotFailure le maximum est ≥ 1 pendant 1 minute, 1 fois consécutive.	CloudWatch alarme. Un instantané automatique a échoué. Cette défaillance est souvent le résultat d'un état de santé de cluster rouge. Voir État du cluster rouge.
		SurgeQueueLength > 100 pendant 1 minute, 15 fois de suite.	CloudWatch alarme si un nombre excessif de demandes sont en attente de routage.
Instance d'Elastic Load Balancing	Non	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.
		SpilloverCount > 1 pendant 1 minute, 15 fois de suite.	CloudWatch alarme si un nombre excessif de demandes ont été rejetées parce que la file d'attente est pleine.

Service	Alerte de sécurité	Nom de l'alerte et condition de déclenchement	Remarques
GuardDuty service	Oui	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.	La liste des types de GuardDuty recherche pris en charge se trouve sur les types de recherche GuardDuty actifs .
Santé	Varie	AWS Health Dashboard	Des notifications sont envoyées en cas de modification du statut des événements AWS Health Dashboard (AWS Health) par rapport aux services de base pris en charge par AMS. Pour plus d'informations, consultez la section Services pris en charge .
AWS Managed Microsoft AD	Non	État d'Active Directory AWS Managed Microsoft AD l'instance envoie un événement de statut actif.	Événement de service. Émis lorsque le répertoire fonctionne normalement après un événement.
		État du répertoire altéré AWS Managed Microsoft AD l'instance envoie un événement d'état de répertoire altéré.	Événement de service. Émis lorsque le répertoire s'exécute dans un état dégradé. Un ou plusieurs problèmes ont été détectés. Il se peut que toutes les opérations liées à l'annuaire ne puissent pas être totalement opérationnelles.

Service	Alerte de sécurité	Nom de l'alerte et condition de déclenchement	Remarques
		État du répertoire inutilisable AWS Managed Microsoft AD l'instance envoie un événement d'état inopérable.	Événement de service. Émis lorsque le répertoire n'est pas fonctionnel. Tous les points de terminaison de l'annuaire ont signalé des problèmes.
		Suppression de l'état du répertoire AWS Managed Microsoft AD l'instance envoie un événement d'état de suppression du répertoire.	Événement de service. Émis lorsque le répertoire est en cours de suppression.
		État du répertoire défaillant AWS Managed Microsoft AD l'instance envoie un événement d'état d'échec.	Événement de service. Émis lorsque le répertoire n'a pas pu être créé.
		RestoreFailed État du répertoire AWS Managed Microsoft AD l'instance envoie un événement d'état du répertoire ayant échoué lors de la restauration.	Événement de service. Émis lors de l'échec de la restauration du répertoire à partir d'un instantané.
Instance Amazon RDS	Non	L'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.

Service	Alerte de sécurité	Nom de l'alerte et condition de déclenchement	Remarques
		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.	Événement de service. RDS-EVENT-0031, catégories d'événements et messages d'événements Amazon RDS.
		Le basculement 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.	Événement de service. RDS-EVENT-0034, catégories d'événements et messages d'événements Amazon RDS.
		Paramètres d'instance de base de données non valides Par exemple, MySQL n'a pas pu démarrer car un paramètre lié à la mémoire est défini trop haut pour cette classe d'instance. L'action du client serait donc de modifier le paramètre de mémoire et de redémarrer l'instance de base de données.	Événement de service. RDS-EVENT-0035, catégories d'événements et messages d'événements Amazon RDS.

Service	Alerte de sécurité	Nom de l'alerte et condition de déclenchement	Remarques
		Instance de IDs base de données de sous-réseau non valide L'instance de base de données se trouve sur un réseau non compatible. Certains sous-réseaux spécifiés ne sont pas valides ou n'existent pas.	Événement de service. RDS-EVENT-0036, catégories d'événements et messages d'événements Amazon RDS.
		Erreur de lecture de la réplique par l'instance de base Une erreur s'est produite lors du processus de réplication en lecture. Pour plus d'informations, consultez le message de l'événement. 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.	Événement de service. RDS-EVENT-0045, catégories d'événements et messages d'événements Amazon RDS.
		Fin de la réplication en lecture de l'instance de base La réplication sur le Read Replica est terminée.	Événement de service. RDS-EVENT-0057, catégories d'événements et messages d'événements Amazon RDS.

Service	Alerte de sécurité	Nom de l'alerte et condition de déclenchement	Remarques
		Erreur lors de la création du compte utilisateur statspack 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, catégories d'événements et messages d'événements 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 récupération autre que FULL. Le modèle de restauration est redevenu FULL et la restauration par mise en miroir a été lancée. (<dbname>: <recovery model found>[,...]).	Événement de service. RDS-EVENT-0066, catégories d'événements et messages d'événements 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.

Service	Alerte de sécurité	Nom de l'alerte et condition de déclenchement	Remarques
		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, catégories d'événements et messages d'événements 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.
		Alerte de faible capacité de stockage lorsque l'instance de base de données a consommé plus de 90 % du stockage alloué	RDS-EVENT-0089, consultez les informations détaillées sur Catégories d'événements et messages d'événements Amazon RDS.
		Service de notification en cas d'échec du dimensionnement pour le cluster de base de données Aurora Serverless.	RDS-EVENT-0143, consultez les informations détaillées sur Catégories d'événements et messages d'événements Amazon RDS.

Service	Alerte de sécurité	Nom de l'alerte et condition de déclenchement	Remarques
		L'instance de base de données est à un état non valide. Aucune action n'est nécessaire. La scalabilité automatique tentera plus tard.	RDS-EVENT-0219, consultez les informations détaillées sur les catégories d'événements et les messages d' événements 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 .
		Cet événement indique que le dimensionnement automatique du stockage de l'instance RDS n'est pas en mesure d'être redimensionné. Plusieurs raisons peuvent expliquer l'échec du dimensionnement automatique.	RDS-EVENT-0223, consultez les informations détaillées sur Catégories d'événements et messages d' événements Amazon RDS .
		La scalabilité automatique du stockage a déclenché une tâche de mise à 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 .
		L'instance de base de données comporte un type de stockage qui est actuellement indisponible dans la zone de disponibilité. La scalabilité automatique tentera plus tard.	RDS-EVENT-0237, consultez les informations détaillées sur Catégories d'événements et messages d' événements Amazon RDS .

Service	Alerte de sécurité	Nom de l'alerte et condition de déclenchement	Remarques
		RDS n'a pas pu allouer la 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 .
		L'espace de stockage de votre 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 .
		CPUUtilization Utilisation moyenne du processeur > 90 % pendant 15 minutes, 2 fois de suite.	CloudWatch alarme.
		DiskQueueDepth La somme est > 75 pendant 1 minute, 15 fois consécutives.	
		FreeStorageSpace Moyenne < 1 073 741 824 octets pendant 5 minutes, 2 fois de suite.	
		SwapUsage Moyenne >= 104 857 600 octets pendant 5 minutes, 2 fois consécutives.	

Service	Alerte de sécurité	Nom de l'alerte et condition de déclenchement	Remarques
Cluster Amazon Redshift	Non	RedshiftClusterStatus L'état du cluster lorsqu'il n'est pas en mode maintenance est inférieur à 1 pendant 5 minutes.	1 représente un cluster sain.
Amazon Macie	Oui	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 Macie pris en charge, consultez la section Analyse des résultats d'Amazon Macie . Notez que Macie n'est pas activé pour tous les comptes.

AMS prend des mesures proactives (dimensionnement du cluster) lorsque cette alerte est déclenchée.

Pour plus d'informations sur les mesures correctives, voir [Correction automatique des alertes par AMS](#).

[Regardez la vidéo d'Andrew pour en savoir plus \(7:03\)](#)

Valeurs par défaut de conservation et de rotation des journaux

Cette section décrit les paramètres par défaut de gestion des journaux AMS ; pour plus d'informations, voir [Gestion des journaux](#).

- Rotation = rotation du journal au sein des instances
- Conservation = Durée pendant laquelle nous conservons les journaux dans Amazon CloudWatch Logs et Amazon Simple Storage Service (S3)

Les journaux sont conservés dans CloudWatch Logs selon les besoins (vous pouvez le configurer) et dans S3. Ils n'expirent pas et ne sont pas supprimés et sont soumis à la durée de vie du service. Pour obtenir des informations détaillées sur la durabilité de S3, consultez la section [Protection des données dans Amazon S3](#).

Vous pouvez demander une modification de la conservation des journaux pour tous les journaux, à l'exception AWS CloudTrail des journaux, qui sont conservés indéfiniment pour des raisons d'audit et de sécurité.

La rotation des journaux est configurée au sein des instances. Par défaut, les journaux du système d'exploitation et de sécurité changent toutes les heures s'ils atteignent plus de 100 Mo, afin de garantir que vous ne manquiez pas de disque dans les instances.

L'agent de journalisation installé dans les instances télécharge le journal en ligne dans CloudWatch Logs, puis les journaux sont archivés dans S3.

Les journaux sont stockés dans CloudWatch Logs et S3 au format brut dans lequel ils sont générés, il n'y a aucun prétraitement.

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 Advanced 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 existants RFCs, 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 :
 - Demandes de modification : découvrez combien RFCs attendent votre réponse et passez à la page de liste des RFC avec ce filtre actif. Découvrez combien RFCs sont en attente de votre approbation et passez à la page de liste des RFC avec ce filtre actif. Vérifiez combien RFCs sont ouverts et passez à la page de liste des RFC avec ce filtre actif. Ouvrez la page de liste en RFCs cliquant sur le lien Afficher tout.
 - Incidents : découvrez combien de cas d'incidents attendent votre réponse et passez à la page de liste des incidents avec ce filtre actif. Vérifiez combien sont ouverts, puis passez à la page de liste des incidents avec ce filtre actif. Ouvrez la page de liste des incidents en cliquant sur le lien Afficher tout.
 - Demandes de service : découvrez combien de demandes de service attendent votre réponse et passez à la page de liste des demandes de service avec ce filtre actif. Vérifiez combien sont ouvertes, puis passez à la page de liste des demandes de service avec ce filtre actif. Ouvrez la page de liste des demandes de service en cliquant sur le lien Afficher tout.
 - Mise à jour récente RFCs : date, lien vers les détails de la RFC et statut
 - Incidents et demandes de service récemment créés : date, lien vers les détails du dossier et type (incident ou demande de service)
- RFCs: Ouvre une liste des éléments existants RFCs pour le compte
- Incidents : ouvre une liste des incidents ouverts pour le compte
- Demandes de service : ouvre une liste des demandes de service ouvertes pour le compte
- Rapports : ouvre la page des rapports et les rapports par défaut, Daily Backup, Daily Patch et Monthly Facturation

- Ressources:
 - VPCs: Ouvre une liste des éléments existants VPCs pour le compte
 - Piles : ouvre une liste des piles existantes pour le compte
 - AMIs: Ouvre la liste des AMS disponibles AMIs
- Présentation des fonctionnalités : informations sur les dernières mises à jour de la console
- Ressources pour les développeurs : une page de fichiers téléchargeables, y compris le SDK de gestion des modifications AMS Advanced, etc.
- Documentation : page d'accueil de la documentation d'AWS Managed Services

Utilisation de l'API et de la CLI AMS

L'API AWS Managed Services (AMS) est similaire à celle APIs des autres AWS services. Vous pouvez en savoir plus sur l'API AMS dans le manuel [AMS API Reference](#).

Points de terminaison HTTP de l'API AMS pour les appels REST

Outre les différents SDKs, AMS fournit une CLI ; vous pouvez également appeler des appels d'API REST contre le point de terminaison AMS.

Il existe deux AMS APIs (le point final pour les deux se trouve dans us-east-1) :

- Gestion des modifications : utilisez cette API pour demander l'accès à votre infrastructure ou pour y apporter des modifications, notamment en créant et en mettant à jour RFCs, en déployant de nouvelles instances, en mettant à jour et en supprimant des instances, en obtenant des informations et en créant AMIs. Le point de terminaison HTTP est :

`https://amscm.us-east-1.amazonaws.com`

- SKMS : utilisez cette API pour obtenir des informations sur votre infrastructure, notamment les piles VPCs, les sous-réseaux et. AMIs Le point de terminaison HTTP est :

`https://amsskms.us-east-1.amazonaws.com`

Installation ou mise à niveau de l'AMS CLI

La CLI AMS est un moyen facile d'interagir avec l'API AMS. Elle est utilisée dans les exemples de cette section. Pour les conventions d'utilisation des AWS CLI et AMS CLI, reportez-vous à la section [Utilisation de l'interface de ligne de commande AWS](#).

Pour plus d'informations sur l'installation de SAML, consultez [Règle de réclamation AD FS et paramètres SAML](#).

Pour installer ou mettre à niveau l'AMS CLI, suivez ces instructions :

Note

Vous devez disposer des informations d'identification d'administrateur pour cette procédure.

L'AWS CLI est une condition préalable à l'utilisation d'AWS Managed Services (AMS) CLIs (Change Management et SKMS).

1. Pour installer l'interface de ligne de commande AWS, consultez [la section Installation de l'interface de ligne de commande AWS](#) et suivez les instructions appropriées. Notez qu'au bas de cette page, vous trouverez des instructions pour utiliser différents programmes d'installation, [Linux](#), [MS Windows](#), [macOS](#), [Virtual Environment](#), [Bundled Installer \(Linux, macOS ou Unix\)](#).

Après l'installation, exécutez `aws help` pour vérifier l'installation.

2. Une fois l'interface de ligne de commande AWS installée, pour installer ou mettre à niveau l'interface de ligne de commande AMS, téléchargez le fichier zip distribuable de l'interface de ligne de commande AMS ou du SDK AMS et décompressez-le. Vous pouvez accéder aux distribuables de l'AMS CLI via le lien [Ressources du développeur](#) dans le menu de navigation gauche de la console AMS.
3. Le fichier README fournit des instructions pour toute installation.

Ouvrez soit :

- ZIP de la CLI : fournit uniquement la CLI AMS.
- ZIP du SDK : fournit tous les AMS APIs et la CLI AMS.

Pour Windows, exécutez le programme d'installation approprié (systèmes 32 ou 64 bits uniquement) :

- 32 bits : ManagedCloudAPI_x86.msi
- 64 bits : ManagedCloudAPI_x64.msi

Pour Mac/Linux, exécutez le fichier nommé : AWSManagedServices_InstallCLI.sh en exécutant cette commande : `sh AWSManagedServices_InstallCLI.sh` Notez que les répertoires `amscm` et `amsskms` ainsi que leur contenu doivent se trouver dans le même répertoire que le fichier `.sh`. `AWSManagedServices_InstallCLI`

4. Si les informations d'identification de votre entreprise sont utilisées par le biais de la fédération avec AWS (configuration par défaut d'AMS), vous devez installer un outil de gestion des informations d'identification qui peut accéder à votre service de fédération. Par exemple, vous pouvez utiliser ce blog de sécurité AWS consacré à la [mise en œuvre d'un accès fédéré aux API et CLI à l'aide de SAML 2.0 et d'AD FS](#) pour vous aider à configurer vos outils de gestion des informations d'identification.
5. Après l'installation, lancez `aws amscm help` et consultez `aws amsskms help` les commandes et les options.

 Note

L'AMS CLI doit être installée pour que ces commandes fonctionnent. Pour installer l'API ou la CLI AMS, rendez-vous sur la page Ressources pour développeurs de la console AMS. Pour des informations de référence sur l'API AMS CM ou l'API AMS SKMS, consultez la section Ressources d'information AMS du guide de l'utilisateur. Vous devrez peut-être ajouter une `--profile` option d'authentification ; par exemple, `aws amsskms ams-cli-command --profile SAML`. Vous devrez peut-être également ajouter `--region` cette option car toutes les commandes AMS sont exécutées à partir de `us-east-1`, par exemple. `aws amscm ams-cli-command --region=us-east-1`

Utilisation de l'API AMS en CLI, Ruby, Python et Java

Vous trouverez ci-dessous une liste d'extraits de code pour le `ListChangeTypeClassificationSummaries` fonctionnement de l'API AMS, dans toutes les langues disponibles.

Pour Python, Ruby et Java SDKs, consultez [Outils pour Amazon Web Services](#) et faites défiler la page jusqu'à la SDKs section. Chaque programme d'installation du SDK contient un fichier README avec des extraits de code supplémentaires.

Exemple d'API AMS vers CLI

Après avoir installé l'AMS CLI (nécessite l'interface de ligne de commande AWS ; voir [Installation ou mise à niveau de l'AMS CLI](#)), vous pouvez exécuter n'importe quelle opération d'API AMS en réformant l'appel en spécifiant d'abord quelle API AMS, `aws amscm` ou `aws amsskms`, puis en exécutant l'action avec des tirets remplaçant Camel Case. Enfin, fournissez des informations d'identification, telles que SAML.

Pour en savoir plus, consultez la section [Utilisation de l'interface de ligne de commande AWS](#).

Exemple :

- API : `'ChangeTypeClassificationSummaries[].[Category,Subcategory,Item,Operation,ChangeTypeId]'`
- CLI : `amscm list-change-type-classification-summaries --query "ChangeTypeClassificationSummaries[*].[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table`

Note

Si vous vous authentifiez avec SAML, ajoutez-le `aws --profile saml` au début de la commande. Par exemple,

```
aws --profile saml amscm list-change-type-classification-summaries --query "ChangeTypeClassificationSummaries[*].[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```


Exemple d'API AMS pour Python

Pour utiliser l'API AMS avec Python, installez l'AMS CLI et installez boto3. Procédez comme suit :

1. Installez l'AMS CLI. Consultez [Installation ou mise à niveau de l'AMS CLI](#).
2. Installez boto3, le AWS SDK pour Python. Pour plus d'informations, consultez cet article de blog [Now Available — AWS SDK for Python \(Boto3\)](#).

```
import boto3
```

3. Téléchargez le client AMS Change Management :

```
cm = boto3.client('amscm')
```

4. Obtenez l'AMS CTs :

```
cts = cm.list_change_type_classification_summaries()  
  
print(cts)
```

Exemples Python

Voici quelques exemples d'utilisation de Python dans AMS, pour créer des EC2 instances, and/or utilisez Lambda.

Exemple en Python pour créer un EC2

Cet exemple montre comment utiliser l' RESTFul API amscm depuis le code Python pour archiver et exécuter des processus RFC.

1. Installez la CLI AMS à un endroit auquel vous avez accès ; vous avez besoin des fichiers qu'elle fournit.
2. Appelez les bibliothèques Python et créez l' EC2 instance :

```
import boto3  
import json  
import time  
  
# Create the amscm client  
cm = boto3.client('amscm')
```

```
# Define the execution parameters for EC2 Create
AMSExecParams = {
    "Description": "EC2-Create",
    "VpcId": "VPC_ID",
    "Name": "My-EC2",
    "TimeoutInMinutes": 60,
    "Parameters": {
        "InstanceAmiId": "INSTANCE_ID",
        "InstanceSubnetId": "SUBNET_ID"
    }
}

# Create the AMS RFC
cts = cm.create_rfc(
    ChangeTypeId="ct-14027q0sjyt1h",
    ChangeTypeVersion="3.0",
    Title="Python Code RFC Create",
    ExecutionParameters=json.dumps(AMSExecParams)
)

# Extract the RFC ID from the response
NewRfcID = cts['RfcId']

# Submit the RFC
RFC_Submit_Return=cm.submit_rfc(RfcId=NewRfcID)

# Check the RFC status every 30 seconds
RFC_Status = cm.get_rfc(RfcId=NewRfcID)
RFC_Status_Code = RFC_Status['Rfc']['Status']['Name']

while RFC_Status_Code != "Success":
    if RFC_Status_Code == "PendingApproval":
        print(RFC_Status_Code)
        time.sleep(30)
    elif RFC_Status_Code == "InProgress":
        print(RFC_Status_Code)
        time.sleep(30)
    elif RFC_Status_Code == "Failure":
        print(RFC_Status_Code)
        break
    else:
        print(RFC_Status_Code)

    RFC_Status = cm.get_rfc(RfcId=NewRfcID)
```

```
RFC_Status_Code = RFC_Status['Rfc']['Status']['Name']
```

Exemple de Python avec Lambda

Cet exemple montre comment intégrer les modèles AMS à votre code afin de pouvoir l'utiliser avec Lambda, ou EC2 dans des endroits que vous ne voulez pas ou ne pouvez pas installer. `amsccli`

Note

AMS ne fournit pas de SDK Python importable spécifique à AMS. Le script `amsccli` d'installation installe les modèles de données de service AMS dans le chemin normal de l'interface de ligne de commande. Pour l'utilisation de la CLI et du système Python, c'est très bien, car `awscli` les deux `boto3` lisent leurs modèles de service à partir des mêmes emplacements par défaut (`~/ .aws/models`). Cependant, lorsque vous souhaitez utiliser les services AMS via `boto3` dans Lambda (ou dans tout autre environnement d'exécution non local), cela se bloque car vous ne disposez plus des modèles de données. Voici une méthode pour résoudre ce problème en empaquetant les modèles de données avec la fonction.

Vous pouvez suivre des étapes simples pour exécuter votre code Python intégré à AMS dans Lambda ou dans un autre environnement d'exécution tel que EC2 Fargate, etc. Le flux de travail suivant montre les étapes nécessaires pour les fonctions Lambda intégrées à AMS.

En ajoutant les modèles de données au package de déploiement du code et en mettant à jour le chemin de recherche du SDK, vous pouvez simuler une expérience du SDK.

Important

Cet exemple et toutes les commandes autres que Python présentées ont été testés sur un ordinateur Mac.

Exemple de flux de travail :

1. Installez la `amsccli`. Cela crée un dossier `~/ .aws/models` sur votre ordinateur (Mac).
2. Copiez les modèles dans un répertoire local : `cp ~/ .aws/models ./models`.

3. Incluez les modèles dans le package de déploiement de votre code.
4. Mettez à jour votre code de fonction pour ajouter les nouveaux modèles au chemin du SDK. Notez que ce code doit être exécuté avant que boto3 ou botocore ne soient importés !

```
# Force Python to search local directory for boto3 data models
import os
os.environ['AWS_DATA_PATH'] = './models'

import boto3
import botocore
```

Note

Comme les modèles d'exemple se trouvent dans un répertoire nommé `models`, nous les ajoutons `./models` à `AWS_DATA_PATH`. Si le répertoire était nommé `/ams/boto3models`, nous ajouterions le code suivant :

```
import os
os.environ['AWS_DATA_PATH'] = './ams/boto3models'

import boto3
import botocore
```

Votre code devrait réussir à trouver les modèles AMS. Pour un exemple plus précis concernant l'emballage, voici le flux de travail spécifique à Lambda.

Exemple de flux de travail AMS Lambda :

Ces étapes appliquent l'exemple générique précédent à la création d'une fonction AWS Lambda.

1. Installez l'amscli. Cela crée un dossier `~/ .aws/models` sur votre ordinateur (Mac).
2. Copiez les modèles dans un répertoire local :

```
cp ~/.aws/models ./models
```

3. Ajoutez les modèles au fichier zip de déploiement de votre fonction :

```
zip -r9 function.zip ./models
```

 Important

Mettez à jour votre code de fonction pour ajouter les nouveaux modèles au chemin du SDK. Notez que ce code doit être exécuté avant que boto3 ou botocore ne soient importés !

```
# Force Python to search local directory for boto3 data models
import os
os.environ['AWS_DATA_PATH'] = './models'

import boto3
import botocore
```

 Note

Comme les modèles d'exemple se trouvent dans un répertoire nommé `models`, nous les ajoutons `./models` à `AWS_DATA_PATH`. Si le répertoire était nommé `/ams/boto3models`, nous ajouterions le code suivant :

```
import os
os.environ['AWS_DATA_PATH'] = './ams/boto3models'

import boto3
import botocore
```

Maintenant, déployez votre fonction :

1. Ajoutez votre code de fonction au fichier zip de déploiement (si ce n'est pas déjà fait) :

```
zip -g function.zip lambda-amscm-test.py
```

2. Créez ou mettez à jour votre fonction avec le fichier zip que vous avez créé (console ou CLI) :

```
aws lambda update-function-code --function-name lambda-amscm-test --zip-file fileb://function.zip --region us-east-1
```

Votre Lambda Python intégré à AMS devrait maintenant fonctionner.

 Note

Votre fonction doit disposer d'autorisations IAM pour, amscm sinon vous recevrez une erreur d'autorisation.

Exemple de code de fonction Lambda pour tester amscm (contenu du fichier .py) : lambda-amscm-test

```
import json

# Force lambda to search local directory for boto3 data models
import os
os.environ['AWS_DATA_PATH'] = './models'

import boto3
import botocore

def lambda_handler(event, context):
    use_session = boto3.session.Session(region_name="us-east-1")
    try:
        cm = use_session.client("amscm")
        cts = cm.list_change_type_categories()
        print(cts)
    except botocore.exceptions.UnknownServiceError:
        print("amscm not found")

    return {
        'statusCode': 200,
        'body': json.dumps('Hello from Lambda!')
    }
```

Résultats du test (succès) :

Réponse de la fonction :

```
{
  "statusCode": 200,
  "body": "\"Hello from Lambda!\""
}
```

```
Request ID:  
"1cea13c0-ed46-43b1-b102-a8ea28529c27"
```

Journaux de fonctions :

```
START RequestId: 1cea13c0-ed46-43b1-b102-a8ea28529c27 Version: $LATEST  
{'ChangeTypeCategories': ['Deployment', 'Internal Infrastructure Management',  
  'Management'], 'ResponseMetadata': {'RequestId': 'e27276a0-e081-408d-  
bcc2-10cf0aa19ece', 'HTTPStatusCode': 200, 'HTTPHeaders': {'x-amzn-requestid':  
  'e27276a0-e081-408d-bcc2-10cf0aa19ece', 'content-type': 'application/x-amz-json-1.1',  
  'content-length': '89', 'date': 'Sun, 10 May 2020 23:21:19 GMT'}, 'RetryAttempts': 0}}  
END RequestId: 1cea13c0-ed46-43b1-b102-a8ea28529c27
```

Exemple d'API AMS pour Ruby

Pour utiliser l'API AMS avec Ruby, installez le SDK AWS Ruby et la CLI AMS. Procédez comme suit :

1. Installez l'AMS CLI. Consultez [Installation ou mise à niveau de l'AMS CLI](#).
2. Installez le SDK AWS Ruby. Consultez la section [Outils pour Amazon Web Services](#).
3. Configurez Ruby avec les commandes suivantes :

```
require 'aws-sdk'  
  
config = {  
  region: 'us-east-1',  
  credentials: Aws::Credentials.new('ACCESS_KEY', 'SECRET_KEY')}
```

4. Obtenez l'AMS CTs :

```
ams_cm = Aws::amscm::Client.new(config)  
  
cts = ams_cm.list_change_type_classification_summaries  
  
print(cts)
```

Exemple d'API AMS vers Java

Pour utiliser l'API AMS avec Java, installez le SDK AWS Java et la CLI AMS. Procédez comme suit :

1. Installez l'AMS CLI. Consultez [Installation ou mise à niveau de l'AMS CLI](#).

2. Installez le SDK AWS Java. Consultez la section [Outils pour Amazon Web Services](#).
3. Configurez Java à l'aide des commandes suivantes :

```
import com.amazonaws.auth.BasicAWSCredentials;

import com.amazonaws.services.amscm.model.AWSManagedServicesCMClient;

import
com.amazonaws.services.amscm.model.ListChangeTypeClassificationSummariesRequest;

import
com.amazonaws.services.amscm.model.ListChangeTypeClassificationSummariesResult;

public static void getChangeTypeClassificationSummaries() {
```

4. Définissez les informations d'identification. Nous vous recommandons de ne pas le coder en dur.

```
final BasicAWSCredentials awsCredsCm =

    new BasicAWSCredentials("ACCESS_KEY", "SECRET_KEY");
```

5. Créez le client AMS Change Management :

```
final AWSManagedServicesCMClient cmClient =

    new AWSManagedServicesCMClient(awsCredsCm);
```

6. Obtenez l'AMS CTs :

```
final ListChangeTypeClassificationSummariesRequest listCtsRequest = new
ListChangeTypeClassification SummariesRequest();

final ListChangeTypeClassificationSummariesResult listCtsResult =

cmClient.listChangeTypeClassificationSummaries(listCtsRequest);

System.out.println("List of CTs");

listCtsResult.getChangeTypeClassificationSummaries().stream()

.map(x -> x.getCategory() + "/" + x.getSubcategory() + "/" +
x.getItem() + "/" + x.getOperation())

.forEach(System.out::println);
```


}

AMS : apportez votre propre EPS

Utilisez la fonction « Bring your own end point security » (BYOEPS) d'AMS pour remplacer l'agent Trend Micro Deep Security par votre propre solution de sécurité des terminaux, ou par une licence Trend Micro. Si vous possédez déjà des licences rentables pour des produits autres que Trend Micro Deep Security, ou si vous disposez d'une équipe qui fournit votre EPS, ou si vous souhaitez utiliser un outil EPS spécifique, utilisez BYOEPS dans vos instances.

BYOEPS fonctionne au niveau du compte. Vos instances du compte utilisent soit BYOEPS, soit l'EPS géré par AMS par défaut :

- zone de landing zone multi-comptes (MALZ) : vous désignez des comptes d'applications qui utilisent BYOEPS ou EPS géré.
- zone de landing zone à compte unique (SALZ) : vos comptes AMS utilisent le BYOEPS ou un EPS géré.

BYOEPS, réduit votre AWS facture en réduisant le coût de Trend Micro Deep Security. L'EPS continue de vous coûter cher, car l'EPS géré par AMS est toujours nécessaire pour protéger les EC2 instances créées et gérées par AMS qui sont nécessaires à la gestion des accès (bastions et hôtes de gestion). Pour calculer l'impact financier total, vous devez prendre en compte le coût des licences de votre nouvel outil et le coût de gestion de l'EPS aux niveaux de service dont vous avez besoin.

L'utilisation du BYOEPS modifie les rôles et les responsabilités de l'AMS en matière de gestion de la sécurité :

- R représente la 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 signifie informé ; une partie qui est informée des progrès, souvent uniquement une fois la tâche ou le résultat livrable terminé.

Gestion de la sécurité	Client	AWS Managed Services
Maintien de licences valides de Managed EPS pour EC2 les instances d'AMS Shared Services	R	C
Configurer Managed EPS pour EC2 les instances d'AMS Shared Services	I	R
Mettre à jour Managed EPS pour EC2 les instances d'AMS Shared Services	I	R
Surveillance des malwares sur EC2 les instances d'AMS Shared Services	I	R
Gestion et mise à jour des signatures de virus pour EC2 les instances d'AMS Shared Services	I	R
Corriger les instances infectées par des logiciels malveillants pour les EC2 instances d'AMS Shared Services	C	R

Lorsque vous utilisez BYOEPS, vous perdez l'un des contrôles de sécurité proposés par AMS. La gestion de la sécurité est toujours assurée par le biais d'outils tels qu'Amazon GuardDuty, Amazon Macie, et de contrôles de processus, tels que les révisions des configurations IAM. L'utilisation du BYOEPS n'affecte pas les certifications et attestations de conformité AMS. Cependant, de nombreux cadres de sécurité et certifications comportent des exigences en matière de protection contre les logiciels malveillants et le code malveillant. Pour garantir la sécurité et la conformité de votre compte,

évaluez les contrôles que vous planifiez pour vous assurer qu'ils répondent aux exigences de sécurité relatives aux certifications de conformité de votre charge de travail.

Activez BYOEPS pour votre compte

Le processus d'activation du BYOEPS comporte trois étapes et en utilise plusieurs. RFCs Consultez les informations suivantes pour en savoir plus sur les trois étapes requises pour activer le BYOEPS. Ensuite, coordonnez-vous avec votre CSDM pour activer BYOEPS pour votre compte.

Rubriques

- [Étape 1 : Prérequis](#)
- [Étape 2 : Activez BYOEPS dans votre compte](#)
- [Étape 3 : Migration de l'instance](#)

Étape 1 : Prérequis

- Le profil d' EC2 instance Amazon par défaut est `customer-mc-ec2-instance-profile`. Si vous utilisez un profil d' EC2 instance Amazon différent en plus du profil par défaut, autorisez l'`ssm:GetParameter` relative à la `/ams/end-point-security` ressource sur votre profil d' EC2 instance.

Si vous ne pouvez pas mettre à jour les profils d' EC2 instance, soumettez une RFC spécifiant les profils d'instance que vous devez mettre à jour.

- Comprenez l'ampleur de ce changement.

Les déploiements via un type de modification automatique (CT) AMS vous permettent de spécifier l'AMI utilisée lors de la création.

Pour utiliser BYOEPS avec des comptes utilisant le système EPS géré par AMS, vous devez travailler avec AMS pour désinstaller les agents Trend Micro de ces EC2 instances et pour mettre à jour le code AMS (par exemple, les scripts de démarrage) sur ces instances. Ces actions peuvent nécessiter un redémarrage. Il est donc recommandé de les exécuter dans le cadre d'une fenêtre de maintenance. Contactez votre CSDM pour identifier une fenêtre de maintenance pour effectuer cette activité et pour créer un plan de migration. En ce qui concerne le plan de migration, posez-vous les questions suivantes :

1. Combien d'instances devez-vous migrer ? Divisez le nombre total d'instances en lots plus petits et incrémentiels.

2. Comment allez-vous diviser les instances par lots ? Par exemple, vous pouvez diviser par groupes de ressources et créer une liste à partager avec l'équipe des opérations AMS.
 3. Combien de temps prendra chaque lot ? Combien de temps total est nécessaire ? N'oubliez pas que vous souhaitez peut-être installer votre outillage EPS préféré dans la même fenêtre de maintenance. Combien de temps cela va-t-il prendre ?
- Votre CSDM partage le plan de migration avec l'équipe des opérations AMS. Si votre parc d'instances est supérieur à 50, collaborez avec votre CSDM pour créer un événement planifié à l'aide du processus de gestion des événements planifiés (PEM). Pour de plus amples informations, consultez [Gestion des événements planifiés dans AWS Managed Services](#).

AMS Operations assure la coordination avec votre CSDM et vous conseille sur la manière de procéder RFCs à la soumission conformément à vos fenêtres de maintenance, en fonction du nombre d'instances présentes dans votre compte.

- Mettez à jour les automatisations ou les processus de lancement d' EC2 instance à l'aide de Custom ou AMIs d'AMS pour utiliser AMS AMIs publié après décembre 2020.

Étape 2 : Activez BYOEPS dans votre compte

Lorsque vous utilisez BYOEPS sur votre compte, les responsabilités d'AMS en matière de gestion de la sécurité changent. Consultez votre équipe chargée de la sécurité et de la plateforme cloud avant d'activer BYOEPS.

Pour demander BYOEPS pour votre compte, soumettez une RFC de mise à jour

« MOO » (Management | Other | Other | Update) avec ct-0xdawir96cy7k, avec les détails suivants :

Please enable BYOEPS for this account/these accounts
Account IDs: *IDs for the accounts for BYOEPS.*

AMS déploie les mises à jour du magasin de paramètres sur le compte et met à jour le profil [d'instance Amazon EC2 IAM](#).

Note

- Les comptes dotés de nouvelles instances lancées qui utilisent la dernière version d'AMS AMIs peuvent ignorer l'installation de l'agent Trend Micro. AMIs les versions antérieures à décembre 2020 ne prennent pas en charge la fonctionnalité BYOEPS. Mettez à jour les

automatisations qui utilisent les anciennes AMIs pour utiliser le dernier AMS AMIs avec le support des fonctionnalités BYOEPS.

- Pour la gestion des EC2 instances existantes, voir Étape 3 : Migrations d'instances

Étape 3 : Migration de l'instance

Utilisez l'une des options suivantes pour migrer vos instances, en fonction de votre cas d'utilisation. Si vous ne savez pas quelle option choisir, contactez votre CA ou votre CSDM.

Comptes dotés d' EC2 instances utilisant le système EPS géré par AMS

Pendant la période de maintenance, conformément à la planification de l'étape 1, les actions suivantes sont effectuées sur chaque instance devant être intégrée à BYOEPS :

- Effectué par AMS : mise à jour du code AMS (scripts de démarrage, modules, etc.) avec les dernières versions. Cela est nécessaire car les anciens scripts de démarrage AMS ne prennent pas en charge les fonctionnalités BYOEPS et réinstallent l'agent Trend Micro à chaque démarrage. Désinstallez également l'agent Trend Micro.
- Effectué par vos soins : installez et configurez votre outil EPS préféré.

Important

Trend Micro Agent fournit une protection contre les malwares. Assurez-vous d'installer une solution de remplacement appropriée pour sécuriser vos instances.

Pour que ces modifications soient soumises RFCs avec modification, tapez ct-2iz9nvw8zlhst, [Trend Micro DSM | Remove Trend Micro EPS Agent \(révision requise\), par lots](#).

Comptes sans EC2 instance utilisant le système EPS géré par AMS

Les comptes dotés de nouvelles instances lancées qui utilisent la dernière version d'AMS AMIs peuvent ignorer l'installation de l'agent Trend Micro. AMIs les versions antérieures à décembre 2020 ne prennent pas en charge la fonctionnalité BYOEPS. Mettez à jour les automatisations qui utilisent les anciennes AMIs pour utiliser le dernier AMS AMIs avec le support des fonctionnalités BYOEPS.

Ajoutez votre agent sur les EC2 instances

Vous pouvez utiliser AMS Patterns pour déployer des agents CrowdStrike ou des outils tels que Qualys, Soumettre une demande de service pour obtenir de l'assistance.

Réception de notifications AMS

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

- Une RFC créée par AMS qui nécessite votre approbation
- Un dossier AMS créé pour étudier une RFC que vous avez créée et qui a échoué
- Événements créés par les alertes de surveillance
- Notifications du service de correction qui vous informent des correctifs à venir
- Demandes de service et rapports d'incidents
- Rapports CRM mensuels
- Annonces AWS importantes occasionnelles (votre CSDM vous contacte si une action de votre part est requise)

Toutes ces notifications sont envoyées aux coordonnées par défaut (e-mail du compte root) que vous avez fournies 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.

Le service de notification AMS propose deux méthodes supplémentaires pour configurer les contacts pour les notifications :

- Marquez vos ressources avec des balises de contact (la valeur clé du tag étant les informations de contact) et fournissez le nom de la clé de balise à votre CSDM. Les alarmes relatives à ces ressources seront envoyées aux contacts indiqués dans la valeur clé, en plus du contact du compte créé lors de l'intégration. Cela est particulièrement utile pour les propriétaires d'applications. Pour de plus amples informations, veuillez consulter [Notification d'alerte basée sur des balises](#).
- (Obligatoire lors de l'intégration) Envoyez à votre CSDM des listes de contacts nommées pour les notifications non basées sur les ressources. Par exemple, vous pouvez avoir une liste nommée SecurityContacts « » et une autre nommée OperationsContacts « », etc. AMS ajoute la liste au service de notification, et les alarmes qui s'appliquent au contexte de cette liste sont envoyées à ces contacts. Cela est particulièrement utile pour les questions d'organisation.

Cette fonctionnalité avancée de routage des alertes est active pour la plupart des CloudWatch alarmes essentielles telles que la défaillance d'une EC2 instance Amazon, l'utilisation de la capacité du volume Amazon Elastic Block Store (Amazon EBS) (utilisation root), utilisation d'Amazon NonRoot EBS, utilisation élevée de la mémoire, utilisation élevée du swap et utilisation élevée du processeur pour Amazon. EC2

En outre, lorsque vous déposez une demande de service ou un rapport d'incident, vous avez la possibilité d'ajouter des « e-mails CC » (fortement recommandé) et ces adresses e-mail reçoivent des notifications concernant la demande de service ou l'incident.

Important

Alors que les adresses e-mail CC fournies dans les demandes de service et les rapports d'incidents reçoivent des notifications par e-mail concernant les communications, d'autres notifications, telles que les notifications d'application de correctifs, apparaissent dans votre liste de demandes de service (un e-mail est également envoyé au contact par défaut), sans vous informer explicitement que vous avez une communication en attente d'attention. C'est pourquoi nous vous recommandons vivement d'ajouter un e-mail CC lorsque c'est possible, et de configurer l'e-mail de contact par défaut en tant que groupe dont tous les utilisateurs d'AMS sont membres.

En outre, vous pouvez demander des notifications spéciales pour les nouvelles AMIs informations, les modifications d'état des RFC et les modifications de configuration de votre compte AMS. Ces services de notification facultatifs sont décrits ci-dessous.

Notifications AMI AMS avec SNS

AMS fournit un service de notification AMI. Vous pouvez l'utiliser pour vous abonner à une rubrique Amazon Simple Notification Service (SNS) qui vous avertit lorsque des mises à jour de l'AMI AMS ont été publiées. Vous pouvez choisir de recevoir des notifications uniquement pour les AMS que AMIs vous utilisez, ou vous pouvez vous inscrire pour recevoir des notifications de mise à jour pour tous les AMS AMIs. Pour plus d'informations sur les sujets liés aux réseaux sociaux, consultez [Qu'est-ce qu'Amazon Simple Notification Service ?](#)

Chaque fois qu' AMIs elles sont publiées, nous envoyons des notifications aux abonnés du sujet correspondant ; cette section décrit comment s'abonner aux notifications de l'AMI AMS.

Exemple de message

```
{
  "Type" : "Notification",
  "MessageId" : "example messageId",
  "TopicArn" : "arn:aws:sns:us-east-1:591688410472:customer-ams-windows2019",
  "Subject" : "New AMS AMIs are Now Available",
  "Message" : "{\"v1\": {\"Message\": \"A new version of the AMS Amazon Machine Images has
been released. You are now able to launch new EC2 stacks from these AMIs.
Please use this time to update any dependencies such as CloudFormation or Autoscaling
groups. Release Notes Windows - Contains latest Windows Patches:
Microsoft Windows Server 2008 R2 Datacenter - (KB2819745, KB3018238, KB4507004,
KB4507437) Microsoft Windows Server 2016 Datacenter Security Enhancedn - (KB4509091,
KB4507459)
Microsoft Windows Server 2016 Datacenter - (KB4509091, KB4507459) Microsoft Windows
Server 2012 R2 Security Enhancedn - (KB3191564, KB3003057, KB3013172, KB3185319,
KB4504418,
KB4506996, KB4507463) Microsoft Windows Server 2012 R2 Standardn - (KB3003057,
KB3013172, KB3185319, KB4504418, KB4506996, KB4507463) Linux - Contains latest Linux
patches -
All AMIs now force domainjoin-cli leave before domainjoin-cli join for better
stability in the domain join process.\"\", \"images\":
{\"images\": {\"image_name\": \"customer-ams-windows2019-2021.08-1\", \"image_id\":
\"ami-05dfa45396fddaa5e\"}}, \"region\": \"us-east-1\"}}\",
  \"Timestamp\" : \"2021-09-03T19:05:57.882Z\",
  \"SignatureVersion\" : \"1\",
  \"Signature\" : \"example sig\",
  \"SigningCertURL\" : \"example url\",
  \"UnsubscribeURL\" : \"example url\"
}
```

Sujets d'AMI AMS auxquels il est possible de s'abonner :

- TOUT : Utiliser `customer-ams-all-amis`. Cet abonnement à cette rubrique vous avertit lorsque l'un des AMS AMIs est mis à jour.
- AMS AWS Linux AMIs : pour Amazon Linux, utilisez `customer-ams-amazon1` et `customer-ams-amazon1-security-enhanced`. Pour Amazon Linux 2, utilisez `customer-ams-amazon2` et `customer-ams-amazon2-security-enhanced`.
- AMS SUSE Linux AMIs : utilisez `customer-ams-sles12` ou `customer-ams-sles15`.
- AMS AWS RedHat AMIs : Utilisez `customer-ams-rhel8`, `customer-ams-rhel8-security-enhanced`, `customer-ams-rhel7`, `customer-ams-rhel7-security-enhanced`.

- AMS AWS CentOS AMIs : Utilisez `customer-ams-centos7`, `customer-ams-centos7-security-enhanced`.
- AMS Ubuntu AMIs : Utilisez `customer-ams-ubuntu18`.
- AMS AWS Windows AMIs : utilisez `customer-ams-windows2019`, `customer-ams-windows2019-security-enhanced`, `customer-ams-windows2016`, `customer-ams-windows2016-security-enhanced`, `customer-ams-windows2012`, `customer-ams-windows2012r2`, `customer-ams-windows2012r2-security-enhanced`, `customer-ams-windows2022`.

Pour vous abonner aux nouvelles notifications AMI d'AMS à l'aide de la console Amazon SNS :

1. [Ouvrez la console Amazon SNS sur le tableau de bord.](#)
2. Dans le coin supérieur droit, passez à la région AWS à AMIs laquelle vous êtes abonné.
3. Dans le volet de navigation de gauche, choisissez Abonnements, puis choisissez Créer un abonnement.
4. Saisissez les informations suivantes :
 - a. ARN du sujet : `arn:aws:sns:{REGION}:287847593866:{AMS_AMI_NAME}`
où *REGION* est la région AWS sélectionnée (où la notification SNS a été créée) et *AMS_AMI_NAME* est l'AMI pour laquelle vous souhaitez recevoir des notifications.
Exemples :
 - Pour vous abonner aux notifications relatives au nouvel AMS Amazon Linux AMIs dans la région AWS us-east-1, utilisez ce Topic ARN = `arn:aws:sns:us-east-1:287847593866:customer-ams-amazon1`
 - Pour vous abonner aux notifications relatives au nouveau serveur AMS Window 2016 AMIs dans la région AWS us-west-2, utilisez ce topic ARN = `arn:aws:sns:us-west-2:287847593866:customer-ams-windows2016`
 - b. Pour Protocole, choisissez E-mail.
 - c. Pour Point de terminaison, entrez une adresse e-mail que vous pouvez utiliser pour recevoir les notifications. Nous recommandons une liste de distribution plutôt que l'adresse e-mail d'un individu.
5. Choisissez Créer un abonnement.

6. Lorsque vous recevez un e-mail de confirmation dont l'objet est « Notification AWS - Confirmation d'abonnement », ouvrez-le et choisissez Confirmer l'abonnement pour terminer votre abonnement.

 Note

Vous n'êtes pas limité au courrier électronique pour le protocole. Pour plus d'informations sur les autres protocoles acceptables et sur leur utilisation, consultez la section [subscribe](#).

Pour vous désabonner des nouvelles notifications AMI d'AMS à l'aide de la console AWS SNS :

1. [Ouvrez la console Amazon SNS sur le tableau de bord](#).
2. Dans la barre de navigation, sélectionnez la région AWS de votre choix. Vous devez utiliser la région AWS dans laquelle vous souhaitez recevoir des notifications pour le correspondant AMIs.
3. Dans le volet de navigation, choisissez Abonnements, sélectionnez l'abonnement, puis choisissez Actions -> Supprimer les abonnements.
4. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer.

Pour vous abonner aux notifications AMS New AMI à l'aide de la commande Deployment | Ingestion | Stack from CloudFormation Template | Create (ct-36cn2avfrj9v) :

1. Pour vous abonner au fichier JSON AmazonLinuxSubscription, créez et enregistrez un fichier de paramètres d'exécution ; cet exemple le nomme CreateSubscribeAmiParams .json :

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Resources": {
    "AmazonLinuxSubscription":{
      "Type" : "AWS::SNS::Subscription",
      "Properties": {
        "TopicArn": "arn:aws:sns:{REGION}:287847593866:{AMS_AMI_NAME}",
        "Protocol": "email",
        "Endpoint": "username@yourdomain.com"
      }
    }
  }
}
```

2. Créez et enregistrez le fichier JSON des paramètres RFC avec le contenu suivant ; cet exemple le nomme fichier `CreateSubscribeAmiRfc.json` :

```
{
  "ChangeTypeId": "ct-36cn2avfrrj9v",
  "ChangeTypeVersion": "1.0",
  "Title": "cfn-ingest-subscribe-ami"
}
```

3. Créez la RFC en spécifiant le `CreateSubscribeAmiRfc` fichier et le `CreateSubscribeAmiParams` fichier :

```
aws amscm create-rfc --cli-input-json file://CreateSubscribeAmiRfc.json --
execution-parameters file://CreateSubscribeAmiParams.json
```

Vous recevez l'identifiant de la nouvelle RFC dans la réponse et pouvez l'utiliser pour soumettre et surveiller la RFC. Tant que vous ne l'avez pas soumise, la RFC reste en cours d'édition et ne démarre pas.

Pour des exemples de création AMIs, consultez la section [Créer une AMI](#).

Pour plus d'informations sur la consommation AMIs par programmation, voir [EC2 stack : creating](#).

Notifications de service

AMS envoie des demandes de service sortantes, ou des notifications de service, lorsque vous devez agir ou être conscient d'un élément susceptible d'avoir un impact sur votre compte ou vos ressources, notamment :

- Impact sur l'infrastructure : AMS envoie une notification de service lorsqu'un service AWS sous-jacent a un impact sur votre infrastructure et que vous devez prendre des mesures avant une certaine date, faute de quoi vous pourriez être victime d'une panne.
- EC2 Problèmes matériels : AMS envoie des notifications de service pour les problèmes EC2 matériels qui vous obligent à redémarrer une EC2 instance avant une certaine date ou pour vous informer qu'AMS redémarrera l'instance pour vous. Il s'agit d'un avis important car le redémarrage peut provoquer une panne et vous devez répondre en indiquant une date acceptable, ou créer une RFC avec `ct-09qbhy7kvtxqw`, pour redémarrer l'instance vous-même. Une notification de service comme celle-ci se ferme automatiquement dans cinq jours si vous ne répondez pas.

Notifications de changement d'état RFC

AMS propose des notifications pour les changements d'état des RFC par e-mail et des CloudWatch événements :

- E-mails via la console AMS : Sur la deuxième page de l'assistant de création d'une RFC, vous pouvez ajouter jusqu'à cinq adresses e-mail pour être averti lorsque l'état de la RFC change.
- CloudWatch Événements : vous pouvez configurer différentes règles et cibles pour que les CloudWatch événements reçoivent des notifications pour chaque changement d'état de la RFC.

Notifications par e-mail

Vous pouvez ajouter des adresses e-mail pour recevoir les modifications d'état d'une RFC créée dans la console AMS ou à l'aide de l'API/CLI AMS.

Dans la console AMS, utilisez l'option Notifications par e-mail, sur la deuxième page de l'assistant de création d'une RFC :

Dans l'API/CLI AMS, ajoutez une ligne comme celle-ci à la section des paramètres RFC de votre RFC (n'ajoutez pas la ligne à la section des paramètres d'exécution) :

```
--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"
```

Le comportement des notifications varie en fonction du type de planification RFC :

- RFCs Réception planifiée de notifications par e-mail sur : Soumis InProgress, planifié, terminé, rejeté, annulé, rejeté automatiquement ou annulé automatiquement.
- RFCs Recevez dès que possible une notification par e-mail sur : Soumis InProgress, Terminé, Rejeté AutoRejected, Annulé ou Annulé automatiquement.

Note

- Les notifications par e-mail sont envoyées depuis cette adresse :no-reply@managedservices.amazonaws.com.

- Les caractères spéciaux et URLs le titre de votre RFC sont supprimés dans les e-mails que nous envoyons. Il s'agit d'une mesure de sécurité.

CloudWatch Notifications d'événements

AMS propose des notifications push pour les changements d'état de la RFC par le biais d'CloudWatch événements. Pour recevoir ces notifications, procédez comme suit :

1. Créez un sujet et un abonnement auxquels les notifications seront envoyées. Vous pouvez nommer le sujet comme bon vous semble ; pour plus d'informations à ce sujet, consultez [Rubrique et abonnement SNS : création](#).
2. Soumettez une RFC avec le type Management | Other | Other | Create change et incluez le sujet SNS et l'abonnement dans la demande d'avis de modification de l'état de la RFC.

Lorsque vous soumettez la demande Management | Other | Other RFC pour cette fonctionnalité, vous pouvez spécifier les changements d'état RFC dont vous souhaitez être informé et les types de modifications, et définir d'autres filtres. Par exemple, vous souhaitez peut-être demander à être averti uniquement lorsque les types de modification de l'accès administrateur sont EventType = RfcSubmitted et EventType = RfcUpdated.

Voici un modèle de notifications d'CloudWatch événements que vous pouvez recevoir (avec toutes les valeurs possibles) :

```
{
  "source ": "aws.managedservices",
  "detail-type": "AMS RFC State Change",
  "detail": {
    "ActionState": "null | AwsActionPending | AwsOperatorAssigned | CustomerActionPending | NotApplicable | NoActionPending",
    "ActualExecutionTimeRange": {
      "StartTime": "null | Actual Start Time",
      "EndTime": "null | Actual End Time"
    },
    "AutomationStatus": "Automated | Manual",
    "AwsAccountId": "AWS Account ID",
    "AwsApprovalStatus": "null | SubmissionPending | NotRequired | ApprovalPending | Rejected | Approved",
    "ChangeTypeId": "Change_Type_ID",
```

```

    "ChangeTypeVersion": "Change_Type_Version",
    "CreatedTime": "Created_Time",
    "CustomerApprovalStatus": "null | SubmissionPending | NotRequired |
ApprovalPending | Rejected | Approved",
    "EventType": "RfcActionStateUpdated | RfcApproved | RfcAutoRejected |
RfcCanceled | RfcCompleted | RfcCreated | RfcInProgress | RfcRejected | RfcSubmitted |
RfcUpdated",
    "LastModifiedTime": "Last_Updated_Time",
    "LastSubmittedTime": "null | Last_Submitted_Time",
    "RequestedExecutionTimeRange": {
        "StartTime": "null | Expected_Start_Time",
        "EndTime": "null | Expected_End_Time"
    },
    "RfcId": "RFC_ID",
    "Status": "Editing | PendingApproval | Scheduled | Rejected | Canceled |
ExecutionLock | InProgress | Success | Failure",
    "Title": "Title"
}
}

```

Les changements d'état RFC pris en charge (EventType), tels qu'ils apparaissent dans la notification d' CloudWatch événements réelle, sont les suivants :

- RfcActionStateUpdated (aucune option de console AMS) : La RFC dans l'un des états, décrit plus loin, a changé.
- RfcApproved (aucune option de console AMS) : La RFC a passé avec succès la validation de l'opérateur and/or AMS du système et sa finalisation a été approuvée.
- RfcAutoRejected (Rejeté automatiquement) : La RFC a échoué à la validation du système ou à l'opérateur AMS et a été rejetée.
- RfcCanceled (Annulée ou annulée automatiquement) : La RFC a été annulée soit par l'émetteur, soit par un opérateur AMS.
- RfcCompleted (Terminé) : Les paramètres d'exécution de la RFC ont été définis, y compris UserData.
- RfcCreated (aucune option de console AMS) : La RFC a été créée avec succès (le JSON et les paramètres soumis étaient valides).
- RfcInProgress (InProgress) : L'exécution du RFC est toujours en cours.
- RfcRejected (Rejeté) : La validation du système ou de l'opérateur AMS ayant échoué par la RFC a été rejetée.

- RfcSubmitted (Soumis) : Le RFC a été soumis et est en cours de validation du système.
- RfcUpdated (aucune option de console AMS) : La RFC a été mise à jour manuellement par un opérateur AMS.

En outre, vous pouvez envoyer CloudWatch des notifications d'événements (CWE) vers l'une des destinations prises en charge et créer vos propres systèmes en plus de ces notifications automatisées :

- EC2 Instances Amazon
- AWS Lambda fonctions
- Flux dans Amazon Kinesis Data Streams
- Flux de livraison dans Amazon Data Firehose
- Groupes de journaux dans Amazon CloudWatch Logs
- Tâches Amazon ECS
- Run Command de Systems Manager
- Systems Manager Automation
- AWS Batch emplois
- Machines d'état Step Functions
- Pipelines en CodePipeline
- CodeBuild projets
- Modèles d'évaluation Amazon Inspector
- Rubriques Amazon SNS
- Files d'attente Amazon SQS
- Cibles intégrées : appel d' EC2 CreateSnapshot EC2 RebootInstances API, appel d' EC2 StopInstances API, appel d'API et appel EC2 TerminateInstances d'API.
- Le bus d'événements par défaut d'un autre compte AWS

Note

Nous envoyons une notification d' CloudWatch événements pour les changements d'état de la RFC, dans la mesure du possible.

Configuration de DNS privés et publics

Lors de l'intégration, AMS met en place un service DNS privé pour les communications entre vos ressources gérées et AMS.

Vous pouvez utiliser AMS Route 53 pour gérer les noms DNS internes des ressources de votre application (serveurs Web, serveurs d'applications, bases de données, etc.) sans exposer ces informations à l'Internet public. Cela ajoute une couche de sécurité supplémentaire et vous permet également de passer d'une ressource principale à une ressource secondaire (souvent appelée « retournement ») en mappant le nom DNS à une adresse IP différente.

Après avoir créé des ressources DNS privées à l'aide de `Deployment | Advanced stack components | DNS (private) | Create (ct-0c38gftq56zj6)` ou `Deployment | Advanced stack components | DNS (public) | Create (ct-0vzsr2nyraedl)`, vous pouvez utiliser `Management | Advanced stack components | DNS (private) | Update (ct-1d55pi44ff21u)` et `Management | Advanced stack components | DNS (public) | Mise à jour (ct-1hzofpphabs3i)`, pour configurer des ensembles d'enregistrements supplémentaires ou mettre à jour des ensembles d'enregistrements existants. CTs Pour les comptes de zone d'atterrissage multi-comptes (MALZ), les ressources DNS créées dans le compte d'application VPCs peuvent être partagées avec le compte de services partagés VPC afin de maintenir un DNS centralisé à l'aide d'AMS AD.

MALZ

Le graphique suivant illustre une configuration DNS possible pour Multi-Account Landing Zone AMS. Il illustre une configuration DNS hybride entre AMS et un réseau client classique. Un enregistrement de nom canonique (CNAME) du serveur DNS du réseau client est transféré au DNS AMS AD dans le compte de services partagés avec un transfert conditionnel dont le CNAME du FQDN AMS est transféré à l'enregistrement A.

SALZ

Le graphique suivant illustre une configuration DNS possible pour une zone d'atterrissage à compte unique (SALZ). Il montre une configuration DNS hybride entre AMS et un réseau client typique. Un CNAME sur le serveur DNS du réseau client est transféré au DNS AMS AD avec un transfert conditionnel dans lequel le CNAME du FQDN AMS est transféré à l'enregistrement A.

SALZ Route53 DNS

Le graphique suivant illustre une configuration DNS possible pour une zone d'atterrissage à compte unique (SALZ). Il montre une configuration DNS hybride entre AMS et un réseau client typique. Un CNAME sur le serveur DNS du réseau client est transféré au DNS AMS AD avec un transfert conditionnel dans lequel le CNAME du FQDN AMS est transféré à l'enregistrement A. Cela permet également d'exploiter Route53 pour le trafic réseau sortant, de sorte que n'importe quelle application du compte peut disposer de la résolution DNS dans le compte présentant la plus haute disponibilité.

Chemins de résolution activés par Route53 :

- Instance tentant de résoudre le nom AMS MAD --> VPC +2 (Route53/ AmazonProvided DNS) --> Redirecteurs conditionnels évalués --> Règle du redirecteur conditionnel Route53 MAD correspondante --> Résolveur de trafic sortant Route53 --> DNS AD géré
- Instance tentant de résoudre le nom du client sur site --> VPC +2 (Route53/ AmazonProvided DNS) --> Redirecteurs conditionnels évalués --> La règle du redirecteur conditionnel sur site Route53 correspond --> Résolveur de trafic sortant Route53 --> DNS sur site du client
- Instance tentant de résoudre le nom Internet --> VPC +2 (Route53/ AmazonProvided DNS) --> Redirecteurs conditionnels évalués --> Aucun redirecteur correspondant --> Service DNS Internet

Pour plus d'informations, consultez les [sections Utilisation du DNS avec votre VPC](#) et [Utilisation de zones hébergées privées](#).

Gestion du trafic de sortie AMS

Par défaut, la route dont le CIDR de destination est 0.0.0.0/0 pour les sous-réseaux privés et d'applications client AMS a une passerelle de traduction d'adresses réseau (NAT) comme cible. Les services AMS TrendMicro et les correctifs sont des composants qui doivent disposer d'un accès de sortie à Internet afin qu'AMS puisse fournir ses services TrendMicro et que les systèmes d'exploitation puissent obtenir des mises à jour.

AMS prend en charge le transfert du trafic de sortie vers Internet via un dispositif de sortie géré par le client, à condition que :

- Il agit comme un proxy implicite (transparent, par exemple).

and

- Il autorise les dépendances HTTP et HTTPS AMS (répertoriées dans cette section) afin de permettre l'application continue des correctifs et la maintenance de l'infrastructure gérée par AMS.

Voici quelques exemples :

- La passerelle de transit (TGW) possède un itinéraire par défaut pointant vers le pare-feu sur site géré par le client via la connexion AWS Direct Connect dans le compte Multi-Account Landing Zone Networking.
- Le TGW dispose d'un itinéraire par défaut pointant vers un point de terminaison AWS dans le VPC de sortie de la zone d'accueil multi-comptes utilisant PrivateLink AWS, pointant vers un proxy géré par le client dans un autre compte AWS.
- Le TGW dispose d'un itinéraire par défaut pointant vers un pare-feu géré par le client dans un autre compte AWS, avec une connexion site-to-site VPN en pièce jointe à la zone d'atterrissage multi-comptes TGW.

AMS a identifié les dépendances HTTP et HTTPS AMS correspondantes, et développe et affine ces dépendances de manière continue. Voir [egressMgmt.zip](#). Outre le fichier JSON, le fichier ZIP contient un fichier README.

Note

- Ces informations ne sont pas exhaustives : certains sites externes obligatoires ne sont pas répertoriés ici.
- N'utilisez pas cette liste dans le cadre d'une liste de refus ou d'une stratégie de blocage.
- Cette liste est conçue comme le point de départ d'un ensemble de règles de filtrage des sorties, dans l'espoir que des outils de reporting seront utilisés pour déterminer précisément où le trafic réel diverge de la liste.

Pour demander des informations sur le filtrage du trafic sortant, envoyez un e-mail à votre CSDM : ams-csdm@amazon.com.

Déploiement de ressources IAM dans AMS Advanced

AMS déploie les ressources IAM dans votre application de zone d'atterrissage multi-comptes (MALZ) et dans vos comptes de zone d'atterrissage à compte unique (SALZ) de deux manières :

- Provisionnement IAM automatisé : cette fonctionnalité d'AMS vous permet de soumettre, de créer, de mettre à jour ou de supprimer des types de modifications pour le provisionnement des rôles ou des politiques IAM, sans examen par l'opérateur, et avec des contrôles de validation IAM et AMS exécutés automatiquement.

Cette fonctionnalité doit être explicitement activée avec le type de modification Management | Managed account | AMS Automated IAM Provisioning with read-write permissions | [Enable \(révision requise\) \(révision requise\) \(ct-1706xvvk6j9hf\)](#). Pour en savoir plus, veuillez consulter la section [Provisionnement IAM automatisé \(AMS\)](#). Une fois le provisionnement IAM automatisé d'AMS activé, vous avez accès aux types de modification de création, de mise à jour et de suppression pour gérer vos ressources IAM.

- Vérifier le type de modification IAM requis : ce type de modification, Deployment | Advanced stack components | Identity and Access Management (IAM) | [Create entity or policy \(review required\) \(ct-3dpd8mdd9jn1r\)](#), nécessite un examen par un opérateur AMS, qui peut parfois prendre quelques jours si des clarifications sont nécessaires.

Note

Quelle que soit la méthode utilisée, un rôle IAM est attribué au ou aux comptes concernés et, une fois le rôle configuré, vous devez l'intégrer dans votre solution de fédération.

Provisionnement IAM automatisé (AMS)

AWS Managed Services (AMS) prend en charge la validation et le provisionnement automatisés des ressources IAM, y compris les rôles et les politiques, à l'aide des demandes de modification (RFCs) et des nouveaux types de modification () d'AMS Advanced. CTs Auparavant, ces demandes étaient soumises à un processus semi-automatisé qui entraînait parfois de longs délais d'attente. Vous pouvez désormais utiliser AMS Automated IAM Provisioning pour provisionner des ressources IAM et obtenir des résultats beaucoup plus rapidement.

Comment fonctionne le provisionnement IAM automatisé dans AMS

Le provisionnement IAM automatisé repose sur des contrôles d'exécution automatisés permettant à IAM de valider les modifications apportées aux ressources IAM. Ces contrôles automatisés, effectués lorsque les types de modification Créer, Mettre à jour ou Supprimer sont exécutés, empêchent le déploiement de ressources IAM trop permissives ou présentant des modèles peu sécurisés sur votre compte. Cela vous permet d'adapter le niveau de rigueur des évaluations IAM à l'expertise de votre équipe. Nous recommandons aux équipes qui découvrent les services cloud et qui ont besoin de vérifications manuelles pour toutes les modifications des ressources IAM d'utiliser le type de modification existant nécessitant une révision : [Deployment | Advanced stack components | Identity and Access Management \(IAM\) | Créer une entité ou une politique \(révision requise\), \(ct-3dpd8mdd9jn1r\)](#). Les équipes ayant AWS l'expertise et le contrôle de leurs environnements peuvent utiliser le provisionnement IAM automatisé pour accélérer leurs déploiements. Vous pouvez utiliser cette fonctionnalité pour effectuer une validation par le biais de contrôles d'exécution automatisés ou pour effectuer la validation et le provisionnement des ressources IAM après une validation réussie.

Important

AWS Managed Services a mis en œuvre de manière proactive une liste de [contrôles d'exécution](#) de validation qui empêchent la création de ressources ou de politiques IAM assorties de certaines autorisations et conditions. Pour une description de ces privilèges et conditions, consultez la section [Déploiement de ressources IAM dans AMS Advanced](#). Les types de modifications automatisés [ct-1n9gfnog5x7fl](#), [ct-1e0xmuy1diafq](#) et [ct-17cj84y7632o6](#) permettent aux utilisateurs maîtrisant la gestion des ressources IAM de fournir des rôles et des politiques IAM autorisant des actions au-delà des privilèges de lecture seule. [En outre, vous pouvez utiliser les rôles créés par le biais des types de modification automatisés ct-1n9gfnog5x7fl, ct-1e0xmuy1diafq et ct-17cj84y7632o6 pour créer les nouvelles ressources.](#) Cependant, les ressources ne peuvent pas suivre la norme de dénomination AMS et ne font pas partie de la pile AMS standard. AMS fournit le soutien opérationnel et de sécurité de ces ressources spécifiques dans la mesure du possible. Bien que les processus manuels et automatisés visent à respecter nos normes de sécurité, il est important de noter qu'il existe des différences dans les contrôles entre les deux. Le provisionnement automatisé permet une plus grande flexibilité dans la création et la mise à jour des rôles et des politiques ; ils ne sont donc pas identiques. Il est recommandé que votre organisation examine attentivement les [contrôles d'exécution](#) de validation répertoriés

dans le guide de l'utilisateur AMS afin de s'assurer qu'ils correspondent aux attentes et aux exigences de votre organisation.

Flux de validation

Flux de validation et de provisionnement

Note

Cette fonctionnalité convient aux équipes expérimentées avec les ressources IAM, AWS et nous ne la recommandons pas aux équipes qui en sont à AWS leur première expérience. Le processus de validation automatique est conçu pour détecter la plupart des erreurs et permet aux équipes de vérifier rapidement les modifications apportées à l'IAM, lorsqu'elles comprennent les autorisations dont elles ont besoin. Pour utiliser les nouveaux types de modifications de manière sûre et efficace, nous vous recommandons de bien comprendre l' AWS IAM et les [contrôles d'exécution](#) proposés par les types de modifications afin de déterminer s'ils conviennent à votre équipe.

Intégration à AMS Provisionnement IAM automatisé dans AMS

Pour utiliser les nouveaux types de modifications, activez d'abord AMS Automated IAM Provisioning en soumettant une RFC en utilisant le type de modification suivant : Gestion | Compte géré | AMS Automated IAM Provisioning avec autorisations de lecture-écriture | [Activer \(révision requise\)](#) (ct-1706xvvk6j9hf). AWS exige que votre organisation suive un processus de gestion des risques liés à la sécurité des clients (CSRM) afin de garantir que l'utilisation de ces types de modifications est conforme à vos politiques organisationnelles. L'équipe AWS des opérations travaille avec vous pour obtenir l'approbation explicite de votre contact avec l'équipe de sécurité sous la forme d'une acceptation des risques dans le cadre de l'examen requis. Pour en savoir plus, consultez le processus de [gestion des risques clients \(CSRM\) de la RFC](#).

Une fois que le RFC pour activer la fonctionnalité AMS Automated IAM Provisioning avec autorisations de lecture-écriture est réussi, AMS active les types de modification du provisionnement IAM automatisé AMS dans le compte utilisé pour soumettre le RFC d'activation. Pour vérifier

qu'AMS Automated IAM Provisioning est activé sur un compte, vérifiez le rôle dans la console IAM. `AWSManagedServicesIAMProvisionAdminRole`

Dans le cadre de l'intégration, AMS fournit IAM Access Analyzer dans la même région AWS que le compte afin de tirer parti de sa fonctionnalité de prévisualisation des accès. IAM Access Analyzer aide à identifier les ressources de votre organisation et les comptes partagés avec une entité externe, valide les politiques IAM par rapport à la grammaire des politiques et aux meilleures pratiques, et génère des politiques IAM basées sur l'activité d'accès dans vos journaux. AWS CloudTrail Pour en savoir plus, consultez la section [Utilisation AWS Identity and Access Management Access Analyzer](#).

Une fois intégré, il `AWSManagedServicesIAMProvisionAdminRole` est déployé sur les comptes activés. Si vous choisissez d'utiliser ce rôle par le biais de la fédération SAML, vous devez l'intégrer à votre solution de fédération.

Dans le cadre de l'intégration, vous pouvez demander à mettre à jour la politique `IAMProvisionAdminRole` de confiance `AWSManaged` des Services afin d'octroyer un autre ARN de rôle IAM à utiliser pour assumer ce rôle. AWS Security Token Service

Utilisation du provisionnement IAM automatisé d'AMS dans AMS

Vous pouvez créer RFCs avec les types de modifications AMS Automated IAM Provisioning suivants.

Note

- Seul le provisionnement basé sur les rôles et les politiques est pris en charge.

Lors de la mise à jour des rôles, l'Update CT remplace la liste existante des noms de ressources Amazon des politiques gérées (ARNs) et le document de politique « assumer un rôle », par la liste fournie des politiques gérées ARNs et du document de politique « assumer un rôle » fournis. Lors d'une mise à jour partielle, par exemple, l'ajout ou la suppression d'un ARN dans la liste existante des politiques gérées ARNs, l'ajout ou la suppression de déclarations de politique individuelles dans le document de politique « assumer un rôle » n'est pas autorisé. De même, lors de la mise à jour des politiques, l'Update CT remplace le document de politique existant et ne permet pas d'ajouter ou de supprimer des déclarations de politique individuelles dans le document de politique existant.

- Lorsque l'option « valider uniquement » est sélectionnée, les contrôles d'exécution sont effectués sans provisionner d'entité ou de politique IAM. Quels que soient les résultats, le

statut de la RFC est « succès ». Le statut « réussite » indique une validation réussie par rapport à l'entité ou à la politique IAM fournie.

- Déploiement | Advanced Stack Components | Identity and Access Management (IAM) | [Création d'une entité ou d'une politique \(autorisations de lecture-écriture\) \(ct-1n9gfnog5x7fl\)](#) : une nouvelle entité ou politique IAM est validée et provisionnée automatiquement.
- Gestion | Advanced Stack Components | Identity and Access Management (IAM) | [Mettre à jour l'entité ou la politique \(autorisations de lecture-écriture\) \(ct-1e0xmuy1diafq\)](#) : une entité ou une politique IAM existante est mise à jour et validée automatiquement.
- Management | Advanced Stack Components | Identity and Access Management (IAM) | [Supprimer une entité ou une politique \(autorisations de lecture-écriture\) \(ct-17cj84y7632o6\)](#) : une entité ou une politique IAM existante provisionnée à l'aide du type de création automatique d'entité ou de changement de politique est supprimée.

Vous ne pouvez appeler les trois précédents qu' CTs en utilisant un rôle IAM dédié :AWSManagedServicesIAMProvisionAdminRole. Ce rôle n'est disponible que dans les comptes qui ont été intégrés à la fonctionnalité à l'aide des autorisations de lecture/écriture Management | Compte géré | AMS Automated IAM Provisioning | [Activer \(révision requise\) \(ct-1706xvvk6j9hf\)](#).

Important

Les types de modification Créer, Mettre à jour et Supprimer sont toujours visibles dans votre compte, mais ils ne sont pas activés par défaut. Si vous essayez de soumettre une RFC en utilisant l'un de ces types de modification sans activer au préalable la fonctionnalité AMS Automated IAM Provisioning, une erreur « non autorisée » s'affiche.

Limites :

- Le Create CT peut vous permettre de créer un rôle ou une politique IAM avec l'autorisation de créer des AWS ressources. Cependant, AWS les ressources créées par ces rôles et politiques ne sont pas gérées par AMS. Il est recommandé de respecter le contrôle de votre organisation afin de limiter la création de tels rôles ou politiques.

- L'Update CT ne peut pas modifier les rôles et politiques IAM créés avec CFN Ingest, le mode Direct Change, le mode développeur ou, dans certains cas, via le manuel ou automatisé AMS Advanced existant. CTs
- Le Delete CT ne peut pas supprimer les rôles ou les politiques existants qui ne sont pas créés avec l'AMS Automated IAM Provisioning Create CT.
- La fonctionnalité AMS Automated IAM Provisioning avec autorisations de lecture-écriture n'est pas prise en charge dans les rôles en mode de changement direct. Cela signifie que vous ne pouvez pas attribuer ou mettre à jour des rôles et des politiques IAM avec des autorisations de lecture-écriture à l'aide de ces rôles.
- Le provisionnement IAM automatisé AMS avec autorisations de lecture/écriture Les types de modification de création, de mise à jour et de suppression ne sont pas compatibles avec le connecteur. ServiceNow

Contrôles d'exécution pour le provisionnement IAM automatisé d'AMS dans AMS

Le provisionnement IAM automatisé tire parti des vérifications et effectue des AWS Identity and Access Management Access Analyzer vérifications et des validations supplémentaires par rapport à la politique de limites AMS. AMS a défini les contrôles et validations supplémentaires en fonction des meilleures pratiques IAM, de l'expérience d'exploitation de la charge de travail des clients dans le cloud et de l'expérience collective d'évaluation manuelle d'AMS IAM.

Vous pouvez consulter les résultats de la vérification de l'exécution des politiques dans le résultat de la demande de modification (RFC). Les résultats incluent l'identifiant de la ressource, son emplacement au sein de la and/or politique de rôle qui a généré les résultats et un message décrivant le contrôle que l'entité ou la ressource IAM n'a pas réussi. Ces résultats vous aident à créer des politiques fonctionnelles et conformes aux meilleures pratiques en matière de sécurité.

Note

Le provisionnement IAM automatisé tente de préciser l'emplacement au sein de l'entité ou de la définition de politique qui ne passe pas le contrôle. Selon le type, l'emplacement peut inclure le nom ou l'ARN de la ressource, ou l'index d'un tableau. Par exemple, une déclaration pour vous aider à ajuster l'entité ou la politique en vue d'un résultat positif.

Pour une expérience fluide de provisionnement IAM automatisé AMS, il est recommandé d'utiliser l'option « valider uniquement » pour exécuter les contrôles de validation jusqu'à ce qu'aucun résultat

ne soit trouvé lors des contrôles de validation signalés dans les sorties RFC. Lorsque les contrôles de validation ne signalent aucun résultat, choisissez **Create copy from the AMS Console** pour créer rapidement une copie de la RFC existante. Lorsque vous êtes prêt à effectuer le provisionnement, dans la section **Paramètres**, changez la valeur **Validation** uniquement de **Oui** à **Non**, puis continuez.

Voici les contrôles d'exécution effectués par AMS Automated IAM Provisioning pour garantir la sécurité de vos ressources IAM :

 Note

Pour configurer des politiques IAM contenant des actions refusées par ces types de modifications automatisées, vous devez suivre le processus de gestion des risques de sécurité des clients (CSRM) RFC. Utilisez le type de modification suivant : **Deployment | Advanced stack components | Identity and Access Management (IAM) | Créer une entité ou une politique (révision requise) (ct-3dpg8mdd9jn1r)**.

- Vérification et validation des politiques d'IAM Access Analyzer : voir également la référence de vérification [des politiques d'Access Analyzer et la validation des politiques](#) d'IAM Access Analyzer.
- Vérifications de la politique des limites des autorisations AMS : actions sur un ensemble de services refusées par défaut. Pour plus d'informations, consultez la section Vérification [des limites d'autorisation du provisionnement IAM automatisé](#).
- Vérifications de la politique des limites des autorisations définies par le client : actions restreintes supplémentaires sur un ensemble de services refusés. Pour plus d'informations, consultez la section Vérification [des limites d'autorisation du provisionnement IAM automatisé](#).
- Contrôles personnalisés définis par AMS : ils identifient diverses politiques ou modèles d'accès non sécurisés et trop permissifs au sein d'une entité ou d'une politique IAM demandée, et rejettent la demande si elle est trouvée. Pour plus d'informations, voir [Éléments de politique AWS JSON : Principal](#).

Résultat	Description
Le rôle est accessible à partir d'un compte externe situé en dehors de votre zone de confiance.	Ce résultat fait référence à un principal répertorié dans la politique de confiance des rôles qui se trouve en dehors de votre zone de confiance . Une zone de confiance est définie comme le

Résultat	Description
	compte dans lequel le rôle est créé ou l' AWS organisation à laquelle appartient le compte. Une entité qui n'appartient pas au compte ou à la même AWS organisation est une entité externe. Pour résoudre ce problème, vérifiez l'identifiant du compte indiqué sur le compte principal ARNs et assurez-vous qu'il vous appartient et qu'il s'agit d'un compte intégré à AMS.
Le rôle est accessible à une entité externe détenue par un compte <i>External_Account_ID</i> qui n'appartient pas au compte propriétaire du client AMS. <i>Account_ID</i>	Ce résultat est généré si la politique de confiance dans les rôles inclut un ARN principal dont l'identifiant de compte ne vous appartient pas et un compte AMS intégré. Pour résoudre ce problème, supprimez un tel principal de la politique de confiance dans les rôles.
L'ID utilisateur canonique n'est pas un principe pris en charge dans la politique de confiance IAM.	Les principes canoniques ne IDs sont pas pris en charge dans la politique de confiance IAM. Pour résoudre le problème, supprimez tout principe de ce type de la politique de confiance en matière de rôle.
Le rôle est accessible via une identité Web externe située en dehors de votre zone de confiance.	Ce résultat est généré si la politique de confiance dans les rôles autorise un fournisseur d'identité Web (IdP) externe autre que l'IdP SAML. Pour résoudre ce problème, passez en revue la politique de confiance dans les rôles et supprimez les instructions qui autorisent l' <code>sts:AssumeRoleWithWebIdentity</code> opération.

Résultat	Description
Le rôle est accessible via la fédération SAML ; toutefois, le fournisseur d'identité SAML (IdP) fourni n'existe pas.	Ce résultat est généré si la politique d'approbation des rôles contient un IdP SAML qui n'existe pas dans votre compte. Pour résoudre le problème, assurez-vous que tous les IdP SAML répertoriés existent dans votre compte.
La politique contient des actions privilégiées équivalentes à l'accès d'un administrateur ou d'un utilisateur avancé. Envisagez de réduire la portée des autorisations à un service, une action ou une ressource spécifique. Si des éléments de stratégie avancés tels que <code>NotAction</code> ou <code>NotResources</code> sont utilisés, assurez-vous qu'ils n'accordent pas plus d'accès que prévu, en particulier dans les instructions <code>Allow</code> .	Il s'agit d'une bonne pratique de sécurité qui consiste AWS Identity and Access Management à n'accorder que les autorisations requises pour effectuer une tâche lorsque vous définissez des autorisations à l'aide de politiques IAM. Pour ce faire, définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations du moindre privilège. Ce résultat est généré lorsque l'automatisation détecte que la politique accorde des autorisations étendues et ne respecte pas le principe du moindre privilège. Pour résoudre le problème, passez en revue et réduisez les autorisations.
La déclaration contient des actions privilégiées pour <code>Service_Name</code> . Envisagez d'exclure ces actions par une déclaration de refus. Reportez-vous à la référence de politique des limites dans la documentation AMS pour obtenir une liste des actions privilégiées.	AMS a identifié certaines actions liées à un service donné comme risquées et nécessitant un examen plus approfondi des risques et leur acceptation par l'équipe de sécurité du client. Ce résultat est généré lorsque l'automatisation détecte la politique donnée accordant de telles autorisations. Pour résoudre ce problème, refusez ces actions dans votre politique. Pour une liste d'actions, reportez-vous à la politique de limites AMS. Pour plus de détails sur la politique de limites de l'AMS, voir Vérification des limites des autorisations de provisionnement IAM automatisé AMS .

Résultat	Description
La déclaration donne accès aux types de modification RFC privilégiés : ct-1n9gfnog5x7fl, ct-1e0xmuy1diafq et ct-17cj84y7632o6 pour le service. <i>Service_Name</i> Envisagez d'étendre les autorisations à des types de modifications spécifiques ou d'exclure ces types de modifications par une déclaration de refus.	Ce résultat est généré si la politique accorde des autorisations pour effectuer des actions liées à la RFC à l'aide des types de modification du provisionnement IAM automatisé (). CTs Ils CTs sont soumis à l'acceptation des risques et ne doivent être utilisés que dans le cadre de rôles intégrés. Vous ne pouvez donc pas leur accorder d'autorisation CTs. Pour résoudre ce problème, refusez les actions RFC utilisant celles-ci CTs.
La déclaration contient des actions privilégiées qui ne sont pas limitées à vos ressources de service <i>Service_Name</i> . Envisagez d'étendre les actions à des ressources spécifiques ou d'exclure des ressources avec des préfixes d'espace de noms AMS. Si des caractères génériques sont utilisés, assurez-vous qu'ils limitent la portée à vos ressources.	Ce résultat est généré si la politique accorde des actions privilégiées qui ne sont pas limitées à vos ressources du service donné. Les jokers créent souvent des politiques trop permissives qui intègrent un large éventail de ressources ou d'actions dans le champ d'application de l'autorisation. Pour résoudre ce problème, réduisez l'étendue des autorisations accordées aux ressources que vous possédez ou excluez les ressources qui se trouvent dans l'espace de noms AMS. Pour obtenir la liste des préfixes d'espaces de noms AMS, consultez la politique de limites dans la documentation AMS. Notez que tous les préfixes ne s'appliquent pas à tous les services. Pour plus de détails sur la politique de limites de l'AMS, voir Vérification des limites des autorisations de provisionnement IAM automatisé AMS.

Résultat	Description
ID de compte ou nom de ressource Amazon (ARN) non valide.	Ce résultat est généré si un ARN ou un ID de compte spécifié dans la politique ou la politique de confiance des rôles n'est pas valide. Pour consulter les ressources de l'ARN de ressource valide pour les services, consultez la référence d'autorisation des services . Assurez-vous que l'identifiant du compte est un numéro à 12 chiffres et que le compte est actif dans AWS.
L'utilisation du caractère générique (*) pour l'identifiant de compte dans l'ARN est limitée.	Ce résultat est généré si un caractère générique (*) est spécifié dans le champ ID de compte d'un ARN. Un joker dans un champ d'identifiant de compte correspond à n'importe quel compte et accorde potentiellement des autorisations involontaires à des ressources. Pour résoudre ce problème, remplacez le joker par un identifiant de compte spécifique.
Le compte de ressources spécifié n'appartient pas au même compte client AMS <i>Account_ID</i> .	Ce résultat est généré si un identifiant de compte spécifié dans un ARN de ressource ne vous appartient pas et n'est pas géré par AMS. Pour résoudre ce problème, assurez-vous que toutes les ressources (telles que spécifiées par leur ARN dans la politique) appartiennent à vos comptes gérés par AMS.
Le nom du rôle se trouve dans l'espace de noms restreint AMS.	Ce résultat est généré si vous essayez de créer un rôle dont le nom commence par un préfixe réservé AMS. Pour résoudre ce problème, attribuez un nom au rôle spécifique à votre cas d'utilisation. Pour une liste des préfixes réservés AMS, voir Préfixes réservés AMS

Résultat	Description
Le nom de la politique se trouve dans l'espace de noms restreint AMS.	Ce résultat est généré si vous essayez de créer une politique dont le nom commence par un préfixe réservé AMS. Pour résoudre ce problème, attribuez à la politique un nom spécifique à votre cas d'utilisation. Pour obtenir la liste des préfixes réservés AMS, consultez la section Préfixes réservés AMS .
L'ID de ressource dans l'ARN se trouve dans l'espace de noms restreint AMS.	Ce résultat est généré si vous essayez de créer une politique qui accorde l'autorisation aux ressources nommées qui se trouvent dans l'espace de noms AMS. Pour résoudre ce problème, assurez-vous d'étendre les autorisations à vos ressources ou de refuser les autorisations aux ressources qui se trouvent dans l'espace de noms AMS. Pour plus d'informations sur les espaces de noms AMS, consultez la section Espaces de noms restreints AMS .
Cas de variable de politique non valide. Mettez à jour la variable sur <i>Variable_Names</i> .	Ce résultat est généré si vous essayez de créer une politique contenant une variable de stratégie globale IAM dans le mauvais cas. Pour résoudre ce problème, utilisez le cas correct pour les variables globales dans votre politique. Pour obtenir la liste des variables globales, consultez la section Clés contextuelles des conditions AWS globales . Pour plus d'informations sur les variables de stratégie, voir Éléments de stratégie IAM : variables et balises

Résultat	Description
L'instruction contient des actions privilégiées qui ne sont pas limitées à vos clés KMS. Envisagez d'étendre ces autorisations à des clés spécifiques ou d'exclure les clés détenues par AMS.	Ce résultat est généré si la politique contient des autorisations qui ne sont pas limitées à des clés KMS spécifiques que vous possédez. Pour résoudre ce problème, étendez l'autorisation à des clés spécifiques ou excluez les clés détenues par AMS. Les clés détenues par AMS ont des ensembles d'alias spécifiques. Pour obtenir la liste des alias de clés détenus par AMS, consultez Vérification des limites des autorisations de provisionnement IAM automatisé AMS .
L'instruction contient des actions privilégiées qui ne sont pas limitées à vos alias de clés KMS. Envisagez d'étendre ces autorisations à vos clés ou alias, ou d'exclure les alias de clés appartenant à AMS.	Ce résultat est généré si la politique contient des autorisations qui ne sont pas limitées à un alias de clé KMS spécifique que vous possédez. Pour résoudre ce problème, étendez l'autorisation à des clés spécifiques ou excluez les clés détenues par AMS. Les clés détenues par AMS ont des ensembles d'alias spécifiques. Pour obtenir la liste des alias de clés détenus par AMS, consultez Vérification des limites des autorisations de provisionnement IAM automatisé AMS .

Résultat	Description
L'instruction contient des actions privilégiées qui ne sont pas correctement limitées à vos clés KMS à l'aide de <code>kms:ResourceAliasesCondition</code> . Envisagez d'utiliser des noms d'alias spécifiques ainsi que l'opérateur <code>set</code> approprié pour la clé de condition. Si des caractères génériques sont utilisés dans les noms d'alias, assurez-vous qu'ils limitent la portée à un ensemble limité de vos clés KMS.	Ce résultat est généré si vous délimitez les autorisations relatives à vos clés KMS à l'aide de conditions et que vous ne les utilisez pas pour vous limiter aux alias de vos clés KMS. Ou, si la clé de <code>kms:ResourceAliasesCondition</code> a une valeur qui inclut également les alias des clés KMS appartenant à AMS. Pour résoudre ce problème, mettez à jour la condition afin de limiter l'autorisation uniquement aux alias de vos clés KMS ou d'exclure les alias des clés KMS détenues par AMS. Pour obtenir la liste des alias de clés détenus par AMS, consultez Vérification des limites des autorisations de provisionnement IAM automatisé AMS .
Le rôle doit être associé à <code>customer_deny_policy</code> . Incluez l'ARN de la politique dans la liste des politiques gérées ARNs.	Ce résultat est généré si le rôle que vous créez n'est pas <code>customer_deny_policy</code> associé. Pour résoudre ce problème, incluez-le <code>customer_deny_policy</code> dans la ARNs liste des politiques gérées.
La politique AWS gérée est trop permissive ou accorde des autorisations limitées par la politique de limites AMS.	Ce résultat est généré si la <code>ManagedPolicyArns</code> valeur du rôle contient une politique gérée par AMS qui fournit un accès complet ou de niveau administrateur au service concerné. Pour résoudre ce problème, passez en revue l'utilisation de la politique AWS gérée et utilisez une politique qui fournit des autorisations limitées ou définissez votre propre politique qui respecte le principe du moindre privilège.

Résultat	Description
La politique gérée par le client se trouve dans un espace de noms AMS restreint.	Ce résultat est généré si une politique gérée par le client dont le nom est préfixé dans l'espace de AWS noms est attachée au rôle. Pour résoudre ce problème, supprimez la politique de la ManagedPolicyArnsliste correspondant au rôle.
Le customer_deny_policy ne peut pas être détaché du rôle. Incluez l'ARN de la politique dans la liste des politiques gérées ARNs.	Ce résultat est généré s'il customer_deny_policy est détaché du rôle lors d'une mise à jour. Pour résoudre ce problème, ajoutez customer_deny_policy le ManagedPolicyArnsdans le champ du rôle et réessayez.
Les politiques gérées par le client ont été mises en place en dehors du service AMS Change Management ou sans validation préalable.	Ce résultat est généré si une ou plusieurs politiques existantes gérées par le client ARNs sont associées à un rôle et que les politiques ne sont pas fournies via le service AMS Change Management (via une RFC). Par exemple, le mode développeur ou le mode changement direct permettent aux clients de mettre en place des politiques IAM sans RFC. Pour résoudre ce problème, supprimez la politique gérée par le client ARNs de la ManagedPolicyArnsliste correspondant au rôle.
Le nombre de politiques gérées fournies ARNs dépasse le quota de politiques attachées par rôle.	Ce résultat est généré si le nombre total de politiques gérées associées au rôle dépasse le quota de politiques par rôle. Pour plus d'informations sur les quotas IAM, consultez les rubriques Quotas IAM et AWS STS, exigences relatives aux noms et limites de caractères . Utilisez ces informations pour réduire le nombre de politiques que vous associez au rôle.

Résultat	Description
La taille de la politique de confiance ({trust_policy}) dépasse le quota de taille de la politique de rôle assumé de {size}.	Ce résultat est généré si la taille du document de politique d'acceptation du rôle dépasse le quota de taille de la politique. Pour plus d'informations sur les quotas IAM, consultez les rubriques Quotas IAM et AWS STS, exigences relatives aux noms et limites de caractères .
La déclaration contient toutes les actions mutatives pour Amazon S3. Envisagez de limiter ces autorisations aux actions requises uniquement. Si des caractères génériques sont utilisés, assurez-vous qu'ils ont une portée limitée d'actions mutatives.	Ce résultat est généré si la politique donnée accorde à toutes les autorisations mutatives d'Amazon Simple Storage Service, indépendamment d'une ou de plusieurs ressources. Pour résoudre ce problème, incluez uniquement les actions mutatives Amazon S3 requises contre vos buckets.
La déclaration contient des actions privilégiées qui ne sont autorisées sur aucun compartiment dans Amazon S3. Envisagez d'ajouter une déclaration niant ces actions.	Ce résultat est généré si la politique accorde des actions privilégiées sur n'importe quel bucket. Pour obtenir la liste des actions privilégiées, voir Vérification des limites des autorisations de provisionnement IAM automatisé AMS . Pour résoudre ce problème, supprimez ou refusez ces actions dans votre politique.
La déclaration contient des actions privilégiées qui ne sont pas limitées à vos compartiments dans Amazon S3. Envisagez d'inclure vos buckets ou d'exclure les buckets avec des préfixes d'espace de noms AMS. Si des caractères génériques sont utilisés, assurez-vous qu'ils correspondent aux compartiments de vos espaces de noms.	Ce résultat est généré si la politique autorise des actions Amazon S3 qui ne sont pas limitées à vos compartiments uniquement. Cela se produit souvent si des caractères génériques sont utilisés lors de la spécification des ressources du bucket. Pour résoudre ce problème, spécifiez les noms des compartiments ou indiquez ARNs que vous êtes propriétaire ou excluez les compartiments dotés de préfixes d'espace de noms AMS.

Résultat	Description
La déclaration contient des actions privilégiées qui ne sont pas limitées à vos compartiments dans Amazon S3. Pensez à éviter d'utiliser des caractères génériques (*) qui couvrent tous les compartiments du compte.	Ce résultat est généré si la politique autorise des actions Amazon S3 qui ne sont pas limitées à votre compartiment. Cela se produit souvent si des caractères génériques sont utilisés lors de la spécification des ressources du bucket. Pour résoudre ce problème, spécifiez les noms des compartiments ou indiquez ARNs que vous êtes propriétaire ou excluez les compartiments dotés de préfixes d'espace de noms AMS.
La déclaration contient un caractère générique de ressource qui s'applique à tous les compartiments Amazon S3, y compris les compartiments inexistants et les compartiments dont vous n'êtes pas le propriétaire. Envisagez de définir la portée des autorisations à l'aide d'une condition et d'une clé de <code>s3:ResourceAccount</code> condition.	Ce résultat est généré si la politique autorise les compartiments spécifiés à l'aide de caractères génériques. L'utilisation de jokers ouvre souvent la porte à des compartiments inexistants ou non propriétaires. Pour résoudre ce problème, utilisez la condition et la clé de <code>aws:ResourceAccount</code> condition pour étendre l'autorisation aux compartiments du compte courant uniquement. Pour plus de détails, consultez Limiter l'accès aux compartiments Amazon S3 détenus par des AWS comptes spécifiques .
La déclaration contient un élément de <code>NotResource</code> politique, qui peut être limité à un grand nombre de compartiments, y compris des compartiments inexistants et des compartiments dont vous n'êtes pas le propriétaire. Envisagez de définir la portée des autorisations à l'aide d'une condition et d'une clé de <code>s3:ResourceAccount</code> condition.	Ce résultat est généré si la politique utilise l'élément de <code>NotResources</code> stratégie pour spécifier les ressources du bucket. L'utilisation de l' <code>NotResource</code> élément peut couvrir un grand nombre de compartiments, y compris des compartiments inexistants ou non propriétaires. Pour résoudre ce problème, utilisez les conditions et la clé de <code>aws:ResourceAccount</code> condition pour étendre l'autorisation aux buckets uniquement au sein du compte courant.

Résultat	Description
La déclaration contient une action Amazon S3 concernant des compartiments <i>Bucket_Name</i> qui n'existent pas, qui ne sont pas détenus par un compte <i>Account_ID</i> ou dont le nom contient un caractère générique susceptible d'être étendu à un grand nombre de compartiments, y compris des compartiments inexistantes et des compartiments dont vous n'êtes pas le propriétaire. Envisagez de définir la portée des autorisations à l'aide d'une condition et d'une clé de <code>s3:ResourceAccount</code> condition	Ce résultat est généré si la politique accorde l'autorisation à des compartiments qui n'existent pas, ne vous appartiennent pas ou dont le nom contient des caractères génériques couvrant un grand nombre de compartiments et que l'accès n'est pas limité au compte courant uniquement. Pour résoudre ce problème, utilisez la condition et la clé de <code>aws:ResourceAccount</code> condition pour étendre l'autorisation aux compartiments du compte courant uniquement.
La déclaration contient une action Amazon S3 concernant des compartiments <i>Bucket_Name</i> qui n'existent pas, qui ne sont pas détenus par compte <i>Account_ID</i> ou dont le nom contient un caractère générique susceptible d'être étendu à un grand nombre de compartiments, y compris des compartiments inexistantes et des compartiments dont vous n'êtes pas le propriétaire. L'accès n'est pas restreint en utilisant <code>s3:ResourceAccount</code> ou en spécifiant le compte de ressources si la condition ne vous appartient pas.	Ce résultat est généré si la politique accorde l'autorisation à des compartiments qui n'existent pas, ne vous appartiennent pas ou dont le nom contient des caractères génériques couvrant un grand nombre de compartiments et que l'accès est limité à un compte spécifique uniquement. Cependant, le compte indiqué dans la clé de <code>aws:ResourceAccount</code> condition ne vous appartient pas et est géré par AMS. Pour résoudre ce problème, mettez à jour la clé de <code>aws:ResourceAccount</code> condition et définissez l'identifiant de compte approprié que vous possédez et qui est géré par AMS.

Résultat	Description
La déclaration contient des actions privilégiées qui ne sont pas limitées à vos instances pour Amazon EC2. Envisagez d'étendre les actions à une instance spécifique ARNs ou d'exclure les instances dont la clé de balise Name contient une valeur dans les préfixes d'espace de noms AMS. Si des caractères génériques sont utilisés, assurez-vous qu'ils correspondent aux espaces de noms que vous possédez.	Ce résultat est généré si la politique accorde des actions privilégiées contre les EC2 instances Amazon détenues par AMS. Les instances AMS sont étiquetées avec la clé Name tag avec des valeurs dans l'espace de noms AMS. Pour résoudre ce problème, spécifiez vos ressources ou excluez les instances AMS avec une condition dont la <code>aws:ResourceTag/Name</code> clé exclut les valeurs de l'espace de noms AMS à l'aide de l'opérateur <code>StringNotLike</code>
L'instruction contient des actions privilégiées qui ne sont pas limitées à vos ressources dans le magasin de AWS Systems Manager paramètres. Envisagez ARNs de spécifier vos paramètres ou d'exclure des paramètres avec des préfixes d'espace de noms AMS. Si des caractères génériques sont utilisés, assurez-vous qu'ils ne concernent que vos paramètres.	Ce résultat est généré si la politique accorde des autorisations à des paramètres qui ne vous appartiennent pas. C'est généralement le cas lorsque des caractères génériques sont utilisés ou que des paramètres avec des préfixes d'espace de noms AMS sont répertoriés sous ressources dans une déclaration de politique . Pour résoudre ce problème, spécifiez les paramètres qui se trouvent dans votre espace de noms ou excluez les paramètres AMS avec une instruction <code>deny</code> .
La déclaration contient des actions privilégiées contre les ressources de AWS Systems Manager. Envisagez de délimiter les autorisations pour lire uniquement les actions ou les actions portant sur vos ressources.	Ce résultat est généré si la politique accorde des autorisations autres que le magasin de paramètres ou des actions en lecture seule sur les ressources de Systems Manager. Pour résoudre ce problème, réduisez les autorisations relatives aux actions en lecture seule ou au stockage des paramètres uniquement.

Résultat	Description
L'instruction contient des actions privilégiées qui ne sont pas limitées à {message} dans la mesure où vous en <i>Service_Name</i> êtes propriétaire. Envisagez d'étendre ces autorisations à des types de ressources spécifiques, le cas échéant, ou d'exclure les ressources détenues par AMS. Si des jokers sont utilisés, assurez-vous qu'ils correspondent<i>Resources</i>. L'instruction contient des actions de balisage de {<i>Service_Name</i>} qui ne sont pas limitées à des valeurs spécifiques pour la clé de balise Name. Envisagez de définir la portée de ces actions en définissant la clé de aws:RequestTag/Name condition avec les valeurs de votre espace de noms ou limitez ces actions en définissant la clé de aws:RequestTag/Name condition avec l'StringNot Like opérateur dont les valeurs se trouvent dans les préfixes de l'espace de noms AMS.	Ce résultat est généré si la politique autorise des actions privilégiées qui ne sont pas accordées sur vos ressources, en particulier pour les ressources nommées. Pour résoudre ce problème, examinez votre liste de ressources et vérifiez si elle ne couvre que les ressources présentes dans votre espace de noms. Vous pouvez également exclure les ressources qui se trouvent dans l'espace de noms AMS. Ce résultat est généré si la politique accorde l'autorisation de balisage pour un service donné et que l'autorisation n'est pas limitée à des clés/valeurs de balise spécifiques. Pour déterminer quelle clé ou valeur peut être utilisée dans les actions de balise, par exemple, lorsque vous demandez d'effectuer les actions, utilisez la aws:RequestTag/tag key condition. Donc, pour résoudre ce problème, utilisez cette clé de condition pour restreindre la clé ou les valeurs dans votre espace de noms. Vous pouvez également refuser la Name balise key (aws:RequestTag/Name) avec des valeurs dans l'espace de noms AMS.
Erreur interne lors de la validation de la politique de confiance des rôles IAM.	Ce résultat est généré lorsque CT Automation rencontre une erreur lors de la validation de la politique de confiance des rôles IAM via le service IAM Access Analyzer. Pour résoudre ce problème, soumettez à nouveau la RFC. Si l'erreur persiste, contactez AMS Operations pour résoudre le problème.

Résultat	Description
Erreur interne lors de la validation de la politique gérée par le client.	Ce résultat est généré lorsque CT Automatio n rencontre une erreur lors de l'ovalidation de la politique gérée par le client via le service IAM Access Analyzer. Pour résoudre ce problème, soumettez à nouveau la RFC. Si l'erreur persiste, contactez AMS Operations pour résoudre le problème.
L'analyseur d'accès est introuvable dans. <i>Région AWS</i> Impossible de vérifier l'aperçu des accès pour la politique de confiance des rôles.	Ce résultat est généré lorsque la ressource IAM Access Analyzer n'est pas trouvée dans le. Région AWS Contactez AMS Operations pour résoudre les problèmes et créer une ressource IAM Access Analyzer dans la région AWS.
Politique de confiance non valide pour le rôle <i>Role_Name</i>	Ce résultat est généré lorsque le rôle IAM fourni contient une politique de confiance non valide. Pour résoudre le problème, passez en revue la politique de confiance afin de vérifier qu'elle est valide.
IAM Access Analyzer a rencontré une erreur interne. Impossible de créer un aperçu des accès pour le rôle <i>Role_Name</i>	Ce résultat est généré lorsque l'automatisation rencontre une erreur lors de la création d'un aperçu des accès pour un rôle via l'analyse ur d'accès IAM. Pour résoudre ce problème, soumettez à nouveau la RFC. Si l'erreur persiste, contactez AMS Operations pour résoudre le problème.
Impossible de créer un aperçu de l'accès pour la politique de confiance du rôle <i>Role_Name</i>	Ce résultat est généré lorsque l'automatisation rencontre une erreur lors de la création d'un aperçu des accès pour un rôle via l'analyse ur d'accès IAM. Pour résoudre ce problème, soumettez à nouveau la RFC. Si l'erreur persiste, contactez AMS Operations pour résoudre le problème.

Résultat	Description
Erreur interne lors de la validation de l'IdP SAML répertorié.	Ce résultat est généré lorsque l'automatisation rencontre une erreur lors de la validation du SAML fourni IdPs répertorié dans la politique de confiance des rôles. Pour résoudre ce problème, soumettez à nouveau la RFC. Si l'erreur persiste, contactez AMS Operations pour résoudre le problème.
Erreur interne lors de la validation des autorisations par rapport à AWS Key Management Service.	Ce résultat est généré lorsque l'automatisation rencontre une erreur lors de la validation des autorisations AWS KMS clés dans la politique fournie. Pour résoudre ce problème, soumettez à nouveau la RFC. Si l'erreur persiste, contactez AMS Operations pour résoudre le problème.
Erreur interne lors de la validation de la politique ARNs gérée répertoriée.	Ce résultat est généré lorsque l'automatisation rencontre une erreur lors de la validation de la politique ARNs gérée répertoriée. Pour résoudre ce problème, soumettez à nouveau la RFC. Si l'erreur persiste, contactez AMS Operations pour résoudre le problème.
Erreur interne lors de la validation de la <code>customer_deny_policy</code> pièce jointe par défaut.	Ce résultat est généré lorsque l'automatisation rencontre une erreur lors de la validation de <code>customer_deny_policy</code> l'attachement au rôle. Pour résoudre ce problème, soumettez à nouveau la RFC. Si l'erreur persiste, contactez AMS Operations pour résoudre le problème.

Résultat	Description
Erreur interne lors de la validation des avertissements de politique gérés pour le rôle <i>Role_Name</i>	Ce résultat est généré lorsque l'automatisation rencontre une erreur lors de la validation de la politique gérée ARNs pour le rôle. Pour résoudre ce problème, soumettez à nouveau la RFC. Si l'erreur persiste, contactez AMS Operations pour résoudre le problème.
Erreur interne lors de la validation par <i>Policy_name</i> rapport à la politique de limites définie par le client AWSManagedServicesIAMProvisionCustomerBoundaryPolicy	Ce résultat est généré lorsque l'automatisation rencontre une erreur lors de la validation de la politique qui contient votre liste de refus personnalisée. Pour résoudre ce problème, soumettez à nouveau la RFC. Si l'erreur persiste, contactez AMS Operations pour résoudre le problème.
La politique de limites définie par le client AWSManagedServicesIAMProvisionCustomerBoundaryPolicy existe dans le compte. Cependant, la politique contient des instructions d'autorisation qui accordent des autorisations. La politique ne doit contenir que des déclarations de refus.	Ce résultat est généré lorsque la politique qui contient votre liste de refus personnalisée inclut une déclaration qui accorde l'autorisation. Bien que la liste de refus personnalisée existe dans votre compte en tant que politique gérée par IAM, elle ne peut pas être utilisée pour la gestion des autorisations. La politique ne doit contenir que des déclarations de refus indiquant que vous souhaitez qu'AMS Automated IAM Provisioning valide et refuse les actions créées par AMS Automated IAM Provisioning dans vos politiques IAM.

Résultat	Description
La déclaration contient des actions privilégiées définies par votre organisation pour Service_Name . Envisagez d'exclure ces actions par une déclaration de refus. Reportez-vous à la politique indiquée dans votre compte pour consulter la liste restreinte d'actions.	Ce résultat est généré lorsque l'automatisation détecte une action dans votre politique que vous avez définie dans la liste de refus personnalisée. Pour résoudre le problème, passez en revue votre déclaration de politique et supprimez toutes les actions définies dans votre liste de refus personnalisée ou ajoutez une déclaration de refus refusant ces actions.
Le rôle doit être POLICY_ARN attaché. Incluez l'ARN de la politique dans la liste des politiques gérées ARNs.	Ce résultat est généré si le rôle que vous créez n'est pas POLICY_ARN associé à ce rôle. Pour résoudre ce problème, incluez-le POLICY_ARN dans le ManagedPolicyArns champ du rôle et réessayez.
Ils ne POLICY_ARN peuvent pas être détachés du rôle. Incluez l'ARN de la politique dans la liste des politiques gérées ARNs.	Ce résultat est généré s'il POLICY_ARN est détaché du rôle lors d'une mise à jour. Pour résoudre ce problème, ajoutez POLICY_ARN le ManagedPolicyArns dans le champ du rôle et réessayez.

Vérification des limites des autorisations de provisionnement IAM automatisé AMS

Les vérifications des limites d'autorisation AMS vous aident à respecter la politique de limite d'autorisation par défaut fournie par AMS. Cette politique est une liste d'actions refusées par AMS Automated IAM Provisioning. Les politiques de provisionnement qui contiennent ces actions restreintes nécessitent une acceptation explicite des risques supplémentaire. Téléchargez la politique ici : [boundary-policy.zip](#).

Utilisez les vérifications de politique de limites d'autorisation définies par le client pour personnaliser les actions de refus au-delà des valeurs par défaut de la politique de limite d'autorisation AMS. Lorsque vous intégrez AMS Automated IAM Provisioning à l'aide du type de modification suivant : Gestion | Compte géré | AMS Automated IAM Provisioning avec autorisations de lecture-écriture | [Activer \(révision requise\) \(ct-1706xvvk6j9hf\)](#), vous pouvez inclure une liste d'actions de refus personnalisées qui spécifient des actions restreintes supplémentaires.

Vous pouvez mettre à jour la liste des actions de refus à l'aide du type de modification : Gestion | Compte géré | Provisionnement IAM automatisé avec autorisations de lecture-écriture | [Mettre à jour la liste de refus personnalisée \(ct-2r9xvd3sdsic0\)](#). Vous devez utiliser le rôle IAM dédié `AWSTrajectoryIAMProvisionAdminRole` pour exécuter ce type de modification.

 Note

- Vous devez fournir une liste complète des actions de refus pour chaque mise à jour. La liste précédente est remplacée par la nouvelle liste.
- La liste des actions de refus ne doit contenir que les actions à refuser. Les actions d'autorisation ne sont pas prises en charge.
- La liste des actions de refus se trouve dans le compte sous la forme d'une politique gérée par IAM nommée `AWSTrajectoryIAMProvisionCustomerBoundaryPolicy`. La politique ne doit être attachée à aucun rôle.
- Le terme limite d'autorisation utilisé pour désigner les actions refusées dans AMS Automated IAM Provisioning a une signification contextuelle différente de celle de la limite d'autorisation IAM. La limite d'autorisation IAM définit l'autorisation maximale qu'une politique peut accorder lors de l'exécution à une entité IAM. Pour plus d'informations sur les limites d'autorisation IAM, consultez la section [Types de politiques](#) dans le guide de AWS Identity and Access Management l'utilisateur. La limite d'autorisation dans AMS Automated IAM Provisioning vous empêche de configurer une politique IAM contenant un certain ensemble d'autorisations, par exemple une liste d'actions refusées.

Résolution des problèmes et des erreurs liés au provisionnement IAM automatisé d'AMS

Vous pouvez rencontrer des problèmes de trois manières lors de l'utilisation d'AMS Automated IAM Provisioning :

- Erreurs RFC : elles peuvent se produire pour diverses raisons, par exemple une saisie incorrecte. Pour de plus amples informations, veuillez consulter [Résolution des erreurs RFC dans AMS](#).
- Erreurs SSM : elles peuvent se produire pour diverses raisons, par exemple un mauvais formatage. Pour plus d'informations, consultez la section [Résolution des problèmes liés à l'automatisation de Systems Manager](#).

- Résultats des contrôles de validation : ils se produisent lorsque l'un des nombreux contrôles de validation exécutés par Automated IAM Provisioning détecte un problème. Pour obtenir la liste des contrôles de validation et des actions recommandées pour les corriger, consultez [Contrôles d'exécution pour le provisionnement IAM automatisé d'AMS dans AMS](#).

Configuration des autorisations dans AMS à l'aide de rôles et de profils IAM

AMS utilise AWS Identity and Access Management (IAM) pour gérer les utilisateurs, des informations d'identification de sécurité telles que les clés d'accès et des autorisations qui contrôlent les AWS ressources auxquelles les utilisateurs et les applications peuvent accéder. AMS fournit un rôle d'utilisateur IAM par défaut et un profil d' EC2 instance Amazon par défaut (qui inclut une déclaration autorisant l'accès aux ressources au rôle d'utilisateur IAM par défaut).

Demande d'un nouveau rôle d'utilisateur IAM ou d'un nouveau profil d'instance

AMS utilise un rôle IAM pour définir les autorisations des utilisateurs via votre service de fédération et un profil d'instance IAM en tant que conteneur pour ce rôle IAM.

Vous pouvez demander un rôle IAM personnalisé avec le type de changement Deployment | Advanced stack components | Identity and Access Management (IAM) | Créer une entité ou une politique (révision requise) (ct-3dpg8mdd9jn1r), ou un profil d'instance IAM avec Management | Applications | Profil d'instance IAM | Créer une gestion | Applications | Profil d'instance IAM | Créer un type de modification (révision requise) (ct-00 (ixp4ch2tiu04). Consultez leur description dans cette section.

Note

AMS applique une politique IAM `customer_deny_policy` qui bloque les espaces de noms et les actions dangereux. Cette politique est attachée par défaut à tous les rôles des clients AMS et pose rarement problème aux utilisateurs. Vos demandes d'utilisateur et de rôle IAM n'incluent pas cette politique, mais l'inclusion automatique des demandes de `customer_deny_policy` rôles IAM permet à AMS de déployer de nouveaux profils d'instance IAM plus rapidement. Vous pouvez demander l'exclusion de cette

`customer_deny_policy` politique. Cependant, cette demande fera l'objet d'un examen de sécurité approfondi et sera probablement refusée pour des raisons de sécurité.

Limitez les autorisations avec des déclarations de politique de rôle IAM

AMS utilise un rôle IAM pour définir les autorisations des utilisateurs via votre service de fédération.

Zone d'accueil à compte unique AMS : voir [SALZ : Rôles d'utilisateur IAM par défaut](#).

Zone d'accueil multi-comptes AMS : voir [MALZ : Rôles des utilisateurs IAM par défaut](#).

Un rôle IAM est une entité IAM qui définit un ensemble d'autorisations pour effectuer des demandes de AWS service. Les rôles IAM ne sont pas associés à un utilisateur ou à un groupe spécifique. Les entités de confiance assument plutôt des rôles, tels que les utilisateurs IAM, les applications ou les AWS services tels qu'Amazon EC2. Pour en savoir plus, consultez [Rôles IAM](#).

Vous pouvez définir la politique souhaitée pour un utilisateur assumant le rôle d'utilisateur AMS IAM en utilisant l'opération d'API AWS Security Token Service (STS) [AssumeRole](#) en transmettant une politique IAM plus restrictive dans le champ de Policy demande.

Des exemples de déclarations de politique que vous pouvez utiliser pour restreindre l'accès à la tomodynamométrie sont fournis ci-dessous.

À l'aide des groupes Active Directory (AD) que vous avez configurés et du fonctionnement de l'API AWS Security Token Service (STS) [AssumeRole](#), vous pouvez définir des autorisations pour certains utilisateurs ou groupes, notamment en restreignant l'accès à certains types de modifications (CTs). Vous pouvez utiliser les déclarations de politique ci-dessous pour restreindre l'accès à la tomodynamométrie de différentes manières.

Instruction de type de modification AMS dans le profil d'instance IAM par défaut qui permet d'accéder à tous les appels d'API AMS (`amscm` et `amsskms`) et à tous les types de modification :

```
{
  "Sid": "AWSManagedServicesFullAccess",
  "Effect": "Allow",
  "Action": [
    "amscm:*",
    "amsskms:*"
  ],
  "Resource": [
```

```

    "*"
  ]
}

```

1. Déclaration autorisant l'accès et toutes les actions pour deux applications spécifiées uniquement CTs, où « Action » correspond aux opérations de l'API AMS (amscmou bienamsskms), et « Ressource » représente le type de modification IDs et le numéro de version existants :

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "amscm:*",
      "Resource": [
        "arn:aws:amscm:*:*:changetype/ct-ID1:1.0",
        "arn:aws:amscm:*:*:changetype/ct-ID2:1.0"
      ]
    }
  ]
}

```

2. Déclaration autorisant l'accès pour CreateRfc UpdateRfc, et SubmitRfc sur les deux seules données spécifiées CTs :
3. Déclaration autorisant l'accès pour CreateRfc UpdateRfc, et SubmitRfc sur tous les éléments disponibles CTs :
4. Déclaration visant à refuser l'accès à toutes les actions relatives à la tomodensitométrie restreinte et à n'en autoriser aucune autre CTs :

Restreindre les autorisations avec les profils d'instance Amazon EC2 IAM

Un profil d'instance IAM est un conteneur pour un rôle IAM que vous pouvez utiliser pour transmettre des informations de rôle à une EC2 instance Amazon lorsque celle-ci démarre.

Il existe actuellement un profil d'instance par défaut AWS Managed Services (AMS) qui accorde des autorisations aux applications exécutées sur l'instance, et non aux utilisateurs qui se connectent à l'instance. `customer-mc-ec2-instance-profile` Vous souhaitez peut-être modifier le profil

d'instance par défaut, ou en créer un nouveau, si vous souhaitez donner à une instance l'accès à quelque chose, sans accorder l'accès à d'autres instances également. Vous pouvez demander un nouveau profil d'instance IAM via le lien [Gestion | Applications | Profil d'instance IAM | Créer un type de modification \(ct-0ixp4ch2tiu04\)](#). Lorsque vous soumettez la RFC, vous pouvez créer votre propre profil d'instance et l'inclure dans le fichier `InstanceProfileDescription`, ou vous pouvez simplement informer AMS (en utilisant le même champ) des modifications que vous souhaitez apporter. Comme il s'agit d'un scanner manuel, AMS doit approuver le changement et vous contactera à ce sujet.

Si vous ne connaissez pas les politiques Amazon IAM, consultez la section [Présentation des politiques IAM](#) pour obtenir des informations importantes. Il existe également un bon article de blog intitulé [Demystifying EC2 Amazon Resource-Level Permissions](#). Notez qu'AMS ne prend actuellement pas en charge le contrôle d'accès basé sur les ressources, mais prend en charge les contrôles au niveau des ressources à l'aide de politiques de rôle IAM (pour une explication de la différence, voir [AWS Services](#) qui fonctionnent avec IAM).

Zone d'atterrissage à compte unique AMS :

Pour consulter un tableau des autorisations accordées par le profil d'instance AMS IAM par défaut, accédez à Profil d'[instance EC2 IAM](#).

Règle de réclamation AD FS et paramètres SAML

ActiveDirectory Règle de réclamation des services de fédération (AD FS) et paramètres SAML pour AWS Managed Services (AMS)

Pour step-by-step obtenir des instructions détaillées sur l'installation et la configuration d'AD FS, voir [Activation de la fédération sur AWS à l'aide de Windows Active Directory, ADFS et SAML 2.0](#).

Configurations des règles de réclamation ADFS

Si vous disposez déjà d'une implémentation ADFS, configurez les éléments suivants :

- Fier sur la confiance des parties
- Règles relatives aux réclamations

Les règles relatives à la confiance et aux réclamations des parties fiables sont décrites dans le blog [Enabling Federation to AWS Using Windows Active Directory, AD FS et SAML 2.0](#)

- Règles relatives aux réclamations :

- Nameid : Configuration par article de blog
- RoleSessionName: configurez comme suit
 - Nom de la règle de réclamation : **RoleSessionName**
 - Boutique d'attributs : **Active Directory**
 - Attribut LDAP : **SAM-Account-Name**
 - Type de réclamation sortante : **https://aws.amazon.com/SAML/Attributes/RoleSessionName**
- Obtenir des groupes AD : configuration par article de [blog](#)
- Réclamation de rôle : configurez comme suit

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([^\d]{12})-"]
```

```
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =  
  RegExReplace(c.Value, "AWS-([^\d]{12})-", "arn:aws:iam::$1:saml-provider/  
  customer-readonly-saml,arn:aws:iam::$1:role/"));
```

console Web

Vous pouvez accéder à la console Web AWS en utilisant le lien ci-dessous en le **[ADFS-FQDN]** remplaçant par le nom de domaine complet de votre implémentation ADFS.

https :**[ADFS-FQDN]**//adfs/ls/IdpInitiatedSignOn.aspx

Votre service informatique peut déployer le lien ci-dessus auprès de la population d'utilisateurs via une politique de groupe.

Accès à l'API et à la CLI avec SAML

Comment configurer l'accès à l'API et à la CLI avec SAML

Les packages python proviennent des articles de blog ci-dessous :

- NTLM : [Comment implémenter un accès fédéré à l'API et à la CLI à l'aide de SAML 2.0 et d'AD FS](#)
- Formulaires : [comment implémenter une solution générale d' API/CLI accès fédéré à l'aide de SAML 2.0](#)

- PowerShell: [Comment configurer un accès d'API fédéré à AWS à l'aide de Windows PowerShell](#)

Configuration du script

1. À l'aide de Notepad++, remplacez la région par défaut par la bonne région
2. À l'aide de Notepad++, désactivez la vérification SSL pour les environnements de test et de développement
3. À l'aide de Notepad++, configurez idpentryurl

```
https://[ADFS-FDQN]/adfs/ls/IdpInitiatedSignOn.aspx?  
loginToRp=urn:amazon:webservices
```

Configuration de Windows

Les instructions ci-dessous concernent les packages python. Les informations d'identification générées seront valides pendant 1 heure.

1. [Téléchargez et installez Python \(2.7.11\)](#)
2. [Téléchargez et installez les outils de la CLI AWS](#)
3. Installez l'AMS CLI :
 - a. Téléchargez le fichier zip des distribuables AMS fourni par votre gestionnaire de prestation de services cloud (CSDM) et décompressez-le.

Plusieurs répertoires et fichiers sont mis à disposition.

- b. Ouvrez le répertoire Managed Cloud Distribuables -> CLI -> Windows ou Managed Cloud Distribuables -> CLI -> Linux/ macOS, selon votre système d'exploitation, et :

Pour Windows, exécutez le programme d'installation approprié (cette méthode ne fonctionne que sur les systèmes Windows 32 ou 64 bits) :

- 32 bits : ManagedCloud API_x86.msi
- 64 bits : ManagedCloud API_x64.msi

Pour Mac/Linux, exécutez le fichier nommé : MC_CLI.sh. Vous pouvez le faire en exécutant cette commande : `sh MC_CLI.sh`. Notez que les répertoires amscm et amsskms ainsi que leur contenu doivent se trouver dans le même répertoire que le fichier MC_CLI.sh.

- c. Si les informations d'identification de votre entreprise sont utilisées via la fédération avec AWS (configuration par défaut d'AMS), vous devez installer un outil de gestion des informations d'identification qui peut accéder à votre service de fédération. Par exemple, vous pouvez utiliser ce blog de sécurité AWS consacré à la [mise en œuvre d'un accès fédéré aux API et CLI à l'aide de SAML 2.0 et d'AD FS](#) pour vous aider à configurer vos outils de gestion des informations d'identification.
 - d. Après l'installation, lancez `aws amscm help` et consultez `aws amsskms help` les commandes et les options.
4. Téléchargez le script SAML requis

Téléchargez vers `c:\aws\scripts`
 5. [Télécharger PIP](#)

Téléchargez vers `c:\aws\downloads`
 6. Utilisation PowerShell, installation de PIP

`<pythondir>. \ python.exe c:\aws\downloads\get -pip.py`
 7. Utilisation PowerShell et installation du module boto

`boto d'<pythondir \ scripts> installation pip`
 8. Utilisation PowerShell du module de demandes d'installation

`demandes d'<pythondir \ scripts> installation pip`
 9. Utilisation PowerShell et installation du module de sécurité des demandes

`<pythondir \ scripts>requêtes d'installation pip [sécurité]`
 10. Utilisation PowerShell et installation du module BeautifulSoup

`<pythondir \ scripts>pip install beautifulsoup4`
 11. En utilisant PowerShell, créez un dossier appelé `.aws` dans le profil de l'utilisateur (`%userprofile%\ .aws`)

`mkdir .aws`
 12. À l'aide de PowerShell, créez un fichier d'identification dans le dossier `.aws`

Informations d'identification du nouvel article : fichier de type `—force`

Le fichier d'informations d'identification ne doit pas avoir d'extension de fichier

Le nom du fichier doit être entièrement en minuscules et contenir les informations d'identification du nom.

13. Ouvrez le fichier d'informations d'identification avec le bloc-notes et collez les données suivantes en spécifiant la bonne région

```
[default]
output = json
region = us-east-1
aws_access_key_id =
aws_secret_access_key =
```

14. Utilisation PowerShell du script SAML et de l'ouverture de session

<pythondir>. \ python.exe c:\aws\scripts\samlapi.py

Nom d'utilisateur : [USERNAME] @upn

Choisissez le rôle que vous souhaitez assumer

Configuration de Linux

Les informations d'identification générées seront valides pendant 1 heure.

1. À l'aide de WinSCP, transférez le script SAML
2. À l'aide de WinSCP, transférez le certificat Root CA (ignorez-le pour le test et le développement)
3. Ajoutez l'autorité de certification ROOT aux certificats racines sécurisés (à ignorer pour le test et le développement)

\$ openssl x509 -inform der -in [certname] .cer -out certificate.pem (ignorer pour le test et le développement)

Ajoutez le contenu de certificate.pem à la fin du fichier/etc/ssl/certs/ca-bundle.crt (à ignorer pour le test de développement)

4. Créez un dossier .aws dans home/ec2-user 5

```
[default]
output = json
```

```
region = us-east-1
aws_access_key_id =
aws_secret_access_key =
```

5. À l'aide de WinSCP, transférez le fichier d'informations d'identification dans le dossier .aws
6. Installer le module de démarrage

```
$ sudo pip install boot
```

7. Module de demandes d'installation

```
Demandes d'installation de $ sudo pip
```

8. Installer le module beautifulsoup

```
$ sudo pip install beautifulsoup4
```

9. Copiez le script dans home/ec2-user

Définissez les autorisations requises

Exécutez le script : samlapi.py

Restreindre avec l'ACL réseau

Une liste de contrôle d'accès réseau (NACL) est une couche de sécurité optionnelle pour votre VPC qui agit comme un pare-feu pour contrôler le trafic entrant et sortant d'un ou de plusieurs sous-réseaux. Vous pouvez configurer un réseau ACLs avec des règles similaires à celles de vos groupes de sécurité afin d'ajouter une couche de sécurité supplémentaire à votre VPC. Pour plus d'informations sur les différences entre les groupes de sécurité et le réseau ACLs, voir [Comparaison des groupes de sécurité et du réseau ACLs](#).

Toutefois, dans la zone d'atterrissage multi-comptes gérée par AMS, afin qu'AMS puisse gérer et surveiller efficacement l'infrastructure, l'utilisation de NACLs est limitée aux domaines suivants :

- NACLs ne sont pas pris en charge dans les comptes multi-comptes Landing Zone Core, à savoir le compte de gestion, le réseau, les services partagés, la journalisation et la sécurité.
- NACLs sont pris en charge dans les comptes d'applications multi-comptes Landing Zone, à condition qu'ils ne soient utilisés que comme liste « à refuser » et qu'ils portent la mention « Tout autoriser » pour permettre les opérations de surveillance et de gestion d'AMS.

Dans les environnements multi-comptes à grande échelle, vous pouvez également tirer parti de fonctionnalités telles que les pare-feux de sortie centralisés pour contrôler le trafic sortant et/ou les tables de routage AWS Transit Gateway dans la zone d'atterrissage multi-comptes AMS pour séparer le trafic réseau entre les différents VPCs

AMS sur Outposts

[AWS Outposts](#) est une solution matérielle gérée qui étend les zones d'atterrissage gérées par AMS aux centres de données des clients. Avec le support AMS activé AWS Outposts, les clients qui recherchent l'expertise cloud, les économies de coûts et la plate-forme standardisée proposées par AMS ne sont plus limités à l'hébergement de ressources internes Régions AWS. Avec AMS activé AWS Outposts, les clients ayant des exigences sur site peuvent désormais se moderniser AWS, tout en profitant des services d'application de correctifs, de sauvegarde, de provisionnement, de gestion des incidents, de continuité des activités et d'optimisation des coûts proposés par AMS.

Une fois qu'un compte AWS Outposts est activé dans votre compte AMS Multi-Account Landing Zone ou Single Account Landing Zone, vous pouvez suivre les processus de gestion des modifications AMS existants pour provisionner et gérer les AWS ressources. L'infrastructure hébergée par AMS peut être gérée en spécifiant votre sous-réseau spécifique AWS Outposts. AWS Outposts les cycles de vie peuvent être gérés directement dans la AWS Outposts console à l'aide du rôle de services d'AWS Outposts auto-provisionnement.

Pour plus d'informations sur le rôle, consultez [AWS Outposts](#).

AWS Outposts gestion de l'installation et des opérations

Le AWS Outposts processus d'intégration à AMS on comprend :

1. Planification des Outposts
2. Validation de commande
3. L'intégration d'Outposts à AMS
4. La gestion du cycle de vie

AWS Outposts planification

Au cours de AWS Outposts la planification, vous identifiez AMS sur les cas AWS Outposts d'utilisation et vous impliquez les principales parties prenantes, y compris l'équipe chargée de votre compte AMS et les AWS Outposts représentants, afin de vous aligner sur la stratégie de capacité.

1. Une fois que les cas d'utilisation nécessitant l'activation AWS Outposts d'AMS ont été identifiés, demandez à l'équipe de votre compte AMS de discuter de la planification des capacités.
2. Une fois que vos besoins en AWS Outposts capacité ont été déterminés, l'équipe de votre compte AMS engage l'équipe de AWS Outposts service pour discuter du plan AWS Outposts d'intégration, des rôles et des responsabilités. Pendant cette période, un point de contact AWS Outposts unique (SPOC) vous est attribué. Le AWS Outposts SPOC aide à finaliser les exigences de AWS Outposts dimensionnement.

AWS Outposts validation de commande

Lors de la validation de la commande, vous créez un AWS Outposts site et vous commandez la capacité requise directement dans la AWS Outposts console ou par l'intermédiaire du représentant de votre AWS Outposts compte.

Une fois que vous, l'équipe chargée du compte AMS et l' AWS Outposts équipe êtes sur la même longueur d'onde, vous pouvez demander le rôle de service AWS Outposts auto-approvisionné en utilisant l'identifiant de type `ct-3qe6io8t6jtny`, afin de créer votre site et de passer commande directement dans la console. AWS Outposts AWS Outposts

Vous pouvez également utiliser le AWS Outposts SPOC pour créer des sites Outpost et des commandes. Votre AWS Outposts SPOC reste chargé de fournir des mises à jour de statut à vous et à l'équipe chargée du compte AMS lors de la validation du site et des commandes, ainsi que de AWS Outposts l'installation.

AWS Outposts intégration à AMS

Une fois votre AWS Outposts unité activée dans votre VPC géré par AMS, vous pouvez demander que des moniteurs soient créés pour suivre la disponibilité, la capacité, les exceptions et la connectivité réseau de votre matériel Outposts. En suivant les étapes de déploiement de la surveillance décrites ci-dessous, votre AWS Outposts matériel est activement surveillé par AMS.

1. Une fois votre AWS Outposts système installé et activé, vous pouvez demander une surveillance AWS Outposts spécifique en soumettant le modèle suivant avec une RFC en utilisant le type de modification Management | Other | Other | Create (`ct-1e1xtak34nx76`). Les opérations AMS garantissent le suivi du AWS Outposts sous-réseau dans l'outillage interne d'AMS.
 - AWS Outposts ID
 - Bloc d'adresse CIDR du sous-réseau

- AWS Outposts Alarmes recommandées :
 - InstanceFamilyCapacityAvailabilityAlert
 - InstanceTypeCapacityAvailabilityAlert
 - EBSVolumeTypeCapacityAvailabilityAlert
 - CapacityExceptionsAlert
 - Direct Connect ConnectionAlert
- Pour chacune des alertes ci-dessus, spécifiez les paramètres suivants :
 - Une statistique (« moyenne ») est recommandée. Les autres options incluent la somme, le maximum, le minimum, le nombre d'échantillons et p90)
 - Période (« 5 minutes ») est recommandée. Les autres options incluent 10 et 30 secondes, 1, 5 et 15 minutes, 1 et 6 heures et 1 jour)
 - Le type de seuil (« statique ») est recommandé. Les « anomalies » sont également des options.)
 - Condition (« Chaque fois que le nombre d'appels est supérieur à », « égal à », « inférieur à » sont également des options.)
 - La valeur de condition (« 25 % ») est configurée par défaut. Un autre entier positif est autorisé.)
 - Sujet de notification (les sujets relatifs aux opérations AMS) sont automatiquement attribués. Cependant, tout autre sujet, ou personnalisé, peut également être ajouté.)

2. Surveillance et support aux opérations

- Les opérations AMS surveillent les AWS Outposts mesures relatives à la déconnexion du réseau ou aux défaillances des composants. AMS Operations fournit des services de première réponse en cas de AWS Outposts problème et passe, si nécessaire, au support Premium ou au EC2 support.
- AMS Operations est disponible pour résoudre les problèmes liés à votre AWS Outposts unité.

3. Lorsque les vérifications de l'état de l' EC2 instance ou de l'état du système échouent, les opérations AMS suivent les processus existants pour remettre l'instance en ligne. Si le redémarrage échoue ou si la AWS Outposts capacité est insuffisante, un membre de l'équipe des opérations AMS vous en informe directement pour déterminer les prochaines étapes.

AWS Outposts gestion du cycle de vie

Une fois que vous avez AWS Outposts été intégré à votre compte AMS, vous êtes averti en cas d'exception de disponibilité, de capacité ou de réseau. Vous pouvez le mettre hors service AWS Outposts directement par le biais de la AWS Outposts console ou du AWS Outposts SPOC.

Vous pouvez gérer AWS Outposts directement dans la AWS Outposts console à l'aide du rôle de AWS Outposts service de provisionnement en libre-service ou du mode développeur. Vous pouvez également en faire la demande AWS Outposts par le biais de votre CSDM, ou point de contact AWS Outposts unique (SPOC).

La haute disponibilité AWS Outposts peut être atteinte en déployant deux unités ou plus AWS Outposts. La configuration de deux ou plus AWS Outposts active l'option de zone de multidisponibilité pour vos instances Amazon Relational Database Service.

Provisionnement de ressources gérées par AMS sur AWS Outposts

Le provisionnement AWS des ressources hébergées sur AWS Outposts (par exemple, Amazon EC2, Amazon EMR, Amazon EKS, Amazon ECS, Amazon EBS et Amazon S3) dans des comptes AMS (comptes Single Account Landing Zone, Multi-Account Landing Zone et Accelerate) est soumis aux mêmes niveaux de support AMS que les ressources dans. Régions AWS Vous pouvez utiliser la gestion des modifications AMS, les services de provisionnement en libre-service ou le mode développeur pour créer et modifier les ressources créées sur. AWS Outposts

Actuellement, tous les types d'instances (M5/M5d, C5/C5d, R5/R5d, i3en, G4dn), Amazon Elastic Block Store, Amazon Elastic Container Service, Amazon Elastic Kubernetes Service, Amazon Elastic Kubernetes Service, Amazon Elastic Load Balancers et le proxy App Mesh Envoy sont disponibles directement sur. DBs AWS Outposts Ces ressources sont éligibles au même soutien aux opérations AMS que les ressources des régions existantes.

Limitations d'AMS sur AWS Outposts

- Le support opérationnel pour les ressources AWS Outposts hébergées dépend de la cohérence de la connectivité réseau. AWS Outposts la déconnexion du réseau empêche les opérations AMS de résoudre les incidents ou les problèmes survenant sur l'unité déconnectée AWS Outposts . Pour AMS sur les imprévus relatifs aux niveaux de AWS Outposts service, consultez les [accords de niveau de AWS service mis à jour \(\) SLAs](#).
- Amazon Relational Database Service :

- Le type de modification create RDS (ct-2z60dyvto9g6c) active par défaut le multi-AZ et nécessite un groupe de sous-réseaux de base de données. Les groupes de sous-réseaux de base de données nécessitent deux sous-réseaux dans deux zones de disponibilité (AZ) distinctes. Si vous n'en avez qu'un AWS Outposts, la création d'un groupe de sous-réseaux de base de données pose problème car il AWS Outposts n'est attribué qu'à une seule AZ. Pour contourner cette limitation, suivez les instructions suivantes :
 1. Demandez un groupe de sous-réseaux de base de données via une RFC avec un CT Management | Other | Other, et spécifiez le sous-réseau sur le. AWS Outposts
 2. Créez un modèle CFN personnalisé sur AWS Outposts lequel déployer RDS et spécifiez le groupe de sous-réseaux créé à l'étape précédente. Pour en savoir plus sur cette procédure, consultez la section [Ressources personnalisées](#).
 3. Demandez à AMS de déployer le modèle CFN contenant l'instance RDS cible via le CT d'ingestion AMS CFN (ct-36cn2avfrj9v).
 4. Notez qu'actuellement, RDS for AWS Outposts ne fournit pas de métriques ni de journaux en raison d'une limitation du service RDS.
- Workload ingest (WIGs) : Linux WIGs ne fonctionne que si la WIGs EC2 pré-instance se trouve sur un autre AWS Outposts sous-réseau. La raison en est que Linux WIGs crée un WIGs nœud dans le sous-réseau de la première EC2 instance en utilisant m4.large, par défaut. Comme AWS Outposts il n'a pas ce type d'instance, WIGs il n'est pas en mesure de lancer son nœud de travail. La solution consiste à créer l' EC2 instance initiale dans un sous-réseau autre que le AWS Outposts sous-réseau, puis à créer l'instance cible. AWS Outposts De plus, actuellement, seuls les types d' EC2 instances basés sur Nitro, notamment C5, C5d, M5, M5d, R5, R5d, G4 et i3en, sont pris en charge sur. AWS Outposts
- Amazon Elastic Block Store (EBS) : Create EBS Volume CT (ct-16xg8qguovg2w) ne fonctionne pas, car les volumes sont créés au lieu du fait que nous AWS Outposts ne fournissons pas le numéro de ressource Amazon (ARN) AWS comme paramètre d'entrée au CT. AWS Outposts
- Connectivité réseau : La connectivité réseau relève de votre responsabilité au AWS Outposts sein de l'équipe.
- Brownfield et prise de contrôle de compte : les comptes AWS Outposts activés dans des comptes autres qu'AMS ne peuvent pas être transférés vers AMS, en raison de la nature de la AWS Outposts facturation et des exigences de support de l'entreprise.

AMS sur la AWS Outposts conformité

AMS sur l'attestation AWS Outposts de conformité

AWS Outposts le plan de contrôle a été certifié conforme à la norme HIPAA, aux normes PCI et ISO. Cependant, la présence d'AMS sur le plan de AWS Outposts contrôle n'a pas été attestée. AWS Outposts Pour cette raison, les clients sont invités à obtenir une attestation de conformité AMS en matière d' AWS Outposts environnement.

Pour contrôler la création de ressources dans l'unité Outpost, les clients sont invités à séparer l'accès des développeurs à l'Outpost, afin d'éviter un accès excessif aux développeurs dans les comptes gérés par AMS standard.

Charges de travail gérées par AMS nécessitant la conformité à FedRAMP

Avant tout, les comptes de gestion AMS doivent d'abord être évalués pour vérifier leur conformité réglementaire, car les données du plan de contrôle seraient transmises AWS Outposts aux comptes de gestion AMS.

Si la certification FedRAMP est requise et que la structure du compte AMS est conforme, il est recommandé de faire appel à un fournisseur de centre de données qui possède déjà la certification requise et possède l'ensemble de l'appliance Service Link (ou qui chiffre déjà les données de sortie).

Enfin, une protection supplémentaire des données peut être mise en place en travaillant avec l'équipe chargée de votre compte pour déployer un SCP qui limite les données au compte hébergeant l' AWS Outposts Outpost et empêche la création de ressources locales dans le compte hébergeant l'Outpost.

Impact sur la conformité existante pour les comptes AMS

Il n'est AWS Outposts pas nécessaire de tester à nouveau la conformité d'un compte tant qu'aucune donnée réglementée n'est consommée et que le compte est séparé logiquement. Les comptes de gestion AMS peuvent gérer des comptes non réglementés et réglementés à condition que les flux de données entre comptes authentication/authorization et entrées/sorties soient séparés. VPCs Par conséquent, même si le compte Outpost non conforme et les comptes d'application conformes existants appartiennent à la même organisation (y compris les services partagés, le réseau, la journalisation, le master et les services AMS de sécurité), le compte de l'application de conformité reste conforme puisque les données sont séparées logiquement.

AMS activé AWS Outposts FAQs

Quels sont les cas d'utilisation éligibles au support AMS AWS Outposts ?

AMS on AWS Outposts peut être utilisé par les entreprises qui ont besoin d'un modèle d'exploitation cloud éprouvé, dont les charges de travail nécessitent une faible latence (par exemple, gestion des robots d'usine et migration des ordinateurs centraux), de l'informatique de pointe (par exemple, des postes de travail distants et une rationalisation des données de pointe) et des charges de transfert de données importantes.

Pourquoi utiliser cette fonctionnalité ?

AMS assure la surveillance du AWS Outposts matériel et fournit une première réponse à tout problème AWS Outposts matériel. En outre, les fonctionnalités de support suivantes pour toutes les ressources gérées hébergées sur AWS Outposts :

- Journalisation, surveillance, garde-corps et gestion des événements
- Gestion de la continuité
- Gestion de la sécurité et des accès
- Gestion des correctifs
- Gestion des modifications
- Gestion automatisée et en libre-service du provisionnement
- Gestion des incidents et des problèmes
- Création de rapports (les rapports relatifs au AWS Outposts matériel ne seront pas initialement pris en charge avec AMS activé AWS Outposts)
- Gestion des demandes de service
- Mode développeur
- Support aux entreprises

Comment utiliser cette fonctionnalité ?

AWS Outposts planification : Au cours de AWS Outposts la planification, vous avez identifié les cas d' AWS Outposts utilisation d'AMS et vous mobiliserez les principales parties prenantes, notamment l'équipe chargée des comptes AMS et les AWS Outposts représentants, afin de vous aligner sur la stratégie de capacité.

Validation des commandes : lors de la validation des commandes, vous créez un AWS Outposts site et vous commandez la capacité requise directement dans la AWS Outposts console ou par l'intermédiaire du responsable de votre AWS Outposts compte.

AWS Outposts intégration à AMS : une fois que votre AWS Outposts unité est activée dans votre VPC géré par AMS, vous pouvez demander à être intégrée à AWS Outposts votre compte AMS en soumettant une demande de modification (RFC) à l'aide du modèle figurant dans le guide de l'utilisateur AMS (). [AWS Outposts](#) AMS Operations crée ensuite un sous-réseau et surveille votre Outpost à l'aide des entrées fournies sur le RFC.

Gestion du cycle de vie : une fois que vous avez AWS Outposts été intégré à votre compte AMS, vous êtes informé de toute exception de disponibilité, de capacité ou de réseau. Vous pouvez mettre le service hors service AWS Outposts directement par le biais de la AWS Outposts console ou de votre point de contact AWS Outposts unique (SPOC).

Quelles sont les limites de l'AMS AWS Outposts ?

Les cas d'utilisation relatifs à la résidence des données (par exemple, lois de localisation des données spécifiques à un pays, etc.) n'ont pas encore été validés pour AMS on AWS Outposts.

AWS Outposts les comptes activés dans des comptes autres qu'AMS ne peuvent pas être transférés vers AMS, en raison de la nature de la AWS Outposts facturation et des exigences du Support aux entreprises.

AWS Outposts le plan de contrôle a été certifié conforme à la norme HIPAA, aux normes PCI et ISO. Cependant, la présence d'AMS sur le plan de AWS Outposts contrôle n'a pas été attestée. AWS Outposts Pour cette raison, les clients sont invités à obtenir une attestation de conformité AMS en matière d' AWS Outposts environnement.

Puis-je me désinscrire de cette fonctionnalité ?

Le provisionnement AWS Outposts dans votre environnement AMS est facultatif. Une fois déployé sur votre compte AMS, il AWS Outposts peut être déprovisionné via la AWS Outposts console à tout moment, s'il n'est plus nécessaire.

Comment AWS Outposts sera facturé AMS on ?

L'augmentation des AWS Outposts frais par AMS sera appliquée au niveau du groupe B.

Comment le contrat de niveau de service AMS sera-t-il modifié pour s'adapter AWS Outposts ?

La gestion des incidents dépendra de AWS Outposts la disponibilité. AWS Outposts la disponibilité dépend de la disponibilité du réseau du client, qui relève de la responsabilité du client. AWS Outposts la disponibilité dépend également de la disponibilité AWS Outposts du matériel, qui dépend des accords de niveau AWS Outposts de service.

Voir aussi [AWS Outposts FAQs](#).

Utilisation de balises dans AMS

Rubriques

- [Marquage automatique de l'infrastructure AMS](#)
- [Tags recommandés par AMS](#)
- [Étiqueter les notes de mise à jour](#)

Fournir des tags peut s'avérer très utile. Pour obtenir des informations détaillées, consultez [Tagging Your Amazon EC2 Resources](#).

RFCs qui créent des instances, telles qu'un bucket Amazon S3 ou un AWS Elastic Load Balancer (ELB), fournissent généralement un schéma qui vous permet d'ajouter jusqu'à sept balises (paires clé/valeur) ; vous pouvez ajouter d'autres balises à votre compartiment S3 en soumettant un Management | Advanced stack components | Amazon S3 storage | Update CT. Amazon EC2, Amazon EFS, Amazon RDS et les schémas à plusieurs niveaux (HA Two-Tiered et HA One-Tiered) autorisent jusqu'à cinquante balises. Les balises sont spécifiées dans la ExecutionParameters partie du schéma.

Lorsque vous utilisez la console AMS, vous devez activer la vue de configuration supplémentaire afin d'ajouter des balises.

Tip

De nombreux schémas de tomographie comportent un Name champ Description et situé en haut du schéma. Ces champs sont utilisés pour nommer la pile ou le composant de pile, ils ne nomment pas la ressource que vous créez. Certains schémas proposent un paramètre pour nommer la ressource que vous créez, d'autres non. Par exemple, le schéma CT pour Create Amazon EC2 stack ne propose pas de paramètre pour nommer l' EC2 instance Amazon. Pour ce faire, vous devez créer une balise avec la clé « Nom » et la valeur que vous souhaitez donner au nom. Si vous ne créez pas une telle balise, votre EC2 instance Amazon s'affiche dans la EC2 console Amazon sans attribut de nom.

Y a-t-il des restrictions relatives aux tags ? Oui

- Les balises sont sensibles à la casse.
- La longueur de clé maximale est de 128 caractères Unicode.

- La longueur de valeur maximale est de 256 caractères Unicode.
- Le nombre maximum d'identifications par ressource est de 50.
- Le préfixe réservé est aws : .
- Les noms et les valeurs de balises générées par AWS reçoivent automatiquement le préfixe aws : , que vous ne pouvez pas attribuer. Les noms des balises définies par l'utilisateur ont le préfixe user : dans le rapport de répartition des coûts.
- Utilisez chaque clé une seule fois pour chaque ressource. Si vous essayez d'utiliser deux fois la même clé sur la même ressource, votre demande est rejetée.
- Les caractères autorisés sont les lettres Unicode, les espaces blancs, les chiffres et les caractères spéciaux suivants : + - =. _ :/

Quels types AWS de ressources sont compatibles avec les balises ? Voir [maintenant Organisez vos AWS ressources en utilisant jusqu'à 50 balises par ressource](#).

Marquage automatique de l'infrastructure AMS

AMS peut étiqueter toutes les ressources créées par AMS à des fins de gestion, dans vos comptes de zone d'atterrissage à comptes multiples (MALZ) et de zone d'atterrissage à compte unique (SALZ) par le biais d'une demande de modification (RFC) avec le type de modification Deployment | Advanced stack components | Tag | Create (révision requise) (ct-0176f0n99vcps). Cela peut vous aider à identifier les ressources créées par AMS à des fins de gestion.

AMS peut identifier automatiquement les ressources créées par AMS en fonction des normes de dénomination et vérifier si la ressource possède les clés et valeurs de balise suivantes : "AppName«," Appld «," AMSResource « et" »EnvironmentType. Si la clé de balise n'existe pas ou si la valeur est vide, ces clés de balise peuvent être créées automatiquement par AMS avec la valeur de balise « ». AMSInfrastructure

Vous pouvez personnaliser les balises que vous souhaitez sur les ressources créées par AMS en fonction des normes de balisage de votre organisation. Vous pouvez inclure vos propres clés et valeurs de balise lorsque vous soumettez la demande à AMS. Respectez les normes de dénomination des AWS balises suivantes : [Meilleures pratiques en matière de balisage](#)

 Note

Pour les comptes MALZ, le balisage personnalisé de l'infrastructure AMS est pris en charge uniquement sur les comptes d'application. Le balisage personnalisé sur les comptes principaux n'est actuellement pas pris en charge.

Si le nom de clé de balise que vous fournissez dans votre RFC existe déjà sur la ressource, la valeur de balise est remplacée par la nouvelle valeur de balise que vous avez fournie dans la RFC.

La longueur totale des paires clé:valeur de la balise ne doit pas dépasser 256 caractères.

Incluez les informations suivantes dans votre RFC avec le type de modification (ct-0176f0n99vcps) Deployment | Advanced stack components | Tag | Create (révision requise) (ct-0176f0n99vcps) pour le balisage des ressources créées par AMS.

1. Liste des comptes de zone d'atterrissage à comptes multiples ou de zones d'atterrissage à compte unique sur lesquels vous souhaitez étiqueter les ressources créées par AMS à des fins de gestion.
2. Nom de clé de balise et valeur de balise requis (si nécessaire). Par défaut, AMS peut étiqueter avec le nom de la clé de balise comme « EnvironmentType » et la valeur de la balise comme « ». AMSInfrastructure [Si vous avez besoin d'un nom de clé de balise et d'une valeur de balise personnalisés, suivez les normes de dénomination des AWS balises : Bonnes pratiques en matière de balisage](#)

Ces ressources sont actuellement prises en charge par le balisage de l'infrastructure AMS :

```
API Gateway
Amazon CloudFront
Amazon DynamoDB
Amazon EBS
Amazon EC2
Amazon OpenSearch Service
Amazon Quantum Ledger Database (QLDB)
Amazon Redshift
Amazon RDS
Amazon S3 (specific buckets only*)
Amazon Simple Queue Service (SQS)
Amazon Simple Notification Service (SNS)
```

Amazon VPC AWS Certificate Manager AWS CloudFormation AWS CloudTrail AWS CodeBuild
 AWS CodePipeline AWS Elastic Beanstalk AWS Lambda AWS Secrets Manager AWS Service
 Catalog AWS Systems Manager AWS WAF Regional
 Elastic Load Balancing

* « arn:aws:s3::awsms-a*-patch-data-* », « arn:aws:s3::ams-a*-log-management-* »,
 « arn:aws:s3::cf-templates-* », « arn:aws:s3::ams-a*-backup-reports-* », « arn:aws:s3::ams-a*-
 * », « arn:aws:s3::ams-a*- -* », « arn:aws:s3::ams-a*- -* », « arn:aws:s3::ams-a*-release-assets-
 * », « arn:aws:s3:: -* », « arn:aws:s3:s3:1 * » patch-data-customer-reports patch-data-raw patch-
 data-reporting ams-cfn-drift-remediation ams-reporting-data-a

Tags recommandés par AMS

AMS recommande les balises suivantes pour les ressources prises en charge. Les tags marqués d'un astérisque (*) sont vivement recommandés.

Note

Vous pouvez utiliser des balises pour planifier l'application de correctifs. Pour plus d'informations, voir [AMS Advanced Patch Orchestrator : un modèle de patching basé sur des balises](#).

Préfixes réservés AMS

Les attributs de ressources AMS doivent respecter certains modèles ; par exemple, les noms de profil d'instance IAM, les BackupVault noms, les noms de balises, etc., ne doivent pas commencer par des préfixes réservés AMS. Ces préfixes réservés sont les suivants :

```
*/aws_reserved/*
ams - *
/ams/*
ams*
AMS*
Ams*
aws*
AWS*
AWS_*
AWSManagedServices*
codedeploy_service_role
CloudTrail*
```



```

Cloudtrail*
customer-mc-*
eps
EPSDB*
IAMPolicy*
INGEST*
LandingZone*
Managed_Services*
managementhost
mc*
MC*
Mc*
MMS*
ms-
NewAMS*
Root*
sentinel*
Sentinel*
sentinel.int.
StackSet-ams*
StackSet-AWS-Landing-Zone
StateMachine*
TemplateId*
VPC_*
UnhealthyInServiceBastion

```

Tags recommandés par AMS

Clé de balise	Valeurs prises en charge	Remarques
AppName*	Sans contrainte.	Identifiez les applications qui résideront sur la ressource ou qui nécessiteront un accès à celle-ci. Cela facilite le suivi et les communications entre AMS et vous.
AppId*		
EnvironmentType *		Faites la distinction entre l'infrastructure de développement, de test et de production en tant qu'environnement de la ressource.
OwnerTeamEmail *	Adresse e-mail de la liste de distribution	Identifiez l'adresse e-mail de la liste de distribution de l'équipe responsable de

Clé de balise	Valeurs prises en charge	Remarques
		la ressource. L'e-mail ne doit pas être un e-mail personnel ; il doit s'agir d'un e-mail anonyme, comme une liste de distribution.
ComplianceFramework	Sans contrainte	Identifiez les contrôles et les politiques à appliquer à la ressource.
CostCenter		Identifiez le centre de coûts ou l'unité commerciale associé à une ressource (généralement pour la répartition des coûts et le suivi).
Customer		Utilisé par les clients AMS disposant de ressources provenant de plusieurs clients (sous-clients AMS). Regrouper les ressources de l'environnement géré en fonction du client spécifique qu'elles desservent. Identifiez un client spécifique sur un groupe particulier de ressources ou de services.
DataClassification		Identifiez le niveau spécifique de confidentialité des données pris en charge par une ressource. Identifiez les contrôles et les politiques à appliquer à la ressource.
HoursOfOperation		Identifiez la date ou l'heure à laquelle une ressource doit être démarrée, arrêtée, supprimée ou modifiée.
OwnerTeam		Identifiez l'équipe responsable de la ressource. Facilite la communication avec l'équipe responsable de la ressource.

Clé de balise	Valeurs prises en charge	Remarques
Patch Group	Vous avez deux options : • Vous pouvez soumettre une demande de service avec les informations décrites dans AMS Advanced Patch Orchestrator : un modèle de patching basé sur des balises, et AMS crée une Patch Group balise pour vous sur les ressources que vous avez spécifiées et à l'aide des informations que vous fournissez. • Si vous avez déjà créé un Patch Group tag sur vos ressources, les valeurs prises en charge ne sont pas limitées.	Quelles ressources inclure dans une fenêtre de maintenance automatique des correctifs.
ProjectId	Sans contrainte	Identifiez les projets soutenus par la ressource.

Clé de balise	Valeurs prises en charge	Remarques
SupportPriority	L'un des six acronymes possibles pour la confidentialité, l'intégrité ou la disponibilité ; l'ordre des acronymes est la priorité. Par exemple, I.C.A. signifierait que la commande porte sur l'intégrité, la confidentialité et la disponibilité. Les autres valeurs acceptables sont C.I.A., C.A.I., I.A.C., A.C.I., et A.I.C.	Identifiez le type de support qui doit être prioritaire : confidentialité, intégrité ou disponibilité.

Étiqueter les notes de mise à jour

[Ces notes sont destinées à être utilisées avec les exemples de modifications de type Tag | Bulk Update et Tag | Bulk Update \(révision requise\).](#)

Remarques sur les balises de mise à jour groupée :

- Services pris en charge :
 - Pour [Tag | Mise à jour en bloc \(révision requise\)](#) : Tout.
 - Pour [Tag | Bulk Update](#) :
 - Auto Scaling
 - Amazon EC2
 - Elastic Load Balancing
 - Amazon RDS
 - Compartiments Amazon S3
- Pour générer le fichier de valeurs séparées par des virgules (CSV), connectez-vous à Resource Groups > Tag Editor dans la AWS console, recherchez les ressources que vous souhaitez baliser,

puis exportez-les vers un fichier CSV. Pour plus d'informations, voir [Exporter les résultats au format CSV](#).

REMARQUE : Nous vous recommandons d'utiliser une URL pré-signée S3 pour indiquer l'emplacement de l'objet CSV.

- Il doit y avoir des colonnes avec les en-têtes Service, Type et Identifier. Ces colonnes sont obligatoires.
- Renommez la colonne Identifier en ID.
- Les valeurs des colonnes Service, Type et Identifier (modifiées en ID) sont celles fournies par l'éditeur de balises sous Resource Groups.
- Si une ressource à baliser n'est pas disponible sous l'éditeur de balises, utilisez le nom de ressource Amazon (ARN) de la ressource comme identifiant de colonne (remplacé par ID) et laissez les champs Service et Type vides.
- Les en-têtes de colonne des balises à ajouter ou à modifier doivent avoir le format Tag : **TagKey**.
- Les en-têtes de colonne des balises à supprimer doivent avoir le format Untag :. **TagKey**
- Chaque ligne correspond à une ressource à baliser ou à débaliser.
- Si une balise doit être ajoutée à une ressource, spécifiez la valeur de la balise dans la **TagKey** colonne Tag : appropriée.
- Si une balise doit être supprimée d'une ressource, spécifiez True dans la **TagKey** colonne Untag : appropriée.
- Si les options Tag : **TagKey** ou Untag : ne **TagKey** s'appliquent pas à une ressource, ajoutez un tiret (-) à la colonne correspondante ou laissez le champ vide.

REMARQUE : Le Untag remplace le Tag. Cela est dû au fait que, contrairement à Tag, le Untag doit être ajouté manuellement au fichier CSV. Nous supposons donc que l'intention était de supprimer, et non de modifier, le tag.

- Toute colonne supplémentaire qui ne correspond pas aux critères est ignorée.

Important

L'exportation de l'éditeur de balises remplit une matrice de toutes les balises par rapport à toutes les ressources, les balises manquantes sont remplies avec la valeur « non étiquetées ». La réutilisation de ce fichier CSV d'exportation comme entrée dans la RFC

entraîne la création de toutes les balises précédemment manquantes, avec des valeurs littérales « non balisées ».

Note

Pour plus d'informations sur l'exportation de balises vers un fichier CSV, voir [Trouver des ressources à étiqueter -> Exporter les résultats au format CSV](#).

Planificateur de ressources AWS Managed Services

Utilisez le planificateur de ressources AWS Managed Services (AMS) pour planifier le démarrage et l'arrêt automatiques des AutoScaling groupes, des EC2 instances Amazon et des instances 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 [Instance Scheduler AWS](#), mais contient des fonctionnalités supplémentaires et des personnalisations spécifiques aux besoins d'AMS.

Note

Par défaut, AMS Resource Scheduler n'interagit pas avec les ressources qui ne font pas partie d'une AWS CloudFormation pile. La ressource doit faire partie d'une pile commençant par « stack- », « sc- » ou « SC- ». Pour planifier les ressources qui ne font pas partie d'une CloudFormation pile, vous pouvez mettre à jour le paramètre `ScheduleNonStackResources` de pile Resource Scheduler sur. Yes

Le planificateur de ressources AMS utilise des périodes et des plannings :

- Les périodes définissent les heures d'exécution du planificateur de ressources, 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, telles que la fenêtre de maintenance SSM, le fuseau horaire, le paramètre de mise en veille prolongée, etc. Ils spécifient le moment où les ressources doivent être exécutées, conformément aux règles de période configurées.

Vous pouvez configurer ces périodes et ces plannings à l'aide des types de modifications automatisés d'AMS Resource Scheduler (CTs).

[Pour plus de détails sur les paramètres disponibles pour AMS Resource Scheduler, consultez la documentation correspondante du planificateur d' AWS instance sur Composants de la solution.](#) Pour une vue architecturale de la solution, consultez la documentation correspondante du planificateur d' AWS instance sur [Architecture](#) overview.html.

Déploiement du planificateur de ressources AMS

Pour déployer le planificateur de ressources AMS, utilisez le type de modification automatique (CT) : Déploiement | Planificateur de ressources AMS | Solution | Déploiement (ct-0ywnhc8e5k9z5) pour créer un RFC qui déploie ensuite la solution dans votre compte. Une fois le RFC exécuté, une CloudFormation pile contenant les ressources du planificateur de ressources AMS avec configuration par défaut est automatiquement provisionnée dans votre compte. Pour en savoir plus sur les types de modification du planificateur de ressources, consultez le planificateur de [ressources AMS](#).

Note

Pour savoir si le planificateur de ressources AMS est déjà déployé dans votre compte, consultez la console AWS Lambda de ce compte et recherchez la fonction Scheduler. AMSResource

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 recommandées [Personnalisation du planificateur de ressources AMS](#), reportez-vous à la section suivante.

Pour effectuer les configurations personnalisées, ou simplement confirmer la configuration du planificateur de ressources,

Personnalisation du planificateur de ressources AMS

[Nous vous recommandons de personnaliser les propriétés suivantes du planificateur de ressources AMS à l'aide des types de modification mis à jour du planificateur de ressources AMS, voir Planificateur de ressources AMS.](#)

- **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`.
- **Services planifiés** : liste séparée par des virgules de 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`.
- **Utiliser CMK** : liste séparée par des virgules des clés gérées par le client (CMK) Amazon KMS pour lesquelles le Resource Scheduler ARNs peut être autorisé à obtenir des autorisations.
- **Utilisation LicenseManager** : une liste séparée par des virgules des gestionnaires de AWS licences ARNs pour lesquels le planificateur de ressources peut être autorisé.

Note

AMS peut, de temps à autre, publier des fonctionnalités et des correctifs pour maintenir AMS Resource Scheduler à jour sur votre compte. Dans ce cas, toutes les personnalisations que vous apportez au planificateur de ressources AMS sont conservées.

Utilisation du planificateur de ressources AMS

Pour configurer le planificateur de ressources AMS après le déploiement de la solution, utilisez le planificateur de ressources automatisé CTs pour créer, supprimer, mettre à jour et décrire (obtenir des détails sur) les périodes du planificateur de ressources AMS (les heures d'exécution du planificateur de ressources) et les calendriers (les périodes configurées et autres options). Pour un exemple d'utilisation des types de modification du planificateur de ressources AMS, consultez le planificateur de [ressources AMS](#).

Pour sélectionner les ressources à gérer par AMS Resource Scheduler, après le déploiement et la création du calendrier, vous utilisez l'AMS Tag Create CTs pour étiqueter les groupes Auto Scaling, les piles Amazon RDS et les EC2 ressources Amazon avec la clé de balise que vous avez fournie lors du déploiement, et le calendrier défini comme valeur de balise. Une fois les ressources balisées, le démarrage ou l'arrêt des ressources sont planifiés selon le calendrier que vous avez défini dans le planificateur de ressources.

L'utilisation d'AMS Resource Scheduler est gratuite. Cependant, la solution en utilise plusieurs Services AWS et ces ressources vous sont facturées au fur et à mesure de leur utilisation. Pour plus de détails, consultez la section [Présentation de l'architecture](#).

Pour désactiver le planificateur de ressources AMS, procédez comme suit :

- Pour une désinscription ou une désactivation temporaire : soumettez une RFC à l'aide du gestionnaire automatisé | AMS Resource Scheduler | State | Disable change type (ct-14v49adibs4db)
- Pour une suppression définitive : soumettez une RFC de gestion | Autre | Autre | Mise à jour (révision requise) (ct-0xdawir96cy7k) demandant la suppression du système d'automatisation des versions du planificateur de ressources

Estimateur de coûts 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 EC2 et 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 $24 \times 0,125 = 3\$$. 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, la AWS facturation commence à suivre les coûts et l'utilisation des ressources gérées par le planificateur de ressources. Une fois ces données disponibles, l'estimateur des économies de coûts commence à calculer les économies de coûts et à publier les données sous l'AMS/ResourceSchedulerespace de noms des métriques dans. CloudWatch

Conseils aux estimateurs de coûts

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](#)

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 à ce sujet, consultez la section [Balises de répartition des coûts définies par l'utilisateur](#). 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.

Bonnes pratiques du planificateur de ressources AMS

Planification d' EC2 instances Amazon

- Le comportement d'arrêt de l'instance doit être défini sur stop et non sur terminate. Ceci est prédéfini stop pour les instances créées avec le type de modification automatique AMS Amazon EC2 Create (ct-14027q0sjyt1h) et peut être défini pour les instances EC2 Amazon créées AWS CloudFormation par ingestion, en définissant la propriété sur.

`InstanceInitiatedShutdownBehavior` stop Si le comportement d'arrêt des instances est défini sur `terminate`, elles se termineront lorsque le planificateur de ressources les arrêtera et le planificateur ne pourra pas les redémarrer.

- Les EC2 instances Amazon qui font partie d'un groupe Auto Scaling ne sont pas traitées individuellement 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 client KMS (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, soumettez une RFC avec le type de modification `Management | AMS Resource Scheduler | Solution | Update` et spécifiez une liste des KMS séparée par des ARNs virgules. CMKs

Planification de groupes 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 AutoScaling groupe 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.

Planification d'instances 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 `Create RDS Instance Snapshot` AWS CloudFormation template 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 peut pas 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.

Chaque instance Amazon RDS dispose d'une fenêtre de maintenance hebdomadaire au cours de laquelle toutes les modifications du système sont appliquées. Pendant la période de maintenance, Amazon RDS démarrera automatiquement les instances qui ont été arrêtées pendant plus de sept jours pour appliquer la maintenance. Notez qu'Amazon RDS n'arrêtera pas l'instance une fois l'événement de maintenance terminé.

Le planificateur permet de spécifier s'il faut ajouter la fenêtre de maintenance préférée d'une instance Amazon RDS comme période d'exécution à son calendrier. La solution démarrera l'instance au début de la fenêtre de maintenance et l'arrêtera à la fin de la fenêtre de maintenance si aucune autre période d'exécution n'indique que l'instance doit s'exécuter et si l'événement de maintenance est terminé.

Si l'événement de maintenance n'est pas terminé à la fin de la fenêtre de maintenance, l'instance sera exécutée jusqu'à l'intervalle de planification suivant la fin de l'événement de maintenance.

Note

Le planificateur ne valide pas le démarrage ou l'arrêt d'une ressource. Il fait l'appel d'API et passe à autre chose. Si l'appel d'API échoue, il enregistre l'erreur à des fins d'investigation.

AWS Systems Manager dans AMS Advanced

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. AWS Le processus AMS pour le développement et la publication de documents SSM suit les AWS meilleures pratiques et nécessite plusieurs évaluations par les pairs tout au long du cycle de vie du document. Pour plus d'informations sur les AWS meilleures pratiques en matière de partage de documents SSM, consultez la section [Meilleures pratiques pour les documents SSM partagés](#).

Documents AMS Advanced SSM disponibles

Les documents AMS Advanced SSM sont disponibles exclusivement pour les clients AMS Advanced et sont utilisés pour automatiser le flux de travail opérationnel nécessaire à l'exploitation de votre compte.

Pour consulter les documents AMS Advanced 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 les instructions de la AWS CLI, consultez la section [Utilisation de documents SSM partagés](#).

Versions des documents AMS Advanced SSM

Les documents SSM prennent en charge le contrôle de version. Les documents AMS Advanced 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 Advanced afin de gérer le compte.

Les numéros de version sont incrémentés à chaque mise à jour d'un document spécifique Région AWS. 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 Advanced SSM, nous vous recommandons de comparer leurs hachages avec la CLI AWS :

```
aws ssm describe-document \  
--name AWSManagedServices-DOCUMENTNAME \  
--region REGION
```

```
--output text --query "Document.Hash"
```

Deux documents SSM sont identiques si leurs hachages correspondent.

Tarification de Systems Manager dans AMS

L'accès aux documents AMS Advanced 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](#).

Comptes AMS externes

AMS propose une assistance au débarquement pour les comptes de zone d'atterrissage à compte unique et les comptes de zone d'atterrissage multicomptes.

AMS ne vous en communique aucune lors AMIs de l'offboarding afin d'éviter toute répercussion sur vos dépendances. Si vous souhaitez supprimer AMS AMIs de votre compte, vous pouvez utiliser l'`cancel-image-launch-permissionAPI` pour masquer des informations spécifiques AMIs. Par exemple, vous pouvez utiliser le script ci-dessous pour masquer tous AMIs les AMS précédemment partagés avec votre compte :

```
for ami in $(aws ec2 describe-images --executable-users self --owners 027415890775 --
query 'Images[].ImageId' --output text) ;
do
    aws ec2 cancel-image-launch-permission --image-id $ami ;
done
```

L'AWS CLI v2 doit être installée pour que le script s'exécute sans erreur. Pour connaître les étapes d'installation de l'interface de ligne de commande AWS, consultez la section [Installation ou mise à jour de la dernière version de l'interface de ligne de commande AWS](#). Pour plus de détails sur la `cancel-image-launch-permission` commande, consultez [cancel-image-launch-permission](#).

Note

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 20^e 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.

Rubriques

- [Déconnectez-vous des comptes de zone d'atterrissage à compte unique AMS](#)
- [Déconnectez-vous des comptes de zone d'atterrissage multi-comptes AMS](#)

Déconnectez-vous des comptes de zone d'atterrissage à compte unique AMS

AMS propose une assistance au débarquement dans les 30 jours précédant la résiliation d'AMS.

Vous devez demander une assistance au débarquement au moins 7 jours avant qu'une telle assistance puisse être fournie. L'assistance au débarquement peut être proposée sous deux formes :

- Transfert de contrôle : AMS vous retransfère le contrôle de votre compte ainsi que les informations d'accès pour toutes les applications gérées par AMS, ou
- Résiliation des ressources en cas de fermeture du compte : AMS supprime toutes les données de votre environnement géré par AMS et met fin au provisionnement de toutes les ressources actives du compte. Lors de la soumission de la demande d'offboarding, les clients peuvent demander à AMS de :
 - Supprimer ou conserver les objets de données (y compris les journaux) stockés dans les compartiments Amazon S3
 - Supprimer ou conserver les compartiments Amazon S3
 - Supprimer ou conserver les points de AWS Backup restauration

Important

Toute autre demande spécifique (sous réserve de plausibilité) doit être communiquée à AMS avant l'initialisation de l'offboarding.

Prérequis facultatifs (si nécessaire) :

Note

Avant la demande de déchargement, les clients peuvent demander l'assistance d'AMS pour transférer leurs données dans le format existant AWS Snowball Edge ou sur tout autre support interfacé AWS avec.

Outre les sauvegardes de données, les données client suivantes peuvent être fournies dans le cadre de l'assistance au débarquement :

- Données stockées dans les services de stockage, y compris les journaux
- Schémas de type de modification spécifiques au client
- CloudFormation modèles pour les schémas de type de modification

Si les activités de désinscription ne sont pas terminées à la fin d'AMS, nous vous transférons le contrôle du ou des comptes pour vous permettre de terminer toute activité en attente.

Fonction	Ce qui a été supprimé	Impact	Actions nécessaires
Surveillance, journalisation, alertes	Surveillance AMS supprimée	AMS n'a plus accès ni visibilité à vos ressources et à votre environnement.	Les imprévus relatifs aux services supprimés ou désabonnés sont à votre charge.
	MMS (Managed Monitoring System) s'est désabonné		
	Resource Tagger et Alarm Manager supprimés		
	CloudWatch Les alertes de base restent sur les ressources existantes		

Fonction	Ce qui a été supprimé	Impact	Actions nécessaires
	GuardDuty et Macie : la propriété vous revient		
Gestion des sauvegardes	L'automatisation AMS Backup est supprimée bien que le AWS Backup service reste disponible. Les coffres-forts et les données de sauvegarde sont conservés sauf demande de suppression.	AMS ne surveille plus les tâches de sauvegarde ni n'effectue d'actions de restauration en cas d'incident. Les alarmes et les alertes sont désactivées. La suppression du rôle de sauvegarde IAM et des clés KMS rend vos sauvegardes AMS inopérantes.	Les plans de sauvegarde AMS doivent être reconfigurés. Toute la responsabilité de la surveillance et de la correction vous revient.
Automatisations AMS pour la gestion des services	Les runbooks d'automatisation AWS SSM sélectionnés par AMS, Amazon Simple Notification Service (SNS) et les fonctions Lambda ne sont plus disponibles. AWS	Aucun accès AMS à vos comptes. Toutes les automatisations sont désactivées.	Toutes les fonctions d'automatisation, y compris les fonctions SSM, SNS et Lambda, doivent être recréées, si nécessaire.
Conformité	Visibilité et surveillance de l'AMS pour tous GuardDuty et suppression des AWS Config règles, bien que ces règles restent sur les comptes.	L'ensemble de la surveillance, des rapports et des mesures correctives fournis par Amazon GuardDuty et AWS Config Rules ne sont plus gérés par AMS.	Surveillance et correction de tous les outils de sécurité et de conformité que vous devez prendre en charge.

Fonction	Ce qui a été supprimé	Impact	Actions nécessaires
Agents sur instance	L'accès au planificateur de ressources, au baliseur de ressources ou à la configuration automatique des instances pour installer les agents requis dans vos EC2 instances est supprimé.	CloudWatch et les agents SSM sur les instances restent en place avec les configurations existantes, mais AMS ne prend plus en charge ces configurations.	Vous gérez le balisage et les configurations des agents sur instance CloudWatch et SSM.
Infrastructure de correctifs et de rapports	AMS ne gère plus les activités avant et après l'application des correctifs, et l'accès et la visibilité à ces services sont supprimés.	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. Les rapports et les compartiments S3 « d'audit » sont laissés dans vos comptes à votre demande. AMS ne génère plus de rapports sur les métriques de service.	Vous conservez les lignes de base des correctifs et les instantanés créés dans le passé. En outre, la configuration des fenêtres de maintenance des correctifs est conservée, mais les correctifs ne sont plus installés ni corrigés par AMS. Tous les rapports sur les indicateurs opérationnels de l'infrastructure relèvent désormais de votre responsabilité.

Fonction	Ce qui a été supprimé	Impact	Actions nécessaires
Gestion des processus	Tous les comptes sont exclus de la gestion des services fournie en cas d'incident, y compris les demandes de service, les problèmes et la gestion des modifications.	Toutes les interruptions de service précédemment corrigées par AMS par le biais d'incidents et de demandes de service, de modifications de l'environnement, ainsi que d'enquêtes sur les causes premières, sont gérées depuis longtemps par AMS.	Vous reprenez la pleine maîtrise de l'ensemble de la gestion des processus .

Déconnectez-vous des comptes de zone d'atterrissage multi-comptes AMS

Il existe deux types de AWS comptes que vous pouvez déconnecter de la zone de landing multicomptes AMS Advanced :

- Comptes d'applications
- Comptes principaux

Pour déconnecter tous les comptes de votre zone de landing multi-comptes AMS, vous devez déconnecter tous les comptes de l'application avant de quitter les comptes Core.

Pour prendre en charge et continuer à exploiter les charges de travail dans des comptes Application ou Core externes, assurez-vous de consulter cette documentation avec l'équipe de votre compte AMS. Cette documentation décrit les modifications effectuées par AMS au cours du processus de déconnexion.

Tâches à accomplir pour assurer le fonctionnement continu des comptes externes

Les tâches suivantes sont requises pour continuer à exploiter les comptes que vous avez retirés de la zone de landing zone multi-comptes AMS :

- Activez le mode développeur : pour obtenir davantage d'autorisations sur vos comptes, activez le mode développeur avant de déconnecter les comptes d'applications d'AMS. Lorsque vous activez le mode développeur, vous pouvez plus facilement apporter les modifications nécessaires pour vous préparer à l'offboarding. N'essayez pas de supprimer ou de modifier les ressources de l'infrastructure AMS. Si vous supprimez les ressources de l'infrastructure AMS, il se peut qu'AMS ne soit pas en mesure de déconnecter correctement votre compte. Pour plus d'informations sur la façon d'activer le mode développeur, consultez [Commencer à utiliser le mode développeur avancé d'AMS](#).

Si vous ne parvenez pas à effectuer les modifications nécessaires pour préparer le désenclavement après avoir activé le mode développeur, contactez l'équipe de votre compte AMS pour discuter de vos besoins.

- Choisissez une autre méthode d'accès à la EC2 pile : une fois que vous avez déconnecté les comptes d'applications d'AMS, vous ne pouvez plus l'utiliser RFCs pour accéder aux ressources de votre pile. Passez en revue [Changements liés à l'offboarding](#), puis choisissez une autre méthode d'accès afin de conserver l'accès à vos piles. Pour de plus amples informations, veuillez consulter [Alternatives d'accès](#).

Comptes d'application AMS externes

Pour déconnecter des comptes d'application de votre environnement de zone de landing zone multi-comptes, effectuez les étapes suivantes pour chaque compte :

1. Vérifiez qu'il n'y a pas d'ouverture RFCs dans le compte. Pour de plus amples informations, veuillez consulter [Création, clonage, mise à jour, recherche et annulation RFCs](#).
2. Vérifiez que vous pouvez accéder à l'adresse e-mail de l'utilisateur principal ou root du compte.
3. À partir du compte d'application, soumettez une RFC avec le type de changement [Compte d'application | Confirmer le débarquement \(ct-2wifo2jxj2rkj\)](#). Dans le RFC, spécifiez le compte d'application à déconnecter.
4. À partir du compte de gestion, soumettez une RFC avec le type de modification [Compte de gestion | Compte d'application hors bord \(ct-0vdiy51oyrhbm\)](#). Dans le RFC, spécifiez le compte d'application à déconnecter. Indiquez également si vous souhaitez supprimer ou conserver le rattachement de la passerelle de transit à la zone de landing zone.
5. Pour vous assurer que la facturation AMS est arrêtée, informez votre CSDM que vous avez retiré le compte.

Les événements suivants se produisent une fois que le compte de l'application est déconnecté :

- Tous les composants sont dissociés des services AMS, mais les ressources que vous avez créées restent dans le compte. Vous pouvez choisir de conserver ou de fermer le compte AMS Offboarded.
- Les comptes principaux et les autres comptes d'application restants fonctionnent normalement une fois qu'un compte d'application est déconnecté.
- La facturation AMS est arrêtée, mais la AWS facturation ne l'est pas tant que vous n'avez pas fermé le compte. Pour plus d'informations, consultez [ce que vous devez savoir avant de fermer votre compte](#).
- Si un compte est fermé, il est visible dans votre organisation dans l'état `suspended` pendant 90 jours. Après 90 jours, le compte fermé est définitivement supprimé et n'est plus visible dans votre organisation.
- Une fois le compte fermé, vous pouvez toujours vous connecter et déposer une demande d'assistance ou un contact Support pendant 90 jours.
- Après 90 jours, tout contenu restant sur le compte est définitivement supprimé et les AWS services restants sont résiliés.

FAQ sur le désenclavement des comptes d'applications

Q : Puis-je utiliser mes rôles IAM fédérés pour continuer à accéder à un compte d'application que j'ai quitté depuis ma zone de landing zone multi-comptes AMS ?

Oui. Les [rôles par défaut créés par AMS AWS Identity and Access Management \(IAM\)](#) restent disponibles dans le compte après le désenclavement d'AMS. Toutefois, ces rôles et politiques sont conçus pour être utilisés avec la gestion des accès AMS. Pour fournir l'accès nécessaire à vos utilisateurs, vous devrez peut-être déployer vos propres ressources IAM.

Q : Comment puis-je obtenir un accès complet à un compte d'application que j'ai quitté depuis ma zone de landing zone multi-comptes AMS ?

Les comptes d'applications externes sont déplacés vers l'unité organisationnelle (UO) obsolète de la structure du compte. AWS Organizations Cette décision lève les restrictions d'accès au SCP qui bloquaient auparavant l'accès des utilisateurs root. Pour plus d'informations sur la réinitialisation des informations d'identification de l'utilisateur root, voir [Réinitialisation d'un mot de passe utilisateur root perdu ou oublié](#).

Q : Quelles sont les modifications apportées lors de la désintégration du compte de l'application ?

Pour plus d'informations sur les actions entreprises par AMS lorsque le service déconnecte des comptes, consultez [Changements liés à l'offboarding](#).

Q : Puis-je déconnecter un compte d'application sans le détacher de la passerelle de transit ?

Oui. Utilisez le type de changement [Compte de gestion | Compte d'application hors bord](#) (ct-0vdiy51oyrhbm) pour soumettre la RFC et spécifiez le paramètre sous la forme. `DeleteTransitGatewayAttachment False`

Q : Combien de temps faut-il pour déconnecter un compte d'application ?

Lorsque vous utilisez le changement de type [Compte de gestion | Compte d'application hors bord](#) (ct-0vdiy51oyrhbm), effectuez le changement dans un délai d'une heure. RFCs

Q : Est-il obligatoire de fermer le compte externe ?

Non La fermeture du compte après le désenclavement d'AMS n'est pas obligatoire. Au cours du processus d'offboarding, AMS supprime l'accès à votre AWS compte et la gestion de celui-ci, mais votre compte et les ressources qu'il contient sont conservés. Il est important de noter qu'après avoir quitté AMS, vous êtes seul responsable de la gestion et de la maintenance de votre AWS compte et de vos ressources. AMS n'est pas responsable des problèmes, incidents ou interruptions de service susceptibles de survenir sur votre compte une fois le processus d'offboarding terminé. Pour plus d'informations, consultez l'[article Comment fermer mon AWS compte ?](#).

Q : Si je soumetts une demande de fermeture de compte, toutes les ressources existantes sont-elles supprimées immédiatement ?

Non La fermeture du compte ne met pas fin à vos ressources. Les ressources du compte sont automatiquement supprimées 90 jours après la demande de fermeture. La facturation AMS s'arrête, mais la facturation AWS des ressources ne s'arrête pas tant que vous n'avez pas fermé le compte. Pour plus d'informations, consultez [ce que vous devez savoir avant de fermer votre compte](#).

Q : Puis-je planifier le désenclavement d'un compte d'application ?

Oui. Vous pouvez le programmer RFCs pour qu'il s'exécute à une heure précise. Cependant, le RFC [Compte d'application | Confirmer le déchargement doit être terminé avant que vous puissiez planifier le compte de gestion | Compte d'application externe](#). Pour plus d'informations, consultez la section [Planification RFC](#).

Déconnexion du compte d'application RACI

- R : Partie responsable. Partie responsable de l'exécution de la tâche répertoriée.
- R : Partie responsable. Partie qui approuve la tâche terminée.
- C : Partie consultée. Partie dont les opinions sont sollicitées, généralement en tant qu'experts en la matière, et avec laquelle il existe une communication bilatérale.
- I : Partie informée. Une partie informée des progrès réalisés, souvent uniquement à l'issue de la tâche ou du livrable.

Activité	Client	AWS Managed Services (AMS)
Prérequis		
Vérifiez l'accès à l'adresse e-mail racine pour chaque identifiant de AWS compte qui sera déconnecté	R	C
Consultez la documentation d'AMS sur les actions recommandées aux clients et préparez les comptes pour le désenclavement d'AMS	R	C
Si nécessaire, soumettez une RFC pour activer le mode développeur afin de préparer les comptes pour le déchargement d'AMS	R	I
Si nécessaire, choisissez une autre méthode d'accès à la EC2 pile.	R	I
Débarquement		
Soumettre RFCs pour confirmer et demander le désenclavement des comptes de l'application	R	I
Déconnectez les composants AMS des comptes d'applications	I	R
Informez AMS CSDM de la présence de comptes hors bord pour arrêter la facturation d'AMS	R	I
Après le décollage		

Activité	Client	AWS Managed Services (AMS)
Réinitialisez le mot de passe du compte utilisateur root et vérifiez l'accès root dans les comptes externes	R	C
Fermez le compte ou suivez les instructions d'AMS sur les actions recommandées aux clients dans la documentation de désenclavement d'AMS pour continuer à gérer les comptes	R	C

Comptes Offboard Core

Pour déconnecter les comptes multi-comptes de la zone de landing zone Core, procédez comme suit :

1. Vérifiez que tous les comptes d'application de la zone de landing zone ont été retirés d'AMS.
2. Vérifiez que vous n'avez aucun compte ouvert RFCs . Pour de plus amples informations, veuillez consulter [Création, clonage, mise à jour, recherche et annulation RFCs](#).
3. Vérifiez que vous pouvez accéder à l'adresse e-mail de l'utilisateur principal ou root pour tous les comptes Core. Pour de plus amples informations, veuillez consulter [Comptes multi-comptes Landing Zone](#).
4. Vérifiez que vous pouvez accéder au numéro de téléphone de l'utilisateur principal ou root du compte de gestion. Utilisez le rôle AWSManagedServicesBillingRole IAM pour mettre à jour le numéro de téléphone. Pour plus d'informations, consultez [Comment mettre à jour le numéro de téléphone associé à mon AWS compte ?](#) .
5. Connectez-vous à votre compte de gestion de zone d'atterrissage AMS et soumettez une demande de service AMS. Dans la demande de service, indiquez que vous souhaitez démonter l'intégralité de votre zone d'atterrissage.

Les événements suivants se produisent une fois que les comptes Core sont déconnectés :

- Tous les composants sont dissociés des services AMS, mais certaines AWS ressources restent dans le compte. Vous pouvez choisir de conserver ou de fermer les comptes Core déconnectés d'AMS.

- La facturation AMS est arrêtée, mais la AWS facturation ne l'est pas tant que vous n'avez pas fermé le compte. Pour plus d'informations, consultez [ce que vous devez savoir avant de fermer votre compte](#).
- Si un compte est fermé, il est visible dans votre organisation dans l'état suspendu pendant 90 jours. Après 90 jours, le compte de membre fermé est définitivement supprimé et n'est plus visible dans votre organisation.
- Une fois le compte fermé, vous pouvez toujours vous connecter et déposer une demande d'assistance ou un contact Support pendant 90 jours.
- Après la fermeture du compte pendant 90 jours, tout contenu restant sur le compte est définitivement supprimé et les AWS services restants sont résiliés.

FAQ sur le désenclavement du compte principal

Q : Puis-je utiliser mes rôles IAM fédérés pour continuer à accéder aux comptes Core externes ?

Oui. Les [rôles par défaut AWS Identity and Access Management \(IAM\) créés par AMS](#) restent disponibles dans le compte déconnecté. Toutefois, ces rôles et politiques sont conçus pour être utilisés avec la gestion des accès AMS. Pour fournir l'accès nécessaire à vos utilisateurs, vous devrez peut-être déployer vos propres ressources IAM.

Q : Comment puis-je obtenir un accès complet au compte MALZ de gestion, de services partagés, de mise en réseau ou à tout autre [compte MALZ non lié à l'application après avoir quitté](#) la zone de landing zone multi-comptes AMS ?

Après le désenclavement, suivez les instructions de la section [Réinitialisation d'un mot de passe utilisateur root perdu ou oublié](#) pour utiliser les informations d'identification de l'utilisateur principal (root) afin d'accéder aux comptes principaux autres que le compte de gestion. Contrairement aux autres types de comptes, le compte de gestion conserve un dispositif d'authentification multifactorielle (MFA) inaccessible associé à l'utilisateur root pour empêcher toute utilisation. Pour retrouver l'accès root, vous devez suivre le processus de [récupération du périphérique MFA perdu](#).

Q : Quelles sont les modifications apportées lors de la désintégration du compte Core ?

Pour plus d'informations sur les actions entreprises par AMS lorsque le service déconnecte des comptes, consultez [Changements liés à l'offboarding](#).

Q : Combien de temps prend le désenregistrement du compte Core ?

Le processus de désintégration du compte Core prend généralement jusqu'à 30 jours. Toutefois, pour vous assurer que toutes les étapes requises sont correctement effectuées, vous devez lancer la demande de déchargement au moins 7 jours avant le début de l'offboarding. Pour faciliter la transition, planifiez à l'avance et soumettez votre demande de déchargement à l'avance.

Q : Comment gérer les composants partagés après le désenclavement d'AMS ?

AMS Managed Active Directory et les autres composants de l'infrastructure de services partagés sont conçus pour l'accès des opérateurs AMS. Vous devrez peut-être mettre à jour les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2), la politique de contrôle des AWS Organizations services (SCP) ou apporter d'autres modifications pour conserver un accès complet à ces composants.

Q : Puis-je fermer des comptes Core non intégrés ?

Par défaut, les comptes d'application ont de multiples dépendances par rapport aux comptes MALZ Core, telles que l'AWS Organizations adhésion, la connectivité au réseau de passerelles de transit et la résolution DNS via AMS Managed Active Directory. Une fois ces dépendances résolues, vous pouvez mettre hors service et fermer le compte Core déconnecté. Pour de plus amples informations, veuillez consulter [Comptes multi-comptes Landing Zone](#).

Déconnexion du compte principal | RACI

- R : Partie responsable. Partie responsable de l'exécution de la tâche répertoriée.
- R : Partie responsable. Partie qui approuve la tâche terminée.
- C : Partie consultée. Partie dont les opinions sont sollicitées, généralement en tant qu'experts en la matière, et avec laquelle il existe une communication bilatérale.
- I : Partie informée. Une partie informée des progrès réalisés, souvent uniquement à l'issue de la tâche ou du livrable.

Activité	Client	AWS Managed Services (AMS)
Prérequis		
Vérifiez l'accès à l'adresse e-mail racine pour chaque identifiant de compte AWS qui sera déconnecté	R	C
Vérifier l'accès au compte de gestion et mettre à jour le numéro de téléphone de l'utilisateur root	R	C
Consultez la documentation d'AMS sur les actions recommandées aux clients et préparez les comptes pour le désenclavement d'AMS	R	C
Débarquement		
Soumettre une demande de service pour demander le débarquement de la zone d'atterrissage	R	I
Déconnectez les composants AMS des comptes principaux	I	R
Après le décollage		
Réinitialisez le mot de passe du compte utilisateur root et vérifiez l'accès root dans les comptes externes	R	C
Fermez les comptes ou suivez les instructions d'AMS sur les actions recommandées aux clients dans la documentation de désenclavement d'AMS pour continuer à gérer les comptes	R	C

Changements liés à l'offboarding

Le tableau suivant décrit les mesures prises par AMS pour le déchargement de plusieurs comptes dans une zone d'atterrissage, les impacts potentiels et les mesures recommandées.

Composant	Account type (Type de compte)	Mesures prises pour décoller	Impacts potentiels	Action recommandée par le client
Gestion de l'accès	Comptes d'applications	Après le déchargement, l'accès à la pile RFCs pour just-in-time un accès limité dans le temps ne peut plus être soumis aux EC2 piles d'accès via les hôtes AMS Bastion AMS ne gère plus les composants liés à l'accès sur les piles de EC2 ressources existantes (agent PBIS Open, scripts de jointure de domaine)	Impossible d'utiliser les bastions AMS via RFS pour accéder aux instances EC2 EC2 les instances lancées à partir d'une instance non fournie par AMS AMIs ne sont pas jointes au domaine Managed Active Directory S'ils ne sont pas supprimés, les scripts de lancement AMS présents dans les piles de ressources existantes peuvent générer des erreurs en raison de dépendances AMS manquantes et empêcher de rejoindre un autre domaine	Utiliser d'autres méthodes pour accéder à l'EC2 instance (voir Alternatives d'accès) Supprimer les scripts de lancement AMS des piles de EC2 ressources existantes (voir Désactiver les scripts de EC2 lancement d'AMS)
Gestion des	Comptes principaux	Si vous avez migré de PBIS Open vers PBIS Enterprise (AD Bridge),	Si la licence PBIS Enterprise est autorisée à expirer,	Si vous avez migré vers PBIS Enterprise (AD Bridge), décidez

Composant	Account type (Type de compte)	Mesures prises pour décoller	Impacts potentiels	Action recommandée par le client
accès (suite)		AMS ne renouvelle plus la licence après avoir quitté le compte principal	les informations d'identification Active Directory ne sont pas valides pour les piles d'instances basées sur Linux EC2 existantes	de conserver les licences ou de les mettre hors service (voir) PBIS Open/Enterprise (pont AD)

Composant	Account type (Type de compte)	Mesures prises pour décoller	Impacts potentiels	Action recommandée par le client
Journalisation, surveillance, Incident/Event gestion	Comptes d'application et de base	Les composants AMS à déployer Alertes issues de la surveillance de base dans AMS sont supprimés Les CloudWatch alarmes Amazon déployées existantes sont conservées mais ne créent plus d'incidents AMS AWS Config les autorisations d'agrégation d'AMS et du compte de sécurité MALZ Core sont supprimées AWS Config les règles restent déployées et Amazon GuardDuty reste activé, mais ne crée plus d'incidents AMS	Les ressources nouvellement créées ne sont pas soumises à une surveillance de base AMS ni à des alarmes Les alarmes métriques d'infrastructure et les événements de sécurité ne génèrent plus d'incidents AMS AWS Config n'est plus agrégé dans un compte central	Définissez, capturez et analysez les métriques opérationnelles pour visualiser les événements liés à la charge de travail et prendre les mesures appropriées. Mettez en œuvre tout flux d'alerte requis pour continuer à appliquer la surveillance opérationnelle et les alarmes requises aux nouvelles ressources et pour recevoir des alertes de sécurité de la part d'Amazon AWS Config et d'Amazon GuardDuty.

Composant	Account type (Type de compte)	Mesures prises pour décoller	Impacts potentiels	Action recommandée par le client
Gestion de la continuité (Backup and Restore)	Comptes d'applications	AMS ne surveille plus les tâches de sauvegarde ni n'exécute les demandes de sauvegarde et de restauration Les coffres-forts de sauvegarde par défaut, la clé de chiffrement de sauvegarde et le rôle de sauvegarde d'AMS restent	Les échecs des opérations de sauvegarde peuvent ne pas être remarqués	Surveillez et examinez les configurations du plan de sauvegarde
Gestion des correctifs	Comptes d'application et de base	AMS ne surveille plus les opérations de correction pour garantir leur bonne exécution ou n'effectue plus de correctifs manuels. AMS ne met plus à jour les composants de l'infrastructure AMS Les lignes de base des correctifs fournies par AMS sont conservées Les runbooks d'automatisation des AWS Systems Manager correctifs fournis par AMS ne sont pas partagés et ne peuvent plus être utilisés	Les échecs des opérations de correction peuvent ne pas être remarqués Les configurations de correctifs existantes qui dépendent des runbooks Systems Manager Automation fournis par AMS doivent être reconfigurées pour continuer sans interruption.	Passez en revue et reconfigurez les configurations d'application des correctifs selon les besoins

Composant	Account type (Type de compte)	Mesures prises pour décoller	Impacts potentiels	Action recommandée par le client
Gestion du réseau	Comptes d'applications	Si cela est spécifié, la pièce jointe à la passerelle de transit dans le compte d'application déconnecté est supprimée.	Le compte d'application externe ne peut plus utiliser de passerelle de transit pour accéder à des services partagés, tels que Managed Active Directory ou d'autres comptes d'application	Spécifiez False de DeleteTransitGatewayAttachment manière à conserver la connectivité de la passerelle de transit
Gestion de la sécurité	Comptes d'applications	Le compte est détaché de la console centrale Trend Micro DSM. De plus, les agents des terminaux ne transmettent plus les alertes via le processus d'incident AMS Les agents Trend Micro restent installés mais ne sont plus gérés ni mis à jour par AMS Les personnalisations d'AMI fournies par AMS qui déploient l'agent Trend Micro ne sont plus maintenues ni mises à jour par AMS	EC2 les détections de programmes malveillants sur les terminaux d'instance peuvent ne pas être remarquées Le micro-agent Trend n'est pas déployé sur des EC2 instances lancées à partir d'une instance non fournie par AMS AMIs	Envisagez des options pour poursuivre ou arrêter Trend Micro (voir Trend Micro Deep Security)

Composant	Account type (Type de compte)	Mesures prises pour décoller	Impacts potentiels	Action recommandée par le client
Gestion de la sécurité (suite)	Comptes principaux	L'infrastructure DSM de Trend Micro est laissée en place dans les comptes Shared Services, mais elle n'est plus maintenue ni mise à jour par AMS Trend Micro DSM ne transmet plus les alertes via le processus d'incident AMS	EC2 les détections de logiciels malveillants sur les terminaux d'instance peuvent passer inaperçues EC2 la protection des terminaux d'instance peut être affectée si l'infrastructure n'est pas maintenue (mises à jour des définitions, licences, etc.)	Décidez de poursuivre ou d'arrêter Trend Micro (voir Trend Micro Deep Security)
Gestion des modifications	Comptes d'application et de base	La console et l'API AMS RFC sont supprimées Les politiques de contrôle de service personnalisées d'AMS (SCPs) qui contiennent des restrictions d'accès au niveau du compte sont détachées lors de la déconnexion du compte Application et supprimées lors de la déconnexion du compte Core	Vous devez utiliser une AWS API native pour créer de nouvelles ressources, modifier des ressources existantes ou mettre à jour des AWS CloudFormation piles existantes Les restrictions d'accès ne sont plus imposées au niveau du compte via AMS fourni SCPs	Assurez-vous que les rôles d'utilisateur fournissent un accès suffisant pour utiliser AWS les services Créer SCPs pour fournir des restrictions d'autorisation au niveau du compte

Composant	Account type (Type de compte)	Mesures prises pour décoller	Impacts potentiels	Action recommandée par le client
Images et automatisations du système d'exploitation AMS pour la gestion des services	Comptes d'application et de base	AMS ne fournit plus de support sur les personnalisations et les scripts de lancement inclus dans AMS fournis EC2 AMIs Les AMS fournis EC2 AMIs restent disponibles sur vos comptes externes Les runbooks Systems Manager Automation fournis par AMS ne sont pas partagés et ne peuvent plus être utilisés.	Après le téléchargement, le fournisseur AMS a AMIs lancé AWS CloudFormation send cfn-signal en FAILURE raison de dépendances manquantes vis-à-vis des composants AMS Les processus opérationnels qui dépendent des runbooks Systems Manager Automation fournis par AMS peuvent échouer	Passez en revue et mettez à jour tous les processus de construction ou opérationnels qui dépendent des runbooks AMS fournis AMIs ou de Systems Manager Automation
Infrastructure de services partagés	Comptes principaux	L'accès AMS est supprimé et AMS ne gère plus les composants partagés, notamment AMS Managed Active Directory AWS Transit Gateway, et AWS Organizations	Perte de gestion liée à l'infrastructure partagée	Réinitialisez l'accès administrateur à AMS Managed Active Directory et assumez la gestion des composants des services partagés

Composant	Account type (Type de compte)	Mesures prises pour décoller	Impacts potentiels	Action recommandée par le client
Génération de rapports	Comptes d'application et de base	AMS ne collecte plus les informations relatives aux comptes ou aux ressources pour les rapports agrégés	Perte de visibilité sur les indicateurs opérationnels et commerciaux (couverture des sauvegardes et des correctifs, gestion des modifications et activité des incidents)	Remplacez tous les rapports de données agrégés nécessaires entre les comptes par leur propre solution
Équipe chargée des comptes et service d'assistance AMS	Comptes d'application et de base	L'équipe chargée des comptes AMS (CSDM, CA) et le centre de service des opérations d'AMS ne prennent plus en charge les comptes externes	Perte de soutien opérationnel lié à l'expertise dans l'architecture de zone d'atterrissage multi-comptes conçue par AMS et les composants associés	Assurez-vous que le personnel est suffisant et que vous connaissez bien la structure des comptes et les ressources pour soutenir les opérations dans l'environnement

Alternatives d'accès

Voici des méthodes alternatives pour conserver l'accès à votre EC2 stack une fois que vous avez quitté les comptes AMS :

- Utilisez le gestionnaire de session pour accéder aux EC2 instances dotées d'autorisations élevées sans avoir besoin de bastions ou d'accès au réseau entrant. Pour de plus amples informations, veuillez consulter [AWS Systems Manager Session Manager](#).

- Joignez EC2 les instances à un autre domaine Active Directory avec de nouvelles informations d'identification de domaine. Si vous l'utilisez AWS Directory Service, consultez [Joindre une EC2 instance à votre AWS Managed Microsoft AD répertoire](#).
- Utilisez des comptes d'utilisateurs locaux que vous avez créés via l'une des autres méthodes d'accès ou via [AWS Systems Manager Run Command](#).

Désactiver les scripts de EC2 lancement d'AMS

Systèmes d'exploitation Linux

Utilisez le gestionnaire de packages de votre distribution pour désinstaller le `ams-modules` package. Par exemple, pour Amazon Linux 2, utilisez `yum remove ams-modules`.

Systèmes d'exploitation Windows

Pour désactiver les scripts de EC2 lancement dans Windows, procédez comme suit :

1. Windows Server 2008/2012/2012r2/2016/2019 :

Désactivez ou supprimez la tâche planifiée de démarrage de Managed Services dans le planificateur de tâches. Pour répertorier les tâches planifiées, exécutez la `Get-ScheduledTask -TaskName '*Ec2*'` commande.

Windows Server 2022 :

Supprimez la [tâche EC2 Launch v2](#). Cette tâche s'exécute par postReady étapes `Initialize-AMSBoot` dans `C : \ \ Amazon ProgramData \ EC2 Launch \ config \ agent-config.yml` sur l'instance. Voici un extrait d'un exemple : `agent-config.yml`

```
{
  "task": "executeScript",
  "inputs": [
    {
      "frequency": "always",
      "type": "powershell",
      "runAs": "localSystem"
    }
  ]
}
```

2. (Facultatif) Supprimez le contenu du fichier suivant :

```
C:\Program Files\WindowsPowerShell\Modules\AWSManagedServices.*  
C:\Windows\System32\WindowsPowerShell\v1.0\Modules  
\AWSManagedServices.Build.Utilities\*
```

PBIS Open/Enterprise (pont AD)

Pour déterminer si vous utilisez l'édition PBIS Open ou PBIS Enterprise (AD Bridge), exécutez la commande suivante dans une instance EC2 gérée sous Linux :

```
yum info | grep pbis
```

Voici un exemple de sortie illustrant PBIS Enterprise (AD Bridge) :

```
Name      : pbis-enterprise  
From repo : pbise  
Name      : pbis-enterprise-devel  
Repo      : pbise  
Description : The pbis-enterprise-devel package includes the development
```

PBIS ouvert

PBIS Open est un produit obsolète qui BeyondTrust n'est plus compatible. Pour plus d'informations, consultez la documentation de [BeyondTrust pbis-open](#).

Pont AD (PBIS Enterprise)

Vous pouvez effectuer l'une des actions suivantes :

- Renouvelez les licences et poursuivez l'exploitation d'AD Bridge. Contactez-nous BeyondTrust pour discuter des licences et de l'assistance.
- Arrêtez d'utiliser AD Bridge. Exécutez la commande Shell suivante pour supprimer le package PBIS-Enterprise des instances gérées par Linux. Pour plus d'informations, consultez la BeyondTrust documentation [Quitter un domaine et désinstaller l'agent AD Bridge](#).

```
$ sudo /opt/pbis/bin/uninstall.sh purge
```

Quittez le domaine Active Directory géré par AMS sans supprimer l'agent PBIS

Vous avez la possibilité de quitter l'Active Directory géré par AMS sans supprimer l'agent PBIS. Utilisez l'une des solutions suivantes, en fonction de votre système d'exploitation :

Linux operating systems

Utilisez le PBIS de l'AD géré par AMS pour exécuter la commande shell suivante afin de dissocier une instance Linux. EC2 Pour plus d'informations, consultez la documentation de [BeyondTrust pbis-open](#) ou d'[BeyondTrust AD Bridge](#), selon la version que vous utilisez.

```
$ sudo /opt/pbis/bin/domainjoin-cli leave
```

Un message d'erreur similaire au suivant peut s'afficher :

```
Error: LW_ERROR_KRB5_REALM_CANT_RESOLVE [code 0x0000a3e1]
Cannot resolve network address for KDC in requested realm
```

Si cette erreur se produit, exécutez les commandes suivantes pour supprimer le registre du fournisseur AD et redémarrer lwsmd les services :

```
$ /opt/pbis/bin/regshell dir '[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory\DomainJoin]'
```

Utilisez l'ID de répertoire généré par la commande précédente (par exemple **A123EXAMPLE.AMAZONAWS.COM**) pour exécuter les commandes suivantes :

```
$ /opt/pbis/bin/regshell delete_tree \
'[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory\DomainJoin\
\DIRECTORID]'
```

```
$ /etc/pbis/redhat/lwsmd restart
```

```
$ /opt/pbis/bin/lwsm restart lwreg
```

Windows operating systems

```
# Collect hostname and domain name using:

Test-ComputerSecureChannel -verbose
```

```
# Disjoin computer from the domain:  
  
netdom remove hostname /domain:domain name /force
```

Note

Assurez-vous de désactiver ou de supprimer la tâche planifiée de Managed Services Startup comme indiqué dans [Désactiver les scripts de EC2 lancement d'AMS](#).

Trend Micro Deep Security

Utilisez l'une des options suivantes pour continuer ou arrêter l'utilisation de Trend Micro Deep Security :

Poursuivre l'utilisation

- (Si vous déconnectez l'intégralité du MALZ) Après avoir déconnecté le compte Core, reconnectez les comptes d'application externes au Trend Micro Deep Security Manager (DSM) existant et conservez les licences dans le compte Shared Services. Pour plus d'informations, consultez [Ajouter des comptes AWS cloud](#) et [Vérifier les informations de votre licence](#).
 1. Connectez-vous au compte de services partagés et accédez à la console Secrets Manager.
 2. Récupérez les informations d'identification de l'administrateur de la console DSM stockées dans le `/ams/eps/` chemin.
 3. Connectez-vous à la console DSM à l'[adresse https://dsm.sentinel.int](https://dsm.sentinel.int).
 4. Choisissez Utiliser le rôle multi-comptes, puis entrez `arn:aws:iam::ACCOUNTID:role/mc_eps_cross_account_role`. Remplacez ACCOUNTID par l'ID du compte de l'application non embarquée.
 5. Choisissez Suivant.
 6. Patientez quelques minutes pour que DSM procède à la découverte du compte et indique que la synchronisation est réussie.
- Reconnectez les comptes d'applications externes à une nouvelle installation de Trend Micro DSM. Pour plus d'informations, voir [Activer et protéger les agents](#) et [Activer l'agent](#).
- Reconnectez les comptes d'applications externes à Trend Micro Cloud One. Pour plus d'informations, voir [Migrer de Deep Security vers Workload Security](#) et [Migrer depuis un DSM sur site](#).

Cesser l'utilisation

- Désinstallez les agents Trend Micro Deep Security des comptes d'applications externes. Pour plus d'informations, voir [Désinstaller Deep Security](#).

Modes de gestion des modifications

AWS Managed Services (AMS) utilise le mode de gestion des modifications pour contrôler les modifications dans AMS Advanced. Les modes de gestion du changement vous aident à maintenir des normes opérationnelles élevées pour l'environnement, à contrôler les risques et à prévenir les impacts négatifs. AMS Advanced propose différents modes qui offrent différents niveaux de contrôle et de risque. Tous les modes, à l'exception du mode géré par le client, sont gérés par AMS. Les modes de gestion des modifications disponibles sont les suivants :

- Mode RFC (anciennement mode CM standard) : fournit un système de « demande de modification » (RFC) et des types de modification personnalisés par AMS () CTs
- Mode Direct Change : identique au mode RFC et utilisation d'AWS APIs et de consoles pour créer des ressources gérées par AMS
- AWS Service Catalog on AMS : similaire au mode Direct Change, mais au lieu d'utiliser le système de gestion des modifications AMS (RFCs), vous utilisez AWS Service Catalog pour créer des ressources qu'AMS gère ensuite.
- Mode développeur : identique au mode Direct Change, seules les ressources que vous créez avec AWS APIs et les consoles ne sont pas gérées par AMS. Vous êtes responsable de leur gestion
- Mode Self Service Provisioning (SSP) : identique au mode développeur, sauf qu'il n'y a pas d'accès au système de gestion des modifications AMS (non) RFCs
- Mode géré par le client : AMS vous fournit une zone d'atterrissage multi-comptes, mais toute la gestion des ressources est de votre responsabilité

Le système de gestion des modifications AWS Managed Services (AMS), qui utilise l'API de gestion des modifications (CM), fournit des opérations permettant de créer et de gérer des demandes de modification (RFCs) pour les comptes de zone d'atterrissage multi-comptes (MALZ) et de zone d'atterrissage à compte unique (SALZ).

Une demande de modification (RFC) est une demande créée par vous ou AMS via l'interface AMS pour apporter une modification à votre environnement géré et inclut un ID de type de modification (CT) pour une opération particulière.

L'API AMS de gestion des modifications (CM) fournit des opérations permettant de créer et de gérer des demandes de modification (RFCs). Vous pouvez créer, mettre à jour, soumettre, approuver, rejeter et annuler RFCs. Les opérateurs AMS peuvent créer, mettre à jour, soumettre, approuver, rejeter, annuler et marquer RFCs comme fermé.

Pour obtenir la liste des préfixes réservés AMS à ne pas utiliser dans les balises ou autres noms, consultez la section [Préfixes réservés](#).

Pour plus d'informations sur chaque type de modification, y compris des schémas et des exemples, consultez le manuel [AMS Change Type Reference](#).

 Note

Tous les appels d'API de gestion des modifications sont enregistrés dans AWS CloudTrail. Pour plus d'informations, consultez la section [Accès à vos journaux](#).

Vue d'ensemble des modes

Utilisez ces informations pour vous aider à sélectionner le mode AWS Managed Services (AMS) approprié pour héberger vos applications, en fonction de la combinaison de flexibilité et de gouvernance prescriptive que vous souhaitez pour atteindre vos objectifs commerciaux.

Le public cible de ces informations est :

- Les équipes clients sont responsables de la stratégie et de la gouvernance de leur zone d'atterrissage. Ces informations aideront l'équipe à jeter les bases d'une zone d'atterrissage gérée par AMS, avec les modes AMS qu'elle aimerait proposer à ses clients internes et externes.
- Les propriétaires d'entreprises et d'applications chargés de migrer leur application vers AMS. Ces informations aideront à planifier la migration des applications, avec le mode AMS approprié à migrer/host leur application. Notez qu'une même application peut être hébergée dans plusieurs modes AMS au cours des différentes phases de son cycle de vie du développement logiciel (SDLC).
- Les partenaires AMS sont chargés de guider les clients sur les différentes options de création et de migration vers AMS.

Ces informations sont particulièrement utiles pendant la phase initiale de configuration de votre plateforme gérée par AMS, et lorsque vous passez de la phase de base à la phase de migration de votre parcours d'adoption du cloud, juste après l'intégration à AMS et que vous vous concentrez sur la gouvernance et les opérations des applications.

Types de modes et de comptes dans AMS

Les modes AWS Managed Services (AMS) peuvent être définis comme les moyens d'interagir avec le service AMS dans le cadre du cadre de gouvernance spécifique à chaque mode. Les différences de zone d'atterrissage, zone d'atterrissage multi-comptes ou MALZ et zone d'atterrissage monocompte ou SALZ sont notées.

 Note

Pour plus de détails sur le déploiement d'applications et le choix du mode AMS approprié, consultez la section [Modes AMS et applications ou charges de travail](#).

Pour des cas d'utilisation réels des différents modes, voir [Cas d'utilisation réels des modes AMS](#)

Le tableau suivant décrit les modes par service AMS.

Fonctionnalité AMS	Mode RFC (ancien mode CM standard)/ OOD *	Mode de changement direct	AWS Service C	Provisionnement en libre-service/ Mode développeur	Géré par le client
Configuration de la zone d'atterrissage	MALZ et SALZ	MALZ et SALZ		MALZ et SALZ	
Gestion des modifications	Planification des modifications, examen des modifications manuelles et enregistrement des modifications	Identique au mode RFC pour les modifications à haut risque telles que l'IAM ou les groupes de sécurité		Aucune	

Fonctionnalité AMS	Mode RFC (ancien mode CM standard)/ OOD *	Mode de changement direct	AWS Service C	Provisionnement en libre-service/ Mode développeur	Géré par le client
Journalisation, surveillance, garde-corps et gestion des événements	Oui (ressources prises en charge)			Non	
Gestion de la continuité	Oui (ressources prises en charge)			Non applicable/ Non	Non
Gestion de la sécurité	Contrôles de sécurité au niveau de l'instance et contrôles au niveau du compte			Contrôles au niveau du compte	Contrôles au niveau de l'organisation AWS
Gestion des correctifs	Oui			Non applicable/ Non	Non
Gestion des incidents et des problèmes	SLA de réponse et de résolution pour les ressources prises en charge par AMS			Réponse (SLA) pour les ressources qui en résultent	Non
Génération de rapports	Oui			Non	
Gestion des demandes de service	Oui			Demandes de support uniquement	Non

* Operations On Demand (OOD) propose une offre aux clients utilisant le mode RFC pour gérer leurs modifications grâce à des ressources dédiées. Pour plus de détails, consultez le [catalogue d'offres Operations on Demand](#) et adressez-vous à votre responsable de prestation de services cloud (CSDM).

 Note

[Mode de provisionnement en libre-service dans AMS](#) et les deux [Mode développeur avancé AMS](#) peuvent sembler convenir à une application dotée d'une architecture complexe ancrée dans les services AWS natifs. Lorsque vous concevez des charges de travail, vous faites des compromis entre excellence opérationnelle et agilité, en fonction de votre contexte commercial. C'est une bonne façon de choisir le mode SSP ou le mode développeur pour votre application. La sélection peut également changer en fonction de la phase SDLC de l'application. Par exemple : lorsque l'application est prête pour la production, le mode SSP peut être une option plus appropriée en raison des barrières de sécurité AMS plus strictes dans ce mode. Les garde-fous sont appliqués sous la forme de contrôles préventifs tels que le contrôle des modifications basé sur le protocole RFC pour les mises à jour IAM et SCPs au niveau de l'unité d'organisation de l'application. Ces décisions professionnelles peuvent orienter vos priorités en matière d'ingénierie. Vous pouvez optimiser pour accroître la flexibilité des propriétaires d'applications en phase de « pré-production » au détriment de la gouvernance et du support opérationnel.

Architecture MALZ et modes AMS associés

La zone de landing zone multi-comptes (MALZ) AMS vous donne la possibilité de provisionner automatiquement des comptes d'applications (ou des comptes de ressources) sous les unités organisationnelles (UO) par défaut : UO gérée par le client, UO gérée ou UO de développement. L'infrastructure fournie dans les comptes d'applications créés dans le cadre de chacun de ces comptes OUs est soumise au mode AMS spécifique proposé par les comptes de base OUs. Il est courant de trouver une combinaison de deux modes ou plus dans le même compte d'application. Par exemple : le mode RFC et le mode SSP peuvent coexister dans un compte géré AMS hébergeant une architecture de pipeline composée d'API Gateway et Lambda pour les fonctions de déclenchement EC2, et de S3 et SQS pour l'ingestion et l'orchestration. Dans ce cas, le mode SSP s'appliquerait à Lambda et à API Gateway.

La figure 1 montre comment les différents modes sont proposés par le biais des fondamentaux OUs d'AMS. Lorsque vous demandez un nouveau compte d'application dans AMS, vous devez sélectionner l'unité d'organisation du compte.

Architecture MALZ et modes AMS associés

AMS s'appuie sur les principes fondamentaux OUs basés sur les meilleures pratiques d'AWS pour gérer les comptes de manière logique à l'aide des politiques de contrôle des services (). SCPs Cela permet d'appliquer le cadre de gouvernance à chaque mode AMS. Toutes les barrières de gouvernance et de sécurité (sous forme de SCPs) appliquées aux fondamentaux sont OUs également appliquées automatiquement. custom/child OUs Un supplément SCPs peut être demandé pour l'enfant OUs. Il est important de comprendre que les comptes d'applications sont différents des modes. Les modes sont appliqués à l'infrastructure fournie dans les comptes et définissent les responsabilités opérationnelles entre AMS et les clients.

Figure 1 : Architecture MALZ et modes AMS associés

Note

Le terme « restrictif » implique que vous pouvez demander des politiques personnalisées pour ces derniers OUs. Elles sont approuvées par AMS afin de garantir qu'elles n'interfèrent pas avec les capacités d'AMS à fournir une excellence opérationnelle. case-by-case Pour une liste détaillée des rambardes AMS, voir Rambardes [AMS dans le guide de l'utilisateur](#).

Modes AMS et applications ou charges de travail

Tenez compte des exigences opérationnelles et de gouvernance de vos applications lorsque vous sélectionnez le bon mode, soit en demandant un nouveau compte d'application, soit en hébergeant l'application dans un compte d'application existant. La sélection du mode AMS approprié pour chaque application ou charge de travail dépend des facteurs suivants :

- Le type de fonction de cycle de vie du SDLC que l'environnement fournira (par exemple, sandbox avec des modifications non modérées, UAT avec des modifications fréquentes, production avec des modifications minimales et hautement réglementée)
- Les politiques de gouvernance nécessaires (appliquées SCPs au niveau de l'UO)

- Modèle opérationnel (si vous souhaitez assumer la responsabilité opérationnelle ou si vous souhaitez l'externaliser à AMS)
- Les résultats commerciaux souhaités, tels que le temps nécessaire pour opérer dans le cloud et le coût des opérations.

 Note

Pour une description des types de mode par service AMS, voir [Types de modes et de comptes dans AMS](#).

Pour des cas d'utilisation réels des différents modes, voir [Cas d'utilisation réels des modes AMS](#)

Le tableau suivant décrit les principales considérations à prendre en compte par les propriétaires d'applications pour les aider à choisir le mode AMS le plus approprié. Les propriétaires d'applications doivent prévoir une phase d'évaluation avant la migration des applications afin de bien comprendre quel mode s'applique à leur application spécifique. Exemple : pour les applications basées sur des services cloud natifs ou sur une architecture sans serveur, la meilleure option pourrait être de commencer à créer et à itérer en mode développeur et de déployer l'infrastructure finale sous forme de code à l'aide du mode AMS Managed — SSP. Dans ce cas, une légère refactorisation peut être nécessaire pour garantir que tous les CloudFormation modèles créés pour un déploiement automatisé respectent les directives d'ingestion établies par AMS. En outre, toutes les autorisations IAM doivent être approuvées par AMS Security afin de garantir qu'elles respectent le modèle du moindre privilège.

Le mode AMS sélectionné pour héberger l'application peut vous aider à élaborer le modèle d'exploitation cloud que vous souhaitez.

 Note

Plusieurs modèles d'exploitation cloud peuvent exister dans une seule zone d'accueil gérée par AMS en fonction des différents modes AMS sélectionnés pour héberger les applications.

Problèmes de décision	Mode CM standard/ OOD *	AWS Service	Mode de changement direct	Provisionnement en libre-service	Mode développeur	Géré par le client

État de préparation opérationnelle

Journalisation, surveillance et gestion des événements	AMS est responsable de toutes les infrastructures gérées		Client responsable des services fournis en libre-service (SSP)	Client responsable des ressources mises à disposition à l'aide du rôle de développeur IAM en dehors du système AMS CM	Client responsable
Gestion de la continuité	Responsabilité d'AMS d'exécuter le plan de sauvegarde sélectionné par le client		Client responsable des services fournis en libre-service (SSP)	Client responsable des ressources mises à disposition à l'aide du rôle de développeur IAM en dehors du système AMS CM	
Gestion de l'accès au	Géré par AMS via AD Trust unidirectionnel avec domaine sur site.		Ne s'applique pas	Client responsable des	

Problèmes de décision	Mode CM standard/ OOD *	AWS Service	Mode de changement direct	Provisionnement en libre-service	Mode développeur	Géré par le client
niveau de l'instance	Nécessite une infrastructure gérée pour rejoindre le domaine AMS				ressources mises à disposition à l'aide du rôle de développeur IAM en dehors du système AMS CM	
Gestion de la sécurité et gestion de l'accès au niveau du compte	Responsabilité d'AMS pour tous les comptes gérés			AMS est responsable de tous les comptes gérés	Client responsable des ressources mises à disposition à l'aide du rôle de développeur IAM en dehors du système AMS CM	

Problèmes de décision	Mode CM standard/ OOD *	AWS Service	Mode de changement direct	Provisionnement en libre-service	Mode développeur	Géré par le client
Gestion des correctifs	Responsabilité d'AMS pour tous les comptes gérés			Client responsable des services fournis en libre-service (SSP)	Client responsable des ressources mises à disposition à l'aide du rôle de développeur IAM en dehors du système AMS CM	
Gestion des modifications	Responsabilité d'AMS pour tous les comptes gérés			Client responsable des services fournis en libre-service (SSP)	Client responsable des ressources mises à disposition à l'aide du rôle de développeur IAM en dehors du système AMS CM	

Problèmes de décision	Mode CM standard/ OOD *	AWS Service	Mode de changement direct	Provisionnement en libre-service	Mode développeur	Géré par le client
Gestion du provisionnement	Prescriptif et standardisé pour les options de provisionnement proposées dans AMS	Flexibilité permettant d'utiliser directement l'API de service AWS pour AWS Service Catalog conformément aux normes prescriptives AMS	Flexibilité permettant d'utiliser directement l'API de service AWS conformément aux normes prescriptives AMS	Flexibilité permettant d'utiliser directement le service AWS APIs pour les services SSP	Flexibilité permettant d'utiliser directement l'API de service AWS pour le provisionnement	
Gestion des incidents et audit	AMS est responsable de tous les comptes gérés				Client responsable des ressources mises à disposition à l'aide du rôle de développeur IAM en dehors du système de gestion des modifications AMS	

Problèmes de décision	Mode CM standard/ OOD *	AWS Service	Mode de changement direct	Provisionnement en libre-service	Mode développeur	Géré par le client
GuardRails et infrastructure partagée (réseau) et cadre de sécurité	Utilisation prescriptive et standardisée des comptes AMS Core					Flexible et sur mesure en tirant parti des comptes AMS Core
Préparation à l'application						
Refactorisation des applications	Une légère refactorisation est nécessaire				Une légère refactorisation est nécessaire (si le provisionnement est effectué à l'aide d'AMS Standard CM)	Pas besoin de refactorisation
Support pour les services AWS	Limité à ce qui est pris en charge par AMS					Non limité
Considérations commerciales						

Problèmes de décision	Mode CM standard/ OOD *	AWS Service	Mode de changement direct	Provisionnement en libre-service	Mode développeur	Géré par le client
Délai de préparation opérationnelle	Trois à six mois			6 mois ou plus selon les compétences opérationnelles des applications du client		6 à 18 mois en fonction de l'infrastructure du client et des compétences opérationnelles des applications
Coûts	\$\$\$\$			\$\$\$	\$\$	\$
Exemples d'applications	Serveur Web avec pile à 3 niveaux, applications conformes aux exigences réglementaires			Serveur Web utilisant API Gateway, application conteneurisée utilisant ECS/EKS	Itération/optimisation sur une application Data Lake utilisant Lambda, Glue, Athena, etc.	Décentralisation, accounts/applications comme le bac à sable ou les applications gérées par des tiers

* Operations On Demand (OOD) propose une offre aux clients utilisant le mode CM standard pour gérer leurs modifications grâce à des ressources dédiées. Pour plus de détails, consultez le [catalogue d'offres Operations on Demand](#) et adressez-vous à votre responsable de prestation de services cloud (CSDM).

 Note

La comparaison des prix entre le mode SSP et le mode développeur suppose que les mêmes services AWS sont fournis.

Comparaison des modes AMS avec les objectifs commerciaux et informatiques

Comme indiqué, si vous recherchez un modèle de gouvernance hautement contrôlé et standardisé pour vos applications, les modes Standard Change, AWS Service Catalog ou Direct Change gérés par AMS sont les meilleurs choix. Si vous avez besoin d'un modèle de gouvernance sur mesure axé sur l'innovation des applications sans avoir besoin de préparation opérationnelle, sélectionnez le mode géré par le client. Avec le mode géré par le client, la mise en œuvre de vos applications peut prendre plus de temps, car il vous incombe de définir les personnes, les processus et les outils nécessaires pour soutenir les capacités opérationnelles telles que la gestion des incidents, la gestion des configurations, la gestion du provisionnement, la gestion de la sécurité, la gestion des correctifs, etc.

Cas d'utilisation réels des modes AMS

Examinez-les pour déterminer comment utiliser les modes AMS.

- Cas d'utilisation 1 : il est impératif pour l'entreprise de réduire ses coûts en quittant son centre de données dans des délais serrés : une entreprise confrontée à un événement commercial important, tel que la sortie d'un centre de données, souhaite réhéberger ses applications sur site dans le cloud. La majeure partie de l'inventaire sur site se compose de serveurs Windows et Linux avec une combinaison de versions de systèmes d'exploitation. Ce faisant, le client souhaite également tirer parti des économies qu'offre le passage au cloud et améliorer le niveau technique et de sécurité de ses applications. Le client souhaite agir rapidement mais ne dispose pas encore de l'expertise interne en matière d'opérations cloud. Le client doit trouver un équilibre entre le refactoring, car trop de refactoring peut être risqué par rapport à un calendrier serré. Cependant, grâce à certaines refactorisations, telles que la mise à jour des versions du système d'exploitation et l'optimisation des bases de données, les applications peuvent atteindre un niveau de performance supérieur. Dans cet exemple, le client peut sélectionner le mode RFC géré par AMS pour réhéberger la plupart de ses applications. AMS assure les opérations d'infrastructure, tout en guidant les équipes opérationnelles des clients sur les meilleures pratiques en matière de sécurité des opérations dans le cloud.

AWS Service Catalog géré par AMS et le mode Direct Change géré par AMS offrent au client une flexibilité supplémentaire tout en obtenant les mêmes résultats et objectifs commerciaux. En outre, le client peut utiliser l'offre AMS Operations On Demand (OOD) pour disposer d'ingénieurs d'exploitation AMS dédiés chargés de prioriser l'exécution des demandes de changement (RFCs).

Tout en déléguant les tâches opérationnelles indifférenciées de l'infrastructure (correctifs, sauvegardes, gestion des comptes, etc.) à AMS, le client peut continuer à se concentrer sur l'optimisation de son application et renforcer ses équipes internes sur les opérations cloud. AMS fournit des rapports mensuels au client sur les économies de coûts et formule des recommandations sur l'optimisation des ressources. Dans ce cas d'utilisation, si le client a décidé de ne pas refactoriser certaines end-of-life applications hébergées sur des versions de système d'exploitation existantes telles que Windows 2003 et 2008, elles peuvent également être migrées vers AMS et hébergées sur un compte utilisant le mode géré par le client.

- Cas d'utilisation 2, création d'un lac de données avec Lambda, Glue et Athena dans les limites sécurisées d'AMS : une entreprise cherche à configurer un lac de données pour répondre aux besoins de reporting de plusieurs applications dans AMS. Le client souhaite utiliser des compartiments S3 pour le stockage des ensembles de données et AWS Athena pour interroger l'ensemble de données pour chaque rapport. S3 et AWS Athena seront déployés dans des comptes gérés AMS distincts. Le compte S3 propose également d'autres services tels que Glue, Lambda et Step Functions pour créer un pipeline d'ingestion de données. Glue, Lambda, Athena et Step Functions sont considérés comme des services Self-Service Provisioning (SSP) dans ce cas. Le client a également déployé une EC2 instance dans le compte qui fait office de tooling/scripting serveur ad hoc. Le client commence par demander à AMS d'activer les services SSP sur son compte AMS Managed. AMS fournit un rôle IAM pour chaque service que le client peut assumer, une fois le rôle intégré à la solution de fédération du client. Pour faciliter la gestion, le client peut également combiner les politiques relatives aux différents rôles IAM en un seul rôle personnalisé, ce qui évite d'avoir à changer de rôle lorsqu'il travaille entre les services AWS. Une fois le rôle activé dans le compte, le client peut configurer les services selon ses besoins. Cependant, le client doit utiliser le système de gestion des modifications AMS pour demander des autorisations supplémentaires, en fonction de son cas d'utilisation.

Par exemple, pour accéder à Glue Crawlers, Glue a besoin d'autorisations supplémentaires. Des autorisations supplémentaires seront également nécessaires pour créer des sources d'événements pour Lambda. Le client travaillera avec AMS pour mettre à jour les rôles IAM afin de permettre à Athena d'accéder à plusieurs comptes pour interroger les compartiments S3. Des mises à jour des rôles de service ou des rôles liés à un service seront également nécessaires par le biais

de la gestion des modifications d'AMS pour que Lambda appelle le service Step Functions et pour Glue pour lire et écrire dans tous les compartiments S3. AMS travaille avec ses clients pour s'assurer que le modèle d'accès avec le moindre privilège est respecté et que les modifications IAM demandées ne sont pas trop permissives et n'exposent pas l'environnement à des risques inutiles. L'équipe du lac de données du client passe du temps à planifier toutes les autorisations IAM nécessaires pour les services spécifiques à l'architecture du client et demande à AMS de les activer. En effet, toutes les modifications IAM sont traitées manuellement et examinées par l'équipe de sécurité AMS. Le temps nécessaire au traitement de ces demandes doit être pris en compte dans le calendrier de déploiement de l'application.

Les services SSP étant opérationnels sur le compte, le client peut demander de l'assistance et signaler les problèmes via la gestion des incidents et les demandes de service AMS. Toutefois, AMS ne surveillera pas activement les indicateurs de performance et de simultanéité pour Lambda, ni les indicateurs de travail pour Glue. Il est de la responsabilité du client de s'assurer que la journalisation et la surveillance appropriées sont activées pour les services SSP. L' EC2 instance et le compartiment S3 du compte sont entièrement gérés par AMS.

- Cas d'utilisation 3, configuration rapide et flexible d'un pipeline de déploiement CI/CD dans AMS : un client cherche à configurer un pipeline CI/CD basé sur Jenkins pour déployer un pipeline de code sur tous les comptes d'applications dans AMS. Le client trouvera peut-être qu'il est préférable d'héberger ce pipeline CI/CD en mode Direct Change (DCM) géré par AMS ou en mode développeur géré par AMS, car cela lui permet de configurer le serveur Jenkins avec la configuration personnalisée requise EC2, avec les autorisations d'accès IAM souhaitées CloudFormation et les compartiments S3 hébergeant le référentiel d'artefacts. Bien que cela puisse également être fait en mode RFC géré par AMS, l'équipe client devra créer plusieurs manuels RFCs pour que les rôles IAM puissent itérer sur l'ensemble d'autorisations approuvées le moins permissif, qui sont examinées manuellement par AMS. DCM permet aux clients d'atteindre leurs objectifs opérationnels sur AWS tout en évitant de devoir créer plusieurs manuels RFCs pour les rôles IAM, lors de l'utilisation du mode RFC géré par AMS, afin d'itérer sur l'ensemble d'autorisations approuvées le moins permissif, qui sont examinées manuellement par AMS. Cela nécessiterait du temps et de la formation de la part du client pour accélérer les processus et les outils AMS. En mode développeur, le client peut commencer par un « rôle de développeur » pour provisionner l'infrastructure à l'aide d'AWS natif APIs. Le moyen le plus rapide et le plus flexible de configurer ce pipeline serait d'utiliser le mode AMS Managed-Developer. Le mode développeur est le moyen le plus rapide et le plus simple, tout en compromettant l'intégration opérationnelle, tandis que le DCM est moins flexible mais fournit le même niveau de support opérationnel que le mode RFC.

- Cas d'utilisation 4, modèle d'exploitation sur mesure au sein de la base AMS : un client souhaite quitter son centre de données dans les délais et l'une de ses applications d'entreprise est entièrement gérée par un MSP tiers, y compris les opérations d'application et les opérations d'infrastructure. En supposant que le client n'ait pas le temps de refactoriser cette application afin qu'elle puisse être exploitée par AMS, le mode géré par le client est une option appropriée. Le client peut profiter de la configuration automatisée et rapide de la zone d'atterrissage gérée par AMS. Ils peuvent tirer parti de la gestion centralisée des comptes qui contrôle la distribution automatique des comptes et la connectivité via le compte réseau centralisé. Cela simplifie également leur facturation en consolidant les frais de tous les comptes gérés par le client via le compte AMS Payer. Le client dispose de la flexibilité nécessaire pour configurer son modèle de gestion des accès sur mesure avec le MSP, indépendamment de la gestion d'accès standard utilisée pour les comptes gérés par AMS. Ainsi, en utilisant le mode géré par le client, ils peuvent configurer un environnement géré AMS tout en répondant à leurs besoins commerciaux en matière de libération de leur environnement sur site. Dans ce cas, si le client possède également des applications Windows qu'il migre vers le cloud et qu'il choisit de les déplacer vers un compte géré par le client, il est responsable de la création d'un modèle d'exploitation cloud. Cela peut être complexe, coûteux et chronophage selon la capacité du client à transformer les processus informatiques traditionnels et à former le personnel. Le client peut économiser du temps et de l'argent en « transférant » ces charges de travail vers un compte géré par AMS et en déléguant les opérations d'infrastructure à AMS.

Note

Les clients peuvent parfois ressentir le besoin de déplacer les comptes d'applications entre le cadre de gouvernance du mode RFC ou SSP et le mode développeur. Par exemple, les clients peuvent héberger une application en mode géré par AMS dans le cadre de la migration initiale, mais ils souhaitent réécrire l'application au fil du temps afin de l'optimiser pour les services AWS natifs du cloud. Ils pouvaient changer le mode du compte de pré-production en passant du mode RFC géré par AMS au mode développeur géré par AMS, ce qui leur donnerait la flexibilité et l'agilité nécessaires au provisionnement de l'infrastructure. Cependant, une fois que les modifications de provisionnement de l'infrastructure ont été apportées à l'aide du « rôle de développeur », la même infrastructure ne peut pas être replacée en mode RFC géré par AMS. Cela est dû au fait qu'AMS ne peut garantir le fonctionnement de l'infrastructure qui a été provisionnée en dehors du système de gestion des modifications AMS. Les clients devront peut-être créer un nouveau compte d'application proposant le mode RFC géré par AMS, puis redéployer la configuration d'infrastructure « optimisée » via des CloudFormation modèles ou intégrée de manière

personnalisée dans un compte géré par AMIs AMS. Il s'agit d'une méthode propre pour déployer une configuration prête pour la production. Une fois déployée, l'application sera soumise à la gouvernance et aux opérations prescriptives de l'AMS. Il en va de même pour le changement de mode entre le mode géré par le client et le mode géré par AMS.

Mode RFC

Le mode RFC est le mode par défaut pour les clients du plan d'exploitation AMS Advanced. Il inclut un système de gestion des modifications avec des demandes de modification ou RFCs un catalogue de types de modifications à utiliser pour demander l'ajout ou la modification dont vous avez besoin sur vos comptes. Ce système de gestion des modifications fournit un niveau de sécurité en limitant les personnes autorisées à apporter des modifications à vos comptes.

Pour plus de détails sur les types de modifications AMS Advanced, voir [Que sont les types de modifications AMS ?](#).

Pour en savoir plus sur l'intégration à AMS Advanced, consultez l'introduction à l'[intégration d'AWS Managed Services](#).

Pour des exemples de types de modification, consultez la section « Informations supplémentaires » pour le type de modification concerné dans la section AMS Advanced Change Type Reference [Change Types par classification](#).

Note

Le mode RFC était auparavant appelé « mode de gestion des modifications » ou « mode CM standard ».

Rubriques

- [En savoir plus sur RFCs](#)
- [Quels sont les types de modifications ?](#)
- [Résolution des erreurs RFC dans AMS](#)

En savoir plus sur RFCs

Les demandes de changement ou RFCs de changement fonctionnent de deux manières. Tout d'abord, certains paramètres sont requis pour le RFC lui-même. Voici les options de l'CreateRfcAPI. Et deuxièmement, certains paramètres sont requis pour l'action de la RFC (les paramètres d'exécution). Pour en savoir plus sur les CreateRfc options, consultez la [CreateRfc](#) section de la référence de l'API AMS. Ces options apparaissent généralement dans la zone Configurations supplémentaires des pages Créer une RFC.

Vous pouvez créer et soumettre une RFC à l'aide de l'CreateRfcAPI, de la `aws amscm create-rfc` CLI ou à l'aide des pages Create RFC de la console AMS. Pour un didacticiel sur la création d'une RFC, voir [Création d'une RFC](#).

Rubriques

- [Quels sont RFCs ?](#)
- [Authentifiez-vous lors de l'utilisation de l'API/CLI AMS](#)
- [Comprendre les évaluations de sécurité RFC](#)
- [Comprendre les classifications des types de modifications RFC](#)
- [Comprendre les états d'action et d'activité des RFC](#)
- [Comprendre les codes d'état RFC](#)
- [Comprendre la mise à jour des RFC CTs et la détection de la dérive des CloudFormation modèles](#)
- [Horaire RFCs](#)
- [Approuver ou rejeter RFCs](#)
- [Demander des périodes d'exécution restreintes de la RFC](#)
- [Création, clonage, mise à jour, recherche et annulation RFCs](#)
- [Utilisez la console AMS avec RFCs](#)
- [En savoir plus sur les paramètres RFC courants](#)
- [Inscrivez-vous pour recevoir le courrier électronique quotidien du RFC](#)

Quels sont RFCs ?

Une demande de modification, ou RFC, vous permet d'apporter une modification à votre environnement géré par AMS ou de demander à AMS d'effectuer une modification en votre nom. Pour créer une RFC, vous devez choisir parmi les types de modification AMS, les paramètres

RFC (tels que le calendrier), puis vous soumettez la demande à l'aide de la console AMS ou des commandes [CreateRfcAPI](#) et [SubmitRfc](#)

Un RFC contient deux spécifications, l'une pour le RFC lui-même et l'autre pour les paramètres du type de modification (CT). Sur la ligne de commande, vous pouvez utiliser une commande RFC intégrée, ou un CreateRfc modèle standard au format JSON, que vous remplissez et soumettez avec le fichier de schéma CT JSON que vous créez (en fonction des paramètres CT). Le nom du CT est une description informelle du CT. Un CSIO (catégorie, sous-catégorie, article, opération) est une description plus formelle d'un CT. Seul l'ID CT doit être spécifié lors de la création d'une RFC.

AMS vous avertit lorsque la modification est terminée avec succès (réussite) ou non (échec).

Note

Pour plus d'informations sur le dépannage des défaillances RFC, consultez [Résolution des erreurs RFC dans AMS](#).

Le graphique suivant illustre le flux de travail d'une RFC que vous avez soumise.

Authentifiez-vous lors de l'utilisation de l'API/CLI AMS

Lorsque vous utilisez l'API/CLI AMS, vous devez vous authentifier avec des informations d'identification temporaires. Pour demander des informations d'identification de sécurité temporaires pour les utilisateurs fédérés [GetFederationToken](#), appelez [AssumeRole](#), [AssumeRoleWithSAML](#) ou [AssumeRoleWithWebIdentity](#) AWS Security Token Service (STS). APIs

Le SAML est un choix courant. Après la configuration, vous ajoutez un argument à chaque opération que vous appelez. Par exemple : `aws --profile saml amscm list-change-type-categories`.

Un raccourci pour les profils SAML 2.0 consiste à définir la variable de profil au début de chaque API/CLI `set AWS_DEFAULT_PROFILE=saml` (pour Windows ; pour Linux, ce serait le `casexport AWS_DEFAULT_PROFILE=saml`). Pour plus d'informations sur la définition des variables d'environnement CLI, consultez [Configuration de l'interface de ligne de commande AWS, Variables d'environnement](#).

Comprendre les évaluations de sécurité RFC

Le processus d'approbation de la gestion des modifications d'AWS Managed Services (AMS) garantit que nous effectuons un examen de sécurité des modifications que nous apportons à vos comptes.

AMS évalue toutes les demandes de modification (RFCs) par rapport aux normes techniques d'AMS. Toute modification susceptible de réduire le niveau de sécurité de votre compte en s'écartant des normes techniques fait l'objet d'un examen de sécurité. Au cours de l'examen de sécurité, AMS met en évidence les risques pertinents et, en cas de risque de sécurité élevé ou très élevé, votre personnel de sécurité autorisé accepte ou rejette le RFC. Tous les changements sont également évalués afin d'évaluer leur impact négatif sur la capacité d'exploitation d'AMS. Si des effets négatifs potentiels sont découverts, des examens et des approbations supplémentaires sont requis au sein de l'AMS.

Normes techniques AMS

Les normes techniques AMS définissent les critères de sécurité, les configurations et les processus minimaux pour établir la sécurité de base de vos comptes. Ces normes doivent être respectées à la fois par AMS et par vous.

Toute modification susceptible de réduire le niveau de sécurité de votre compte en s'écartant des normes techniques est soumise à un processus d'acceptation des risques, dans le cadre duquel le risque pertinent est mis en évidence par AMS et accepté ou rejeté par le personnel de sécurité autorisé de votre côté. Tous ces changements sont également évalués afin de déterminer s'il y aurait un impact négatif sur la capacité d'AMS à gérer le compte et, dans l'affirmative, des examens et des approbations supplémentaires sont requis au sein d'AMS.

Processus RFC de gestion des risques liés à la sécurité des clients (CSRM)

Lorsqu'un membre de votre organisation demande une modification de votre environnement géré, AMS examine la modification afin de déterminer si la demande risque de détériorer le niveau de sécurité de votre compte en ne respectant pas les normes techniques. Si la demande réduit le niveau de sécurité du compte, AMS informe le contact de votre équipe de sécurité du risque pertinent et exécute la modification ; ou, si la modification introduit un risque de sécurité élevé ou très élevé dans l'environnement, AMS demande l'approbation explicite de votre contact de l'équipe de sécurité sous la forme d'une acceptation des risques (expliqué ci-dessous). Le processus d'acceptation des risques par le client AMS est conçu pour :

- Assurez-vous que les risques sont clairement identifiés et communiqués aux bons propriétaires

- Minimisez les risques identifiés pour votre environnement
- Obtenez et documentez l'approbation des contacts de sécurité désignés qui comprennent le profil de risque de votre organisation
- Réduisez les frais opérationnels permanents liés aux risques identifiés

Comment accéder aux normes techniques et aux risques élevés ou très élevés

Nous avons mis à votre disposition la documentation relative aux normes techniques AMS

<https://console.aws.amazon.com/artifact/>sous forme de rapport à titre de référence. Consultez la documentation relative aux normes techniques d'AMS pour savoir si une modification nécessiterait l'acceptation des risques par votre contact de sécurité autorisé avant de soumettre une demande de modification (RFC).

Pour accéder au rapport sur les normes techniques, recherchez « AWS Managed Services (AMS) Technical Standards » dans la barre de recherche de l'onglet AWS Artifact Rapports après vous être connecté avec la valeur par défaut `AWSManagedServicesChangeManagementRole`.

Note

Le document de norme technique AMS est accessible au client `_ReadOnly_Role` dans la zone d'atterrissage à compte unique. Dans la zone de landing zone multi-comptes, les `AWSManaged ServicesAdminRole` données utilisées par les administrateurs de sécurité et `AWSManaged ServicesChangeManagementRole` celles utilisées par les équipes d'application peuvent être utilisées pour accéder au document. Si votre équipe utilise un rôle personnalisé, créez un autre RFC pour demander l'accès et nous mettrons à jour le rôle personnalisé spécifié.

Comprendre les classifications des types de modifications RFC

Les types de modifications que vous utilisez lors de la soumission d'une RFC sont divisés en deux grandes catégories :

- Déploiement : cette classification est destinée à la création de ressources.
- Gestion : cette classification sert à mettre à jour ou à supprimer des ressources. La catégorie Gestion contient également des types de modifications permettant d'accéder aux instances, de chiffrer ou de partager AMIs, ainsi que de démarrer, d'arrêter, de redémarrer ou de supprimer des piles.

Comprendre les états d'action et d'activité des RFC

RfcActionState(API)/Activity State (console) vous aident à comprendre le statut de l'intervention humaine, ou de l'action, sur une RFC. Utilisé principalement à des fins manuelles RFCs, il vous RfcActionState aide à comprendre quand une action est requise par vous ou par AMS Operations, et vous aide à voir quand AMS Operations travaille activement sur votre RFC. Cela fournit une transparence accrue sur les actions entreprises sur un RFC au cours de son cycle de vie.

RfcActionState(API)/Définitions de l'état de l'activité (console) :

- **AwsOperatorAssigned:** Un opérateur AWS travaille activement sur votre RFC.
- **AwsActionPending:** Une réponse ou une action d'AWS est attendue.
- **CustomerActionPending:** Une réponse ou une action du client est attendue.
- **NoActionPending:** Aucune action n'est requise de la part d'AWS ou du client.
- **NotApplicable:** Cet état ne peut pas être défini par les opérateurs ou les clients AWS et n'est utilisé que pour RFCs ceux qui ont été créés avant le lancement de cette fonctionnalité.

Les états d'action de la RFC varient selon que le type de modification soumis nécessite une révision manuelle et que la planification est définie sur ASAP ou non.

- **ActionStateModifications RFC** lors de la révision, de l'approbation et du début d'un type de modification manuelle avec planification différée :
 - Une fois que vous avez soumis une RFC manuelle planifiée, ActionStateelle change automatiquement AwsActionPendingpour indiquer qu'un opérateur doit revoir et approuver la RFC.
 - Lorsqu'un opérateur commence à examiner activement votre RFC, le ActionStatechangement devient. AwsOperatorAssigned
 - Lorsque l'opérateur approuve votre RFC, le statut de la RFC passe à Planifié et passe ActionStateautomatiquement à. NoActionPending
 - Lorsque l'heure de début planifiée de la RFC est atteinte, le statut de la RFC passe à InProgress, et le statut passe ActionStateautomatiquement AwsActionPendingà, pour indiquer qu'un opérateur doit être affecté à la révision de la RFC.
 - Lorsqu'un opérateur commence à exécuter activement le RFC, il le remplace par ActionState. AwsOperatorAssigned
 - Une fois terminé, l'opérateur ferme le RFC. Cela change automatiquement le ActionStateen NoActionPending.

Important

- Vous ne pouvez pas définir les états d'action. Ils sont soit définis automatiquement en fonction des modifications apportées à la RFC, soit définis manuellement par les opérateurs AMS.
- Si vous ajoutez de la correspondance à une RFC, elle `ActionState` est automatiquement définie sur `AwsActionPending`
- Lorsqu'une RFC est créée, elle `ActionState` est automatiquement définie sur `NoActionPending`
- Lorsqu'un RFC est soumis, le `ActionState` est automatiquement défini sur `AwsActionPending`
- Lorsqu'un RFC est rejeté, annulé ou terminé avec un statut de réussite ou d'échec, `ActionState` est automatiquement remis à `NoActionPending`.
- Les états d'action sont activés à la fois pour le mode automatique et le mode manuel RFCs, mais ils sont surtout importants pour le mode manuel, RFCs car ce type d' RFCs état nécessite souvent des communications.

Passez en revue les exemples de cas d'utilisation des états d'action RFC

Cas d'utilisation : visibilité sur le processus RFC manuel

- Une fois que vous avez soumis une RFC manuelle, l'état d'action de la RFC change automatiquement `AwsActionPending` pour indiquer qu'un opérateur doit examiner et approuver la RFC. Lorsqu'un opérateur commence à examiner activement votre RFC, l'état d'action de la RFC passe à `AwsOperatorAssigned`
- Prenons l'exemple d'un RFC manuel qui a été approuvé et planifié et qui est prêt à être exécuté. Une fois que le statut RFC passe à `InProgress`, l'état de l'action RFC passe automatiquement à `AwsActionPending` Il change à `AwsOperatorAssigned` nouveau lorsqu'un opérateur commence à exécuter activement le RFC.
- Lorsqu'un RFC manuel est terminé (fermé comme « Succès » ou « Échec »), l'état de l'action RFC change `NoActionPending` pour indiquer qu'aucune autre action n'est nécessaire de la part du client ou de l'opérateur.

Cas d'utilisation : correspondance RFC

- Lorsqu'il s'agit d'une RFC manuelle `Pending Approval`, un opérateur AMS peut avoir besoin d'informations supplémentaires de votre part. Les opérateurs publieront une correspondance à la RFC et changeront l'état d'action de la RFC en `CustomerActionPending` Lorsque vous répondez en ajoutant une nouvelle correspondance RFC, l'état de l'action RFC passe automatiquement à `AwsActionPending`
- Lorsqu'une RFC automatique ou manuelle échoue, vous pouvez ajouter une correspondance aux détails de la RFC, en demandant à l'opérateur AMS pourquoi la RFC a échoué. Lorsque votre correspondance est ajoutée, l'état de l'action RFC est automatiquement défini sur `AwsActionPending` Lorsque l'opérateur AMS prend la RFC pour consulter votre correspondance, l'état de l'action RFC passe à `AwsOperatorAssigned` Lorsque l'opérateur répond en ajoutant une nouvelle correspondance RFC, l'état de l'action RFC peut être défini sur `CustomerActionPending`, indiquant qu'une autre réponse du client est attendue, ou sur `NoActionPending`, indiquant qu'aucune réponse du client n'est requise ou attendue.

Comprendre les codes d'état RFC

Les codes d'état RFC vous aident à suivre vos demandes. Vous pouvez observer ces codes d'état lors de l'exécution d'une RFC dans la sortie de la CLI ou en actualisant la page de liste des RFC dans la console.

Vous pouvez également voir les codes d'une RFC sur la page de détails de cette RFC, qui peut ressembler à ceci :

Il se peut que votre liste contienne une RFC que vous n'avez pas soumise. Lorsque les opérateurs AMS utilisent un CT interne uniquement, ils le soumettent dans une RFC et celui-ci s'affiche dans votre liste de RFC. Pour de plus amples informations, veuillez consulter [Types de modifications internes uniquement](#).

Important

Vous pouvez demander des notifications en cas de changement d'état de la RFC. Pour plus de détails, voir [Notifications de changement d'état RFC](#).

Codes d'état RFC

Réussite	Échec
Modification : le RFC a été créé mais n'a pas été soumis PendingApproval /Soumis : Le RFC a été soumis et le système détermine s'il doit être approuvé, et obtient cette approbation, si nécessaire Approuvé par AWS/Approuvé par le client : le RFC a été approuvé. RFCs Les automatismes sont approuvés par AWS, RFCs les manuels sont approuvés par les opérateurs et, parfois, par les clients Planifié : la RFC a passé avec succès les vérifications de syntaxe et d'exigences et son exécution est prévue InProgress: le RFC est en cours d'exécution, notez RFCs que le provisionnement de plusieurs ressources ou s'il est de longue durée prend plus de temps à exécuter UserData Exécuté : La RFC a été exécutée Succès/Réussite : La RFC a été terminée avec succès	Rejetés : RFCs sont généralement rejetés parce qu'ils échouent à la validation ; par exemple, une ressource inutilisable, c'est-à-dire un sous-réseau, est spécifiée Annulés : RFCs sont généralement annulés parce qu'ils ne passent pas la validation avant l'expiration de l'heure de début configurée Échec : le RFC a échoué ; consultez le résultat pour StatusReason les raisons de l'échec, et les opérations AMS créent automatiquement un ticket d'incident et communiquent avec vous selon vos besoins

Note

Les demandes annulées ou rejetées RFCs peuvent être soumises à nouveau en utilisant [UpdateRfc](#); voir également [Mettre à jour RFCs](#).

Si la RFC satisfait à toutes les conditions nécessaires (par exemple, tous les paramètres requis sont spécifiés), le statut passe à `PendingApproval` (même une approbation automatique est CTs requise, ce qui se produit automatiquement si les vérifications de syntaxe et de paramètres sont réussies). S'il ne passe pas, le statut passe à `Rejected`. Le `StatusReason` fournit des informations sur les rejets ; les `ExecutionOutput` champs fournissent des informations sur l'approbation et la finalisation. Les codes d'erreur incluent :

- `InvalidRfcStateException`: Le statut de la RFC n'autorise pas l'opération appelée. Par exemple, si la RFC est passée à l'état Soumis, elle ne peut plus être modifiée.
- `InvalidRfcScheduleException`: Les `TimeoutInMinutes` paramètres `StartTime` `EndTime`, ou ont été violés.
- `InternalServerError`: Le système a rencontré un problème.
- `InvalidArgumentException`: Un paramètre est mal spécifié ; par exemple, une valeur inacceptable est utilisée.
- `ResourceNotFoundException`: aucune valeur, telle que l'ID de pile, est introuvable.

Si les heures de début et de fin planifiées demandées (également appelées fenêtre d'exécution des modifications) se produisent avant que la modification ne soit approuvée, le statut de la RFC passe à `Canceled`. Si la modification est approuvée, le statut de la RFC passe à `Scheduled`. La fenêtre de modification pour ASAP RFCs correspond à l'heure de soumission plus la `ExpectedExecutionDuration` valeur du CT.

À tout moment avant l'arrivée de la fenêtre d'exécution des modifications, une modification planifiée (soumise avec un `RequestedStartTime` dans la CLI) peut être modifiée ou annulée. Si la modification planifiée est modifiée, elle doit ensuite être soumise à nouveau.

Lorsque l'heure de début des modifications arrive (planifiée ou dès que possible) et une fois les approbations terminées, le statut change `InProgress` et aucune modification ne peut être apportée. Si la modification est terminée dans la fenêtre d'exécution des modifications spécifiée, le statut passe à `Success`. Si une partie de la modification échoue, ou si la modification est toujours en cours à la fin de la fenêtre d'exécution des modifications, le statut passe à `Failure`.

Note

Pendant l'état `InProgress` ou le `Failure` changement d'état, le RFC ne peut pas être modifié ou annulé. `Success`

Le schéma suivant illustre les statuts RFC depuis l'appel CreateRFC jusqu'à la résolution.

Comprendre la mise à jour des RFC CTs et la détection de la dérive des CloudFormation modèles

Les ressources mises en service dans AMS utilisent un AWS CloudFormation modèle modifié. Si un paramètre d'une ressource est modifié directement via la console de AWS gestion d'un service, l'enregistrement de CloudFormation création de cette ressource est désynchronisé. Si cela se produit et que vous essayez d'utiliser un type de modification de mise à jour AMS pour mettre à jour la ressource dans AMS, AMS fait référence à la configuration de ressource d'origine et réinitialise éventuellement les paramètres modifiés. Cette réinitialisation peut être dommageable, c'est pourquoi AMS interdit les types RFCs de modifications de mise à jour si des modifications supplémentaires de configuration AMS sont détectées.

Pour obtenir la liste des types de modifications apportées aux mises à jour, utilisez le filtre de console.

Assainissement de la dérive FAQs

Questions et réponses sur la remédiation à la dérive de l'AMS. Il existe deux types de modifications que vous pouvez utiliser pour initier la correction de la dérive : l'un est mode d'exécution = manuel ou « révision requise », l'autre est mode d'exécution = automatisé.

Ressources prises en charge pour la correction de la dérive (ct-3king0u4l33zf)

Il s'agit des ressources prises en charge par le type de modification de correction de la dérive (ct-3king0u4l33zf). Pour corriger n'importe quelle ressource, utilisez plutôt le type de modification « révision requise » (ct-34sxfo53yuzah).

```
AWS::EC2::Instance
AWS::EC2::SecurityGroup
AWS::EC2::VPC
AWS::EC2::Subnet
AWS::EC2::NetworkInterface
AWS::EC2::EIP
AWS::EC2::InternetGateway
AWS::EC2::NatGateway
AWS::EC2::NetworkAcl
AWS::EC2::RouteTable
AWS::EC2::Volume
```

```
AWS::AutoScaling::AutoScalingGroup
AWS::AutoScaling::LaunchConfiguration
AWS::AutoScaling::LifecycleHook
AWS::AutoScaling::ScalingPolicy
AWS::AutoScaling::ScheduledAction
AWS::ElasticLoadBalancing::LoadBalancer
AWS::ElasticLoadBalancingV2::Listener
AWS::ElasticLoadBalancingV2::ListenerRule
AWS::ElasticLoadBalancingV2::LoadBalancer
AWS::CloudWatch::Alarm
```

Types de modifications liées à la remédiation à la dérive

Questions et réponses sur l'utilisation des types de modifications de correction de la dérive AMS.

Pour obtenir la liste des ressources prises en charge pour la fonctionnalité de correction de la dérive, consultez [Ressources prises en charge pour la correction de la dérive \(ct-3king0u4l33zf\)](#).

Important

La correction de la dérive modifie les and/or paramètres du modèle de pile et il est obligatoire de mettre à jour vos référentiels de modèles locaux ou toute automatisation mettant à jour ces piles afin d'utiliser le modèle et les paramètres de pile les plus récents. L'utilisation d'anciens and/or paramètres de modèle sans synchronisation peut entraîner des modifications dommageables des ressources sous-jacentes.

Le CT automatisé sans révision (ct-3king0u4l33zf) prend en charge la correction de seulement 10 ressources par RFC. Pour corriger les ressources restantes par lots de 10, créez-en de nouvelles RFCs jusqu'à ce que toutes les ressources soient corrigées.

Quel type de modification de correction de dérive dois-je utiliser ?

Nous recommandons d'utiliser la tomodensitométrie automatisée sans révision (ct-3king0u4l33zf) lorsque :

- Vous essayez d'effectuer une mise à jour d'une ressource de pile existante à l'aide d'un CT automatique et la RFC est DRIFTED rejetée telle quelle.
- Vous avez utilisé un Update CT dans le passé et celui-ci a échoué car la pile était dérivée. Vous n'avez pas besoin de réessayer une mise à jour et vous pouvez utiliser la révision requise, manuelle ou CT à la place.

Nous recommandons d'utiliser la tomodesitométrique manuelle requise (ct-34sxfo53yuzah) uniquement lorsque les types de ressources dérivées ne sont pas pris en charge par la correction de la dérive, aucune révision requise, automatique, la tomodesitométrique (ct-3kinq0u4l33zf), ou lorsque la correction de la dérive, aucune révision requise, automatisée, échoue.

Quelles sont les modifications apportées à la pile lors de la correction ?

La correction nécessite la mise à jour des and/or paramètres du modèle de pile en fonction des propriétés dérivées. La correction met également à jour la politique de pile de la pile pendant la correction et rétablit la politique de pile à sa valeur précédente une fois la correction terminée.

Comment pouvons-nous voir les modifications apportées aux and/or paramètres du modèle de pile ?

Dans la réponse à la RFC, un résumé des modifications est fourni avec les informations suivantes :

- `ChangeSummaryJson`: contient un résumé des modifications apportées aux and/or paramètres du modèle de pile dans le cadre de la correction de la dérive. La correction s'effectue en plusieurs phases. Ce résumé des modifications comprend les modifications apportées aux différentes phases. Si la correction est réussie, vérifiez les modifications apportées à la dernière phase. Consultez `ExecutionPlan` le JSON pour les phases exécutées dans l'ordre. Par exemple, `RestoreReferences` la section lorsqu'elle est présente est toujours exécutée à la fin et contient du JSON pour les modifications apportées après la correction. Si la correction est exécutée en `DryRun` mode, aucune de ces modifications n'aurait été appliquée à la pile.
- `PreRemediationStackTemplateAndConfigurationJson`: contient un instantané de configuration de la `CloudFormation` pile, y compris le modèle, les paramètres et les sorties, `StackPolicyBody` avant que la correction ne soit déclenchée sur la pile.

Que dois-je faire une fois la correction effectuée ?

 Important

Vous devez mettre à jour vos référentiels de modèles locaux, ou toute automatisation, qui mettrait à jour la pile corrigée, avec le modèle et les paramètres les plus récents fournis dans le résumé de la RFC. Il est très important de le faire car l'utilisation des anciens and/or paramètres du modèle peut entraîner d'autres modifications destructrices des ressources de la pile.

Ma demande sera-t-elle prise en compte au cours de cette correction ?

La correction est un processus hors ligne qui est effectué uniquement sur la configuration de la CloudFormation pile. Aucune mise à jour n'est effectuée sur la ressource sous-jacente.

Puis-je continuer à utiliser Management | Other | Other RFCs pour effectuer des mises à jour des ressources après la correction ?

Nous vous recommandons de toujours effectuer des mises à jour pour empiler les ressources à l'aide de la mise à jour automatique disponible CTs. Lorsque la mise à jour disponible CTs ne correspond pas à votre cas d'utilisation, utilisez Management | Other | Other requests.

La remédiation crée-t-elle de nouvelles ressources dans la pile ?

La correction ne crée aucune nouvelle ressource dans la pile. Toutefois, la correction crée de nouvelles sorties et met à jour la section des [métadonnées](#) du modèle de pile afin de stocker le résumé de la correction à titre de référence.

Les mesures correctives seront-elles toujours couronnées de succès ?

La correction nécessite une analyse et une validation minutieuses de la configuration du modèle afin de déterminer si elle peut être effectuée. Dans les scénarios où ces validations échouent, le processus de correction est arrêté et aucune modification n'est apportée au modèle ou aux paramètres de la pile. En outre, la correction ne peut être effectuée que sur les types de ressources pris en charge.

Comment puis-je effectuer des mises à jour pour empiler les ressources en cas d'échec de la correction ?

Vous pouvez utiliser le CT Management | Other | Other | Update (ct-0xdawir96cy7k) pour demander des modifications. AMS surveille ces scénarios et travaille à l'amélioration de la solution de correction.

Puis-je corriger des piles contenant à la fois des types de ressources pris en charge et des types de ressources non pris en charge ?

Oui. Toutefois, la correction n'est effectuée que si les types de ressources pris en charge se trouvent à la dérive dans la pile. Si des types de ressources non pris en charge sont DÉRIVÉS, la correction ne se poursuit pas.

Puis-je demander une correction pour les piles créées par le biais d'une ingestion autre que CFN ?
CTs

Oui. La correction peut être effectuée sur les piles quel que soit le type de modification utilisé pour créer la pile.

Puis-je connaître les modifications qui seraient apportées à la pile avant la correction ?

Oui. Les deux types de modifications fournissent une `DryRun` option que vous pouvez utiliser pour demander des modifications qui seraient effectuées si la pile était corrigée. Cependant, les modifications finales de correction peuvent différer en fonction de la dérive présente sur la pile au moment de la correction.

Horaire RFCs

La fonction de planification vous permet de choisir une heure de début pour RFCs. Les options suivantes sont disponibles dans la fonction de planification :

- Exécutez cette modification dès que possible : AMS exécute le RFC dès qu'il est approuvé. La plupart CTs sont automatiquement approuvés. Utilisez cette option si vous ne souhaitez pas que le RFC démarre à un moment précis.
- Planifiez cette modification : définissez un jour, une heure et un fuseau horaire pour l'exécution de la RFC. Pour les types de modifications automatisés, il est recommandé de demander une heure de début au moins 10 minutes après la date prévue de soumission de la RFC. Pour les types de modifications requis, vous devez demander une heure de début au moins 24 heures après la date prévue de soumission de la RFC. Si la RFC n'est pas approuvée à l'heure de début configurée, elle est rejetée.

Définissez un calendrier RFC

Pour planifier un RFC, appliquez l'une des méthodes suivantes :

Exécutez cette modification dès que possible :

- Console : Ne rien faire. Cela utilise le calendrier RFC par défaut.
- API ou CLI : supprimez les `RequestedEndTime` options `RequestedStartTime` et dans l'opération `Create RFC`.

Les « révisions requises » dès que possible RFCs sont rejetées automatiquement si elles ne sont pas approuvées dans les trente jours suivant leur soumission.

Programmez cette modification :

- Console : sélectionnez le bouton radio Planifier cette modification. Une zone d'heure de début s'ouvre. Entrez manuellement un jour ou utilisez le widget calendrier pour sélectionner un jour. Entrez une heure, en UTC, exprimée au format ISO 8601, et utilisez la liste déroulante pour sélectionner un lieu. Par défaut, AMS utilise le format ISO 8601 YYYYMMDDThhmmss Z ou:MM:SSZ, l'un ou YYYY-MM-DDThh l'autre format étant accepté.

Note

L'heure de fin par défaut est de 4 heures à compter de l'heure de début que vous avez saisie. Pour définir l'heure de fin de votre modification planifiée au-delà de 4 heures, utilisez l'API ou la CLI pour exécuter la modification.

- API ou CLI : soumettez des valeurs pour les RequestedEndTime paramètres RequestedStartTime et dans le cadre de l'opération Create RFC. La transmission d'un RequestedEndTime paramètre configuré n'arrête pas l'exécution d'un type de modification automatique qui a déjà commencé. Pour un type de modification « révision requise », si le délai RequestedEndTime est atteint alors que les recherches sur les opérations d'AMS sont toujours en cours et que vous êtes en communication avec AMS, vous pouvez demander une extension ou vous pouvez être invité à soumettre à nouveau le RFC.

Tip

Pour un exemple d'affichage de l'heure UTC, voir [UTC](#) sur le site Web de Time-IS.
Exemple de format ISO 8601 pour une date/time valeur du 5 décembre 2016 à 14 h 20 :
2016-12-05T 14:20:00 Z ou 20161205T142000Z.

Si vous fournissez...

- uniquement aRequestedStartTime, le RFC est considéré comme planifié et RequestedEndTime est renseigné à l'aide de la ExecutionDurationInMinutes valeur.
- seulement unRequestedEndTime, nous en lançons un InvalidArgumentException.
- les deux RequestedStartTime et RequestedEndTime nous les RequestedEndTime remplaçons par l'heure de début spécifiée plus la ExecutionDurationInMinutes valeur.
- ni l'un RequestedStartTime ni l'autreRequestedEndTime, nous conservons ces valeurs nulles et la RFC est traitée comme une RFC ASAP.

 Note

Pour toutes les modifications planifiées RFCs, une heure de fin non spécifiée est écrite comme étant l'heure de la date spécifiée `RequestedStartTime` plus l'`ExpectedExecutionDurationInMinutes` attribut du type de modification soumis. Par exemple, si la valeur `ExpectedExecutionDurationInMinutes` est « 60 » (minutes) et que la valeur spécifiée `RequestedStartTime` est `2016-12-05T14:20:00Z` (5 décembre 2016 à 4 h 20), l'heure de fin réelle sera fixée au 5 décembre 2016 à 5 h 20. Pour trouver le `ExpectedExecutionDurationInMinutes` type de modification correspondant à un type de modification spécifique, exécutez cette commande :

```
aws amscm --profile saml get-change-type-version --  
change-type-id CHANGE_TYPE_ID --query "ChangeTypeVersion.  
{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

Utilisez l'option RFC Priority

Utilisez l'option `Priorité` dans les types de execution `mode = manual` modifications pour avertir AMS Operations de l'urgence de la demande.

Option prioritaire dans `execution mode = manual` :

Spécifiez la priorité d'une RFC manuelle comme élevée, moyenne ou faible. RFCs classés comme élevés sont examinés et approuvés avant d' RFCs être classés comme moyens, sous réserve des objectifs de niveau de service de la RFC (SLOs) et de leurs délais de soumission. RFCs dont la priorité est faible ou aucune priorité spécifiée sont traitées dans l'ordre dans lequel elles ont été soumises.

Approuver ou rejeter RFCs

RFCs soumis avec approbation obligatoire (manuel) CTs doit être approuvé par vous ou par AMS. Les CTs pré-approbations sont traitées automatiquement. Pour de plus amples informations, veuillez consulter [Exigences d'approbation CT](#).

 Note

Lorsque vous utilisez « révision requise » CTs, AMS vous recommande d'utiliser l'option `ASAP Scheduling` (choisissez `ASAP` dans la console, laissez les heures de début et de fin

vides dans l'API/CLI) car elles CTs nécessitent qu'un opérateur AMS examine la RFC et communique éventuellement avec vous avant qu'elle ne puisse être approuvée et exécutée. Si vous les planifiez RFCs, veillez à prévoir au moins 24 heures. Si l'approbation n'intervient pas avant l'heure de début prévue, le RFC est automatiquement rejeté.

Si un RFC nécessitant une approbation est soumis avec succès par AMS, vous devez l'approuver explicitement. Ou, si vous soumettez une RFC nécessitant une approbation, elle doit être approuvée par AMS. Si vous devez approuver une RFC soumise par AMS, un e-mail ou une autre communication prédéterminée vous est envoyé pour demander l'approbation. La communication inclut l'identifiant RFC. Une fois la communication envoyée, effectuez l'une des opérations suivantes :

- Approuver ou rejeter par console : utilisez la page de détails de la RFC correspondante :
- API/CLI Approve : [ApproveRfc](#) marque une modification comme approuvée. L'action doit être prise à la fois par le propriétaire et par l'exploitant, si les deux sont nécessaires. Voici un exemple de commande d'approbation de la CLI. Dans l'exemple suivant, remplacez RFC_ID par l'ID RFC approprié.

```
aws amscm approve-rfc --rfc-id RFC_ID
```

- Rejet API/CLI : [RejectRfc](#) marque une modification comme rejetée. Voici un exemple de commande de rejet de la CLI. Dans l'exemple suivant, remplacez RFC_ID par l'ID RFC approprié.

```
aws amscm reject-rfc --rfc-id RFC_ID --reason "no longer relevant"
```

Demander des périodes d'exécution restreintes de la RFC

Anciennement connus sous le nom de jours d'interdiction, vous pouvez demander à limiter certaines périodes. Aucune modification ne peut être effectuée pendant ces périodes.

Pour définir une période d'exécution restreinte, utilisez l'opération

[UpdateRestrictedExecutionTimes](#) API et définissez une période spécifique, en UTC. La période que vous spécifiez remplace toutes les périodes précédentes qui ont été spécifiées. Si vous soumettez une RFC pendant la durée d'exécution restreinte spécifiée, la soumission échoue avec le message d'erreur Invalid RFC Schedule. Vous pouvez spécifier jusqu'à 200 périodes restreintes. Par

défaut, aucune période restreinte n'est définie. Voici un exemple de commande de demande (avec l'authentification SAML configurée) :

```
aws amscm --profile saml update-restricted-execution-times --restricted-execution-times='[{"TimeRange":{"StartTime":"2018-01-01T12:00:00Z","EndTime":"2018-01-01T12:00:01Z"}}]'
```

Vous pouvez également consulter vos `RestrictedExecutionTimes` paramètres actuels en exécutant l'opération [ListRestrictedExecutionTimes](#) API. Exemple :

```
aws amscm --profile saml list-restricted-execution-times
```

Si vous souhaitez soumettre une RFC pendant une durée d'exécution limitée spécifiée, ajoutez le `RestrictedExecutionTimesOverride` avec la valeur de `OverrideRestrictedTimeRanges`, puis soumettez la RFC comme vous le feriez normalement. Il est recommandé de n'utiliser cette méthode que pour une RFC critique ou d'urgence. Pour plus d'informations, consultez la référence d'API pour [SubmitRfc](#).

Création, clonage, mise à jour, recherche et annulation RFCs

Les exemples suivants vous présentent différentes opérations RFC.

Rubriques

- [Création d'une RFC](#)
- [Cloner RFCs \(recréer\) avec la console AMS](#)
- [Mettre à jour RFCs](#)
- [Trouvez RFCs](#)
- [Annuler RFCs](#)

Création d'une RFC

Création d'une RFC avec la console

Voici la première page du processus de création de RFC dans la console AMS, avec les cartes Quick ouvertes et les types de modification Browse actifs :

Voici la première page du processus de création de RFC dans la console AMS, avec l'option Sélectionner par catégorie active :

Comment cela fonctionne :

1. Accédez à la page Créer une RFC : Dans le volet de navigation de gauche de la console AMS, cliquez RFC pour ouvrir la page de RFCs liste, puis cliquez sur Créer une RFC.
2. Choisissez un type de modification (CT) populaire dans la vue Parcourir les types de modification par défaut, ou sélectionnez un CT dans la vue Choisir par catégorie.

- Parcourir par type de modification : vous pouvez cliquer sur un CT populaire dans la zone de création rapide pour ouvrir immédiatement la page Run RFC. Notez que vous ne pouvez pas choisir une ancienne version CT avec création rapide.

Pour trier CTs, utilisez la zone Tous les types de modifications dans l'affichage Carte ou Tableau. Dans l'une ou l'autre vue, sélectionnez un CT, puis cliquez sur Créer une RFC pour ouvrir la page Exécuter une RFC. Le cas échéant, une option Créer avec une ancienne version apparaît à côté du bouton Créer une RFC.

- Choisissez par catégorie : sélectionnez une catégorie, une sous-catégorie, un article et une opération et la zone de détails du CT s'ouvre avec une option permettant de créer avec une ancienne version, le cas échéant. Cliquez sur Créer une RFC pour ouvrir la page Exécuter une RFC.
3. Sur la page Run RFC, ouvrez la zone de nom du CT pour voir la boîte de détails du CT. Un sujet est requis (il est renseigné pour vous si vous choisissez votre CT dans la vue Parcourir les types de modification). Ouvrez la zone de configuration supplémentaire pour ajouter des informations sur le RFC.

Dans la zone Configuration de l'exécution, utilisez les listes déroulantes disponibles ou entrez des valeurs pour les paramètres requis. Pour configurer les paramètres d'exécution facultatifs, ouvrez la zone de configuration supplémentaire.

4. Lorsque vous avez terminé, cliquez sur Exécuter. S'il n'y a aucune erreur, la page RFC créée avec succès s'affiche avec les détails de la RFC soumise et le résultat d'exécution initial.
5. Ouvrez la zone Paramètres d'exécution pour voir les configurations que vous avez soumises. Actualisez la page pour mettre à jour l'état d'exécution de la RFC. Vous pouvez éventuellement annuler la RFC ou en créer une copie à l'aide des options en haut de la page.

Création d'une RFC avec la CLI

Comment cela fonctionne :

1. Utilisez soit le Inline Create (vous émettez une `create-rfc` commande avec tous les paramètres RFC et d'exécution inclus), soit le Template Create (vous créez deux fichiers JSON, un pour les paramètres RFC et un pour les paramètres d'exécution) et émettez la `create-rfc` commande avec les deux fichiers en entrée. Les deux méthodes sont décrites ici.
2. Soumettez la `aws amscm submit-rfc --rfc-id ID` commande RFC : avec l'ID RFC renvoyé.

Surveillez la `aws amscm get-rfc --rfc-id ID` commande RFC :

Pour vérifier la version du type de modification, utilisez cette commande :

```
aws amscm list-change-type-version-summaries --filter  
Attribute=ChangeTypeId,Value=CT_ID
```

Note

Vous pouvez utiliser n'importe quel `CreateRfc` paramètre avec n'importe quelle RFC, qu'ils fassent ou non partie du schéma du type de modification. Par exemple, pour recevoir des notifications lorsque le statut de la RFC change, ajoutez cette ligne `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}\"` aux paramètres RFC de la demande (et non aux paramètres d'exécution). Pour obtenir la liste de tous les `CreateRfc` paramètres, consultez le manuel [AMS Change Management API Reference](#).

CRÉATION EN LIGNE :

Émettez la commande `create-rfc` avec les paramètres d'exécution fournis en ligne (évités les guillemets lorsque vous fournissez des paramètres d'exécution en ligne), puis soumettez l'ID RFC renvoyé. Par exemple, vous pouvez remplacer le contenu par quelque chose comme ceci :

```
aws amscm create-rfc --change-type-id "CT_ID" --change-type-version "VERSION" --title  
"TITLE" --execution-parameters "{\"Description\": \"example\"}"
```

CRÉATION D'UN MODÈLE :

Note

Cet exemple de création d'une RFC utilise le type de changement de pile Load Balancer (ELB).

1. Trouvez le scanner approprié. La commande suivante recherche dans les résumés de classification CT ceux qui contiennent « ELB » dans le nom de l'élément et crée une sortie de la catégorie, de l'élément, de l'opération et de l' ChangeTypeIdentifiant sous forme de tableau (la sous-catégorie pour les deux est). Advanced stack components

```
aws amscm list-change-type-classification-summaries --query
  "ChangeTypeClassificationSummaries[?contains(Item, 'ELB')].
  [Category,Item,Operation,ChangeTypeId]" --output table
```

```
-----
|                               CtSummaries                               |
+-----+-----+-----+-----+-----+-----+
| Deployment| Load balancer (ELB) stack | Create | ct-123h45t6uz7jl |
| Management| Load balancer (ELB) stack | Update | ct-01tm873rsebx9 |
+-----+-----+-----+-----+-----+-----+-----+
```

2. Trouvez la version la plus récente du CT :

ChangeTypeIdet ChangeTypeVersion : L'ID de type de modification pour cette procédure pas à pas est ct-123h45t6uz7jl (create ELB). Pour connaître la dernière version, exécutez cette commande :

```
aws amscm list-change-type-version-summaries --filter
  Attribute=ChangeTypeId,Value=ct-123h45t6uz7jl
```

3. Découvrez les options et les exigences. La commande suivante génère le schéma dans un fichier JSON nommé CreateElbParams .json.

```
aws amscm get-change-type-version --change-type-id "ct-123h45t6uz7jl" --query
  "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateElbParams.json
```

4. Modifiez et enregistrez le fichier JSON des paramètres d'exécution. Cet exemple nomme le fichier CreateElbParams .json.

Pour un CT de provisionnement, le StackTemplateId est inclus dans le schéma et doit être soumis dans les paramètres d'exécution.

En TimeoutInMinutes ce qui concerne le nombre de minutes autorisées pour la création de la pile avant l'échec de la RFC, ce paramètre ne retardera pas l'exécution de la RFC, mais vous devez prévoir suffisamment de temps (par exemple, ne spécifiez pas « 5 »). Les valeurs valides sont de « 60 » à « 360 », pour les CTs applications de longue durée UserData : Create EC2 and Create ASG. Nous recommandons le maximum autorisé de « 60 » pour tous les autres CTs approvisionnements.

Fournissez l'ID du VPC dans lequel vous souhaitez que la pile soit créée ; vous pouvez obtenir l'ID du VPC à l'aide de la commande CLI. `aws amsskms list-vpc-summaries`

```
{
  "Description":      "ELB-Create-RFC",
  "VpcId":            "VPC_ID",
  "StackTemplateId":  "stm-sdhopv000000000000",
  "Name":             "MyElbInstance",
  "TimeoutInMinutes": 60,
  "Parameters": {
    "ELBSubnetIds":      ["SUBNET_ID"],
    "ELBHealthCheckHealthyThreshold": 4,
    "ELBHealthCheckInterval": 5,
    "ELBHealthCheckTarget": "HTTP:80/",
    "ELBHealthCheckTimeout": 60,
    "ELBHealthCheckUnhealthyThreshold": 5,
    "ELBScheme":         false
  }
}
```

5. Exportez le modèle RFC JSON dans un fichier de votre dossier actuel nommé CreateElbRfc.json :

```
aws amscm create-rfc --generate-cli-skeleton > CreateElbRfc.json
```

6. Modifiez et enregistrez le fichier CreateElbRfc.json. Comme vous avez créé les paramètres d'exécution dans un fichier séparé, supprimez la ExecutionParameters ligne. Par exemple, vous pouvez remplacer le contenu par quelque chose comme ceci :

```
{
```



```
"ChangeTypeVersion":    "2.0",  
"ChangeTypeId":         "ct-123h45t6uz7jl",  
"Title":                "Create ELB"  
}
```

7. Créez le RFC. La commande suivante spécifie le fichier de paramètres d'exécution et le fichier de modèle RFC :

```
aws amscm create-rfc --cli-input-json file://CreateElbRfc.json --execution-  
parameters file://CreateElbParams.json
```

Vous recevez l'identifiant de la nouvelle RFC dans la réponse et vous pouvez l'utiliser pour soumettre et surveiller la RFC. Tant que vous ne l'avez pas soumise, la RFC reste en cours d'édition et ne démarre pas.

Conseils

Note

Vous pouvez utiliser l'AMS API/CLI pour créer une RFC sans créer de fichier JSON RFC ou de fichier JSON de paramètres d'exécution CT. Pour ce faire, vous utilisez la `create-rfc` commande et ajoutez les paramètres RFC et d'exécution requis à la commande, c'est ce qu'on appelle « Inline Create ». Notez que tous les approvisionnements CTs contiennent dans le `execution-parameters` bloc un `Parameters` tableau contenant les paramètres de la ressource. Les paramètres doivent comporter des guillemets séparés par une barre oblique inversée (`\`).

L'autre méthode documentée pour créer une RFC s'appelle « Template Create ». C'est ici que vous créez un fichier JSON pour les paramètres RFC et un autre fichier JSON pour les paramètres d'exécution, et que vous soumettez les deux fichiers avec la `create-rfc` commande. Ces fichiers peuvent servir de modèles et être réutilisés pour le futur. RFCs Lorsque vous créez RFCs à l'aide de modèles, vous pouvez utiliser une commande pour créer le fichier JSON avec le contenu souhaité en exécutant une commande comme indiqué. Les commandes créent un fichier nommé « `parameters.json` » avec le contenu affiché ; vous pouvez également utiliser ces commandes pour créer le fichier RFC JSON.

Cloner RFCs (recréer) avec la console AMS

Vous pouvez utiliser la console AMS pour cloner une RFC existante.

Pour cloner ou recréer une RFC à l'aide de la console AMS, procédez comme suit :

1. Trouvez la RFC appropriée. Dans le menu de navigation de gauche, cliquez sur RFCs.

Le RFCs tableau de bord s'ouvre.

2. Parcourez les pages jusqu'à ce que vous trouviez le RFC que vous souhaitez cloner. Utilisez l'option Filtrer pour affiner la liste. Choisissez le RFC que vous souhaitez cloner.

La page de détails de la RFC s'ouvre.

3. Cliquez sur Créer une copie.

La page Créer une demande de modification s'ouvre avec toutes les options définies comme dans la RFC d'origine.

4. Apportez les modifications souhaitées. Pour définir des options supplémentaires, remplacez l'option de base par Avancé. Après avoir défini toutes les options, choisissez Soumettre.

La page de détails du RFC actif s'ouvre avec un nouvel identifiant RFC pour le RFC cloné et le RFC cloné apparaît dans le tableau de bord RFC.

Mettre à jour RFCs

Vous pouvez soumettre à nouveau un RFC qui a été rejeté ou qui n'a pas encore été soumis, en le mettant à jour puis en le soumettant, ou en le soumettant à nouveau. Notez que la plupart RFCs sont rejetées parce que le paramètre spécifié est RequestedStartTime passé avant la soumission ou parce qu'il n' TimeoutInMinutes est pas adapté à l'exécution de la RFC (étant donné TimeoutInMinutes que cela ne prolonge pas une RFC réussie, nous vous recommandons de toujours définir ce paramètre sur au moins « 60 » et jusqu'à « 360 » pour un groupe Amazon EC2 ou Amazon EC2 Auto Scaling ayant une longue durée d'exécution). Cette section décrit comment utiliser la version CLI de la UpdateRfc commande pour mettre à jour une RFC avec un nouveau paramètre RFC, ou de nouveaux paramètres à l'aide d'un JSON stringifié ou d'un fichier de paramètres mis à jour.

Cet exemple décrit l'utilisation de la version CLI de l' UpdateRfc API AMS (voir [Update RFC](#)). Bien qu'il existe des types de modifications pour mettre à jour certaines ressources (DNS privé et public,

pires d'équilibreurs de charge et configuration de correctifs de pile), il n'existe aucun CT pour mettre à jour une RFC.

Nous vous recommandons de soumettre une UpdateRfc opération à la fois. Si vous soumettez plusieurs mises à jour, par exemple sur une pile DNS, les mises à jour risquent d'échouer en tentant de mettre à jour le DNS en même temps.

DONNÉES REQUISES RfcId : La RFC que vous êtes en train de mettre à jour.

DONNÉES FACULTATIVES ExecutionParameters : À moins que vous ne mettiez à jour un champ non obligatoire `Description`, vous devez par exemple soumettre des paramètres d'exécution modifiés pour résoudre les problèmes à l'origine du rejet ou de l'annulation de la RFC. Toutes les valeurs non nulles soumises remplacent ces valeurs dans la RFC d'origine.

1. Trouvez le RFC rejeté ou annulé pertinent, vous pouvez utiliser cette commande (vous pouvez remplacer la valeur `parCanceled`) :

```
aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Rejected
```

2. Vous pouvez modifier n'importe lequel des paramètres RFC suivants :

```
{
  "Description": "string",
  "ExecutionParameters": "string",
  "ExpectedOutcome": "string",
  "ImplementationPlan": "string",
  "RequestedEndTime": "string",
  "RequestedStartTime": "string",
  "RfcId": "string",
  "RollbackPlan": "string",
  "Title": "string",
  "WorstCaseScenario": "string"}
```

Exemple de commande mettant à jour le champ `Description` :

```
aws amscm update-rfc --description "AMSTestNoOpsActionRequired" --rfc-id "RFC_ID"
--region us-east-1
```

Exemple de commande mettant à jour le `ExecutionParameters VpcId` champ :

```
aws amscm update-rfc --execution-parameters "{\"VpcId\":\"VPC_ID\"}" --rfc-id "RFC_ID" --region us-east-1
```

Exemple de commande mettant à jour la RFC avec un fichier de paramètres d'exécution contenant les mises à jour ; voir un exemple de fichier de paramètres d'exécution à l'étape 2 de : [EC2 stack | Create](#) :

```
aws amscm update-rfc --execution-parameters file://CreateEc2ParamsUpdate.json --rfc-id "RFC_ID" --region us-east-1
```

3. Soumettez à nouveau la RFC en utilisant `submit-rfc` le même identifiant RFC que celui que vous aviez lors de sa création initiale :

```
aws amscm submit-rfc --rfc-id RFC_ID
```

Si le RFC réussit, vous ne recevez aucun message de confirmation ou d'erreur sur la ligne de commande.

4. Pour surveiller l'état de la demande et afficher le résultat d'exécution, exécutez la commande suivante.

```
aws amscm get-rfc --rfc-id RFC_ID
```

Trouvez RFCs

Rechercher une demande de modification (RFC) à l'aide de la console

Pour rechercher une RFC à l'aide de la console AMS, procédez comme suit.

Note

Cette procédure s'applique uniquement aux personnes planifiées RFCs, c' RFCs est-à-dire qui n'ont pas utilisé l'option ASAP.

1. Dans le menu de navigation de gauche, cliquez sur RFCs.

Le RFCs tableau de bord s'ouvre.

2. Parcourez la liste ou utilisez l'option Filtrer pour affiner la liste.

La liste RFC change en fonction des critères de filtre.

3. Choisissez le lien Objet de la RFC que vous souhaitez.

La page de détails de la RFC s'ouvre pour cette RFC avec des informations telles que l'ID de la RFC.

4. S'il y en a plusieurs RFCs dans le tableau de bord, vous pouvez utiliser l'option Filtrer pour effectuer une recherche par RFC :

- **Objet** : La ligne d'objet ou le titre (dans l'API/CLI) attribué à la RFC lors de sa création.
- **ID RFC** : identifiant de la RFC.
- **État de l'activité** : Si vous connaissez l'état de la RFC, vous pouvez choisir entre `AwsOperatorAssigned` le fait qu'un opérateur examine actuellement la RFC, `AwsActionPending` ce qui signifie qu'un opérateur AMS doit effectuer quelque chose avant que l'exécution de la RFC ne puisse se poursuivre, ou `CustomerActionPending` le fait que vous devez prendre certaines mesures avant que l'exécution de la RFC puisse se poursuivre.
- **État** : Si vous connaissez le statut de la RFC, vous pouvez choisir entre :
 - **Planifié** : RFCs qui étaient programmés.
 - **Annulés** : RFCs qui ont été annulés.
 - **En cours** : RFCs en cours.
 - **Succès** : RFCs exécuté avec succès.
 - **Refusés** : RFCs qui ont été rejetés.
 - **Édition** : RFCs qui sont en cours de modification.
 - **Échec** : RFCs cela a échoué.
 - **En attente d'approbation** : RFCs cela ne peut pas se poursuivre tant qu'AMS ou vous n'avez pas approuvé. Cela indique généralement que vous devez approuver le RFC. Vous aurez reçu une notification de service à ce sujet dans votre liste de demandes de service.
- **Type de modification** : Choisissez la catégorie, la sous-catégorie, l'article et l'opération, et l'identifiant du type de modification est récupéré pour vous.
- **Heure de début ou heure de fin demandée** : cette option de filtre vous permet de choisir Avant ou Après, puis de saisir une date et, éventuellement, une heure (hh:mm et fuseau horaire). Ce filtre fonctionne correctement uniquement comme prévu RFCs (pas dès que possible RFCs).

- **Objet** : Le sujet (ou le titre, si la RFC a été créée avec l'API/CLI) que vous avez attribuée à la RFC.
- **ID du type de modification** : utilisez l'identifiant du type de modification soumis avec la RFC.

La recherche vous permet d'ajouter les filtres, comme le montre la capture d'écran ci-dessous.

5. Cliquez sur le lien **Objet** de la RFC que vous souhaitez.

La page de détails de la RFC s'ouvre pour cette RFC avec des informations telles que l'ID de la RFC.

Recherche d'une demande de modification (RFC) à l'aide de la CLI

Vous pouvez utiliser plusieurs filtres pour trouver une RFC.

Pour vérifier la version du type de modification, utilisez cette commande :

```
aws amscm list-change-type-version-summaries --filter  
Attribute=ChangeTypeId,Value=CT_ID
```

Note

Vous pouvez utiliser n'importe quel `CreateRfc` paramètre avec n'importe quelle RFC, qu'ils fassent ou non partie du schéma du type de modification. Par exemple, pour recevoir des notifications lorsque le statut de la RFC change, ajoutez cette ligne `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}\"` aux paramètres RFC de la demande (et non aux paramètres d'exécution). Pour obtenir la liste de tous les `CreateRfc` paramètres, consultez le manuel [AMS Change Management API Reference](#).

Si vous ne notez pas l'ID RFC et que vous devez le retrouver ultérieurement, vous pouvez utiliser le système de gestion des modifications (CM) AMS pour le rechercher et affiner les résultats à l'aide d'un filtre ou d'une requête.

1. Le [ListRfcSummaries](#) fonctionnement de l'API CM comporte des filtres. Vous pouvez [filtrer](#) les résultats en fonction d'un Attribute et Value combiné dans une opération logique ET, ou en fonction d'un AttributeCondition, d'un etValues.

Filtrage RFC

Attribut	Valeurs valides	Conditions valides	État par défaut	Remarques
ActualEndTime	Toute chaîne représentant une date ISO86 01 (par exemple, « 20170101T000000Z »)	Avant, après, entre	Aucune	La condition Avant ou Après n'accepte qu'une seule valeur dans le champ Valeurs. La condition Between doit avoir exactement deux valeurs dans le champ Valeurs, la première valeur devant représenter une date antérieure à la deuxième valeur
ActualStartTime	Toute chaîne représentant une date ISO86 01 (par exemple, « 20170101T000000Z »)	Avant, après, entre	Aucune	La condition Avant ou Après n'accepte qu'une seule valeur dans le champ Valeurs. La condition Between doit avoir exactement deux valeurs dans le champ Valeurs, la première valeur devant représenter une date antérieure à la deuxième valeur

Attribut	Valeurs valides	Conditions valides	État par défaut	Remarques
AutomationStatusId	Manuel, automatisé	Égal à	Égal à	Il n'y a que deux statuts d'automatisation
ChangeTypeId	Tout identifiant de type de modification valide ; par exemple, ct-123h45t6uz7jl	Égal à	Égal à	Trouver un type de changement ou un CSIO
ChangeTypeVersion	Tout identifiant de type de modification valide ; par exemple, 1.0	Égal à	Égal à	Trouver un type de changement ou un CSIO
CreatedBy	N'importe quelle chaîne (la longueur maximale autorisée est de 2 048 caractères)	Contains	Contains	Le CreatedBy champ de la RFC contient l'ARN de l'utilisateur qui l'a créée
CreatedTime	Toute chaîne représentant une date ISO86 01 (par exemple, « 20170101T000000Z »)	Avant, après, entre	Aucune	La condition Avant ou Après n'accepte qu'une seule valeur dans le champ Valeurs. La condition Between doit avoir exactement deux valeurs dans le champ Valeurs, la première valeur devant représenter une date antérieure à la deuxième valeur

Attribut	Valeurs valides	Conditions valides	État par défaut	Remarques
LastModifiedTime	Toute chaîne représentant une date ISO86 01 (par exemple, « 20170101T000000Z »)	Avant, après, entre	Aucune	La condition Avant ou Après n'accepte qu'une seule valeur dans le champ Valeurs. La condition Between doit avoir exactement deux valeurs dans le champ Valeurs, la première valeur devant représenter une date antérieure à la deuxième valeur
LastSubmittedTime	Toute chaîne représentant une date ISO86 01 (par exemple, « 20170101T000000Z »)	Avant, après, entre	Aucune	La condition Avant ou Après n'accepte qu'une seule valeur dans le champ Valeurs. La condition Between doit avoir exactement deux valeurs dans le champ Valeurs, la première valeur devant représenter une date antérieure à la deuxième valeur

Attribut	Valeurs valides	Conditions valides	État par défaut	Remarques
RequestedEndTime	Toute chaîne représentant une date ISO86 01 (par exemple, « 20170101T000000Z »)	Avant, après, entre	Aucune	La condition Avant ou Après n'accepte qu'une seule valeur dans le champ Valeurs. La condition Between doit avoir exactement deux valeurs dans le champ Valeurs, la première valeur devant représenter une date antérieure à la deuxième valeur
RequestedStartTime	Toute chaîne représentant une date ISO86 01 (par exemple, « 20170101T000000Z »)	Avant, après, entre	Aucune	La condition Avant ou Après n'accepte qu'une seule valeur dans le champ Valeurs. La condition Between doit avoir exactement deux valeurs dans le champ Valeurs, la première valeur devant représenter une date antérieure à la deuxième valeur
RfcStatusId	Annulé, modification, échec, InProgress, PendingApproval,, rejeté, planifié, réussite	Égal à	Égal à	Actualisez la liste RFC dans la console AMS ou exécutez GetRfc

Attribut	Valeurs valides	Conditions valides	État par défaut	Remarques
Title	Tout titre RFC valide	Contains	Contains	Les expressions régulières dans chaque champ individuel ne sont pas prises en charge. Recherche insensible aux majuscules et minuscules

Exemples :

Pour trouver tous les éléments RFCs liés au SQS (où le SQS est contenu dans la partie Item du CT), vous pouvez utiliser cette commande : IDs

```
list-rfc-summaries --query 'RfcSummaries[?contains(Item.Name, `SQS`)].
[Category.Id,Subcategory.Id,Type.Id,Item.Id,RfcId]' --output table
```

Ce qui renvoie quelque chose comme ceci :

```
-----
|                               ListRfcSummaries                               |
+-----+-----+-----+-----+-----+-----+
|Deployment| Advanced Stack Components |SQS   |Create |ct-123h45t6uz7j1|
|Management| Monitoring & Notification |SQS   |Update |ct-123h45t6uz7j1|
+-----+-----+-----+-----+-----+-----+

```

Un autre filtre disponible `list-rfc-summaries` est `AutomationStatusId` de rechercher ceux RFCs qui sont automatisés ou manuels :

```
aws amscm list-rfc-summaries --filter Attribute=AutomationStatusId,Value=Automated
```

Un autre filtre `list-rfc-summaries` disponible pour : Title (Objet dans la console) :

Attribute=Title, Value=*RFC-TITLE*

Exemple de la nouvelle structure de demande en JSON qui renvoie RFCs où :

- (Le titre CONTIENT l'expression « Windows 2012 » OU « Amazon Linux ») ET
- (RfcStatusId ÉGAL À « Succès » OU InProgress « ») ET
- (20170101T000000Z <= <= 20170103T000000Z) ET (RequestedStartTime <= 20170103T000000Z) ActualEndTime

```
{
  "Filters": [
    {
      "Attribute": "Title",
      "Values": ["Windows 2012", "Amazon Linux"],
      "Condition": "Contains"
    },
    {
      "Attribute": "RfcStatusId",
      "Values": ["Success", "InProgress"],
      "Condition": "Equals"
    },
    {
      "Attribute": "RequestedStartTime",
      "Values": ["20170101T000000Z", "20170103T000000Z"],
      "Condition": "Between"
    },
    {
      "Attribute": "ActualEndTime",
      "Values": ["20170103T000000Z"],
      "Condition": "Before"
    }
  ]
}
```

Note

Avec une version plus avancée Filters, AMS a l'intention de supprimer les champs suivants dans une prochaine version :

- Valeur : le champ Valeur fait partie du champ Filtres. Utilisez le champ Valeurs qui prend en charge des fonctionnalités plus avancées.
- RequestedEndTimeRange: utilisez le champ RequestedEndTime intégré aux filtres qui prend en charge des fonctionnalités plus avancées
- RequestedStartTimeRange: utilisez le champ RequestedStartTime intégré aux filtres qui prend en charge des fonctionnalités plus avancées.

Pour plus d'informations sur l'utilisation des requêtes CLI, consultez [Comment filtrer la sortie avec l'option --query](#) et la référence du langage de requête, [JMESPath Spécification](#).

2. Si vous utilisez la console AMS :

Accédez à la page de RFCsliste. Si nécessaire, vous pouvez filtrer sur le sujet de la RFC, qui est celui que vous avez saisi comme RFC Title lorsque vous l'avez créée.

Conseils

Note

Cette procédure s'applique uniquement aux personnes planifiées RFCs, c' RFCs est-à-dire qui n'ont pas utilisé l'option ASAP.

Annuler RFCs

Vous pouvez annuler une RFC à l'aide de la console ou de l'API/CLI AMS.

Pour annuler une RFC avec la console, recherchez la RFC dans votre liste de RFC, ouvrez-la, cliquez sur Annuler.

Données requises :

- Reason: Pourquoi annulez-vous le RFC ?
- RfcId: Le RFC que vous êtes en train d'annuler.

1. En général, vous annulez une RFC juste après l'avoir soumise (l'identifiant de la RFC devrait donc être pratique) ; sinon, vous ne pourrez pas l'annuler à moins de l'avoir planifiée et que

ce soit avant l'heure de début spécifiée. Si vous avez besoin de trouver l'ID RFC, vous pouvez utiliser cette commande (vous pouvez Value remplacer le par par PendingApproval un RFC approuvé manuellement) :

```
aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Scheduled
```

2. Exemple de commande pour annuler une RFC :

```
aws amscm cancel-rfc --reason "Bad Stack ID" --rfc-id "RFC_ID" --profile saml --  
region us-east-1
```

Utilisez la console AMS avec RFCs

La console AMS fournit des fonctionnalités qui vous aideront à réussir la création et la soumission RFCs.

Utiliser la page Liste des RFC (console)

La page de RFCs liste de la console AMS propose les options suivantes :

- Recherche RFC avancée via un filtre. Pour plus d'informations, consultez [Trouvez RFCs](#).
- Trouver la dernière fois que la RFC a été modifiée. Cette valeur représente la dernière fois que le statut de la RFC a été modifié.
- Affichage des détails de la RFC avec le sujet de la RFC. Le choix de ce lien ouvre la page de détails de cette RFC.
- Affichage de l'état de la RFC. Pour plus d'informations, veuillez consulter [Comprendre les codes d'état RFC](#)

Utiliser la création rapide RFC (console)

Utilisez les cartes de création rapide RFC, ou le tableau de liste, ou choisissez les types de modification RFCs par classification.

Pour en savoir plus, veuillez consulter la section [Création d'une RFC](#).

Ajouter de la correspondance RFC et des pièces jointes (console)

Vous pouvez ajouter de la correspondance à une RFC une fois qu'elle a été soumise et avant qu'elle ne soit approuvée, par exemple lorsqu'elle est dans l'état « PendingApproval ». Une fois qu'une RFC est approuvée (dans l'état « Planifié » ou InProgress « »), la correspondance ne peut pas être ajoutée, car elle pourrait être interprétée comme une modification de la demande. Une fois qu'un RFC est terminé (dans un état « Annulé », « Rejeté », « Succès » ou « Échec »), la correspondance est à nouveau activée, bien que la correspondance soit désactivée une fois qu'un RFC est fermé pendant plus de 30 jours.

Note

Chaque correspondance est limitée à 5 000 caractères.

Limitations relatives aux pièces jointes :

- Seulement trois pièces jointes par correspondance.
- Limite de cinquante pièces jointes par RFC.
- La taille de chaque pièce jointe doit être inférieure à 5 Mo.
- Seuls les fichiers texte sont acceptés, tels que le texte en clair (.txt), les valeurs séparées par des virgules (.csv), le JSON (.json) ou le YAML (.yaml). Dans le cas du format YAML, le fichier doit être joint en utilisant l'extension .yaml de fichier.

Note

Les fichiers texte contenant du contenu XML sont interdits. Si vous avez du contenu XML à partager avec AMS, utilisez une demande de service.

- Les noms de fichiers sont limités à 255 caractères, avec uniquement des chiffres, des lettres, des espaces, des tirets (-), des traits de soulignement (_) et des points (.).
- La mise à jour et la suppression de pièces jointes sur une RFC ne sont actuellement pas prises en charge.

Pour ajouter de la correspondance et des pièces jointes à une RFC, procédez comme suit :

1. Dans la console AMS, sur la page de détails d'une RFC, recherchez la section Correspondance au bas de la page.

Avant toute correspondance :

Après quelques correspondances :

2. Pour ajouter une nouvelle correspondance, saisissez votre message dans la zone de texte Répondre. Pour joindre des fichiers liés à la correspondance, choisissez Ajouter une pièce jointe, puis sélectionnez les fichiers souhaités.
3. Lorsque vous avez terminé, choisissez Soumettre.

La nouvelle correspondance, ainsi que les liens vers les fichiers joints, apparaissent dans la liste de correspondance sur la page de détails du RFC.

Configuration des notifications par e-mail RFC (console)

La page de création des demandes de modification de la console AMS vous permet d'ajouter des adresses e-mail afin de recevoir des notifications en cas de modification de l'état des RFC :

En outre, vous pouvez ajouter des adresses e-mail pour les notifications relatives à tout type de modification, par exemple :

```
aws amscm create-rfc --change-type-id <Change type ID>
                    --change-type-version 1.0 --title "TITLE"
                    --notification "{\"Email\": {\"EmailRecipients\" :
[\"email@example.com\"]}}\""
```

Ajoutez une ligne similaire (`--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}\"`) à toute demande de modification en ligne ou de modèle dans la partie des paramètres RFC de la demande, et non dans la partie des paramètres.

En savoir plus sur les paramètres RFC courants

Les paramètres RFC que vous devez soumettre sont les suivants, ainsi que les paramètres couramment utilisés dans RFCs :

- Informations sur le type de modification : `ChangeTypeId` et `ChangeTypeVersion`. Pour obtenir la liste des types de modifications IDs et des numéros de version, consultez la section [Référence des types de modifications](#).

Exécutez `list-change-type-classification-summaries` dans la CLI avec l'argument `query` pour affiner les résultats. Par exemple, affinez les résultats pour modifier les types dont le `Item` nom contient « Access ».

```
aws amscm list-change-type-classification-summaries --query
  "ChangeTypeClassificationSummaries [?contains (Item, 'access')].
  [Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

Exécutez `get-change-type-version` et spécifiez l'ID du type de modification. La commande suivante permet d'obtenir la version CT pour `ct-2tylseo8rxfsc`.

```
aws amscm get-change-type-version --change-type-id ct-2tylseo8rxfsc
```

- Titre : nom de la RFC ; celui-ci devient le sujet de la RFC dans la liste des RFC de la console AMS et vous pouvez effectuer une recherche à l'aide de la `GetRfc` commande et d'un filtre `Title`
- Planification : si vous souhaitez une RFC planifiée, vous devez inclure les `RequestedEndTime` paramètres `RequestedStartTime` et, ou utiliser l'option de console Planifier cette modification. Pour une RFC ASAP (qui s'exécute dès qu'elle est approuvée), lorsque vous utilisez la CLI, laissez `RequestedStartTime` et `RequestedEndTime` null. Lorsque vous utilisez la console, acceptez l'option ASAP.

En cas `RequestedStartTime` d'oubli, la RFC est rejetée.

- Provisionnement CTs : les paramètres d'exécution, ou `Parameters` les paramètres spécifiques requis pour provisionner la ressource. Ils varient considérablement en fonction du scanner.
- Non-provisionnement CTs : ceux CTs qui ne fournissent pas de ressource, telle que access CTs ou Other | Other, ou qui ne suppriment pas de pile, ont des paramètres d'exécution minimaux et aucun `Parameters` blocage.
- Certains exigent RFCs également que vous spécifiez un `TimeoutInMinutes`, ou combien de minutes sont autorisées pour la création de la pile avant l'échec de la RFC. Les valeurs valides sont comprises entre 60 (minutes) et 360, pour les longues durées. `UserData` Si l'exécution ne peut pas être terminée avant que le seuil ne `TimeoutInMinutes` soit dépassé, la RFC échoue. Toutefois, ce paramètre ne retarde pas l'exécution de la RFC.

- RFCs qui créent des instances, telles qu'un compartiment S3 ou un ELB, fournissent généralement un schéma qui vous permet d'ajouter jusqu'à sept balises (paires clé/valeur). Vous pouvez ajouter d'autres balises à votre compartiment S3 en soumettant une RFC à l'aide de la rubrique Déploiement | Composants de pile avancés | Tag | Créer un type de modification (ct-3cx7we852p3af). EC2, EFS, RDS et les schémas à plusieurs niveaux (HA à deux niveaux et HA à un niveau) autorisent jusqu'à cinquante balises. Les balises sont spécifiées dans la ExecutionParameters partie du schéma. Fournir des tags peut s'avérer très utile. Pour plus d'informations, consultez la section [Marquage de vos EC2 ressources Amazon](#).

Lorsque vous utilisez la console AMS, vous devez ouvrir la zone de configuration supplémentaire afin d'ajouter des balises.

 Tip

De nombreux schémas CT comportent un Name champ Description et situé en haut du schéma. Ces champs sont utilisés pour nommer la pile ou le composant de la pile, ils ne nomment pas la ressource que vous créez. Certains schémas proposent un paramètre pour nommer la ressource que vous créez, d'autres non. Par exemple, le schéma CT pour Create EC2 stack ne propose pas de paramètre pour nommer l' EC2 instance. Pour ce faire, vous devez créer une balise avec la clé « Nom » et la valeur que vous souhaitez donner au nom. Si vous ne créez pas une telle balise, votre EC2 instance s'affiche dans la EC2 console sans attribut name.

Utilisez l'option RFC AWS Region

L'API AMS et les points de terminaison CLI (amscmetamsskms) sont disponibles. us-east-1 Si vous fédérez avec le langage SAML (Security Assertion Markup Language), des scripts vous sont fournis lors de l'intégration pour définir votre région AWS sur us-east-1. Si vous utilisez SAML, il n'est pas nécessaire de spécifier l'--regionoption lorsque vous émettez une commande. Si votre SAML est configuré pour utiliser us-east-1 mais que votre compte ne se trouve pas dans AWS cette région, vous devez spécifier la région associée au compte lorsque vous émettez d'autres commandes (par exemple,). AWS aws s3

 Note

La plupart des exemples de commandes fournis dans ce guide n'incluent pas l'option `--region`.

Inscrivez-vous pour recevoir le courrier électronique quotidien du RFC

Vous pouvez vous inscrire pour recevoir un e-mail quotidien résumant l'activité RFC sur votre compte au cours des dernières 24 heures à l'aide de la fonction RFC digest. La fonction RFC Digest est un processus rationalisé qui réduit le nombre de notifications par e-mail que vous recevez concernant votre compte. RFCs Le résumé de la RFC peut réduire le risque que vous manquiez des actions en attente de réponse.

Pour activer la fonction de résumé RFC, contactez votre responsable de prestation de services cloud (CSDM) d'AMS. La CSDM vous abonne. Vous pouvez demander jusqu'à 20 adresses e-mail (ou alias) à inclure dans votre liste d'e-mails RFC Digest. L'horaire actuel des e-mails est fixé à 09:00 UTC-8.

Pour désactiver la fonction de résumé RFC, contactez votre CSDM avec votre demande.

Si vous ne configurez pas de résumé RFC et souhaitez recevoir des notifications vous concernant RFCs, ou si vous souhaitez obtenir des informations plus détaillées sur vos RFCs que celles fournies par le résumé des RFC, utilisez le système de gestion des modifications pour configurer des notifications d' CloudWatch événements ou des notifications par e-mail pour chaque RFC sur lequel vous souhaitez obtenir des informations. Pour plus d'informations sur la configuration des notifications RFC, consultez la section Notifications de [changement d'état des RFC](#).

Les sujets contenus dans le résumé de la RFC sont les suivants :

- En attente d'approbation du client : listes RFCs dont le PendingApprovalstatut est en attente de votre approbation
- Réponse du client en attente : listes RFCs qui attendent votre réponse à la correspondance RFC
- En attente d'approbation ou de réponse d'AWS : listes RFCs en attente d'une réponse ou d'une approbation de la part d'AMS
- Terminé : listes RFCs en état de réussite, d'échec, d'annulation et de rejet

Voici un exemple de résumé RFC :

Quels sont les types de modifications ?

Le type de modification fait référence à l'action exécutée par une demande de modification (RFC) AWS Managed Services (AMS) et englobe l'action de modification elle-même, ainsi que le type de modification (manuel ou automatique). AMS possède une vaste collection de types de modifications qui ne sont pas utilisés par les autres services Web Amazon. Vous utilisez ces types de modification lorsque vous soumettez une demande de modification (RFC) pour déployer, gérer ou accéder à des ressources.

Rubriques

- [Automatisé et manuel CTs](#)
- [Exigences d'approbation CT](#)
- [Modifier les versions de type](#)
- [Création de types de modifications](#)
- [Mettre à jour les types de modifications](#)
- [Types de modifications internes uniquement](#)
- [Schémas de type de changement](#)
- [Gestion des autorisations pour les types de modifications](#)
- [Supprimer les informations sensibles des types de modifications](#)
- [Recherche d'un type de modification à l'aide de l'option de requête](#)

Automatisé et manuel CTs

Une contrainte sur les types de modification est de savoir s'ils sont automatisés ou manuels. Il s'agit de l'AutomationStatusIdattribut de type de modification, appelé mode d'exécution dans la console AMS.

Les types de modifications automatisées ont des résultats et des délais d'exécution attendus et sont exécutés par le système automatisé AMS, généralement en une heure ou moins (cela dépend largement des ressources que le CT fournit). Les types de modifications manuelles sont rares, mais ils sont traités différemment car ils nécessitent qu'un opérateur AMS agisse sur le RFC avant de pouvoir l'exécuter. Cela implique parfois de communiquer avec l'émetteur de la RFC, de sorte que les types de modifications manuelles nécessitent des durées variables.

Pour toutes les modifications planifiées RFCs, une heure de fin non spécifiée est écrite comme étant l'heure de la date spécifiée `RequestedStartTime` plus l'`ExpectedExecutionDurationInMinutes` attribut du type de modification soumis. Par exemple, si la valeur `ExpectedExecutionDurationInMinutes` est « 60 » (minutes) et que la valeur spécifiée `RequestedStartTime` est `2016-12-05T14:20:00Z` (5 décembre 2016 à 4 h 20), l'heure de fin réelle sera fixée au 5 décembre 2016 à 5 h 20. Pour trouver le `ExpectedExecutionDurationInMinutes` type de modification correspondant à un type de modification spécifique, exécutez cette commande :

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

Note

RFCs Planifié avec mode d'exécution = Manuel, dans la console, doit être configuré pour fonctionner au moins 24 heures dans le futur. Cette mise en garde ne s'applique pas à l'API/CLI AMS, mais il est tout de même important de planifier le manuel au moins 8 heures RFCs à l'avance.

Note

Lorsque vous utilisez « révision requise » CTs, AMS vous recommande d'utiliser l'option ASAP Scheduling (choisissez ASAP dans la console, laissez les heures de début et de fin vides dans l'API/CLI) car elles CTs nécessitent qu'un opérateur AMS examine la RFC et communique éventuellement avec vous avant qu'elle ne puisse être approuvée et exécutée. Si vous les planifiez RFCs, veillez à prévoir au moins 24 heures. Si l'approbation n'intervient pas avant l'heure de début prévue, le RFC est automatiquement rejeté.

AMS a pour objectif de répondre à un scanner manuel dans les quatre heures et vous répondra dès que possible, mais l'exécution du RFC peut prendre beaucoup plus de temps.

Pour une liste de ceux CTs qui sont manuels et qui nécessitent une révision par AMS, consultez le fichier CSV Change Type, disponible sur la page Ressources pour développeurs de la console.

YouTube Vidéo : [Comment puis-je trouver les types de modifications automatisés pour AMS RFCs ?](#)

Pour trouver le mode d'exécution d'un CT dans la console AMS, vous devez utiliser l'option de recherche Parcourir les types de modification. Les résultats indiquent le mode d'exécution du ou des types de modification correspondants.

Pour rechercher le AutomationStatus type de modification correspondant à un type de modification spécifique à l'aide de la CLI AMS, exécutez cette commande :

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --  
query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

Vous pouvez également rechercher les types de modifications dans le manuel [AMS Change Type Reference](#), qui fournit des informations sur tous les types de modifications AMS.

Note

API/CLI Les AMS ne font pas actuellement partie d'AWSAPI/CLI. To access the AMS API/CLI. Vous pouvez télécharger le SDK AMS via la console AMS.

Exigences d'approbation CT

AMS CTs a toujours deux conditions d'approbation, AwsApprovalIdCustomerApprovalIdqui indiquent si la RFC exige qu'AMS, vous ou quelqu'un d'autre approuve l'exécution.

La condition d'approbation est quelque peu liée au mode d'exécution ; pour plus de détails, voir [Automatisé et manuel CTs](#).

Pour connaître les conditions d'approbation d'un CT, vous pouvez consulter le manuel [AMS Change Type Reference](#) ou exécuter [GetChangeTypeVersion](#). Les deux vous donneront également le mode CT **AutomationStatusId** ou Exécution.

Vous pouvez approuver à RFCs l'aide de la console AMS ou à l'aide de la commande suivante :

```
aws amscm approve-rfc --rfc-id RFC_ID
```

Condition d'approbation CT

Si la condition d'approbation du CT est	Il nécessite l'approbation de	And
AwsApprovalId: Required	Le système de changement de type AMS,	Aucune action n'est requise. Cette condition est typique de l'automatisation CTs.
AwsApprovalId: NotRequiredIfSubmitter	Le système de changement de type AMS et personne d'autre, si la RFC soumise concerne le compte pour lequel elle a été soumise,	Aucune action n'est requise. Cette condition est typique des manuels CTs car ils seront toujours revus par les opérateurs AMS.
CustomerApprovalId: NotRequired	Le système de changement de type AMS,	Si la RFC passe les vérifications de syntaxe et de paramètres, elle est approuvée automatiquement.
CustomerApprovalId: Required	Le système AMS change de type et vous,	Une notification vous est envoyée et vous devez approuver explicitement la RFC, soit en répondant à la notification, soit en exécutant l' ApproveRfc opération.
CustomerApprovalId: NotRequiredIfSubmitter	L'AMS change de type de système et personne d'autre, si vous avez soumis la RFC.	Si la RFC passe les vérifications de syntaxe et de paramètres, elle est approuvée automatiquement.

Si la condition d'approbation du CT est	Il nécessite l'approbation de	And
Incident de sécurité urgent ou correctif	AMS	Est approuvé et mis en œuvre automatiquement.

Modifier les versions de type

Les types de modifications sont versionnés et la version change lorsqu'une mise à jour majeure est apportée au type de modification.

Après avoir sélectionné un type de modification à l'aide de la console AMS, vous avez la possibilité d'ouvrir la zone de configuration supplémentaire et de sélectionner une version du type de modification. Vous pouvez également spécifier une version du type de modification sur la ligne de API/CLI commande. Vous souhaitez peut-être le faire pour diverses raisons, notamment :

- Vous savez que la version du type de modification de mise à jour que vous souhaitez doit correspondre à la version du type de modification que vous avez utilisée pour créer la ressource que vous souhaitez maintenant mettre à jour. Par exemple, vous pouvez avoir une instance Elastic Load Balancer (ELB) que vous avez créée avec le type de modification ELB Create version 1. Pour le mettre à jour, choisissez ELB Update version 1.
- Vous souhaitez utiliser une version de type de modification comportant des options différentes de celles du type de modification le plus récent. Nous ne le recommandons pas car les mises à jour AMS changent de type principalement pour des raisons de sécurité et nous vous recommandons de toujours choisir la version la plus récente.

Création de types de modifications

Les types de création de modification sont mis en correspondance version-to-version avec les types de modification de mise à jour. En d'autres termes, la version du type de modification que vous utilisez pour provisionner une ressource doit correspondre à la version du type de modification Mettre à jour que vous utiliserez ultérieurement pour modifier cette ressource. Par exemple, si vous créez un compartiment S3 avec le type de modification Create S3 Bucket version 2.0, et que vous souhaitez ultérieurement soumettre une RFC pour modifier ce compartiment S3, vous devez également utiliser le type de changement de compartiment Update S3 version 2.0, même s'il existe un type de changement de compartiment Update S3 avec la version 3.0.

Nous vous recommandons de conserver une trace de l'ID et de la version du type de modification que vous utilisez lorsque vous approvisionnez une ressource avec le type Créer une modification au cas où vous souhaiteriez ultérieurement utiliser un type de modification Mettre à jour pour la modifier.

Mettre à jour les types de modifications

AMS fournit des types de modification de mise à jour pour mettre à jour les ressources créées avec Create change types. Les types de modification de mise à jour doivent correspondre version-to-version au type de création de modification utilisé à l'origine pour provisionner la ressource.

Nous vous recommandons de conserver une trace de l'ID et de la version du type de modification que vous utilisez lors du provisionnement d'une ressource afin de faciliter sa mise à jour.

YouTube Vidéo : [Comment utiliser la mise à jour CTs pour modifier les ressources d'un compte AWS Managed Services \(AMS\) ?](#)

Types de modifications internes uniquement

Vous pouvez voir les types de modifications destinés à un usage interne uniquement. Cela vous permet de savoir quelles actions AMS peut ou doit entreprendre. S'il existe un type de modification interne que vous souhaiteriez mettre à votre disposition, soumettez une demande de service.

Par exemple, il existe un CT de gestion | Surveillance et notification | Suppression des CloudWatch alarmes | Mise à jour CT qui est uniquement interne. AMS l'utilise pour déployer des mises à jour de l'infrastructure (telles que des correctifs) afin de désactiver les notifications d'alarme susceptibles de déclencher par erreur les mises à jour. Lorsque ce CT est soumis, vous remarquerez le RFC correspondant au CT dans votre liste de RFC. Tout CT interne déployé dans un RFC apparaît dans votre liste RFC.

Schémas de type de changement

Tous les types de modifications fournissent un schéma JSON pour votre contribution à la création, à la modification ou à l'accès aux ressources. Le schéma fournit les paramètres, ainsi que leurs descriptions, pour que vous puissiez créer une demande de modification (RFC).

L'exécution réussie d'une RFC entraîne une sortie d'exécution. Pour le provisionnement RFCs, le résultat de l'exécution inclut un « stack_id » qui représente le stack in CloudFormation et qui peut être recherché dans la console. CloudFormation La sortie d'exécution inclut parfois la sortie de l'ID de l'instance créée et cet ID peut être utilisé pour rechercher l'instance dans la console AWS correspondante. Par exemple, le résultat d'exécution de Create ELB CT inclut un « stack_id » dans

lequel il est possible de faire des recherches CloudFormation et génère une valeur KEY=ELB value=consultable dans la console Amazon pour Elastic Load <stack-xxxx>Balancing. EC2

Examinons un schéma de tomodensitométrie. Il s'agit du schéma d' CodeDeploy Application Create, un schéma assez petit. Certains schémas comportent de très grandes Parameter surfaces.

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "name": "Create CodeDeploy application",
  "description": "Use to create an AWS CodeDeploy applicati
on
resource with the specified name.",
  "type": "object",
  "properties": {
    "Description": {
      "description": "The reason for the request.",
      "type": "string",
      "minLength": 1,
      "maxLength": 500
    },
    "VpcId": {
      "description": "ID of the vpc to use, in the form
vpc-0123abcd or vpc-01234567890abcdef.",
      "type": "string",
      "pattern": "^vpc-[a-z0-9]{8}$"
    },
    "StackTemplateId": {
      "description": "Must be stm-sft6rv000000000000",
      "type": "string",
      "enum": ["stm-sft6rv000000000000"]
    },
    "Name": {
      "description": "A name for the stack or stack component
;
this becomes the Stack Name.",
      "type": "string",
      "minLength": 1,
      "maxLength": 255
    },
    "Tags": {
      "description": "Up to seven tags (key/value pairs) to
categorize the resource.",
```

La première partie du schéma fournit des informations à AMS sur le type de modification demandé.

```

    "type": "array",
    "items": {
      "type": "object",
      "properties": {
        "Key": {
          "type": "string",
          "minLength": 1,
          "maxLength": 127
        },
        "Value": {
          "type": "string",
          "minLength": 1,
          "maxLength": 255
        }
      },
      "additionalProperties": false,
      "required": [
        "Key",
        "Value"
      ]
    },
    "minItems": 1,
    "maxItems": 7
  },
  "TimeoutInMinutes": {
    "description": "The maximum amount of time, in minutes,
to
    allow for execution of the change. This will not prolong
execution,
    but the RFC fails if the change is not completed in the
specified time.
    Valid values are 60 up to 360, for long-running
UserData.",
    "type": "number",
    "minimum": 0,
    "maximum": 60
  },
  "Parameters": {
    "description": "Specifications for the stack.",
    "type": "object",
    "properties": {
      "CodeDeployApplicationName": {
        "description": "The name of an AWS CodeDeploy
application.",

```

Le TimeoutInMinutes paramètre vous permet d'indiquer une date limite pour exécuter le type de modification. Les valeurs valides sont comprises entre 60 et 360, pour les longues durées. UserData

La section Paramètre s vous permet de définir les paramètre s de la ressource que vous créez ou de l'action que vous demandez.

Les sections « propriétés supplémentaires » vous indiquent

```
        "type": "string",
        "minLength": 1,
        "maxLength": 100,
        "pattern": "^[a-zA-Z0-9._+=,e-]{1,100}$"
    }
},
"additionalProperties": false,
"required": [
    "CodeDeployApplicationName"
]
}
},
"additionalProperties": false,
"required": [
    "Description",
    "VpcId",
    "StackTemplateId",
    "Name",
    "TimeoutInMinutes",
    "Parameters"
]
}
```

quels paramètres sont obligatoires et lesquels sont facultatifs.

Note

Ce schéma autorise jusqu'à sept balises ; toutefois EC2, les schémas EFS, RDS et de création à plusieurs niveaux autorisent jusqu'à 50 balises.

Gestion des autorisations pour les types de modifications

Vous pouvez utiliser une politique personnalisée pour limiter les types de modifications (CTs) disponibles pour les différents groupes ou utilisateurs.

Pour en savoir plus sur cette procédure, consultez la section [Configuration des autorisations](#) du guide de l'utilisateur AMS.

Supprimer les informations sensibles des types de modifications

Les schémas de type de modification AMS proposent un attribut de paramètre, "metadata": "ams:sensitive": "true" qui est utilisé pour les paramètres susceptibles de

contenir des informations sensibles, telles qu'un mot de passe. Lorsque cet attribut est défini, l'entrée fournie est masquée. Notez que vous ne pouvez pas définir cet attribut de paramètre. Toutefois, si vous travaillez avec AMS pour créer un type de modification et que vous souhaitez masquer un paramètre en entrée, vous pouvez le demander.

Recherche d'un type de modification à l'aide de l'option de requête

Cet exemple montre comment utiliser la console AMS pour trouver le type de modification approprié pour la RFC que vous souhaitez soumettre.

Vous pouvez utiliser la console ou le API/CLI pour rechercher un ID de type de modification (CT) ou une version. Il existe deux méthodes, soit la recherche, soit le choix de la classification. Pour les deux types de sélection, vous pouvez trier la recherche en choisissant le plus fréquemment utilisé, le plus récemment utilisé ou Alphabétique.

YouTube Vidéo : [Comment créer une RFC à l'aide de l'AWS Managed Services CLI et où puis-je trouver le schéma CT ?](#)

Dans la console AMS, sur la page RFCs-> Créer une RFC :

- Lorsque l'option Parcourir par type de modification est sélectionnée (valeur par défaut), vous pouvez soit :
 - Utilisez la zone de création rapide pour sélectionner l'une des solutions les plus populaires d'AMS CTs. Cliquez sur une étiquette et la page Run RFC s'ouvre avec l'option Objet remplie automatiquement pour vous. Complétez les options restantes selon vos besoins et cliquez sur Exécuter pour soumettre la RFC.
 - Vous pouvez également faire défiler l'écran jusqu'à la zone Tous les types de modification et commencer à taper un nom CT dans la case d'option. Vous n'avez pas besoin du nom exact ou complet du type de modification. Vous pouvez également rechercher un CT par identifiant de type de modification, classification ou mode d'exécution (automatique ou manuel) en saisissant les mots pertinents.

Lorsque la vue Cartes par défaut est sélectionnée, les cartes CT correspondantes apparaissent au fur et à mesure que vous tapez, sélectionnez une carte et cliquez sur Créer une RFC. Une fois la vue sous forme de tableau sélectionnée, choisissez le CT approprié et cliquez sur Créer une RFC. Les deux méthodes ouvrent la page Run RFC.

- Sinon, pour explorer les choix de type de modification, cliquez sur Choisir par catégorie en haut de la page pour ouvrir une série de boîtes d'options déroulantes.

- Choisissez une catégorie, une sous-catégorie, un article et une opération. La zone d'information correspondant à ce type de modification apparaît et un panneau apparaît en bas de page.
- Lorsque vous êtes prêt, appuyez sur Entrée pour afficher la liste des types de modifications correspondants.
- Choisissez un type de modification dans la liste. La zone d'information correspondant à ce type de modification apparaît au bas de la page.
- Une fois que vous avez sélectionné le type de modification correct, choisissez Create RFC.

Note

L'AMS CLI doit être installée pour que ces commandes fonctionnent. Pour installer l'API ou la CLI AMS, rendez-vous sur la page Ressources pour développeurs de la console AMS. Pour des informations de référence sur l'API AMS CM ou l'API AMS SKMS, consultez la section Ressources d'information AMS du guide de l'utilisateur. Vous devrez peut-être ajouter une `--profile` option d'authentification ; par exemple, `aws amsskms ams-cli-command --profile SAML`. Vous devrez peut-être également ajouter `--region` cette option car toutes les commandes AMS sont exécutées à partir de `us-east-1`, par exemple. `aws amscm ams-cli-command --region=us-east-1`

Note

Les points de terminaison AMS API/CLI (`amscm` et `amsskms`) se trouvent dans la région AWS de Virginie du Nord, `us-east-1`. En fonction de la configuration de votre authentification et de la région AWS dans laquelle se trouvent votre compte et vos ressources, vous devrez peut-être en ajouter `--region us-east-1` lors de l'émission de commandes. Vous devrez peut-être également ajouter `--profile saml`, s'il s'agit de votre méthode d'authentification.

Pour rechercher un type de modification à l'aide de l'API AMS CM (voir [ListChangeTypeClassificationSummaries](#)) ou de la CLI :

Vous pouvez utiliser un filtre ou une requête pour effectuer une recherche. L' `ListChangeTypeClassificationSummaries` opération comporte des options de [filtres](#) pour `Category`, `SubcategoryItem`, et `Operation`, mais les valeurs doivent correspondre exactement aux valeurs

existantes. Pour des résultats plus flexibles lors de l'utilisation de la CLI, vous pouvez utiliser l'option `--queryoption`.

Changer le type de filtrage avec l'API/CLI AMS CM

Attribut	Valeurs valides	Condition valide/par défaut	Remarques
ChangeTypeId	Toute chaîne représentant un ChangeTypeId (par exemple : ct-abc123xyz7890)	Égal à	Pour le type de modification IDs, consultez la référence du type de modification. Pour le type de modification IDs, voir Trouver un type de modification ou CSIO.
Catégorie	Tout texte de forme libre	Contains	Les expressions régulières dans chaque champ individuel ne sont pas prises en charge. Recherche insensible aux majuscules et minuscules
Sous-catégorie			
Élément			
Opération			

1. Voici quelques exemples de classification des types de modification de liste :

La commande suivante répertorie toutes les catégories de types de modifications.

```
aws amscm list-change-type-categories
```

La commande suivante répertorie les sous-catégories appartenant à une catégorie spécifiée.

```
aws amscm list-change-type-subcategories --category CATEGORY
```

La commande suivante répertorie les éléments appartenant à une catégorie et à une sous-catégorie spécifiées.

```
aws amscm list-change-type-items --category CATEGORY --subcategory SUBCATEGORY
```

2. Voici quelques exemples de recherche de types de modifications à l'aide de requêtes CLI :

La commande suivante recherche dans les résumés de classification CT ceux qui contiennent « S3 » dans le nom de l'élément et crée une sortie de la catégorie, de la sous-catégorie, de l'élément, de l'opération et de l'ID de type de modification sous forme de tableau.

```
aws amscm list-change-type-classification-summaries --query
  "ChangeTypeClassificationSummaries [?contains(Item, 'S3')].
  [Category, Subcategory, Item, Operation, ChangeTypeId]" --output table
```

```
+-----+
|          ListChangeTypeClassificationSummaries          |
+-----+-----+-----+-----+-----+
|Deployment|Advanced Stack Components|S3|Create|ct-1a68ck03fn98r|
+-----+-----+-----+-----+-----+
```

3. Vous pouvez ensuite utiliser l'ID du type de modification pour obtenir le schéma CT et examiner les paramètres. La commande suivante génère le schéma dans un fichier JSON nommé Creates3Params.Schema.json.

```
aws amscm get-change-type-version --change-type-id "ct-1a68ck03fn98r"
  --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
  CreateS3Params.schema.json
```

Pour plus d'informations sur l'utilisation des requêtes CLI, consultez [Comment filtrer la sortie avec l'option --query](#) et la référence du langage de requête, [JMESPath Spécification](#).

4. Une fois que vous avez obtenu l'identifiant du type de modification, nous vous recommandons de vérifier la version du type de modification afin de vous assurer qu'il s'agit de la dernière version. Utilisez cette commande pour trouver la version correspondant à un type de modification spécifié :

```
aws amscm list-change-type-version-summaries --filter
  Attribute=ChangeTypeId,Value=CHANGE_TYPE_ID
```


Pour trouver le `AutomationStatus` type de modification correspondant à un type de modification spécifique, exécutez cette commande :

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --  
query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

Pour trouver le `ExpectedExecutionDurationInMinutes` type de modification correspondant à un type de modification spécifique, exécutez cette commande :

```
aws amscm --profile saml get-change-type-version --change-type-id ct-14027q0sjyt1h  
--query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

Résolution des erreurs RFC dans AMS

De nombreuses défaillances RFC de provisionnement AMS peuvent être étudiées dans la CloudFormation documentation. Voir [Résolution des problèmes liés à AWS CloudFormation : résolution des erreurs](#)

Des suggestions de résolution des problèmes supplémentaires sont fournies dans les sections suivantes.

Erreurs RFC de « gestion » dans AMS

Les types de changement de catégorie AMS « Management » (CTs) vous permettent de demander l'accès aux ressources ainsi que de gérer les ressources existantes. Cette section décrit certains problèmes courants.

Erreurs d'accès RFC

- Assurez-vous que le nom d'utilisateur et le FQDN que vous avez spécifiés dans la RFC sont corrects et existent dans le domaine. Pour obtenir de l'aide pour trouver votre nom de domaine complet, consultez la section [Trouver votre nom](#) de domaine complet.
- Assurez-vous que l'ID de pile que vous avez spécifié pour l'accès est EC2 une pile associée. Les piles telles que ELB et Amazon Simple Storage Service (S3) ne sont pas candidates à l'accès. Utilisez plutôt votre rôle d'accès RFCs en lecture seule pour accéder aux ressources de ces piles. Pour obtenir de l'aide pour trouver un identifiant de pile, voir [Trouver une pile IDs](#)

- Assurez-vous que l'identifiant de pile que vous avez fourni est correct et qu'il appartient au compte concerné.

Pour obtenir de l'aide concernant d'autres défaillances RFC d'accès, consultez la section [Gestion des accès](#).

YouTube Vidéo : [Comment lancer correctement une demande de modification \(RFC\) pour éviter les rejets et les échecs ?](#)

Erreurs de planification RFC (manuelle) CT

La plupart des types de modifications sont ExecutionMode = automatisés, mais certains sont ExecutionMode = manuels, ce qui affecte la façon dont vous devez les planifier pour éviter une défaillance de la RFC.

RFCs Planifié avec ExecutionMode =Manual, il doit être configuré pour s'exécuter au moins 24 heures dans le futur si vous utilisez la console AMS pour créer le RFC. Cette mise en garde ne s'applique pas à l'API/CLI AMS, mais il est tout de même important de planifier le manuel au moins 8 heures RFCs à l'avance.

AMS a pour objectif de répondre à un scanner manuel dans les quatre heures et vous contactera dès que possible, mais l'exécution de la RFC peut prendre beaucoup plus de temps.

Utilisation RFCs avec mise à jour manuelle CTs

AMS Operations rejette Management | Other | Other RFCs pour les mises à jour des piles, lorsqu'il existe un type de modification de mise à jour pour le type de pile que vous souhaitez mettre à jour.

Erreurs de suppression de pile RFC

Défaillances de la pile de suppression RFC : si vous utilisez le CT Management | Standard Stacks | Stack | Delete, vous verrez les événements détaillés dans la AWS CloudFormation console pour la pile portant le nom de la pile AMS. Vous pouvez identifier votre pile en la comparant au nom qu'elle porte dans la console AMS. La AWS CloudFormation console fournit plus de détails sur les causes des défaillances.

Avant de supprimer une pile, vous devez réfléchir à la manière dont elle a été créée. Si vous avez créé la pile à l'aide d'un AMS CT et que vous n'avez ni ajouté ni modifié les ressources de la pile, vous pouvez vous attendre à la supprimer sans problème. Cependant, il est conseillé de supprimer toutes les ressources ajoutées manuellement d'une pile avant de soumettre une RFC de suppression de pile à son encontre. Par exemple, si vous créez une pile à l'aide de la pile complète CT (HA Two

Tier), elle inclut un groupe de sécurité - SG1. Si vous utilisez ensuite AMS pour créer un autre groupe de sécurité - SG2, et que vous référencez le nouveau groupe SG1 créé SG2 dans le cadre de la pile complète, puis que vous utilisez la pile de suppression CT pour supprimer la pile, il ne SG1 sera pas supprimé car il est référencé par SG2.

Important

La suppression de piles peut avoir des conséquences indésirables et imprévues. Pour cette raison, AMS préfère **pas** supprimer des piles ou empiler des ressources pour le compte de ses clients. Notez qu'AMS supprimera uniquement les ressources en votre nom (par le biais d'un type de modification soumis par Gestion | Autre | Autre | Mettre à jour) qu'il n'est pas possible de supprimer en utilisant le type de modification automatique approprié à supprimer. Considérations supplémentaires :

- Si les ressources sont activées pour la « protection contre la suppression », AMS peut vous aider à débloquent ce type de modification en soumettant une modification de type Gestion | Autre | Autre | Mise à jour et, une fois la protection contre la suppression de la protection contre la suppression, vous pouvez utiliser le CT automatique pour supprimer cette ressource.
- Si une pile contient plusieurs ressources et que vous souhaitez supprimer uniquement un sous-ensemble des ressources de la pile, utilisez le type de modification CloudFormation Update (voir [CloudFormation Ingest Stack : Updating](#)). Vous pouvez également soumettre un type de modification Gestion | Autre | Autre | Mettre à jour et les ingénieurs d'AMS peuvent vous aider à élaborer l'ensemble de modifications, si nécessaire.
- Si vous rencontrez des problèmes lors de l'utilisation de l' CloudFormation Update CT en raison de dérives, AMS peut vous aider en soumettant une mise à jour Management | Other | Other | pour résoudre le problème (dans la mesure où cela est pris en charge par le CloudFormation service AWS) et en fournissant une ChangeSet que vous pouvez ensuite valider et exécuter à l'aide du CT, du Management/Custom Stack/Stack From CloudFormation Template/Approve changeset et de la mise à jour automatisés.

AMS applique les restrictions ci-dessus afin de garantir qu'il n'y ait pas de suppressions de ressources inattendues ou imprévues.

Pour plus d'informations, consultez [Résolution des problèmes liés à AWS CloudFormation : la suppression de la pile échoue](#).

Erreurs DNS de mise à jour RFC

Plusieurs RFCs pour mettre à jour une zone hébergée DNS peuvent échouer, parfois sans raison. La création simultanée de plusieurs RFCs zones hébergées pour mettre à jour les zones hébergées du DNS (privées ou publiques) peut entraîner l'échec de certaines RFCs d'entre elles car elles tentent de mettre à jour la même pile en même temps. La gestion des modifications AMS rejette ou échoue ceux RFCs qui ne sont pas en mesure de mettre à jour une pile parce que la pile est déjà mise à jour par une autre RFC. AMS vous recommande de créer une RFC à la fois et d'attendre qu'elle aboutisse avant d'en créer une nouvelle pour la même pile.

Erreurs d'entités RFC IAM

AMS fournit un certain nombre de rôles et de profils IAM par défaut dans des comptes AMS conçus pour répondre à vos besoins. Cependant, il se peut que vous deviez demander des ressources IAM supplémentaires de temps en temps.

Le processus de soumission des RFCs demandes de ressources IAM personnalisées suit le flux de travail standard pour le manuel RFCs, mais le processus d'approbation inclut également un examen de sécurité pour garantir que les contrôles de sécurité appropriés sont en place. Par conséquent, le processus prend généralement plus de temps que les autres manuels RFCs. Pour réduire le temps de cycle de ces RFCs appareils, veuillez suivre les instructions suivantes.

Pour plus d'informations sur ce que nous entendons par révision IAM et sur la manière dont elle correspond à nos normes techniques et à notre processus d'acceptation des risques, consultez [Comprendre les évaluations de sécurité RFC](#).

Demandes de ressources IAM courantes :

- Si vous demandez une politique concernant une application majeure compatible avec le cloud, par exemple CloudEndure, consultez le fichier d'exemple de CloudEndure politique IAM préapprouvée par AMS : décompressez le fichier d'[exemple de zone d'atterrissage WIGs Cloud Endure](#) et ouvrez le `customer_cloud_endure_policy.json`

Note

Si vous souhaitez une politique plus permissive, discutez de vos besoins avec vous CloudArchitect/CSDM et obtenez, si nécessaire, un examen de sécurité AMS et une approbation avant de soumettre une RFC mettant en œuvre la politique.

- Si vous souhaitez modifier une ressource déployée par AMS dans votre compte par défaut, nous vous recommandons de demander une copie modifiée de cette ressource plutôt que de modifier la ressource existante.
- Si vous demandez des autorisations pour un utilisateur humain (au lieu de les associer à l'utilisateur), associez les autorisations à un rôle, puis accordez à l'utilisateur l'autorisation d'assumer ce rôle. Pour plus de détails sur cette procédure, consultez la section [Accès temporaire à la console AMS Advanced](#).
- Si vous avez besoin d'autorisations exceptionnelles pour une migration ou un flux de travail temporaire, indiquez une date de fin pour ces autorisations dans votre demande.
- Si vous avez déjà discuté de l'objet de votre demande avec votre équipe de sécurité, fournissez la preuve de son approbation à votre CSDM avec le plus de détails possible.

Si AMS rejette une RFC IAM, nous fournissons une raison claire pour le rejet. Par exemple, nous pouvons rejeter une demande de création de politique IAM et expliquer en quoi cette politique est inappropriée. Dans ce cas, vous pouvez apporter les modifications identifiées et soumettre à nouveau la demande. Si des précisions supplémentaires sur le statut d'une demande sont nécessaires, soumettez une demande de service ou contactez votre CSDM.

La liste suivante décrit les risques typiques qu'AMS essaie d'atténuer lors de l'examen de votre IAM RFCs. Si votre RFC IAM présente l'un de ces risques, cela peut entraîner le rejet du RFC. Dans les cas où vous avez besoin d'une exception, AMS demande l'approbation de votre équipe de sécurité. Pour obtenir une telle exception, coordonnez-vous avec votre CSDM.

Note

AMS peut, pour quelque raison que ce soit, refuser toute modification des ressources IAM au sein d'un compte. Pour toute question concernant le rejet d'une RFC, contactez AMS Operations via une demande de service ou contactez votre CSDM.

- Augmentation des privilèges, telle que les autorisations qui vous permettent de modifier vos propres autorisations ou de modifier les autorisations d'autres ressources du compte. Exemples :
 - L'utilisation `iam:PassRole` avec un autre rôle plus privilégié.
 - Autorisation d'accéder aux politiques attach/detach IAM à partir d'un rôle ou d'un utilisateur.
 - Modification des politiques IAM dans le compte.
 - Possibilité d'effectuer des appels d'API dans le contexte de l'infrastructure de gestion.

- Autorisations permettant de modifier les ressources ou les applications requises pour vous fournir les services AMS. Exemples :
 - Modification de l'infrastructure AMS telle que les bastions, l'hôte de gestion ou l'infrastructure EPS.
 - Suppression des fonctions de gestion des journaux AWS Lambda, ou des flux de journaux.
 - Suppression ou modification de l'application de CloudTrail surveillance par défaut.
 - Modification de l'Active Directory (AD) des services d'annuaire.
 - Désactivation des CloudWatch alarmes (CW).
 - Modification des principes, des politiques et des espaces de noms déployés dans le compte dans le cadre de la zone de landing zone.
- Déploiement d'une infrastructure en dehors des meilleures pratiques, telles que les autorisations qui permettent la création d'une infrastructure dans un état mettant en danger la sécurité de vos informations. Exemples :
 - Création de compartiments S3 publics ou non chiffrés ou partage public de volumes EBS.
 - Le provisionnement d'adresses IP publiques.
 - Modification des groupes de sécurité pour permettre un accès étendu.
- Des autorisations trop larges susceptibles d'avoir un impact sur les applications, telles que des autorisations susceptibles d'entraîner une perte de données, une perte d'intégrité, une configuration inappropriée ou des interruptions de service pour votre infrastructure et les applications du compte. Exemples :
 - Désactiver ou rediriger le trafic réseau via APIs like `ModifyNetworkInterfaceAttribute` ou `UpdateRouteTable`
 - Désactivation de l'infrastructure gérée en détachant les volumes des hôtes gérés.
- Les autorisations pour les services ne font pas partie de la description du service AMS et ne sont pas prises en charge par AMS.

Les services non répertoriés dans la description du service AMS ne peuvent pas être utilisés dans les comptes AMS. Pour demander de l'aide pour une fonctionnalité ou un service, veuillez contacter votre CSDM.

- Autorisations qui ne répondent pas à l'objectif que vous vous êtes fixé, soit parce qu'elles sont trop généreuses, soit trop conservatrices, soit parce qu'elles ne sont pas appliquées aux bonnes ressources. Exemples :
 - Demande d'`s3:PutObject` autorisation d'accès à un compartiment S3 doté d'un chiffrement KMS obligatoire, sans `KMS:Encrypt` autorisation d'accès à la clé correspondante.

- Autorisations relatives à des ressources qui n'existent pas dans le compte.
- IAM RFCs où la description de la RFC ne semble pas correspondre à la demande.

Erreurs RFC « Déploiement »

Les types de changement de catégorie AMS « Déploiement » (CTs) vous permettent de demander que diverses ressources prises en charge par AMS soient ajoutées à votre compte.

La plupart des AMS CTs qui créent une ressource sont basés sur AWS CloudFormation des modèles. En tant que client, vous avez un accès en lecture seule à tous les services AWS. Vous pouvez notamment AWS CloudFormation identifier rapidement la AWS CloudFormation pile qui représente votre pile en fonction de la description de la pile à l'aide de la AWS CloudFormation console. La pile défaillante sera probablement dans l'état DELETE_COMPLETE. Une fois que vous avez identifié la AWS CloudFormation pile, les événements vous indiqueront la ressource spécifique qui n'a pas pu être créée et pourquoi.

Utilisation de CloudFormation la documentation pour résoudre les problèmes

La plupart des approvisionnements AMS RFCs utilisent un CloudFormation modèle et cette documentation peut être utile pour le dépannage. Consultez la documentation de ce AWS CloudFormation modèle :

- Créer une défaillance de l'équilibreur de charge d'application : [AWS::ElasticLoadBalancingV2::LoadBalancer \(Application Load Balancer\)](#)
- Créer un groupe Auto Scaling : [AWS::AutoScaling::AutoScalingGroup \(Auto Scaling Group\)](#)
- Créer un cache memcached : [AWS::ElastiCache::CacheCluster \(cluster de cache\)](#)
- Créer un cache Redis : [AWS::ElastiCache::CacheCluster \(cluster de cache\)](#)
- Créer une zone hébergée DNS (utilisée avec Create DNS privé/public) : [AWS::Route53::HostedZone \(Zone hébergée R53\)](#)
- Créer un ensemble d'enregistrements DNS (utilisé avec Create DNS privé/public) : [AWS::Route53::RecordSet \(Resource Record Sets\)](#)
- Créer une EC2 pile : [AWS::EC2::Instance \(Elastic Compute Cloud\)](#)
- Créer un système de fichiers Elastic (EFS) : [AWS::EFS::FileSystem \(Elastic File System\)](#)
- Créer un équilibreur de charge : [AWS::ElasticLoadBalancing::LoadBalancer \(Elastic Load Balancer\)](#)

- Créer une base de données RDS : [AWS::RDS::DBInstance \(base de données relationnelle\)](#)
- Créez Amazon S3 : [AWS::S3::Bucket \(service de stockage simple\)](#)
- Créer une file d'attente : [AWS::SQS::Queue \(service de file d'attente simple\)](#)

RFC créant des erreurs AMIs

Une Amazon Machine Image (AMI) est un modèle qui contient une configuration logicielle (par exemple, un système d'exploitation, un serveur d'applications et des applications). À partir d'une AMI, vous lancez une instance, qui est une copie de l'AMI exécutée en tant que serveur virtuel dans le cloud. AMIs sont très utiles et nécessaires pour créer des EC2 instances ou des groupes Auto Scaling ; toutefois, vous devez respecter certaines exigences :

- L'instance que vous spécifiez `Ec2InstanceId` doit être dans un état arrêté pour que la RFC réussisse. N'utilisez pas d'instances du groupe Auto Scaling (ASG) pour ce paramètre car l'ASG mettra fin à une instance arrêtée.
- Pour créer une Amazon Machine Image (AMI) AMS, vous devez commencer par une instance AMS. Avant de pouvoir utiliser l'instance pour créer l'AMI, vous devez la préparer en vous assurant qu'elle est arrêtée et dissociée de son domaine. Pour plus de détails, consultez [Créer une image de machine Amazon standard à l'aide de Sysprep](#)
- Le nom que vous spécifiez pour la nouvelle AMI doit être unique dans le compte, sinon la RFC échoue. La procédure à suivre est décrite dans [AMI | Create](#), et pour plus de détails, consultez [AWS AMI Design](#).

Note

Pour plus d'informations sur la préparation à la création d'AMI, voir [AMI | Create](#).

RFCs création EC2s d' ASGs erreurs

En cas de EC2 défaillances ASG avec délais d'expiration, AMS vous recommande de vérifier si l'AMI utilisée est personnalisée. Si tel est le cas, reportez-vous aux étapes de création d'AMI incluses dans ce guide (voir [AMI | Créer](#)) pour vous assurer que l'AMI a été créée correctement. Une erreur courante lors de la création d'une AMI personnalisée est de ne pas suivre les étapes du guide pour renommer ou invoquer Sysprep.

RFCs création d'erreurs RDS

Les défaillances d'Amazon Relational Database Service (RDS) peuvent survenir pour de nombreuses raisons, car vous pouvez utiliser de nombreux moteurs différents lorsque vous créez le RDS, et chaque moteur a ses propres exigences et limites. [Avant de tenter de créer une pile AMS RDS, examinez attentivement les valeurs des paramètres AWS RDS, voir Create. DBInstance](#)

Pour en savoir plus sur Amazon RDS en général, y compris les recommandations relatives à la taille, consultez la documentation [Amazon Relational Database Service](#).

RFCs création d'erreurs Amazon S3

L'une des erreurs les plus courantes lors de la création d'un compartiment de stockage S3 est le fait de ne pas utiliser un nom unique pour le compartiment. Si vous soumettez un compartiment S3 Create CT portant le même nom qu'un compartiment précédemment soumis, il échouera car un compartiment S3 portant ce nom existerait déjà BucketName. Cela sera détaillé dans la AWS CloudFormation console, où vous verrez que l'événement stack indique que le nom du bucket est déjà utilisé.

Validation RFC et erreurs d'exécution

Les échecs RFC et les messages associés diffèrent dans les messages de sortie sur la page de détails RFC de la console AMS pour une RFC sélectionnée :

- Les raisons des échecs de validation ne sont disponibles que dans le champ État
- Les raisons des échecs d'exécution sont disponibles dans les champs de sortie et de statut de l'exécution.

Messages d'erreur RFC

Lorsque vous rencontrez l'erreur suivante pour les types de modifications répertoriés (CTs), vous pouvez utiliser ces solutions pour vous aider à trouver la source des problèmes et à les résoudre.

```
{"errorMessage":"An error has occurred during RFC execution. We are investigating the issue.", "errorType":"InternalError"}
```

Si vous avez besoin d'une assistance supplémentaire après avoir consulté les options de dépannage suivantes, contactez AMS par correspondance RFC ou créez une demande de service. Voir

[Correspondance et pièce jointe RFC \(console\)](#) et [Création d'une demande de service dans AMS](#) pour plus de détails.

Erreurs d'ingestion de charge de travail (WIGS)

Note

Les outils de validation pour Windows et Linux peuvent être téléchargés et exécutés directement sur vos serveurs locaux, ainsi que sur les EC2 instances d'AWS. Vous pouvez les trouver dans le guide du développeur d'applications avancées d'AMS intitulé [Migrating workloads : Linux pre-ingestion validation](#) et [Migrating workloads : Windows pre-ingestion validation](#).

- Assurez-vous que l' EC2 instance existe dans le compte AMS cible. Par exemple, si vous avez partagé votre AMI d'un compte non-AMS vers un compte AMS, vous devrez créer une EC2 instance dans votre compte AMS avec l'AMI partagée avant de pouvoir soumettre une RFC d'ingestion de charge de travail.
- Vérifiez si le trafic de sortie est autorisé pour les groupes de sécurité attachés à l'instance. L'agent SSM doit être en mesure de se connecter à son point de terminaison public.
- Vérifiez si l'instance dispose des autorisations nécessaires pour se connecter à l'agent SSM. Ces autorisations sont fournies avec `lecustomer-mc-ec2-instance-profile`, vous pouvez vérifier cela dans la EC2 console :

EC2 erreurs d'arrêt de la pile d'instances

- Vérifiez si l'instance est déjà arrêtée ou terminée.
- Si l' EC2 instance est en ligne et que le `InternalError` message d'erreur s'affiche, soumettez une demande de service pour qu'AMS examine la situation.
- Notez que vous ne pouvez pas utiliser le type de changement `Management | Advanced stack components | EC2 instance stack | Stop ct-3mvt2zkyveqj` pour arrêter une instance d'Auto Scaling group (ASG). Si vous devez arrêter une instance ASG, soumettez une demande de service.

EC2 la pile d'instances crée des erreurs

Le `InternalError` message provient de CloudFormation ; une raison de statut `CREATION_FAILED`. Vous pouvez obtenir des informations détaillées sur la défaillance d'une CloudWatch pile dans les événements de pile en suivant ces étapes :

- Dans la console de gestion AWS, vous pouvez consulter la liste des événements de la pile lors de la création, de la mise à jour ou de la suppression de votre pile. Recherchez dans cette liste l'événement qui a échoué, puis consultez la raison du statut correspondant.

La raison du statut peut contenir un message d'erreur provenant d'AWS CloudFormation ou d'un service spécifique qui peut vous aider à comprendre le problème.

- Pour plus d'informations sur l'affichage des événements de stack, consultez la section [Visualisation des données et des ressources AWS CloudFormation Stack sur l'AWS Management Console](#).

EC2 erreurs de restauration du volume d'instance

AMS crée une RFC de dépannage interne en cas d'échec de la restauration du volume d' EC2 instance. Cela est fait parce que la restauration du volume d' EC2 instance est un élément important de la reprise après sinistre (DR) et AMS crée automatiquement cette RFC de dépannage interne pour vous.

Lorsque le RFC de dépannage interne est créé, une bannière s'affiche vous fournissant des liens vers le RFC. Cette RFC de dépannage interne vous donne une meilleure visibilité sur les échecs RFC et, plutôt que de soumettre une nouvelle tentative RFCs entraînant les mêmes erreurs, ou de vous obliger à contacter AMS manuellement en cas d'échec, vous pouvez suivre vos modifications et savoir qu'AMS est en train de remédier à l'échec. Cela réduit également la métrique time-to-recovery (TTR) associée à leur modification, car les opérateurs AMS travaillent de manière proactive sur l'échec de la RFC au lieu d'attendre votre demande.

Comment obtenir de l'aide concernant un RFC

Vous pouvez contacter AMS pour identifier la cause première de votre échec. Les heures d'ouverture d'AMS sont 24 heures par jour, 7 jours par semaine, 365 jours par an.

AMS vous propose plusieurs moyens de demander de l'aide ou de faire des demandes de service.

- Pour demander des informations ou des conseils, ou pour accéder à un service informatique géré par AMS, ou pour demander un service supplémentaire à AMS, utilisez la console AMS et soumettez une demande de service. Pour plus de détails, consultez [la section Création d'une](#)

[demande de service](#). Pour des informations générales sur les demandes de service AMS, consultez la section [Gestion des demandes de service](#).

- 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 rapport d'incident. Pour plus de détails, voir [Signaler un incident](#). Pour des informations générales sur la gestion des incidents AMS, consultez la section [Réponse aux incidents](#).
- Pour des questions spécifiques sur la façon dont vous ou vos ressources ou applications travaillez avec AMS, ou pour aggraver un incident, envoyez un e-mail à l'une ou plusieurs des adresses suivantes :
 1. Tout d'abord, si vous n'êtes pas satisfait de la demande de service ou de la réponse au rapport d'incident, envoyez un e-mail à votre CSDM : ams-csdm@amazon.com
 2. Ensuite, si l'escalade est requise, vous pouvez envoyer un e-mail au responsable des opérations AMS (mais votre CSDM le fera probablement) : ams-opsmanager@amazon.com
 3. Toute autre escalade serait adressée au directeur de l'AMS : ams-director@amazon.com
 4. Enfin, vous pouvez toujours joindre le vice-président de l'AMS : ams-vp@amazon.com

Mode de changement direct dans AMS

Rubriques

- [Commencer à utiliser le mode Direct Change](#)
- [Sécurité et conformité](#)
- [Gestion du changement en mode Direct Change](#)
- [Création de piles à l'aide du mode Direct Change](#)
- [Cas d'utilisation du mode de changement direct](#)

Le mode Direct Change (DCM) d'AWS Managed Services (AMS) étend la gestion des modifications d'AMS Advanced en fournissant un AWS accès natif aux comptes AMS Advanced Plus et Premium pour provisionner et mettre à jour les AWS ressources. Avec DCM, vous avez la possibilité d'utiliser une AWS API native (console ou CLI/SDK) ou des demandes de modification de gestion des modifications AMS Advanced (RFCs). Dans les deux cas, les ressources et leurs modifications sont entièrement prises en charge par AMS, y compris la surveillance, les correctifs, les sauvegardes et la gestion des réponses aux incidents. Les ressources fournies via DCM sont enregistrées dans le système de gestion des connaissances des services AMS (SKMS), jointes au domaine Active

Directory géré par AMS (le cas échéant) et exécutent les agents de gestion AMS. Utilisez les outils existants (par exemple CloudFormation, le AWS SDK et le CDK) pour développer et déployer des stacks gérés par AMS. CloudFormation

 Note

Le mode Direct Change ne supprime pas la gestion des modifications AMS RFCs. Vous avez un accès complet à AMS RFCs avec DCM.

[Regardez la vidéo d'Akash pour en savoir plus \(6h30\)](#)

Commencer à utiliser le mode Direct Change

Commencez par vérifier les conditions préalables, puis soumettez une demande de modification (RFC) sur votre compte AMS Advanced éligible.

1. Vérifiez que le compte que vous souhaitez utiliser avec DCM répond aux exigences :
 - Le compte est AMS Advanced Plus ou Premium.
 - Service Catalog n'est pas activé sur le compte. À l'heure actuelle, nous ne prenons pas en charge l'intégration de comptes à la fois à DCM et à Service Catalog. Si vous êtes déjà inscrit à Service Catalog mais que vous êtes intéressé par DCM, discutez de vos besoins avec votre responsable de prestation de services cloud (CSDM). Si vous décidez de passer de Service Catalog à DCM, déconnectez Service Catalog. Pour ce faire, incluez la demande dans la demande de modification ci-dessous. Pour plus de détails sur Service Catalog dans AMS, consultez [AMS and Service Catalog](#).
2. Soumettez une demande de modification (RFC) à l'aide de la commande Gestion | Compte géré | Mode de changement direct | Activer le type de modification (ct-3rd4781c2nnhp). Pour un exemple de procédure pas à pas, voir [Mode de changement direct | Activer](#).

Une fois le CT traité, les rôles IAM prédéfinis `AWSManagedServicesUpdateRole` sont provisionnés dans le compte spécifié. `AWSManagedServicesCloudFormationAdminRole`

3. Attribuez le rôle approprié aux utilisateurs qui ont besoin d'un accès au DCM à l'aide de votre processus de fédération interne.

 Note

Vous pouvez spécifier un nombre illimité de SAMLIdentity fournisseurs, de AWS services et d'entités IAM (rôles, utilisateurs, etc.) pour assumer les rôles. Vous devez fournir au moins un : SAMLIdentityProviderARNsIAMEntityARNs, ouAWSServicePrincipals. Pour plus d'informations, contactez le service IAM de votre entreprise ou votre architecte cloud AMS (CA).

Rôles et politiques IAM en mode Changement direct

Lorsque le mode Direct Change est activé dans un compte, les nouvelles entités IAM suivantes sont déployées :

`AWSManagedServicesCloudFormationAdminRole`: ce rôle permet d'accéder à la CloudFormation console, de créer et de mettre à jour des CloudFormation piles, d'afficher des rapports de dérive, de créer et d'exécuter CloudFormation ChangeSets. L'accès à ce rôle est géré par le biais de votre fournisseur SAML.

Les politiques gérées déployées et associées au rôle

`AWSManagedServicesCloudFormationAdminRole` sont les suivantes :

- Compte d'application AMS Advanced multi-comptes landing zone (MALZ)
 - `AWSManagedServices_CloudFormationAdminPolicy1`
 - `AWSManagedServices_CloudFormationAdminPolicy2`
 - Cette politique représente les autorisations accordées à `AWSManagedServicesCloudFormationAdminRole`. Vous et vos partenaires utilisez cette politique pour accorder l'accès à un rôle existant dans le compte et permettre à ce rôle de lancer et de mettre à jour des CloudFormation stacks dans le compte. Cela peut nécessiter des mises à jour supplémentaires de la politique de contrôle des services (SCP) AMS pour permettre à d'autres entités IAM de lancer CloudFormation des stacks.
- Compte de zone d'atterrissage à compte unique (SALZ) AMS Advanced
 - `AWSManagedServices_CloudFormationAdminPolicy1`
 - `AWSManagedServices_CloudFormationAdminPolicy2`
 - `cdk-legacy-mode-s3-access` [politique en ligne]
 - `AWS ReadOnlyAccess` politique

AWSManagedServicesUpdateRole: ce rôle accorde un accès restreint au AWS service en aval APIs. Le rôle est déployé avec des politiques gérées qui fournissent des opérations d'API mutantes et non mutantes, mais limitent en général les opérations mutantes (telles que Create/Delete/PUT) à certains services tels que les ressources et la configuration de l'infrastructure IAM, KMS, GuardDuty VPC, AMS, etc. L'accès à ce rôle est géré par le biais de votre fournisseur SAML.

Les politiques gérées déployées et associées au rôle **AWSManagedServicesUpdateRole** sont les suivantes :

- Compte d'application de zone d'atterrissage multi-comptes AMS Advanced
 - **AWSManagedServicesUpdateBasePolicy**
 - **AWSManagedServicesUpdateDenyPolicy**
 - **AWSManagedServicesUpdateDenyProvisioningPolicy**
 - **AWSManagedServicesUpdateEC2Et RDSPolicy**
 - **AWSManagedServicesUpdateDenyActionsOnAMSInfraPolitique**
- Compte de zone d'atterrissage à compte unique AMS Advanced
 - **AWSManagedServicesUpdateBasePolicy**
 - **AWSManagedServicesUpdateDenyProvisioningPolicy**
 - **AWSManagedServicesUpdateEC2Et RDSPolicy**
 - **AWSManagedServicesUpdateDenyActionsOnAMSInfraPolitique 1**
 - **AWSManagedServicesUpdateDenyActionsOnAMSInfraPolitique 2**

En outre, la stratégie gérée est également **ViewOnlyAccess** associée au **AWSManagedServicesUpdateRole** rôle de stratégie AWS gérée.

Sécurité et conformité

La sécurité et la conformité sont une responsabilité partagée entre AMS Advanced et vous, en tant que client. Le mode AMS Advanced Direct Change ne modifie pas cette responsabilité partagée.

Sécurité en mode Direct Change

AMS Advanced offre une valeur ajoutée avec une zone d'atterrissage prescriptive, un système de gestion du changement et une gestion des accès. Lorsque vous utilisez le mode Changement direct, ce modèle de responsabilité ne change pas. Cependant, vous devez être conscient des risques supplémentaires.

Le rôle « Mise à jour » du mode de changement direct (voir [Rôles et politiques IAM en mode Changement direct](#)) fournit des autorisations élevées permettant à l'entité qui y a accès d'apporter des modifications aux ressources d'infrastructure des services pris en charge par AMS au sein de votre compte. Avec des autorisations élevées, les risques varient en fonction de la ressource, du service et des actions, en particulier dans les situations où une modification incorrecte est apportée en raison d'un oubli, d'une erreur ou d'un non-respect de votre processus interne et de votre cadre de contrôle.

Conformément aux normes techniques de l'AMS, les risques suivants ont été identifiés et les recommandations suivantes sont formulées. Des informations détaillées sur les normes techniques AMS sont disponibles via AWS Artifact. Pour y accéder AWS Artifact, contactez votre CSDM pour obtenir des instructions ou rendez-vous sur [Getting Started with](#). AWS Artifact

AMS-STD-001 : Marquage

Normes	Est-ce que ça se casse	Risques	Recommandations
Toutes les ressources détenues par AMS doivent avoir la paire clé-valeur suivante	Oui. Interruptions pour CloudFormationCloudTrail, EFS OpenSearch, CloudWatch Logs, SQS, SSM, Tagging api, car ces services ne supportent pas la aws : TagsKey condition de restriction du balisage pour l'espace de noms AMS.	Un balisage incorrect des ressources AMS peut avoir un impact négatif sur les opérations de reporting, d'alerte et de correction de vos ressources, du côté AMS.	L'accès doit être restreint pour apporter des modifications aux exigences de balisage par défaut d'AMS pour toute personne autre que les équipes AMS.
Toutes les balises appartenant à AMS autres que celles répertoriées ci-dessus doivent avoir des préfixes tels que AMS* ou MC* au cas où. upper/lower/mix	La norme indiquée dans le tableau AMS-STD-003 ci-dessous indique que vous pouvez modifier l'environ		

Normes	Est-ce que ça se casse	Risques	Recommandations
	nement et Appld AppName, mais pas pour les ressources appartenant à AMS. Non réalisable par le biais des autorisations IAM.		
Aucune balise figurant sur les piles appartenant à AMS ne doit être supprimée en fonction de vos demandes de modification.	Oui CloudFormation ne prend pas en charge la aws : TagsKey condition de restriction des balises pour l'espace de noms AMS.		
Vous n'êtes pas autorisé à utiliser la convention de dénomination des balises AMS dans votre infrastructure, comme indiqué dans le tableau AMS-STD-002, ci-dessous.	Oui. Interruptions pour CloudFormation Amazon Elastic File System (EFS), OpenSearch CloudWatch Logs, Amazon Simple Queue Service (SQS), Amazon Systems Manager (SSM), Tagging API ; ces services ne supportent pas la condition de restriction du balisage pour aws : TagsKey l'espace de noms AMS. CloudTrail		

AMS-STD-002 : Identity and Access Management (IAM)

Normes	Est-ce que ça se casse	Risques	Recommandations
4.7 Les actions qui contournent le processus de gestion des modifications (RFC) ne doivent pas être autorisées, telles que le démarrage ou l'arrêt d'une instance, la création de compartiments S3 ou d'instances RDS, etc. Les comptes en mode développeur et les services en mode Self-Service Provisioned (SSPS) sont exemptés tant que les actions sont effectuées dans les limites du rôle attribué.	Oui. L'objectif des actions en libre-service vous permet d'effectuer des actions en contournant le système AMS RFC.	Le modèle d'accès sécurisé est une facette technique essentielle d'AMS et un utilisateur IAM pour l'accès à la console ou par programme contourne ce contrôle d'accès. L'accès des utilisateurs IAM n'est pas surveillé par la gestion des modifications d'AMS. L'accès est CloudTrail uniquement connecté.	L'utilisateur IAM doit être limité dans le temps et bénéficier d'autorisations basées sur le moindre privilège et. need-to-know

AMS-STD-003 : Sécurité réseau

Normes	Est-ce que ça se casse	Risques	Recommandations
S2. L'adresse IP élastique sur EC2 les instances ne doit être utilisée que dans le cadre d'un accord	Oui. Les actions en libre-service vous permettent d'associer et de dissocier des	L'ajout d'une adresse IP élastique à une instance l'expose à Internet. Cela augmente le risque de	Bloquez tout trafic inutile vers cette instance par le biais de groupes de sécurité et vérifiez

Normes	Est-ce que ça se casse	Risques	Recommandations
formel d'acceptation des risques ou d'un cas d'utilisation valide par les équipes internes.	adresses IP élastiques (EIP).	divulcation d'informations et d'activités non autorisées.	que vos groupes de sécurité sont attachés à l'instance afin de garantir qu'elle autorise le trafic uniquement lorsque cela est nécessaire pour des raisons professionnelles.
S14. Le peering VPC et les connexions aux terminaux entre les comptes appartenant au même client peuvent être autorisés.	Oui. Impossible dans le cadre de la politique IAM.	Le trafic sortant de votre compte AMS n'est pas surveillé une fois la limite du compte franchie.	Nous vous recommandons de peering uniquement avec les comptes AMS que vous possédez. Si votre cas d'utilisation l'exige, utilisez des groupes de sécurité et des tables de routage pour limiter les plages de trafic, les ressources et les types de trafic pouvant sortir via la connexion appropriée.

Normes	Est-ce que ça se casse	Risques	Recommandations
La base AMS AMIs peut être partagée entre des comptes gérés par AMS et non gérés, à condition que nous puissions vérifier qu'ils appartiennent à la même organisation. AWS		AMIs peut contenir des données sensibles et peut être exposé à des comptes non intentionnels.	Partagez uniquement AMIs avec le compte appartenant à votre organisation ou validez le cas d'utilisation et les informations du compte avant de partager en dehors de l'organisation.

AMS-STD-007 : Journalisation

Normes	Est-ce que ça se casse	Risques	Recommandations
19. Tout journal peut être transféré d'un compte AMS à un autre compte AMS du même client.			Partagez les journaux uniquement avec les comptes gérés par votre AWS organisation, ou validez le cas d'utilisation et les informations du compte avant de les partager en dehors de votre organisation.
20. Tout journal ne peut être transféré d'AMS vers un compte autre qu'AMS uniquement si le compte non-AMS appartient au même client AMS (en confirmant qu'il appartient au même AWS Organisations compte ou en	Oui. La politique IAM ne permet pas de vérifier que les comptes clients appartiennent à la même organisation.	Les journaux peuvent contenir des données sensibles et ils peuvent être exposés à des comptes non intentionnels.	Nous pouvons vérifier cela de plusieurs manières, consultez votre responsable de prestation de services cloud (CSDM).

Normes	Est-ce que ça se casse	Risques	Recommandations
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.			

Collaborez avec votre équipe interne d'autorisation et d'authentification pour contrôler en conséquence les autorisations relatives aux rôles du mode Changement direct.

Conformité en mode Direct Change

Le mode Direct Change est compatible avec les charges de travail en production et hors production. Il est de votre responsabilité de garantir le respect de toutes les normes de conformité (par exemple, PHI, HIPAA, PCI) et de vous assurer que l'utilisation du mode Direct Change est conforme à vos cadres et normes de contrôle internes.

Gestion du changement en mode Direct Change

La gestion du changement est le processus qu'AMS Advanced utilise pour mettre en œuvre les demandes de modification. Une demande de modification (RFC) est une demande créée par vous-même ou par AMS Advanced via l'interface AMS Advanced pour apporter une modification à votre environnement géré et inclut un ID de type de modification (CT) AMS Advanced pour une opération particulière. Pour plus d'informations, consultez la section [Gestion des modifications](#).

Note

Le mode Direct Change ne supprime pas la gestion des RFCs modifications d'AMS. Vous avez toujours un accès complet à AMS RFCs avec DCM.

Le mode AMS Direct Change (DCM) étend la gestion des modifications d'AMS Advanced en fournissant un AWS accès natif aux comptes AMS Advanced Plus et Premium pour provisionner et mettre à jour les AWS ressources. Les utilisateurs qui ont obtenu l'autorisation du mode Direct

Change via les rôles IAM peuvent utiliser AWS l'accès API natif pour approvisionner et modifier les ressources de leurs comptes AMS Advanced. Les utilisateurs peuvent toujours utiliser la gestion des modifications AMS Advanced RFCs en utilisant les mêmes rôles IAM. Dans les deux cas, les ressources et leurs modifications sont entièrement prises en charge par AMS, y compris la surveillance, les correctifs, les sauvegardes et la gestion de la réponse aux incidents. Les utilisateurs qui n'ont pas le rôle approprié dans ces comptes doivent utiliser le processus RFC de gestion des modifications AMS Advanced pour apporter des modifications.

Cas d'utilisation de la gestion du changement

Pour des raisons de sécurité, certaines modifications apportées à AMS Advanced ne peuvent être effectuées que par le biais du processus de demande de modification (RFC) de gestion des modifications. Elle `AWSManagedServicesCloudFormationAdminRole` est limitée aux actions entreprises par le biais de CloudFormation (CFN). Pour en savoir plus sur la création de piles via DCM, voir [Création de piles à l'aide du mode Direct Change](#). Elle `AWSManagedServicesUpdateRole` est limitée aux actions suivantes.

[Pour des exemples de procédures pas à pas pour chaque type de modification, y compris le type de modification Gestion | Compte géré | Mode de changement direct | Activer \(ct-3rd4781c2nnhp\), consultez la section « Informations supplémentaires » pour le type de modification correspondant dans la section AMS Advanced Change Type Reference Change Type Reference Change Types par classification.](#)

Service	Action
AWS Key Management Service (AWS KMS)	Mettre à jour
AWS Certificate Manager	Création
AWS Identity and Access Management (JE SUIS)	N'importe quel compte
AWS VPN	N'importe quel compte
Planificateur de ressources AMS	
AWS Backup	Création d'un plan de sauvegarde
Ingestion de la charge de travail AMS (WIGs)	N'importe quel compte

Service	Action
Filtrage de sortie AMS (géré par Palo Alto)	N'importe quel compte
Modifications du compte AMS Advanced MALZ	
Amazon GuardDuty	
Accès avancé à AMS Stack	N'importe quel compte
Volume Amazon Elastic Block Store (EBS)	Supprimer
Chiffrement par défaut d'Amazon Elastic Block Store (EBS)	Activer le chiffrement par défaut
Amazon Elastic Compute Cloud (Amazon EC2)	Modifier le nom d'hôte
Amazon Machine Images (AMI)	Supprimer, partager
Groupe EC2 de sécurité Amazon	N'importe quel compte
AMS (SSPS avancé)	
AWS Microsoft AD géré	
Mode développeur AMS Advanced	
Amazon Simple Storage Service (Amazon S3)	Création de politiques relatives aux compartiments S3
AWS Systems Manager	Création

Création de piles à l'aide du mode Direct Change

Pour que la pile soit gérée par `AMSAWSManagedServicesCloudFormationAdminRole`, deux conditions sont requises lors du lancement de piles à l' CloudFormation aide de :

- Le modèle doit contenir un `AmsStackTransform`.
- Le nom de la pile doit commencer par le préfixe `stack-` suivi d'une chaîne alphanumérique de 17 caractères.

 Note

Pour utiliser correctement le `AmsStackTransform`, vous devez reconnaître que votre modèle de pile contient la `CAPABILITY_AUTO_EXPAND` capacité permettant à AWS CloudFormation (CFN) de créer ou de mettre à jour la pile. Pour ce faire, vous devez transmettre le `CAPABILITY_AUTO_EXPAND` cadre de votre demande de création de pile. Le CFN rejette la demande si cette fonctionnalité n'est pas reconnue lors de `AmsStackTransform` son inclusion dans le modèle. La console CFN garantit que vous transmettez cette fonctionnalité si vous avez la transformation dans votre modèle, mais elle peut être manquée lorsque vous interagissez avec CFN via leur API. Vous devez transmettre cette fonctionnalité chaque fois que vous utilisez les appels d'API CFN suivants :

- [CreateChangeSet](#)
- [CreateStack](#)
- [UpdateStack](#)

Lors de la création ou de la mise à jour d'une pile avec DCM, les mêmes validations et augmentations de CFN Ingest et Stack Update CTs sont effectuées sur la pile. Pour plus d'informations, consultez les [directives d'AWS CloudFormation ingestion, les meilleures pratiques](#) et les limites. L'exception à cette règle est que les groupes de sécurité AMS par défaut (SGs) ne seront attachés à aucune EC2 instance autonome ni à aucune instance EC2 des groupes Auto Scaling (ASGs). Lorsque vous créez votre CloudFormation modèle, avec des EC2 instances autonomes ou ASGs, vous pouvez associer le modèle par défaut SGs.

 Note

Les rôles IAM peuvent désormais être créés et gérés à l'aide du `AWSManagedServicesCloudFormationAdminRole`.

Par défaut, AMS SGs possède des règles d'entrée et de sortie qui permettent aux instances de se lancer correctement et d'y accéder ultérieurement via SSH ou RDP par les opérations AMS et par vous. Si vous trouvez que les groupes de sécurité AMS par défaut sont trop permissifs, vous pouvez créer les vôtres SGs avec des règles plus restrictives et les associer à votre instance, à condition que cela vous permette, ainsi qu'aux opérations AMS, d'accéder à l'instance lors d'incidents.

Les groupes de sécurité AMS par défaut sont les suivants :

- SentinelDefaultSecurityGroupPrivateOnly: Accessible dans le modèle CFN via ce paramètre SSM /ams/\${VpcId}/SentinelDefaultSecurityGroupPrivateOnly
- SentinelDefaultSecurityGroupPrivateOnlyEgressAll: Accessible dans le modèle CFN via ce paramètre SSM /ams/\${VpcId}/SentinelDefaultSecurityGroupPrivateOnlyEgressAll

Transformation AMS

Ajoutez une Transform déclaration à votre CloudFormation modèle. Cela ajoute une CloudFormation macro qui valide et enregistre la pile auprès d'AMS au moment du lancement.

Exemple JSON

```
"Transform": {
  "Name": "AmsStackTransform",
  "Parameters": {
    "StackId": {"Ref" : "AWS::StackId"}
  }
}
```

Exemple YAML

```
Transform:
  Name: AmsStackTransform
  Parameters:
    StackId: !Ref 'AWS::StackId'
```

Ajoutez également l'Transforminstruction lors de la mise à jour du modèle d'une pile existante.

Exemple JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description" : "Create an SNS Topic",
  "Transform": {
    "Name": "AmsStackTransform",
    "Parameters": {
      "StackId": {"Ref" : "AWS::StackId"}
    }
  }
}
```

```

    }
  },
  "Parameters": {
    "TopicName": {
      "Type": "String",
      "Default": "HelloWorldTopic"
    }
  },
  "Resources": {
    "SnsTopic": {
      "Type": "AWS::SNS::Topic",
      "Properties": {
        "TopicName": {"Ref": "TopicName"}
      }
    }
  }
}

```

Exemple YAML

```

AWSTemplateFormatVersion: '2010-09-09'
Description: Create an SNS Topic
Transform:
  Name: AmsStackTransform
  Parameters:
    StackId: !Ref 'AWS::StackId'
Parameters:
  TopicName:
    Type: String
    Default: HelloWorldTopic
Resources:
  SnsTopic:
    Type: AWS::SNS::Topic
    Properties:
      TopicName: !Ref TopicName

```

Nom de la pile

Le nom de la pile doit commencer par le préfixe `stack-` suivi d'une chaîne alphanumérique de 17 caractères. Cela permet de maintenir la compatibilité avec les autres systèmes AMS qui fonctionnent sur la pile AMS IDs.

Voici des exemples de méthodes permettant de générer une pile compatible IDs :

Bash :

```
echo "stack-$(env LC_CTYPE=C tr -dc 'a-z0-9' < /dev/urandom | head -c 17)"
```

Python :

```
import string
import random

'stack-' + ''.join(random.choices(string.ascii_lowercase + string.digits, k=17))
```

PowerShell :

```
"stack-" + ( -join ((0x30..0x39) + ( 0x61..0x7A) | Get-Random -Count 17 | %
{[char]$_})) )
```

Cas d'utilisation du mode de changement direct

Les cas d'utilisation du mode de changement direct sont les suivants :

Fourniture et gestion des ressources par AWS CloudFormation

- Intégrez l' CloudFormation outillage et les processus existants.

Gestion continue des ressources et mises à jour

- Petits changements atomiques à faible risque.
- Modifications qui seraient autrement exécutées par le biais d'une RFC manuelle ou automatisée.
- Outillage nécessitant un accès natif à AWS l'API.
- Le rôle DCM peut être utilisé si vous êtes en phase de migration. Les équipes de migration exploitent les autorisations du DCM pour créer ou modifier des piles.
- Les rôles DCM peuvent être utilisés dans le CI/CD pipeline pour créer de nouvelles tâches AMIs, créer des tâches Amazon ECS, etc.

Mode développeur avancé AMS

Rubriques

- [Commencer à utiliser le mode développeur avancé d'AMS](#)
- [Sécurité et conformité en mode développeur](#)
- [Gestion des modifications en mode développeur](#)
- [Infrastructure de provisionnement en mode AMS Developer](#)
- [Contrôles Detective en mode AMS Developer](#)
- [Journalisation, surveillance et gestion des événements en mode AMS Developer](#)
- [Gestion des incidents en mode AMS Developer](#)
- [Gestion des correctifs en mode AMS Developer](#)
- [Gestion de la continuité en mode AMS Developer](#)
- [Gestion de la sécurité et des accès en mode AMS Developer](#)

Le mode développeur d'AWS Managed Services (AMS) utilise des autorisations élevées dans les comptes AMS Advanced Plus et Premium pour fournir et mettre à jour les ressources AWS en dehors du processus de gestion des modifications d'AMS Advanced. Pour ce faire, le mode AMS Advanced Developer exploite les appels d'API AWS natifs au sein de l'AMS Advanced Virtual Private Cloud (VPC), ce qui vous permet de concevoir et de mettre en œuvre une infrastructure et des applications dans votre environnement géré.

Lorsque vous utilisez un compte sur lequel le mode développeur est activé, la gestion de la continuité, la gestion des correctifs et la gestion des modifications sont fournies pour les ressources mises en service via le processus de gestion des modifications AMS Advanced ou à l'aide d'une image machine AMS Amazon (AMI). Toutefois, ces fonctionnalités de gestion AMS ne sont pas proposées pour les ressources provisionnées via le mode natif AWS APIs.

Vous êtes responsable de la surveillance des ressources d'infrastructure mises en service en dehors du processus de gestion des modifications AMS Advanced. Le mode développeur est compatible avec les charges de travail en production et hors production. Avec des autorisations élevées, vous avez la responsabilité accrue de garantir le respect des contrôles internes.

 Important

Les ressources que vous créez en mode Développeur ne peuvent être gérées par AMS Advanced que si elles sont créées à l'aide des processus de gestion des modifications d'AMS Advanced.

Le mode développeur est l'un des modes AMS Advanced que vous pouvez utiliser. Pour de plus amples informations, veuillez consulter [Vue d'ensemble des modes](#).

Commencer à utiliser le mode développeur avancé d'AMS

Découvrez les différents comptes AMS Advanced dotés du mode développeur AMS Advanced et découvrez comment implémenter avec succès le mode développeur.

Rubriques

- [Avant de commencer avec le mode développeur AMS](#)
- [Prérequis pour le mode développeur AMS](#)
- [Comment implémenter le mode AMS Advanced Developer](#)
- [Autorisations du mode développeur avancé AMS](#)

Avant de commencer avec le mode développeur AMS

Avant d'implémenter le mode développeur, vous devez savoir certaines choses.

AMS Advanced ne peut pas gérer les piles ou les ressources existantes dans un DevMode compte créé en dehors du processus de gestion des modifications d'AMS Advanced par le biais de demandes de modification (RFCs). Cependant, tant que le compte est ouvert DevMode, AMS Advanced continue de gérer les ressources mises à disposition via le processus de gestion des modifications AMS Advanced avec RFCs.

Vous ne pouvez pas commencer par un DevMode compte et le convertir ultérieurement en compte d'application géré par AMS Advanced.

Prérequis pour le mode développeur AMS

Les conditions préalables à la mise en œuvre du mode développeur sont les suivantes :

- Vous devez être un client AMS Advanced avec au moins un compte AMS Advanced Plus ou Premium intégré.
- Tout compte que vous utilisez doit être un compte AMS Advanced Plus ou Premium.
- Zone d'atterrissage multi-comptes (MALZ) : vous devez utiliser le rôle `AWSTManagedServicesDevelopmentRole` prédéfini AWS Identity and Access Management (IAM). Vous demandez ce rôle. La section suivante décrit comment obtenir des autorisations en mode développeur.

- Zone d'atterrissage à compte unique (SALZ) : vous devez utiliser le rôle `customer_developer_role` prédéfini AWS Identity and Access Management (IAM). Vous demandez ce rôle. La section suivante décrit comment obtenir des autorisations en mode développeur.

Comment implémenter le mode AMS Advanced Developer

Vous implémentez le mode développeur en demandant que votre compte AMS Advanced éligible soit provisionné avec le rôle IAM prédéfini :

- MALTE : `AWSTManagedServicesDevelopmentRole`
- SEL : `customer_developer_role`

Vous attribuez ensuite le rôle aux utilisateurs concernés dans votre réseau fédéré.

AMS Advanced vous recommande de vous assurer que votre utilisation du mode développeur est conforme à vos cadres et normes de contrôle internes, car le mode développeur crée deux vecteurs de changement : la gestion des modifications AMS Advanced pour les ressources gérées par AMS Advanced et la fédération des rôles gérée par le client pour les ressources que vous gérez en tant que client. Bien que les processus AMS Advanced restent conformes à nos déclarations, les processus clients et les cadres de contrôle peuvent avoir besoin d'être mis à jour.

Pour implémenter le mode développeur dans votre compte AMS Advanced

1. Vérifiez que le compte que vous souhaitez utiliser avec le mode développeur répond aux exigences répertoriées dans [Prérequis pour le mode développeur AMS](#).
2. Soumettez une demande de modification (RFC) en utilisant le type de modification (CT) Management | Compte géré | Mode développeur | Activer (révision requise). Pour un exemple d'utilisation de ce CT, voir [Mode développeur | Activer \(révision requise\)](#).

Une fois le CT traité, le rôle IAM prédéfini (`AWSTManagedServicesDevelopmentRole` pour MALZ, `customer_developer_role` pour SALZ) est configuré dans le compte demandé.

3. Attribuez le rôle approprié aux utilisateurs qui ont besoin d'accéder au mode développeur à l'aide de votre processus de fédération interne.

AMS Advanced vous recommande de limiter l'accès afin d'empêcher le provisionnement ou la modification de ressources non souhaités ou non approuvés.

Autorisations du mode développeur avancé AMS

Le rôle prédéfini (`AWSManagedServicesDevelopmentRole` pour MALZ, `customer_developer_role` pour SALZ) autorise la création de ressources d'infrastructure applicative au sein du VPC AMS Advanced, y compris les rôles IAM, tout en limitant l'accès aux composants de service partagés gérés par AMS Advanced (par exemple, les hôtes de gestion, les contrôleurs de domaine, Trend Micro EPS, les bastions et les services AWS non pris en charge). Le rôle restreint également l'accès aux éléments suivants Services AWS : Amazon GuardDuty, AWS Organizations AWS Directory Service APIs, et AMS Advanced logs.

Bien que le rôle vous permette de créer des rôles IAM supplémentaires, les mêmes limites d'autorisations incluses dans l'accès en mode développeur sont appliquées à tout rôle IAM créé par le `AWSManagedServicesDevelopmentRole`.

Sécurité et conformité en mode développeur

La sécurité et la conformité sont une responsabilité partagée entre AMS Advanced et vous en tant que client. Le mode développeur avancé d'AMS vous transfère la responsabilité partagée pour les ressources mises à disposition en dehors du processus de gestion des modifications ou fournies par le biais de la gestion des modifications, mais mises à jour avec les autorisations du mode développeur. Pour plus d'informations sur le partage des responsabilités, consultez [AWS Managed Services](#).

Précautions :

- DevMode vous permet, à vous et à votre équipe autorisée, de contourner les deny-by-default principes fondamentaux de la sécurité AMS. Les avantages, le libre-service et la réduction du temps d'attente pour l'AMS doivent être mis en balance avec les inconvénients. Tout le monde peut effectuer des actions inattendues et destructrices à l'insu de son équipe de sécurité. Les types de modifications automatisés permettant d'activer le mode Dev et le mode Direct Change sont exposés, et toute personne autorisée de votre organisation peut les exécuter CTs et activer ces modes.
- Vous êtes responsable de la gestion des autorisations d'exécution du CT à partir de votre base d'utilisateurs.
- AMS ne gère pas les autorisations d'exécution du CT

Recommandations :

- Protéger
 - Les clients peuvent empêcher l'accès à ce CT par le biais d'autorisations, voir [Restreindre les autorisations avec les déclarations de politique relatives aux rôles IAM](#)
 - Empêchez l'accès à ce CT en implémentant un proxy tel qu'un système ITSM
 - Utilisez des politiques de contrôle des services (SCPs) qui empêchent les politiques et les comportements selon les besoins, voir [AMS Preventative and Detective Controls Library](#)
- Détecter
 - Surveillez l'exécution de vos RFC CTs (Activer le mode développeur ct-1opjmhuddw194 et le mode de changement direct, activation ct-3rd4781c2nnhp) et répondez en conséquence
 - Vérifiez vos and/or comptes pour détecter la présence des ressources IAM afin d'identifier les comptes sur lesquels le mode développeur ou le mode changement direct ont été déployés
- Répondez
 - Supprimez des comptes en mode développeur si nécessaire

Sécurité en mode développeur

AMS Advanced offre une valeur ajoutée avec une zone d'atterrissage prescriptive, un système de gestion du changement et une gestion des accès. Lorsque vous utilisez le mode développeur, la valeur de sécurité d'AMS Advanced est conservée en utilisant la même configuration de compte que les comptes AMS Advanced standard qui établit le réseau renforcé de sécurité AMS Advanced de base. Le réseau est protégé par la limite d'autorisations appliquée dans le rôle (AWSManagedServicesDevelopmentRole pour MALZ, customer_developer_role pour SALZ), ce qui empêche l'utilisateur de décomposer les protections des paramètres établies lors de la configuration du compte.

Par exemple, les utilisateurs dotés du rôle peuvent accéder à Amazon Route 53, mais la zone hébergée interne AMS Advanced est restreinte. Les mêmes limites d'autorisations sont appliquées à un rôle IAM créé par le AWSManagedServicesDevelopmentRole, ce AWSManagedServicesDevelopmentRole qui empêche l'utilisateur de décomposer les protections des paramètres établies lors de l'intégration du compte à AMS Advanced.

Conformité en mode développeur

Le mode développeur est compatible avec les charges de travail en production et hors production. Il est de votre responsabilité de garantir le respect de toutes les normes de conformité (par exemple,

PHI, HIPAA, PCI) et de vous assurer que l'utilisation du mode développeur est conforme à vos cadres et normes de contrôle internes.

Gestion des modifications en mode développeur

La gestion du changement est le processus utilisé par le service AMS Advanced pour mettre en œuvre les demandes de modification. Une demande de modification (RFC) est une demande créée par vous ou par AMS Advanced via l'interface AMS Advanced pour apporter une modification à votre environnement géré et inclut un ID de type de modification (CT) pour une opération particulière. Pour de plus amples informations, veuillez consulter [Modes de gestion des modifications](#).

La gestion des modifications n'est pas appliquée dans les comptes AMS Advanced où les autorisations du mode développeur sont accordées. Les utilisateurs qui ont obtenu une autorisation en mode développeur avec le rôle IAM (AWSManagedServicesDevelopmentRole pour MALZ, customer_developer_role pour SALZ) peuvent utiliser l'accès à l'AWS API native pour approvisionner et modifier les ressources de leurs comptes AMS Advanced. Les utilisateurs qui n'ont pas le rôle approprié dans ces comptes doivent utiliser le processus de gestion des modifications AMS Advanced pour apporter des modifications.

Important

Les ressources que vous créez en mode Développeur ne peuvent être gérées par AMS Advanced que si elles sont créées à l'aide des processus de gestion des modifications d'AMS Advanced. Les demandes de modification soumises à AMS Advanced pour des ressources créées en dehors du processus de gestion des modifications d'AMS Advanced sont rejetées par AMS Advanced car elles doivent être traitées par vous.

Restrictions relatives à l'API des services de provisionnement en libre-service

Tous les services auto-provisionnés d'AMS Advanced sont pris en charge en mode développeur. L'accès aux services auto-approvisionnés est soumis aux limites décrites dans les sections du guide de l'utilisateur correspondant à chacun d'entre eux. Si aucun service auto-approvisionné n'est disponible avec votre rôle en mode développeur, vous pouvez demander un rôle mis à jour via le type de changement de mode développeur.

Les services suivants ne fournissent pas un accès complet au service APIs :

Services auto-provisionnés restreints en mode développeur

Service	Remarques
Amazon API Gateway	Tous les APIs appels Gateway sont autorisés, sauf SetWebACL .
Application Autoscaling	Peut uniquement enregistrer ou désenregistrer des cibles évolutives, et définir ou supprimer une politique de dimensionnement.
AWS CloudFormation	Impossible d'accéder aux CloudFormation piles dont le nom est préfixé par mc -
AWS CloudTrail	Impossible d'accéder ou de modifier les CloudTrail ressources dont le nom est préfixé par ams - and/or mc -.
Amazon Cognito (groupes d'utilisateurs)	Impossible d'associer des jetons logiciels. Impossible de créer des groupes d'utilisateurs, des tâches d'importation d'utilisateurs, des serveurs de ressources ou des fournisseurs d'identité.
AWS Directory Service	Seules les AWS Directory Service actions suivantes sont requises par Connect les WorkSpaces services. Toutes les autres actions du Service d'annuaire sont refusées par la politique de limite d'autorisation du mode développeur : • ds:AuthorizeApplication • ds:CreateAlias • ds:CreateIdentityPoolDirectory • ds>DeleteDirectory • ds:DescribeDirectories

Service	Remarques
	• <code>ds:GetAuthorizedApplicationDetails</code> • <code>ds:ListAuthorizedApplications</code> • <code>ds:UnauthorizeApplication</code> Dans les comptes de zone d'atterrissage à compte unique, la politique de limite refuse explicitement l'accès au répertoire géré AMS Advanced utilisé par AMS Advanced pour maintenir l'accès aux comptes compatibles avec le mode développement.
Amazon Elastic Compute Cloud	Impossible d'accéder à Amazon EC2 APIs contenant la chaîne : <code>DhcpOptions Gateway, Subnet, VPC, et VPN</code>. Impossible d'accéder aux EC2 ressources Amazon dont le préfixe de balise est <code>AMS,, mcManagementHostASG , and/or sentinel</code> ou de les modifier.
Amazon EC2 (Rapports)	Seul l'accès à la vue est accordé (ne peut pas être modifié). Remarque : Amazon EC2 Reports est en train de déménager. L'élément de menu Rapports sera supprimé du menu de navigation de EC2 la console Amazon. Pour consulter vos rapports EC2 d'utilisation d'Amazon après sa suppression, utilisez la console AWS Billing and Cost Management.

Service	Remarques
AWS Identity and Access Management (JE SUIS)	Impossible de supprimer les limites d'autorisation existantes ou de modifier les politiques de mot de passe utilisateur IAM. Impossible de créer ou de modifier des ressources IAM à moins d'utiliser le rôle IAM approprié (AWSManagedServicesDevelopmentRole pour MALZ, customer_developer_role pour SALZ)). Impossible de modifier les ressources IAM préfixées par :ams,,mc,customer_deny_policy . and/or sentinel Lors de la création d'une nouvelle ressource IAM (rôle, utilisateur ou groupe), la limite d'autorisation (MALZ :AWSManagedServicesDevelopmentRolePermissionsBoundary , SALZ :ams-app-infra-permissions-boundary) doit être attachée.
AWS Key Management Service (AWS KMS)	Impossible d'accéder aux clés KMS gérées par AMS Advanced ou de les modifier.
AWS Lambda	Impossible d'accéder ou de modifier AWS Lambda les fonctions préfixées parAMS.
CloudWatch Journaux	Impossible d'accéder aux flux de CloudWatch journaux dont le nom est préfixé par :mc,,awslambda, and/or AMS.
Amazon Relational Database Service (Amazon RDS)	Impossible d'accéder ou de modifier les bases de données Amazon Relational Database Service (Amazon RDS) DBs () dont le nom est préfixé par :. mc -

Service	Remarques
AWS Resource Groups	Ne peut accéder qu'aux Get actions de List l'API Search Resource Group et Resource Group.
Amazon Route 53	Impossible d'accéder aux ressources gérées par Route53 AMS Advanced ou de les modifier.
Amazon S3	Impossible d'accéder aux compartiments Amazon S3 dont le nom est préfixé par :ams - *, amsms - a, ou. mc - a
AWS Security Token Service	La seule API de service de jetons de sécurité autorisée est DecodeAuthorizationMessage .
Amazon SNS	Impossible d'accéder aux rubriques SNS dont le nom est préfixé par : AMS-Energon-Topic , ou. MMS-Topic
AWS Systems Manager (SSM)	Impossible de modifier les paramètres SSM préfixés par amsmc, ou. svc Impossible d'utiliser l'API SSM sur SendCommand des EC2 instances Amazon dont le tag est préfixé par ams ou. mc
AWS Balisage	Vous n'avez accès qu'aux actions de l'API de AWS balisage préfixées par. Get

Service	Remarques
AWS Lake Formation	Les actions AWS Lake Formation d'API suivantes sont refusées : • <code>lakeformation:DescribeResource</code> • <code>lakeformation:GetDataLakeSettings</code> • <code>lakeformation:DeregisterResource</code> • <code>lakeformation:RegisterResource</code> • <code>lakeformation:UpdateResource</code> • <code>lakeformation:PutDataLakeSettings</code>
Amazon Elastic Inference	Vous pouvez uniquement appeler l'action Elastic Inference API. <code>elastic-inference:Connect</code> Cette autorisation est incluse dans <code>customer_sagemaker_admin_policy</code> le document joint <code>aucustomer_sagemaker_admin_role</code> . Cette action vous donne accès à l'accélérateur Elastic Inference.
AWS Shield	Aucun accès à ces services APIs ou à cette console.
Amazon Simple Workflow Service	Aucun accès à ces services APIs ou à cette console.

Infrastructure de provisionnement en mode AMS Developer

Les utilisateurs qui ne possèdent pas le rôle IAM en mode développeur `AWSManagedServicesDevelopmentRole`, dans les comptes où le mode développeur est activé, sont tenus de suivre le processus de gestion des modifications AMS Advanced qui tire parti d'AMS Advanced. AMIs Les utilisateurs ayant le bon rôle

(MALZ :AWSManagedServicesDevelopmentRole, SALZ :customer_developer_role) peuvent utiliser le système de gestion des modifications AMS Advanced et AMS Advanced, AMIs mais ce n'est pas obligatoire.

Note

Une AWS AMI qui n'a pas été traitée via l'ingestion de charge de travail AMS Advanced ou qui n'a pas été créée dans un compte AMS Advanced n'inclura pas les configurations requises par AMS Advanced.

Contrôles Detective en mode AMS Developer

Cette section a été supprimée car elle contient des informations sensibles relatives à la sécurité AMS. Ces informations sont disponibles dans la documentation de la console AMS. Pour accéder à AWS Artifact, vous pouvez contacter votre CSDM pour obtenir des instructions ou consulter [Getting Started with AWS Artifact](#).

Journalisation, surveillance et gestion des événements en mode AMS Developer

La journalisation, la surveillance et la gestion des événements ne sont pas disponibles pour les ressources mises en service en dehors du processus de gestion des modifications AMS Advanced, ni pour les ressources fournies par le biais de la gestion des modifications puis modifiées par un compte à l'aide des autorisations du mode développeur.

Gestion des incidents en mode AMS Developer

Aucune modification des délais de réponse aux incidents. La résolution des incidents est la meilleure solution pour les ressources mises en service en dehors du processus de gestion des modifications, ou pour les ressources fournies par le biais de la gestion des modifications puis modifiées par un compte à l'aide des autorisations du mode développeur.

Note

Le contrat de niveau de service (SLA) AMS ne s'applique pas aux ressources créées ou mises à jour en dehors du système de gestion des modifications AMS (demandes de modification ou RFCs), mode développeur inclus ; par conséquent, les ressources mises à

jour ou créées en mode développeur sont automatiquement dégradées au niveau P3 et le support AMS fait de son mieux.

Gestion des correctifs en mode AMS Developer

La gestion des correctifs n'est pas disponible pour les ressources mises en service en dehors du processus de gestion des modifications AMS Advanced, ni pour les ressources fournies par le biais de la gestion des modifications puis modifiées par un compte à l'aide des autorisations du mode développeur. Délais d'application des correctifs :

- Pour une mise à jour de sécurité critique : dans les 10 jours ouvrables suivant la publication par le fournisseur pour les ressources fournies dans le cadre de la gestion des modifications, puis modifiées par un compte à l'aide des autorisations du mode développeur.
- Pour une mise à jour importante : dans les 2 mois suivant la publication par le fournisseur pour les ressources fournies par le biais de la gestion des modifications, puis modifiées par un compte à l'aide des autorisations du mode développeur.

Gestion de la continuité en mode AMS Developer

La gestion de la continuité n'est pas disponible pour les ressources mises en service en dehors du processus de gestion des modifications AMS Advanced, ni pour les ressources fournies par le biais de la gestion des modifications puis modifiées par un compte à l'aide des autorisations du mode développeur.

Le délai de lancement de la restauration de l'environnement peut prendre jusqu'à 12 heures pour les ressources mises en service en dehors du processus de gestion des modifications AMS Advanced, ou pour les ressources fournies par le biais de la gestion des modifications puis modifiées par un compte à l'aide des autorisations du mode développeur.

Gestion de la sécurité et des accès en mode AMS Developer

La protection contre les programmes malveillants est de votre responsabilité pour les ressources mises en service en dehors du processus de gestion des modifications AMS Advanced, ou pour les ressources fournies par le biais de la gestion des modifications puis modifiées par un compte à l'aide des autorisations du mode développeur. L'accès aux instances Amazon Elastic Compute Cloud (Amazon EC2) non provisionnées via AMS Advanced change management peut être contrôlé par des paires de clés au lieu de fournir un accès fédéré.

Mode de provisionnement en libre-service dans AMS

Le mode Self-Service Provisioning (SSP) d'AWS Managed Services (AMS) fournit un accès complet aux fonctionnalités natives des AWS services et des API dans les comptes gérés par AMS. Vous accédez aux services par le biais de AWS Identity and Access Management rôles standardisés et délimités. AMS prend en charge les demandes de service et la gestion des incidents. Les alertes, la surveillance, la journalisation, les correctifs, les sauvegardes et la gestion des modifications relèvent de votre responsabilité. Dans de nombreux cas, les services de provisionnement en libre-service (SSPS) sont autogérés, c'est-à-dire sans serveur, et ne nécessitent pas la gestion de certaines tâches opérationnelles telles que l'application de correctifs. Vous bénéficiez de l'utilisation de ces services dans les limites de l'environnement définies par AMS Guardrails et toute modification de l'IAM (y compris les rôles liés aux services, les rôles de service, les rôles entre comptes ou les mises à jour des politiques) doit être approuvée par AMS Operations afin de maintenir la sécurité de base de la plateforme. Vous pouvez utiliser des AWS CloudFormation modèles pour automatiser le déploiement de ces services, mais cela n'est pas pris en charge pour tous les services SSP.

Important

Utilisez le mode SSP dans vos comptes AWS Managed Services (AMS) pour accéder aux AWS services et les utiliser, avec les restrictions indiquées.

Il y a des Services AWS que vous pouvez utiliser sans gestion AMS, dans votre compte AMS. Les services du mode Self-Service Provisioning, ou SSPS en abrégé, comment les ajouter à votre compte AMS et FAQs pour chacun d'entre eux, sont décrits dans la section.

Les services d'approvisionnement en libre-service sont proposés tels quels, et vous êtes responsable de leur gestion. AMS ne fournit aucune alerte, surveillance, journalisation ou application de correctifs pour les ressources associées à ces services. AMS fournit des rôles IAM qui vous permettent d'utiliser le service dans votre compte AMS en toute sécurité. Les AMS SLAs ne s'appliquent pas.

Pour les ressources que vous fournissez en libre-service, AMS fournit la gestion des incidents, les contrôles de détection et les garde-fous, les rapports, les ressources désignées (Cloud Service Delivery Manager et Cloud Architect), la sécurité et l'accès, ainsi que le support technique via les demandes de service. En outre, le cas échéant, vous assumez la responsabilité de la gestion de la continuité, de la gestion des correctifs, de la surveillance de l'infrastructure et de la gestion des modifications pour les ressources fournies ou configurées en dehors du système de gestion des modifications AMS.

Commencer à utiliser le mode SSP dans AMS

Le provisionnement en libre-service est l'un des modes AMS que vous pouvez utiliser pour les zones d'atterrissage multicomptes (MALZ). Pour de plus amples informations, veuillez consulter [Vue d'ensemble des modes](#).

Pour fournir des fonctionnalités de provisionnement en libre-service, AMS a créé des rôles IAM élevés avec des limites d'autorisation afin de limiter les modifications involontaires liées à l'accès direct. Service AWS Les rôles n'empêchent pas tous les changements et vous devez respecter vos contrôles internes et vos politiques de conformité, et vérifier que tous Services AWS ceux utilisés répondent aux certifications requises. Il s'agit du mode de provisionnement en libre-service. Pour plus de détails sur les exigences de AWS conformité, voir [AWS Conformité](#).

Pour ajouter un service d'approvisionnement en libre-service à votre compte d'application de zone d'atterrissage multi-comptes, utilisez le service Gestion | AWS Service | Service auto-approvisionné | Ajouter un type de modification (CT), soit le CT requis pour la révision, soit le CT automatique, comme indiqué pour le service.

Note

Pour demander à AMS de fournir un service de provisionnement en libre-service supplémentaire, déposez une demande de service.

Utilisez AMS SSP pour configurer Amazon API Gateway sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon API Gateway directement depuis votre compte géré AMS. [Amazon API Gateway](#) est un service entièrement géré qui permet aux développeurs de créer, publier, gérer, surveiller et sécuriser facilement APIs à n'importe quelle échelle. À l'aide de REST, AWS Management Console vous pouvez créer une porte d'entrée WebSocket APIs permettant aux applications d'accéder aux données, à la logique métier ou aux fonctionnalités de vos services principaux, tels que les charges de travail exécutées sur Amazon Elastic Compute Cloud EC2 ([Amazon](#)), le code exécuté sur [AWS Lambda](#) n'importe quelle application Web ou les applications de communication en temps réel.

API Gateway gère toutes les tâches liées à l'acceptation et au traitement de centaines de milliers d'appels d'API simultanés, notamment la gestion du trafic, le contrôle des autorisations et des accès,

la surveillance et la gestion des versions d'API. API Gateway n'impose aucun frais minimum ni aucun coût de démarrage. Vous ne payez que pour les appels d'API que vous recevez et pour la quantité de données transférées. Grâce au modèle de tarification échelonnée d'API Gateway, vous pouvez réduire vos coûts à mesure que votre utilisation des API augmente. Pour en savoir plus, consultez [Amazon API Gateway](#).

FAQ : API Gateway dans AMS

Q : Comment puis-je demander l'accès à Amazon API Gateway depuis mon compte AMS ?

Demandez l'accès à API Gateway en soumettant une RFC avec le type de modification Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Cette RFC attribue les rôles IAM suivants à votre compte : `customer_apigateway_author_role` et `customer_apigateway_cloudwatch_role`. Une fois les rôles configurés dans votre compte, vous devez intégrer les rôles dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon API Gateway sur mon compte AMS ?

- La configuration d'API Gateway est limitée aux ressources sans préfixes AMS- ou sans MC- préfixes afin d'empêcher toute modification de l'infrastructure AMS.
- CREATELes privilèges pour VPCLink sont désactivés afin d'empêcher la création non réglementée d'Elastic Load Balancers. VPCLinks Si nécessaire, consultez [Application Load Balancer](#) | Create.

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon API Gateway dans mon compte AMS ?

Cela dépend du type d'API Gateway que vous souhaitez déployer. Il peut s'agir d'un service autonome, mais il peut également demander l'accès à des services existants (par exemple, un équilibreur de charge réseau).

Utilisez AMS SSP pour provisionner Alexa for Business sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Alexa for Business directement depuis votre compte géré par AMS. Alexa for Business est un service qui permet à votre entreprise et à vos employés d'utiliser Alexa pour travailler davantage. Avec Alexa for Business, vous pouvez utiliser Alexa comme assistante intelligente pour être plus productif dans les salles de réunion, à votre bureau et même avec les appareils Alexa que vous utilisez déjà à la

maison ou en déplacement. Les responsables informatiques et des installations peuvent utiliser Alexa for Business pour mesurer et augmenter l'utilisation des salles de réunion existantes sur leur lieu de travail.

Pour en savoir plus, consultez [Alexa for Business](#).

FAQ sur Alexa for Business dans AWS Managed Services

Q : Comment puis-je demander l'accès à Alexa for Business depuis mon compte AMS ?

Demandez l'accès en soumettant un type de modification Gestion | AWS service | Service auto-provisionné | Ajouter (révision requise) (ct-3qe6io8t6jtny). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_alex_console_role` Un `customer_alex_device_setup_user` est également créé pour l'outil de configuration des appareils fourni par Alexa for Business ; cet outil de configuration des appareils peut ensuite être utilisé pour configurer vos appareils. Une fois les rôles configurés dans votre compte, vous devez intégrer les rôles dans votre solution de fédération.

La passerelle Alexa for Business vous permet de connecter Alexa for Business à vos terminaux Cisco Webex et Poly Group Series pour contrôler les réunions avec votre voix. Le logiciel de passerelle s'exécute sur votre matériel sur site et transmet en toute sécurité les directives de conférence d'Alexa for Business à votre terminal Cisco. La passerelle a besoin de deux paires d'AWS informations d'identification pour communiquer avec Alexa for Business. Nous fournissons deux utilisateurs IAM à accès limité : `customer_alex_gateway_installer_user` et `customer_alex_gateway_execution_user` pour vos passerelles Alexa for Business, l'un pour l'installation de la passerelle et l'autre pour l'exploitation de la passerelle ; ceux-ci peuvent être demandés en soumettant une RFC avec le type de changement de déploiement | Composants de pile avancés | Identity and Access Management (IAM) | Créer une entité ou une politique (révision requise) type de modification (ct-3dpd8mdd9jn1r).

Note

Pour générer des rapports d'utilisation et les envoyer à Amazon S3, spécifiez le nom du compartiment Amazon S3 dans la RFC du service auto-provisionné.

Q : Quelles sont les restrictions relatives à l'utilisation d'Alexa for Business sur mon compte AMS ?

Il n'y a aucune restriction. Toutes les fonctionnalités d'Alexa for Business sont disponibles avec le rôle de service autonome Alexa for Business.

Q : Quels sont les prérequis ou les dépendances pour utiliser Alexa for Business sur mon compte AMS ?

- Si vous avez l'intention WPA2 d'utiliser le Wi-Fi d'entreprise pour configurer vos appareils partagés, spécifiez ce type de sécurité réseau dans l'outil de configuration des appareils, pour lequel un AWS Private Certificate Authority est requis.
- AMS crée uniquement des clés secrètes qui commencent par l'espace de noms « A4B ». Ceci est limité uniquement à cet espace de noms.

Q : Quelles fonctionnalités d'Alexa for Business doivent être séparées RFCs ?

Pour enregistrer un appareil Alexa Voice Service (AVS) auprès d'Alexa for Business, donnez accès au créateur d'appareils intégré Alexa. Pour ce faire, un rôle IAM doit être créé dans la console Alexa for Business qui peut être déployé à l'aide du type de modification Management | Other | Other. Cela permet au fabricant d'appareils AVS d'enregistrer et de gérer des appareils auprès d'Alexa for Business en votre nom.

Utilisez AMS SSP pour approvisionner Amazon AppStream 2.0 sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon AppStream 2.0 (AppStream 2.0) directement depuis votre compte géré par AMS. AppStream La version 2.0 vous permet de déplacer vos applications de bureau vers AWS, sans les réécrire. Vous pouvez installer vos applications sur la AppStream version 2.0, définir des configurations de lancement et mettre vos applications à la disposition des utilisateurs. AppStream La version 2.0 propose une large sélection d'options de machine virtuelle afin que vous puissiez sélectionner le type d'instance qui correspond le mieux aux exigences de votre application et définir les paramètres de mise à l'échelle automatique afin de répondre facilement aux besoins de vos utilisateurs finaux. AppStream La version 2.0 vous permet de lancer des applications sur votre propre réseau, ce qui signifie que vos applications peuvent interagir avec vos AWS ressources existantes.

Amazon AppStream 2.0 vous permet d'installer, de tester et de mettre à jour rapidement et facilement vos applications à l'aide du générateur d'images. Toutes les applications qui s'exécutent sous Microsoft Windows Server 2012 R2, Windows Server 2016 ou Windows Server 2019 sont prises en charge et vous n'avez pas besoin d'apporter de modifications. Une fois les tests terminés, vous pouvez définir les configurations de lancement des applications, les paramètres utilisateur par défaut et publier votre image pour que les utilisateurs puissent y accéder.

Pour en savoir plus, consultez la section [AppStream 2.0](#).

AppStream FAQ sur la version 2.0 dans AWS Managed Services

Q : Comment puis-je demander l'accès à la AppStream version 2.0 dans mon compte AMS ?

Demandez l'accès à la AppStream version 2.0 en soumettant une RFC avec le type de modification Management | AWS Service | Self-provisioned Service | Add (ct-3qe6io8t6jtny). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_appstream_console_role`

A `customer_appstream_stream_role` est également déployé pour diffuser des applications qui nécessitent que les utilisateurs soient authentifiés à l'aide de leurs informations de connexion Active Directory.

Une fois les rôles configurés dans votre compte, vous devez intégrer les rôles dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation de la AppStream version 2.0 dans mon compte AMS ?

- Les fonctionnalités suivantes doivent être configurées par l'équipe de Support AMS et nécessitent des fonctionnalités spécifiques RFCs. Les instructions relatives à la demande de fonctionnalités supplémentaires se trouvent dans la section 4.
- Création et diffusion à partir des points de terminaison VPC de l'interface.
- Support des points de terminaison Amazon S3 pour les dossiers personnels et la persistance des paramètres d'application sur un réseau privé.
- Création et choix du rôle IAM qui sera disponible sur toutes les instances de streaming de flotte.
- Rejoindre les flottes AppStream 2.0 et les domaines Microsoft Active Directory de créateurs d'images.
- Création de rapports d'utilisation personnalisés AppStream 2.0.
- L'image de marque personnalisée n'est actuellement pas prise en charge.

Q : Quels sont les prérequis ou les dépendances pour utiliser la AppStream version 2.0 dans mon compte AMS ?

Lorsque vous soumettez la RFC à Onboard AppStream 2.0, incluez le nom du compartiment Amazon S3 à utiliser pour le rapport d'utilisation de la AppStream version 2.0. Le nom du bucket est ajouté au

customer-appstream-usagereports-policy bucket créé lors de l'intégration de la AppStream version 2.0.

Q : Quelles fonctionnalités AppStream 2.0 doivent être séparées RFCs ?

- Afin de choisir un point de terminaison VPC d'interface pour la AppStream version 2.0, soumettez une RFC de type Management | Other | Other | Update pour créer un point de terminaison VPC dans votre compte. Pour connaître les étapes de création de points de terminaison personnalisés pour la AppStream version 2.0, consultez la section [Création et diffusion à partir de points de terminaison VPC d'interface](#) dans AppStream le guide de l'utilisateur de la version 2.0.
- Support des points de terminaison Amazon S3 pour les dossiers personnels et la persistance des paramètres d'application sur un réseau privé ; il suffit de demander des points de terminaison VPC Amazon S3 à l'aide d'une RFC de type Management | Other | Other | Create change. La RFC doit inclure le compartiment Amazon S3 cible hébergeant le contenu du dossier de base ou les paramètres de l'application (compartiments Amazon S3), respectivement. Cette RFC fournira à AppStream 2.0 les autorisations nécessaires pour accéder aux points de terminaison Amazon S3 VPC. Pour savoir comment créer des points de terminaison personnalisés pour les flux, consultez la section [Utilisation des points de terminaison Amazon S3 VPC pour les dossiers personnels et la persistance des paramètres d'application](#) dans AppStream le guide de l'utilisateur 2.0.
- Afin de créer et de choisir un rôle IAM qui sera disponible sur toutes les instances de streaming de flotte, soumettez une RFC Deployment | Advanced stack components | Identity and Access Management (IAM) | Create entity or policy (révision requise) type de modification (ct-3dpd8mdd9jn1r) demandant le rôle IAM avec la politique requise. Le nom du rôle IAM doit toujours commencer par le préfixe « customer_appstream ».
- Les flottes et les générateurs d'images Amazon AppStream 2.0 peuvent être joints à des domaines dans Microsoft Active Directory en soumettant une RFC de type de modification Management | Other | Other | Update pour la création d'un compte de service dans Active Directory (AD). Les autorisations minimales requises pour rejoindre Microsoft Active Directory sont définies dans la documentation AppStream 2.0 à la section [Octroi d'autorisations pour créer et gérer des objets informatiques Active Directory](#).
- Pour créer des rapports d'utilisation AppStream 2.0 personnalisés, soumettez une RFC de type Management | Other | Other | Create change type demandant ce qui suit :
 - AppStreamUsageReports« Création d'une pile CFN
 - « customer_appstream_usagereports_role » doit être fourni dans le compte
 - Fournissez également les informations suivantes :

- Fournissez une expression CRON pour planifier l'exécution de Crawler. Par défaut, il est 23h00 UTC tous les jours.
- L'ARN du compartiment Amazon S3 doit être utilisé pour les résultats des requêtes Athena. Ce compartiment doit avoir le préfixe suivant : `aws-athena-query-results`
- Journal des rapports d'utilisation (ARN) du compartiment Amazon S3 pour la AppStream version 2.0.

Une fois le rôle configuré, intégrez-le à votre solution de fédération et connectez-vous, puis accédez à Athena pour générer AWS Glue des rapports personnalisés à l'aide du rôle de rapport d'utilisation. Pour plus de détails sur l'utilisation des rapports d'utilisation AppStream 2.0, voir [Créer des rapports personnalisés et analyser les données d'utilisation AppStream 2.0](#) dans la documentation AppStream 2.0.

Utilisez AMS SSP pour approvisionner Amazon Athena sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon Athena (Athena) directement depuis votre compte géré AMS. Athena est un service de requête interactif qui vous aide à analyser les données dans Amazon S3 à l'aide du SQL standard. Athena fonctionnant sans serveur, vous n'avez pas d'infrastructure à gérer et vous ne payez que pour les requêtes que vous exécutez. Vous pointez sur vos données dans Amazon S3, vous définissez le schéma et vous lancez des requêtes à l'aide du SQL standard. La plupart des résultats sont fournis en quelques secondes. Avec Athena, vous n'avez pas besoin de tâches complexes extract-transform-load (ETL) pour préparer vos données en vue de leur analyse. Cela permet à toute personne possédant des compétences en SQL d'analyser rapidement des ensembles de données à grande échelle. Pour en savoir plus, consultez [Amazon Athena](#).

FAQ : Athéna dans AMS

Q : Comment puis-je demander l'accès à Amazon Athena depuis mon compte AMS ?

Demandez l'accès à Athena en soumettant une RFC avec le type de modification Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_athena_console_role`. Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon Athena sur mon compte AMS ?

Il n'y a aucune restriction. Toutes les fonctionnalités d'Amazon Athena sont disponibles sur votre compte AMS.

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon Athena dans mon compte AMS ?

Athena dépend largement du AWS Glue service, car il utilise les données catalog/metastore créées avec AWS Glue. Par conséquent, les autorisations AWS Glue sont incluses dans la RFC Athena réussie.

Le rôle `customer_athena_console_role` a une condition préalable pour un compartiment Amazon S3. Pour créer un nouveau compartiment, utilisez le CT automatisé `ct-1a68ck03fn98r` (Déploiement | Composants de pile avancés | Stockage S3 | Création). Lorsque vous utilisez ce scanner automatisé pour créer un compartiment S3 pour Athena, le nom du compartiment doit commencer par un préfixe `athena-query-results-`*

Utilisez AMS SSP pour approvisionner Amazon Bedrock sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon Bedrock directement dans votre compte géré AMS. Amazon Bedrock est un service entièrement géré qui met à votre AWS disposition des modèles de base très performants (FMs) issus de startups spécialisées dans l'IA via une API unifiée. Vous pouvez choisir parmi une large gamme de modèles de fondation pour trouver le modèle le mieux adapté à votre cas d'utilisation. Amazon Bedrock propose également un large éventail de fonctionnalités permettant de créer des applications d'IA générative alliant sécurité, confidentialité et IA responsable. Avec Amazon Bedrock, vous pouvez facilement expérimenter et évaluer les meilleurs modèles de fondation adaptés à vos cas d'utilisation, les personnaliser en privé avec vos données à l'aide de techniques telles que l'affinement et la génération augmentée de récupération (RAG), et créer des agents qui exécutent des tâches à l'aide des systèmes et des sources de données de votre entreprise.

Grâce à l'expérience sans serveur d'Amazon Bedrock, vous pouvez démarrer rapidement, personnaliser en privé les modèles de base avec vos propres données, les intégrer et les déployer facilement et en toute sécurité dans vos applications à l'aide des outils AWS sans avoir à gérer d'infrastructure. Pour plus d'informations, consultez [Amazon Bedrock](#).

FAQ : Amazon Bedrock dans AMS

Q : Comment puis-je demander l'accès à Amazon Bedrock depuis mon compte AMS ?

Pour demander l'accès à Amazon Bedrock, soumettez une RFC avec le type de modification Management | AWS Service | Self-provisioned Service | Add (révision requise) (ct-3qe6io8t6jtny). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_bedrock_console_role`. Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon Bedrock sur mon compte AMS ?

- Les bases de connaissances Amazon Bedrock ne sont pas prises en charge par défaut dans le cadre du rôle SSPS en raison de leur dépendance à l'égard d'Amazon OpenSearch Service Serverless, qui n'est actuellement pas pris en charge sur AMS.
- Bedrock Studio n'est pas pris en charge car il dépend de services non pris en charge tels qu'Amazon. DataZone

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon Bedrock dans mon compte AMS ?

- Les modèles d'abonnement tiers qui nécessitent AWS Marketplace des autorisations doivent être effectués par le rôle par défaut (`AWSTrustedServicesAdminRoles` sur MALZ et `Customer_ReadOnly_Role` sur SALZ). Cela est dû au fait que le rôle par défaut inclut AWS Marketplace les autorisations.
- Si le chiffrement des données est utilisé, vous devez fournir l'ARN de la AWS KMS clé lorsque vous demandez la création du rôle de console. En outre, le nom du bucket Amazon S3 utilisé doit comporter « bedrock ».

Utilisez AMS SSP pour approvisionner Amazon sur CloudSearch votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux CloudSearch fonctionnalités d'Amazon directement depuis votre compte géré par AMS. Amazon CloudSearch est un service géré dans le AWS cloud que vous utilisez de manière rentable pour configurer, gérer et faire évoluer une solution de recherche pour votre site Web ou votre application. Amazon CloudSearch prend en charge 34 langues et propose des fonctionnalités de recherche populaires telles que le surlignage, la saisie semi-automatique et la recherche géospatiale. Pour en savoir plus, consultez [Amazon CloudSearch](#).

 Note

AWS a fermé l'accès des nouveaux clients à Amazon CloudSearch à compter du 25 juillet 2024. Les clients CloudSearch existants d'Amazon peuvent continuer à utiliser le service normalement. AWS continue d'investir dans l'amélioration de la sécurité, de la disponibilité et des performances d'Amazon CloudSearch, mais nous ne prévoyons pas d'introduire de nouvelles fonctionnalités.

Pour comprendre les différences entre Amazon CloudSearch et Amazon OpenSearch Service, et pour savoir comment passer à OpenSearch Service, contactez votre architecte cloud (CA) pour obtenir des conseils. Pour plus d'informations sur la transition vers le OpenSearch service, consultez la section [Transition d'Amazon CloudSearch vers le OpenSearch service Amazon Service](#).

FAQ sur Amazon CloudSearch dans AWS Managed Services

Q : Comment puis-je demander l'accès CloudSearch à Amazon via mon compte AMS ?

Demandez l'accès à Amazon CloudSearch en soumettant une RFC avec le type de modification Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Cette RFC attribue les rôles IAM suivants à votre compte : `customer_csearch_admin_role` et `customer_csearch_dev_role`. Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon sur CloudSearch mon compte AMS ?

Toutes les fonctionnalités d'Amazon CloudSearch sont disponibles dans votre compte AMS. Toutes les solutions de base de données prises en charge par AMS sont actuellement prises en charge sur Amazon. CloudSearch Notez qu'à l'heure actuelle, DynamoDB est la seule solution de base de données AWS gérée qui ne peut pas être indexée.

Q : Quelles sont les conditions préalables ou les dépendances pour utiliser Amazon CloudSearch dans mon compte AMS ?

Amazon CloudSearch dépend de la collaboration d'Amazon S3 avec les fournisseurs d'identité pour analyser automatiquement les données d'entrée et déterminer les champs de la table. L'accès à Amazon S3 n'est pas fourni avec cette RFC et doit être demandé séparément dans une demande de service.

Utilisez AMS SSP pour approvisionner Amazon CloudWatch Synthetics sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon Synthetics directement CloudWatch depuis votre compte géré AMS. Vous pouvez utiliser Amazon CloudWatch Synthetics pour créer des « canaris » afin de surveiller vos points de terminaison et APIs

Les canaries sont des scripts configurables, écrits en Node.js ou Python, qui s'exécutent selon un calendrier. Ils créent des fonctions Lambda dans votre compte qui utilisent Node.js ou Python comme cadre. Les scripts Canary fonctionnent sur les protocoles HTTP et HTTPS. Les canaris vérifient la disponibilité et la latence de vos terminaux et peuvent stocker les données relatives au temps de chargement et les captures d'écran de l'interface utilisateur. Ils surveillent votre REST APIs et le contenu de votre site Web, et ils peuvent détecter les modifications non autorisées dues au phishing, à l'injection de code et aux scripts intersites. URLs

Les Canaries suivent les mêmes itinéraires et effectuent les mêmes actions qu'un client, ce qui vous permet de vérifier en permanence votre expérience client, même lorsque vos applications n'ont aucun trafic client. En utilisant les scripts Canary, vous pouvez découvrir les problèmes avant vos clients. Pour en savoir plus, consultez [Amazon CloudWatch : Utilisation de la surveillance synthétique](#).

FAQ sur Amazon CloudWatch Synthetics dans AWS Managed Services

Q : Comment puis-je demander l'accès à Amazon CloudWatch Synthetics depuis mon compte AMS ?

Demandez l'accès à Amazon CloudWatch Synthetics en soumettant une RFC avec le type de modification Management AWS | service | Self-provisioned service | Add (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte : « customer_cw_synthetics_console_role » et « customer_cw_synthetics_canary_lambda_role ». Une fois configuré dans votre compte, vous devez intégrer le rôle « customer_cw_synthetics_console_role » dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon CloudWatch Synthetics sur mon compte AMS ?

Il n'existe aucune restriction quant à l'utilisation d'Amazon CloudWatch Synthetics dans votre compte AMS. Il est interdit de créer des rôles pour les canaris en dehors du rôle de service fourni par AMS « customer_cw_synthetics_canary_lambda_role ».

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon CloudWatch Synthetics dans mon compte AMS ?

Les canaris créent et utilisent un compartiment Amazon CloudWatch Synthetics S3 par défaut : "- - »
cw-syn-results *`\${accountnumber}`* *`\${default-region}`*

Utilisez AMS SSP pour approvisionner des groupes d'utilisateurs Amazon Cognito sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités des groupes d'utilisateurs Amazon Cognito directement depuis votre compte géré AMS. Les groupes d'utilisateurs Amazon Cognito fournissent un répertoire d'utilisateurs sécurisé pouvant accueillir des centaines de millions d'utilisateurs. En tant que service entièrement géré, les groupes d'utilisateurs d'Amazon Cognito peuvent être configurés sans avoir à se soucier de la mise en place d'une infrastructure de serveur. Ce service vous permet de gérer un pool d'utilisateurs finaux que vous pouvez utiliser pour l'intégrer à vos applications internes. Ce service vous offre une alternative à une base de données personnalisée ou à un annuaire des utilisateurs finaux pour les applications Web ou mobiles. Dans le même temps, les groupes d'utilisateurs Amazon Cognito fournissent l'ensemble complet des fonctionnalités d'un service d'annuaire, telles que les politiques relatives aux mots de passe, l'authentification multifactorielle, la récupération des mots de passe et l'auto-inscription aux services. Cela permet également à l'application de fédérer l'accès dans d'autres services publics populaires tels qu'OpenID, Facebook, Amazon ou Google.

Amazon Cognito est divisé en deux produits principaux. Groupes d'utilisateurs Amazon Cognito et fournisseur d'identité Amazon Cognito. Cette section se concentre sur les groupes d'utilisateurs Amazon Cognito, qui donnent accès à d'autres AWS services tels qu'Amazon S3 ou DynamoDB. Le service vous permet d'utiliser des groupes d'utilisateurs Amazon Cognito, ou un fournisseur d'identité tiers, pour fournir un accès aux AWS services. Il permet également d'accéder aux AWS services en utilisant un accès invité anonyme. En raison de la puissance des groupes d'utilisateurs d'Amazon Cognito, ceux-ci seraient gérés manuellement sous la forme d' case-by-case un service manuel d'utilisation, afin d'éviter d'éventuelles failles de sécurité dans le compte. Pour en savoir plus, consultez la section [Groupes d'utilisateurs Amazon Cognito](#).

FAQ sur les groupes d'utilisateurs Amazon Cognito dans AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès aux groupes d'utilisateurs Amazon Cognito sur mon compte AMS ?

La mise en œuvre des groupes d'utilisateurs Amazon Cognito dans AMS est un processus en deux étapes :

1. Soumettez un type de modification Management | Other | Other | Create (ct-1e1xtak34nx76) et demandez la création des groupes d'utilisateurs Amazon Cognito dans votre compte AMS. Incluez les informations suivantes :
 - AWS Région.
 - Nom du groupe d'utilisateurs Cognito.
 - Si vous souhaitez utiliser Amazon Simple Email Service (Amazon SES) pour envoyer des messages et des notifications au lieu du service de messagerie interne Cognito par défaut, le client doit fournir une adresse e-mail déjà validée pour le service Amazon SES dans le compte. Cette adresse sera utilisée pour les champs « De » et « REPLY-TO » du message. Ils doivent également indiquer la région dans laquelle Amazon SES a été activé (us-east-1, eu-west-1 ou us-west-2).
 - Si vous souhaitez utiliser des SMS pour des mots de passe à usage unique et pour la vérification, le client doit l'indiquer.
2. Demandez l'accès utilisateur en soumettant un type de gestion | AWS service | service auto-approvisionné | Ajouter un type de modification (ct-1w8z66n899dct). Cette RFC attribue les rôles IAM suivants à votre compte : `customer_cognito_admin_role` et `customer_cognito_importjob_role`. Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération. Ces rôles vous permettent de gérer les groupes d'utilisateurs Amazon Cognito, de gérer vos utilisateurs et groupes dans le pool, de créer des tâches d'importation pour les utilisateurs, de modifier les messages de notification et d'abonnement, d'associer des applications au groupe d'utilisateurs, de gérer vous-même l'ajout de services de fédération au pool et de supprimer des pools déjà créés.

Q : Quelles sont les restrictions relatives à l'utilisation des groupes d'utilisateurs Amazon Cognito dans mon compte AMS ?

Vous ne serez pas en mesure de créer les groupes d'utilisateurs Amazon Cognito. Cette action nécessite la création de rôles IAM pour tirer parti des services utilisés par Amazon Cognito, tels qu'Amazon SES et Amazon Simple Notification Service (Amazon SNS).

Q : Quels sont les prérequis ou les dépendances pour utiliser les groupes d'utilisateurs Amazon Cognito dans mon compte AMS ?

Si vous souhaitez utiliser Amazon SES pour envoyer des messages et des notifications par e-mail à vos groupes d'utilisateurs, ils doivent déjà activer le service Amazon SES dans le compte et valider l'adresse e-mail qui doit être utilisée dans les champs « FROM » et « REPLY-TO » des e-mails

envoyés. Pour plus d'informations sur la validation des adresses e-mail à l'aide d'Amazon SES, consultez la section [Vérification des adresses e-mail dans Amazon SES](#).

Utilisez AMS SSP pour approvisionner Amazon Comprehend sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon Comprehend directement dans votre compte géré AMS. Amazon Comprehend est un service de traitement du langage naturel (NLP) qui utilise l'apprentissage automatique pour trouver des informations et des relations dans le texte. Aucune expérience en apprentissage automatique n'est requise. Amazon Comprehend utilise le machine learning pour vous aider à découvrir les informations et les relations contenues dans vos données non structurées. Le service identifie la langue du texte, extrait des phrases, des lieux, des personnes, des marques ou des événements clés, comprend le caractère positif ou négatif du texte, analyse le texte à l'aide de la tokenisation et de parties du discours, et organise automatiquement une collection de fichiers texte par sujet. Vous pouvez également utiliser les fonctionnalités AutoML d'Amazon Comprehend pour créer un ensemble personnalisé d'entités ou de modèles de classification de texte spécialement adaptés aux besoins de votre organisation. Pour en savoir plus, consultez [Amazon Comprehend](#).

FAQ sur Amazon Comprehend dans AWS Managed Services

Q : Comment puis-je demander l'accès à Amazon Comprehend depuis mon compte AMS ?

La console Amazon Comprehend et les rôles d'accès aux données peuvent être demandés en soumettant deux services AMS : RFCs

Demandez l'accès en soumettant un type de modification Gestion | AWS service | Service auto-approvisionné | Ajouter (révision requise) (ct-3qe6io8t6jtny). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_comprehend_console_role` Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon Comprehend sur mon compte AMS ?

La fonctionnalité Create New IAM Role via la console Amazon Comprehend est restreinte. Sinon, toutes les fonctionnalités d'Amazon Comprehend sont disponibles sur votre compte AMS.

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon Comprehend dans mon compte AMS ?

Amazon S3 et AWS Key Management Service (AWS KMS) sont nécessaires pour utiliser Amazon Comprehend, si les compartiments Amazon S3 sont chiffrés à l'aide de clés. AWS KMS

Utilisez AMS SSP pour approvisionner Amazon Connect sur votre compte AMS

Note

Après mûre réflexion, nous avons décidé de mettre fin au support d'Amazon Connect Voice ID à compter du 20 mai 2026. Amazon Connect Voice ID n'acceptera plus de nouveaux clients à compter du 20 mai 2025. En tant que client existant disposant d'un compte inscrit au service avant le 20 mai 2025, vous pouvez continuer à utiliser les fonctionnalités d'Amazon Connect Voice ID. Après le 20 mai 2026, vous ne pourrez plus utiliser Amazon Connect Voice ID.

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon Connect directement depuis votre compte géré par AMS. Amazon Connect est un centre de contact cloud omnicanal qui aide les entreprises à fournir un service client de qualité supérieure à moindre coût. Amazon Connect fournit une expérience fluide via la voix et le chat aux clients et aux agents. Cela inclut un ensemble d'outils pour le routage basé sur les compétences, de puissantes analyses historiques et en temps réel, ainsi que des outils de gestion easy-to-use intuitifs, le tout assorti d'une pay-as-you-go tarification.

Vous pouvez créer une ou plusieurs instances des instances du centre de contact virtuel dans des comptes de zone d'atterrissage multi-comptes AMS ou dans des comptes de zone d'atterrissage à compte unique. Vous pouvez utiliser les fournisseurs d'identité SAML 2.0 existants pour accéder aux agents ou utiliser le support natif d'Amazon Connect pour la gestion du cycle de vie des utilisateurs.

En outre, vous pouvez demander des free/direct numéros de téléphone payants pour chaque instance Amazon Connect depuis la console Amazon Connect. Vous pouvez créer des flux de contacts riches pour obtenir l'expérience client et le routage souhaités à l'aide d'une interface utilisateur easy-to-use graphique. Les flux de contacts peuvent tirer parti de AWS Lambda fonctions pour s'intégrer aux magasins de données et aux API sur site. Vous pouvez également activer le streaming de données à l'aide de Kinesis Streams et Firehose.

Les enregistrements d'appels, les transcriptions de chat et les rapports sont stockés dans un compartiment Amazon S3 chiffré à l'aide d'une AWS KMS clé. Les journaux des flux de contacts peuvent être enregistrés dans des groupes de CloudWatch journaux.

Pour en savoir plus, consultez [Amazon Connect](#).

FAQ sur Amazon Connect dans AWS Managed Services

Q : Comment puis-je demander l'accès à Amazon Connect depuis mon compte AMS ?

Demandez l'accès en soumettant un type de modification Gestion | AWS service | Service auto-approvisionné | Ajouter (révision requise) (ct-3qe6io8t6jtny). Cette RFC attribue les rôles IAM suivants à votre compte : `customer_connect_console_role` et `customer_connect_user_role`. Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon Connect sur mon compte AMS ?

Il n'y a aucune restriction. Toutes les fonctionnalités d'Amazon Connect sont disponibles sur votre compte AMS.

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon Connect dans mon compte AMS ?

- Vous devez créer une AWS KMS clé et un compartiment Amazon S3 à l'aide d'AMS standard RFCs ; le compartiment Amazon S3 est nécessaire pour stocker les enregistrements d'appels et les transcriptions de chat.
- Si vous souhaitez intégrer Active Directory (AD), un connecteur AD est requis pour l'intégration entre les instances Amazon Connect hébergées par AMS et vos services d'annuaire locaux. L'AD Connector peut être configuré dans votre compte en demandant une RFC « Management | Other | Other ».
- Vous pouvez activer les services d'auto-approvisionnement facultatifs suivants en fonction de vos besoins en matière de flux de contacts.
 - AWS Lambda: vous pouvez utiliser les fonctions Lambda pour étendre les flux de contacts afin de tirer parti des magasins de données sur site existants ou. APIs Vous pouvez utiliser le service Lambda auto-provisionné pour créer les fonctions Lambda.
 - Amazon Kinesis Data Streams : vous pouvez créer des flux de données pour permettre le streaming de données vers des applications externes. Vous pouvez diffuser les enregistrements de suivi des contacts ou les événements des agents.

- Amazon Kinesis Data Firehose : vous pouvez créer Data Firehose pour diffuser de gros volumes d'enregistrements de suivi des contacts vers des applications externes.
- Amazon Lex : vous pouvez utiliser les chatbots Amazon Lex pour créer des flux de contacts intelligents en tirant parti des services Amazon Alexa pour une expérience client enrichie et une automatisation.
- Q : Comment puis-je demander l'ajout d'une liste de pays pour les appels sortants ou entrants ?

Pour ajouter une liste de pays pour les appels sortants ou entrants, soumettez une demande de service à AMS.

Utilisez AMS SSP pour approvisionner Amazon Data Firehose sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon Data Firehose directement depuis votre compte géré par AMS. Firehose est le moyen le plus simple de charger de manière fiable des données de streaming dans des lacs de données, des magasins de données et des outils d'analyse. Il peut capturer, transformer et charger des données de streaming dans Amazon S3, Amazon Redshift, Amazon OpenSearch Service et [Splunk](#), permettant ainsi des analyses en temps quasi réel avec les outils de business intelligence et les tableaux de bord existants que vous utilisez déjà aujourd'hui. Il s'agit d'un service entièrement géré qui s'adapte automatiquement au débit de vos données et ne nécessite aucune administration continue. Il peut également regrouper, compresser, transformer et chiffrer les données avant de les charger, minimisant ainsi la quantité de stockage utilisée à destination et renforçant la sécurité. Pour en savoir plus, consultez [Qu'est-ce qu'Amazon Data Firehose ?](#)

FAQ sur Firehose dans AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès à Amazon Data Firehose depuis mon compte AMS ?

Demandez l'accès en soumettant un type de modification Gestion | AWS service | Service auto-approvisionné | Ajouter (révision requise) (ct-3qe6io8t6jtny). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_kinesis_firehose_user_role` Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation de Firehose sur mon compte AMS ?

Il n'y a aucune restriction. Toutes les fonctionnalités d'Amazon Data Firehose sont disponibles sur votre compte AMS.

Q : Quels sont les prérequis ou les dépendances pour utiliser Firehose dans mon compte AMS ?

De nouveaux rôles IAM liés à un service doivent être demandés pour chaque flux de diffusion. Vous pouvez également réutiliser un seul rôle lié à un service pour tous les flux en mettant à jour la politique des rôles avec les autorisations de ressources requises (y compris les compartiments S3, les clés KMS, les fonctions Lambda et les flux Kinesis).

Après avoir soumis le RFC pour ajouter Firehose, un ingénieur des opérations AMS vous contactera par le biais d'une demande de service pour ARNs les ressources que vous souhaitez connecter à Data Firehose (par exemple AWS KMS, S3, Lambda et Kinesis Streams).

Utilisez AMS SSP pour approvisionner Amazon DevOps Guru sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon DevOps Guru directement depuis votre compte géré par AMS. Amazon DevOps Guru est un service d'exploitation entièrement géré qui permet aux développeurs et aux opérateurs d'améliorer facilement les performances et la disponibilité de leurs applications. DevOpsGuru vous permet de vous décharger des tâches administratives associées à l'identification des problèmes opérationnels afin que vous puissiez rapidement mettre en œuvre des recommandations pour améliorer votre application. DevOpsGuru crée des informations réactives que vous pouvez utiliser pour améliorer votre application dès maintenant. Il crée également des informations proactives pour vous aider à éviter les problèmes opérationnels susceptibles d'affecter votre application à l'avenir. DevOpsGuru applique l'apprentissage automatique pour analyser vos données opérationnelles ainsi que les indicateurs et événements de votre application afin d'identifier les comportements qui s'écartent des modèles de fonctionnement normaux. Vous êtes averti lorsque DevOps Guru détecte un problème ou un risque opérationnel. Pour chaque problème, DevOps Guru présente des recommandations intelligentes pour résoudre les problèmes opérationnels actuels et futurs.

Pour en savoir plus, consultez [Qu'est-ce qu'Amazon DevOps Guru ?](#)

FAQ sur Amazon DevOps Guru dans AWS Managed Services

Q : Comment puis-je demander l'accès à Amazon DevOps Guru depuis mon compte AMS ?

Pour demander un accès, soumettez un type de modification Gestion | AWS Service | Service auto-approvisionné | Ajouter (révision requise) (ct-3qe6io8t6jtny). Cette RFC attribue le rôle IAM suivant à

vosre compte : `customer_devopsguru_role` Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon DevOps Guru sur mon compte AMS ?

Il n'y a aucune restriction. Toutes les fonctionnalités d'Amazon DevOps Guru sont disponibles sur votre compte AMS.

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon DevOps Guru dans mon compte AMS ?

Il n'y a aucun prérequis. DevOpsGuru exploite les AWS services suivants : Amazon CloudWatch Logs, RDS Insights, AWS X-Ray AWS Lambda, et. AWS CloudTrail

Utilisez AMS SSP pour approvisionner Amazon DocumentDB (compatible avec MongoDB) sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon DocumentDB (compatible avec MongoDB) directement depuis votre compte géré AMS. Amazon DocumentDB (compatible avec MongoDB) est un service de base de données de documents rapide, évolutif, hautement disponible et entièrement géré qui prend en charge les charges de travail MongoDB. Amazon DocumentDB vous offre les performances, l'évolutivité et la disponibilité dont vous avez besoin pour exécuter des charges de travail MongoDB critiques à grande échelle. Amazon DocumentDB implémente l'API open source MongoDB 3.6 Apache 2.0 en émulant les réponses qu'un client MongoDB attend d'un serveur MongoDB, ce qui vous permet d'utiliser vos pilotes et outils MongoDB existants avec Amazon DocumentDB. Dans Amazon DocumentDB, le stockage et le calcul sont découplés, ce qui permet à chacun d'évoluer indépendamment, et vous pouvez augmenter la capacité de lecture à des millions de requêtes par seconde en ajoutant jusqu'à 15 répliques de lecture à faible latence, quelle que soit la taille de vos données. Amazon DocumentDB est conçu pour garantir une disponibilité de 99,99 % et réplique six copies de vos données dans trois zones de AWS disponibilité (AZs). Vous pouvez utiliser AWS Database Migration Service (DMS) gratuitement (pendant six mois) pour migrer vos bases de données MongoDB sur site ou Amazon Elastic Compute Cloud (Amazon) vers Amazon DocumentDB sans pratiquement aucune interruption de service. Pour en savoir plus, consultez [Amazon DocumentDB \(compatible avec MongoDB\)](#).

FAQ sur Amazon DocumentDB dans AWS Managed Services

Q : Comment puis-je demander l'accès à Amazon DocumentDB depuis mon compte AMS ?

Les rôles de console et d'accès aux données Amazon DocumentDB peuvent être demandés en soumettant deux AMS RFCs, l'accès à la console et l'accès aux données :

Demandez l'accès à Amazon DocumentDB en soumettant une RFC avec le type de modification Management | AWS service | Self-provisioned Service | Add (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_documentdb_role`. Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon DocumentDB dans mon compte AMS ?

Amazon DocumentDB nécessite des autorisations spécifiques à Amazon RDS. Dans la mesure où AMS gère entièrement Amazon RDS, le rôle IAM d'Amazon DocumentDB inclut certaines restrictions relatives aux actions sur Amazon RDS. Les restrictions suivantes s'appliquent :

- L'accès au `DeleteDBInstance` et `DeleteDBCluster` APIs a été restreint. Pour utiliser ces suppressions APIs, soumettez une RFC avec le type de modification Management | Advanced stack components | Identity and Access Management (IAM) | Update entity ou policy (révision requise) (ct-27tuth19k52b4).
- Vous ne pouvez pas ajouter ou supprimer de balises sur les instances Amazon RDS.
- Vous ne pouvez pas rendre publique votre instance Amazon DocumentDB.

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon DocumentDB dans mon compte AMS ?

Amazon S3 et AWS KMS sont nécessaires pour utiliser Amazon DocumentDB, si les compartiments Amazon S3 sont chiffrés à l'aide de clés. AWS KMS

Utilisez AMS SSP pour approvisionner Amazon DynamoDB sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon DynamoDB (DynamoDB) directement dans votre compte géré AMS. Amazon DynamoDB est une base de données de documents et de valeurs clés qui fournit des performances à un chiffre en millisecondes à n'importe quelle échelle. Il s'agit d'une base de données multirégionale et multiactive entièrement gérée, dotée de fonctions intégrées de sécurité, de sauvegarde et de restauration, ainsi que de mise en cache en mémoire pour les applications à l'échelle d'Internet. Pour en savoir plus, veuillez consulter la section [Amazon DynamoDB](#).

Amazon DynamoDB Accelerator (Dax) est un service de mise en cache à écriture simultanée conçu pour simplifier l'ajout d'un cache à des tables DynamoDB. DAX est destiné aux applications qui requièrent des lectures hautement performantes.

FAQ sur DynamoDB dans AWS Managed Services

Q : Comment puis-je demander l'accès à DynamoDB et DAX dans mon compte AMS ?

Demandez l'accès à DynamoDB et DAX en soumettant une RFC avec le type de modification Management AWS | Service | Self-provisioned Service | Add (ct-1w8z66n899dct). Cette RFC fournit les rôles et politiques IAM suivants à votre compte :

- Nom du rôle DynamoDB : `customer_dynamodb_role`

Nom du rôle du service DAX : `customer_dax_service_role`

- Nom de la politique DynamoDB : `customer_dynamodb_policy`

Politique de service DAX : `customer_dax_service_policy`

Une fois provisionnée dans votre compte, vous devez l'intégrer `customer_dynamodb_role` à votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation de DynamoDB dans mon compte AMS ?

Toutes les fonctionnalités DynamoDB sont prises en charge, y compris DynamoDB Accelerator (DAX).

Lorsque vous créez des alarmes pour une table donnée, le nom de l'alarme doit être préfixé par « client* » ; par exemple, `customer-employee-table-high-put-latency`

Lorsque vous créez une rubrique Amazon SNS pour DynamoDB, elle doit être nommée `:. dynamodb`

Pour supprimer la rubrique Amazon SNS créée par DynamoDB, soumettez une RFC de type Management | Other | Other | Update change.

Q : Quels sont les prérequis ou les dépendances pour utiliser DynamoDB dans mon compte AMS ?

Il n'existe aucune condition préalable ni dépendance pour utiliser DynamoDB dans votre compte AMS.

Utilisez AMS SSP pour approvisionner Amazon Elastic Container Registry sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon Elastic Container Registry (Amazon ECR) directement depuis votre compte géré AMS. Amazon Elastic Container Registry est un registre de conteneurs [Docker](#) entièrement géré qui permet aux développeurs de stocker, de gérer et de déployer facilement des images de conteneurs Docker. Amazon ECR est intégré à [Amazon Elastic Container Service \(Amazon ECS\)](#), ce qui simplifie votre flux de travail du développement à la production. Amazon ECR élimine le besoin d'exploiter vos propres référentiels de conteneurs ou de vous soucier de la mise à l'échelle de l'infrastructure sous-jacente. Amazon ECS héberge vos images dans une architecture hautement disponible et évolutive, ce qui vous permet de déployer des conteneurs de manière fiable pour vos applications. L'intégration avec AWS Identity and Access Management (IAM) fournit un contrôle au niveau des ressources de chaque référentiel. Avec Amazon ECR, il n'y a aucun frais initial ni engagement. Vous ne payez que pour la quantité de données que vous stockez dans vos référentiels et de données transférées sur Internet.

Pour en savoir plus, consultez [Amazon Elastic Container Registry](#).

FAQ sur le registre des conteneurs Amazon Elastic dans AWS Managed Services

Q : Comment puis-je demander l'accès à Amazon ECR depuis mon compte AMS ?

Demandez l'accès à Amazon ECR en soumettant une RFC avec le type de modification Management | AWS service | Self-provisioned Service | Add (ct-1w8z66n899dct). Cette RFC fournit les rôles IAM suivants à votre compte : `customer_ecr_console_role`, et `customer_ecr_poweruser_instance_profile` avec les politiques IAM associées, `customer_ecr_console_policy` et `customer_ecr_poweruser_instance_profile_policy`, respectivement. Une fois configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon ECR sur mon compte AMS ?

Il existe des restrictions concernant les espaces de noms AMS pour l'utilisation d'Amazon ECR dans votre compte AMS. Les images du conteneur ne doivent pas être préfixées par « AMS- » ou « Sentinel- ».

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon ECR dans mon compte AMS ?

Il n'existe aucune condition préalable ni dépendance pour utiliser Amazon ECR dans votre compte AMS.

Utilisez AMS SSP pour configurer EC2 Image Builder sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités EC2 d'Image Builder directement dans votre compte géré AMS. EC2 Image Builder est un AWS service entièrement géré qui facilite l'automatisation de la création, de la gestion et du déploiement d'images de serveur personnalisées, sécurisées et up-to-date « dorées », préinstallées et préconfigurées avec des logiciels et des paramètres répondant à des normes informatiques spécifiques.

Vous pouvez utiliser la AWS Management Console AWS CLI ou APIs créer des images personnalisées dans votre AWS compte. Lorsque vous utilisez le AWS Management Console, l'assistant Amazon EC2 Image Builder vous guide à travers les étapes à suivre pour :

- Fournir des artefacts de départ
- Ajouter et supprimer des logiciels
- Personnaliser les paramètres et les scripts
- Exécuter les tests sélectionnés
- Diffuser des images dans les AWS régions

Les images que vous créez sont créées dans votre compte et peuvent être configurées en permanence pour les correctifs du système d'exploitation. Pour en savoir plus, consultez [EC2 Image Builder](#).

EC2 FAQ sur Image Builder dans AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès à EC2 Image Builder dans mon compte AMS ?

Demandez l'accès en soumettant un type de modification Gestion | AWS service | Service auto-provisionné | Ajouter (révision requise) (ct-3qe6io8t6jtny). Grâce à cette RFC, le rôle IAM suivant sera fourni dans votre compte : `customer_ec2_imagebuilder_role` Une fois configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions applicables à EC2 Image Builder ?

AMS ne prend pas en charge l'utilisation des valeurs par défaut des services pour la configuration de l'infrastructure. Vous pouvez créer une nouvelle configuration d'infrastructure ou utiliser une configuration existante.

AMS ne prend actuellement pas en charge la création de recettes de conteneurs.

Q : Quels sont les prérequis ou les dépendances nécessaires pour activer EC2 Image Builder ?

- EC2 Rôle lié à un service Image Builder : il n'est pas nécessaire de créer manuellement un rôle lié à un service. Lorsque vous créez votre première ressource Image Builder dans la AWS Management Console AWS CLI ou l' AWS API, Image Builder crée pour vous le rôle lié au service.
- Les instances utilisées pour créer des images et exécuter des tests à l'aide d'Image Builder doivent avoir accès au service Systems Manager. L'agent SSM sera installé sur l'image source s'il n'est pas déjà présent, et il sera supprimé avant la création de l'image.
- AWS IAM : le rôle IAM que vous associez à votre profil d'instance doit être autorisé à exécuter les composants de génération et de test inclus dans votre image. Les politiques de rôle IAM suivantes doivent être associées au rôle IAM associé aux profils d'instance : `EC2InstanceProfileForImageBuilder` et `AmazonSSMManagedInstanceCore` Le nom du rôle IAM doit contenir le `*imagebuilder*` mot clé.
- Si vous configurez la journalisation, le profil d'instance spécifié dans la configuration de votre infrastructure doit disposer d'`s3:PutObject` autorisations pour le compartiment cible (`arn:aws:s3:::{bucket-name}/*`). Exemples :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::{bucket-name}/*"
    }
  ]
}
```

- Créez une rubrique SNS nommée « imagebuilder » pour recevoir les alertes et notifications d' EC2 Image Builder.

Utilisez AMS SSP pour approvisionner Amazon ECS sur AWS Fargate votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS Fargate fonctionnalités d'Amazon ECS directement depuis votre compte géré AMS. AWS Fargate est une technologie que vous pouvez utiliser avec Amazon ECS pour exécuter des conteneurs (voir [Containers on AWS](#)) sans avoir à gérer des serveurs ou des clusters d' EC2 instances Amazon. Ainsi AWS Fargate, vous n'avez plus besoin de provisionner, de configurer ou de dimensionner des clusters de machines virtuelles pour exécuter des conteneurs. Vous n'avez plus à choisir de types de serveurs, décider quand mettre à l'échelle vos clusters ni optimiser les packs de clusters.

Pour en savoir plus, consultez [Amazon ECS sur AWS Fargate](#).

FAQ sur Amazon ECS sur Fargate dans AWS Managed Services

Q : Comment puis-je demander l'accès à Amazon ECS sur Fargate depuis mon compte AMS ?

Demandez l'accès à Amazon ECS sur Fargate en soumettant une RFC avec le type de modification Management AWS | service | Self-provisioned service | Add (ct-1w8z66n899dct). Cette RFC fournit les rôles IAM suivants à votre compte : `customer_ecs_fargate_console_role` (si aucun rôle IAM existant n'est fourni pour associer la politique ECS),, `customer_ecs_fargate_events_service_role`, `customer_ecs_task_execution_service_role`, `customer_ecs_codedeploy_service_role` et `AWSServiceRoleForApplicationAutoScaling_ECSService`. Une fois les rôles configurés dans votre compte, vous devez intégrer les rôles dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon ECS sur Fargate dans mon compte AMS ?

- La surveillance et la journalisation des tâches Amazon ECS sont considérées comme relevant de votre responsabilité, car les activités au niveau du conteneur se déroulent au-dessus de l'hyperviseur et les capacités de journalisation sont limitées par Amazon ECS on Fargate. En tant qu'utilisateur d'Amazon ECS sur Fargate, nous vous recommandons de prendre les mesures nécessaires pour activer la journalisation de vos tâches Amazon ECS. Pour plus d'informations, consultez [Activer le pilote de journal awslogs pour vos conteneurs](#).

- La sécurité et la protection contre les programmes malveillants au niveau du conteneur sont également considérées comme relevant de votre responsabilité. Amazon ECS on Fargate n'inclut pas Trend Micro ni les composants de sécurité réseau préconfigurés.
- Ce service est disponible pour les comptes AMS de zone d'atterrissage à comptes multiples et de zone d'atterrissage à compte unique.
- Amazon ECS [Service Discovery](#) est limité par défaut dans le rôle d'auto-provisionnement, car des autorisations élevées sont requises pour créer des zones hébergées privées Route 53. Pour activer Service Discovery sur un service, soumettez un type de modification Gestion | Autre | Autre | Mise à jour. Pour fournir les informations requises pour activer Service Discovery pour votre service Amazon ECS, consultez le [manuel Service Discovery](#).
- AMS ne gère ni ne limite actuellement les images utilisées pour le déploiement dans des conteneurs sur Amazon ECS Fargate. Vous pourrez déployer des images depuis Amazon ECR, Docker Hub ou tout autre référentiel d'images privé. Par conséquent, nous vous conseillons de ne pas déployer d'images publiques ou non sécurisées, car elles peuvent entraîner une activité malveillante sur le compte.

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon ECS sur Fargate dans mon compte AMS ?

- Les dépendances d'Amazon ECS par rapport à Fargate sont les suivantes ; toutefois, aucune action supplémentaire n'est requise pour activer ces services avec votre rôle d'auto-provisionnement :
 - CloudWatch journaux
 - CloudWatch événements
 - CloudWatch alarmes
 - CodeDeploy
 - App Mesh
 - Cloud Map
 - Route 53
- Selon votre cas d'utilisation, les ressources suivantes sont celles sur lesquelles Amazon ECS s'appuie et peut avoir besoin avant d'utiliser Amazon ECS sur Fargate dans votre compte :
 - Groupe de sécurité à utiliser avec le service Amazon ECS. Vous pouvez utiliser le module Déploiement | Composants de pile avancés | Groupe de sécurité | Créer (auto) (ct-3pc215bnwb6p7) ou, si votre groupe de sécurité nécessite des règles spéciales, utiliser

Déploiement | Composants de pile avancés | Groupe de sécurité | Créer (révision requise) (ct-10xx2g2d7hc90). Remarque : Le groupe de sécurité que vous sélectionnez avec Amazon ECS doit être créé spécifiquement pour Amazon ECS où réside le service ou le cluster Amazon ECS. Pour en savoir plus, consultez la section Groupe de sécurité sur [Configuration avec Amazon ECS](#) et [sécurité dans Amazon Elastic Container Service](#).

- Équilibreur de charge d'application (ALB), équilibreur de charge réseau (NLB), équilibreur de charge classique (ELB) pour l'équilibrage de charge entre les tâches.
- Groupes cibles pour ALBs.
- Ressources de maillage d'applications (par exemple, routeurs virtuels, services virtuels, nœuds virtuels) à intégrer à votre cluster Amazon ECS.
- À l'heure actuelle, AMS n'a aucun moyen d'atténuer automatiquement les risques associés à la prise en charge des autorisations des groupes de sécurité lorsqu'ils sont créés en dehors des types de modifications AMS standard. Nous vous recommandons de demander un groupe de sécurité spécifique à utiliser avec votre cluster Fargate afin de limiter la possibilité d'utiliser un groupe de sécurité non conçu pour être utilisé avec Amazon ECS.

Utilisez AMS SSP pour activer Amazon EKS sur AWS Fargate votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS Fargate fonctionnalités d'Amazon EKS directement depuis votre compte géré AMS. AWS Fargate est une technologie qui fournit une capacité de calcul adaptée à la demande pour les conteneurs (pour comprendre les conteneurs, voir [Que sont les conteneurs ?](#)). Ainsi AWS Fargate, vous n'avez plus besoin de provisionner, de configurer ou de dimensionner des groupes de machines virtuelles pour exécuter des conteneurs. Vous n'avez plus à choisir de types de serveurs, à décider quand vos clusters doivent être mis à l'échelle, ni à optimiser les packs de clusters.

Amazon Elastic Kubernetes Service (Amazon EKS) intègre AWS Fargate Kubernetes à l'aide de contrôleurs AWS conçus à l'aide du modèle extensible en amont fourni par Kubernetes. Ces contrôleurs s'exécutent dans le cadre du plan de contrôle Kubernetes géré par Amazon EKS et sont chargés de planifier les pods Kubernetes natifs sur Fargate. Les contrôleurs Fargate comprennent un nouveau planificateur qui s'exécute parallèlement au planificateur Kubernetes par défaut, en plus de plusieurs contrôleurs d'admission mutants et validants. Lorsque vous démarrez un pod qui répond aux critères d'exécution sur Fargate, les contrôleurs Fargate exécutés dans le cluster reconnaissent, mettent à jour et programment le pod sur Fargate.

Pour en savoir plus, consultez [Amazon EKS on AWS Fargate Now Generally Available](#) et le [Guide des meilleures pratiques d'Amazon EKS en matière de sécurité](#) (qui inclut des « recommandations » telles que « Vérifier et révoquer les accès anonymes inutiles », etc.).

 Tip

AMS propose un type de modification, Deployment | Advanced stack components | Identity and Access Managment (IAM) | Create OpenID Connect provider (ct-30ecvfi3tq4k3), que vous pouvez utiliser avec Amazon EKS. Pour un exemple, voir [Identity and Access Management \(IAM\) | Create OpenID Connect Provider](#).

FAQ sur Amazon EKS sur AWS Fargate AWS Managed Services

Q : Comment puis-je demander l'accès à Amazon EKS sur Fargate depuis mon compte AMS ?

Demandez l'accès en soumettant un type de modification Gestion | AWS service | Service auto-approvisionné | Ajouter (révision requise) (ct-3qe6io8t6jtny). Cette RFC attribue le rôle IAM suivant à votre compte.

- `customer_eks_fargate_console_role`.

Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

- Ces rôles de service autorisent Amazon EKS on Fargate à appeler d' AWS autres services en votre nom :
 - `customer_eks_pod_execution_role`
 - `customer_eks_cluster_service_role`

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon EKS sur Fargate dans mon compte AMS ?

- La création de EC2 groupes de nœuds [gérés](#) ou [autogérés](#) n'est pas prise en charge dans AMS. Si vous devez utiliser des nœuds de EC2 travail, contactez votre responsable de prestation de services cloud (CSDM) ou votre architecte cloud (CA) AMS.
- AMS n'inclut pas Trend Micro ni les composants de sécurité réseau préconfigurés pour les images de conteneur. Vous devez gérer vos propres services de numérisation d'images afin de détecter les images de conteneur malveillantes avant le déploiement.

- EKCTL n'est pas pris en charge en raison des interdépendances. CloudFormation
- Lors de la création du cluster, vous êtes autorisé à désactiver la journalisation du plan de contrôle du cluster. Pour plus d'informations, consultez [Journalisation du plan de contrôle Amazon EKS](#). Nous vous conseillons d'activer toutes les API, l'authentification et la journalisation d'audit importantes lors de la création du cluster.
- Lors de la création du cluster, l'accès aux points de terminaison du cluster pour les clusters Amazon EKS est défini par défaut sur public ; pour plus d'informations, consultez la section [Contrôle d'accès aux points de terminaison du cluster Amazon EKS](#). Nous recommandons que les points de terminaison Amazon EKS soient définis comme privés. Si des points de terminaison sont requis pour un accès public, il est recommandé de les définir comme publics uniquement pour des plages d'adresses CIDR spécifiques.
- AMS ne dispose d'aucune méthode pour forcer et restreindre les images utilisées pour le déploiement dans des conteneurs sur Amazon EKS Fargate. Vous pouvez déployer des images depuis Amazon ECR, Docker Hub ou tout autre référentiel d'images privé. Par conséquent, il existe un risque de déploiement d'une image publique susceptible d'entraîner une activité malveillante sur le compte.
- Le déploiement de clusters EKS via le kit de développement cloud (CDK) ou CloudFormation Ingest n'est pas pris en charge dans AMS.
- Vous devez créer le groupe de sécurité requis à l'aide de [ct-3pc215bnwb6p7 Déploiement | Composants de pile avancés | Groupe de sécurité | Créer](#) et référencer dans le fichier manifeste pour la création d'entrées. Cela est dû au fait que le rôle `customer-eks-alb-ingress-controller-role` n'est pas autorisé à créer des groupes de sécurité.

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon EKS sur Fargate dans mon compte AMS ?

Pour utiliser le service, les dépendances suivantes doivent être configurées :

- Pour s'authentifier auprès du service, KUBECTL aws-iam-authenticator doit être installé ; pour plus d'informations, consultez la section [Gestion](#) de l'authentification du cluster.
- Kubernetes repose sur un concept appelé « comptes de service ». Afin d'utiliser la fonctionnalité des comptes de service au sein d'un cluster Kubernetes sur EKS, une RFC Management | Other | Other | Update est requise avec les entrées suivantes :
 - [Obligatoire] Nom du cluster Amazon EKS

- [Obligatoire] Espace de noms du cluster Amazon EKS dans lequel le compte de service (SA) sera déployé.
- [Obligatoire] Nom Amazon EKS Cluster SA.
- [Obligatoire] Nom de la politique IAM et permissions/document à associer.
- [Obligatoire] Le nom du rôle IAM est demandé.
- [Facultatif] URL du fournisseur OpenID Connect. Pour de plus amples informations, veuillez consulter
 - [Activation des rôles IAM pour les comptes de service de votre cluster](#)
 - [Présentation de rôles IAM précis pour les comptes de service](#)
- Nous recommandons de configurer et de surveiller les règles de configuration pour
 - Points de terminaison de clusters publics
 - Journalisation des API désactivée

Il est de votre responsabilité de surveiller et de corriger ces règles de Config.

Si vous souhaitez déployer un [contrôleur ALB Ingress](#), soumettez une RFC Management | Other | Other Update pour configurer le rôle IAM nécessaire à utiliser avec le pod ALB Ingress Controller. Les entrées suivantes sont requises pour créer des ressources IAM à associer à ALB Ingress Controller (incluez-les dans votre RFC) :

- [Obligatoire] Nom du cluster Amazon EKS
- [Facultatif] URL du fournisseur OpenID Connect
- [Facultatif] Espace de noms du cluster Amazon EKS dans lequel le service de contrôleur d'entrée ALB (Application Load Balancer) sera déployé. [par défaut : kube-system]
- [Facultatif] Nom du compte de service Amazon EKS Cluster (SA). [par défaut : aws-load-balancer-controller]

Si vous souhaitez activer le chiffrement des enveloppes secrètes dans votre cluster (ce que nous recommandons), indiquez la clé KMS IDs que vous souhaitez utiliser, dans le champ de description de la RFC pour ajouter le service (Gestion | service | Service auto-provisionné | Ajouter (AWS ct-1w8z66n899dct). Pour en savoir plus sur le chiffrement d'enveloppe, consultez [Amazon EKS ajoute le chiffrement d'enveloppe pour les secrets avec AWS KMS](#).

Utilisez AMS SSP pour approvisionner Amazon EMR sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon EMR directement depuis votre compte géré par AMS. Amazon EMR est la plateforme cloud de pointe pour le traitement de grandes quantités de données à l'aide d'outils open source tels qu'Apache Spark, Apache Hive, Apache, Apache Flink HBase, Apache Hudi et Presto. Avec Amazon EMR, vous pouvez exécuter des analyses à l'échelle du pétaoctet pour moins de la moitié du coût des solutions sur site traditionnelles et plus de 3 fois plus rapidement qu'Apache Spark standard. Pour les tâches de courte durée, vous pouvez faire tourner des clusters vers le haut ou vers le bas et payer à la seconde pour les instances utilisées. Pour les charges de travail de longue durée, vous pouvez créer des clusters hautement disponibles qui s'adaptent automatiquement à la demande.

Vous pouvez créer une ou plusieurs instances des clusters Amazon EMR dans des comptes de zone d'atterrissage multi-comptes AMS ou dans des comptes de zone d'atterrissage à compte unique pour prendre en charge les clusters Amazon EMR transitoires et persistants. Vous pouvez également activer l'authentification Kerberos pour authentifier les utilisateurs à partir du domaine Active Directory local.

Vous pouvez tirer parti de plusieurs magasins de données avec les clusters Amazon EMR pour prendre en charge les outils et bibliothèques Hadoop spécifiques à des cas d'utilisation. Les clusters Amazon EMR peuvent être créés à l'aide d'instances OnDemand ou Spot et configurer le dimensionnement automatique pour gérer la capacité et réduire les coûts.

Les fichiers journaux du cluster peuvent être archivés dans un compartiment Amazon S3 à des fins de journalisation et de débogage. Vous pouvez également accéder aux interfaces Web hébergées dans le cluster Amazon EMR afin de répondre aux exigences d'administration Hadoop ou de créer des carnets de notes pour les clients.

Pour en savoir plus, consultez [Amazon EMR](#).

FAQ sur Amazon EMR dans AWS Managed Services

Q : Comment puis-je demander l'accès à Amazon EMR depuis mon compte AMS ?

Demandez l'accès en soumettant un type de modification Gestion | AWS service | Service auto-approvisionné | Ajouter (révision requise) (ct-3qe6io8t6jtny). Cette RFC attribue les rôles IAM suivants à votre compte :

- `customer_emr_cluster_instance_profile`

- `customer_emr_cluster_autoscaling_role`
- `customer_emr_console_role`
- `customer_emr_cluster_service_role`

Une fois qu'il est configuré dans votre compte, vous devez intégrer le `customer_emr_console_role` dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon EMR sur mon compte AMS ?

Lorsque vous créez Amazon EMR sur un EC2 cluster depuis la console AWS, nous vous conseillons d'utiliser l'option `Create Cluster — Advanced`. Les clusters Amazon EMR doivent être créés en ajoutant la balise avec la clé « `for-use-with-amazon-` » avec la valeur « `true emr-managed-policies` ». Sélectionnez les configurations suivantes dans les options de sécurité :

- Sélectionnez des rôles personnalisés pour votre cluster :
 - Rôle EMR : `customer_emr_cluster_service_role`
 - EC2 Profil d'instance : `customer_emr_cluster_instance_profile`
 - Rôle Auto Scaling : `customer_emr_cluster_autoscaling_role`
- EC2 Groupes de sécurité :
 - Master : `ams-emr-master-security-group`
 - Noyau et tâche : `ams-emr-worker-security-group`
 - Accès au service : `ams-emr-serviceaccess-security-group`

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon EMR dans mon compte AMS ?

AMS crée des groupes de sécurité par défaut pour les nœuds Amazon EMR master, worker et services.

Les modèles de lancement et les groupes de sécurité à utiliser avec les clusters Amazon EMR doivent avoir la clé de balise « `for-use-with-amazon- emr-managed-policies` » avec la valeur « `true` ».

Le profil d'instance de cluster Amazon EMR par défaut permet d'accéder aux ressources telles que les compartiments s3 et les tables Dynamodb dont le nom contient « `emr` ». Vous pouvez demander des politiques IAM supplémentaires pour utiliser les ressources supplémentaires à utiliser avec Amazon EMR. Les ARN de ressources suivants peuvent être utilisés avec les tâches Amazon EMR à l'aide du `customer_emr_cluster_instance_profile` :

- `arn:aws:dynamodb : *:*.table/*emr*`
- `arn:aws:kinesis : *:*.stream/*emr*`
- `arn:aws:sns : *:* : *emr*``arn:aws:sqs : *:* : *emr*`
- `arn:aws:sqs : *:* : *emr*`
- `arn:aws:sqs : *:*.AWS- -* ElasticMapReduce`
- `arn:aws:sdb : *:*.domain : *emr*`
- `arn:aws:s3 : ::*emr*`

Si l'authentification Kerberos est requise pour le cluster Amazon EMR :

- Indiquez le nom de domaine à utiliser pour chaque cluster Amazon EMR kerberisé et les adresses IP Active Directory sur site.
- Exigences en matière d'infrastructure :

Zone d'accueil multi-comptes (MALZ) : soumettez une RFC pour créer un nouveau compte d'application géré ou un nouveau VPC dans un compte d'application existant.

Zone d'atterrissage à compte unique (SALZ) : soumettez une RFC pour créer un nouveau sous-réseau dans votre VPC.

- Configurez la confiance entrante pour le domaine du cluster sur l'Active Directory sur site.
- Soumettez une RFC pour configurer les zones DNS pour le domaine dans Managed AD.
- Configuration du domaine :

MALZ : Soumettez une RFC de gestion | Autre | Autre | Mise à jour (ct-0xdawir96cy7k) pour mettre à jour l'option DHCP du VPC définie pour utiliser le nom de domaine comme suffixe de nom de domaine.

SALZ : Soumettez une RFC de gestion | Autre | Autre | Mise à jour (ct-0xdawir96cy7k) pour générer une nouvelle AMI Amazon EMR afin d'utiliser le domaine spécifique pour le suffixe du nom de domaine.

Pour déployer Amazon EMR studio, le rôle `customer_emr_cluster_service_role` doit obligatoirement disposer d'un bucket Amazon Simple Storage Service. Pour créer le bucket, utilisez le CT automatisé `ct-1a68ck03fn98r` (Déploiement | Composants de pile avancés | Stockage S3 | Création). Lorsque vous utilisez ce CT automatisé pour créer un compartiment Amazon S3 pour

Amazon EMR, le nom du compartiment doit commencer par le préfixe. `customer-emr-*` Vous devez également créer le compartiment dans la même AWS région que le cluster Amazon EMR.

Utilisez AMS SSP pour approvisionner Amazon sur EventBridge votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux EventBridge fonctionnalités d'Amazon directement depuis votre compte géré par AMS. Amazon EventBridge est un service de bus d'événements sans serveur qui permet de connecter facilement vos applications à des données provenant de diverses sources. EventBridge fournit un flux de données en temps réel à partir de vos propres applications, applications Software-as-a-Service (SaaS) et AWS services et achemine ces données vers des cibles telles que AWS Lambda. Vous pouvez configurer des règles de routage pour déterminer où envoyer vos données pour créer des architectures d'application qui réagissent en temps réel à toutes vos sources de données. EventBridge vous permet de créer des architectures pilotées par les événements, qui sont faiblement couplées et distribuées.

Pour en savoir plus, consultez [Amazon EventBridge](#).

EventBridge dans la FAQ AWS Managed Services

Q : Comment puis-je demander l'accès EventBridge à mon compte AMS ?

Demandez l'accès à EventBridge en soumettant une RFC avec le type de modification Management | AWS service | Self-provisioned Service | Add (ct-1w8z66n899dct). Cette RFC attribue les rôles IAM suivants à votre compte : `customer_eventbridge_role` et `customer_eventbridge_scheduler_execution_role` Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Le rôle d'exécution `customer_eventbridge_scheduler_execution_role` est un rôle IAM que EventBridge Scheduler assume pour interagir avec d'autres personnes en votre Services AWS nom. Les politiques d'autorisation associées à ce rôle accordent au EventBridge planificateur l'accès pour appeler des cibles.

Note

Par défaut, EventBridge Scheduler utilise des clés AWS détenues EventBridge pour chiffrer les données. Pour utiliser une clé gérée par le client pour chiffrer les données, soumettez

la RFC EventBridge à l'aide du type de modification Management | AWS Service | Self-provisioned Service | [Ajouter \(révision requise\) \(ct-3qe6io8t6jtny\) pour](#) le provisionnement du service.

Q : Quelles sont les restrictions d'utilisation EventBridge sur mon compte AMS ?

Vous devez envoyer AMS RFCs et créer les ressources suivantes : rôles de service pour déclencher le traitement par lots, file d'attente SQS, CodeBuild CodePipeline, et commandes SSM.

Q : Quels sont les prérequis ou les dépendances pour pouvoir utiliser EventBridge mon compte AMS ?

Vous devez demander un rôle de EventBridge service auprès d'une RFC en utilisant le type de modification Deployment | Advanced stack components | Identity and Access Management (IAM) | Create entity or policy (révision requise) (ct-3dpd8mdd9jn1r) avant de l'utiliser pour déclencher d'EventBridge autres ressources AWS, telles que Lambda, Amazon SNS, Amazon SQS ou Amazon Logs. AWS Batch CloudWatch Spécifiez les services à invoquer lorsque vous demandez votre rôle de service. Pour en savoir plus sur les autorisations requises pour appeler des cibles, consultez la section [Utilisation de politiques basées sur les ressources](#) pour. EventBridge

EventBridge est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un Service AWS utilisateur EventBridge. CloudTrail doit être activé et autorisé à stocker les fichiers journaux dans des compartiments S3. Remarque : Tous les comptes AMS sont CloudTrail activés, aucune action n'est donc nécessaire.

Q : Une clé est requise pour le rôle customer_eventbridge_scheduler_execution_role (facultatif, s'il est utilisé pour le chiffrement). AWS Key Management Service Comment adopter le chiffrement des données AWS KMS CMKs au repos/en transit ?

Par défaut, le EventBridge planificateur chiffre les métadonnées des événements et les données des messages qu'il stocke sous une clé AWS propriétaire (chiffrement au repos). EventBridge Le planificateur chiffre également les données transmises entre le EventBridge planificateur et d'autres services à l'aide du protocole TLS (Transport Layer Security) (chiffrement en transit).

Si votre cas d'utilisation spécifique nécessite que vous contrôliez et auditez les clés de chiffrement qui protègent vos données sur EventBridge Scheduler, vous pouvez utiliser une clé gérée par le client.

Vous devez demander une RFC en utilisant le type de modification Management Service AWS | | Self-provisioned Service | Add (révision requise) avant d'utiliser Amazon EventBridge pour intégrer l'autorisation. AWS KMS

Utilisez AMS SSP pour approvisionner Amazon Forecast sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon Forecast (Forecast) directement depuis votre compte géré AMS. Amazon Forecast est un service entièrement géré qui utilise l'apprentissage automatique pour fournir des prévisions très précises.

Note

AWS a fermé l'accès des nouveaux clients à Amazon Forecast à compter du 29 juillet 2024. Les clients existants d'Amazon Forecast peuvent continuer à utiliser le service normalement. AWS continue d'investir dans l'amélioration de la sécurité, de la disponibilité et des performances d'Amazon Forecast, mais AWS ne prévoit pas d'introduire de nouvelles fonctionnalités.

Si vous souhaitez utiliser Amazon Forecast, contactez votre CSDM afin qu'il vous explique comment transférer [votre utilisation d'Amazon Forecast vers Amazon Canvas](#). SageMaker

Basé sur la même technologie que celle utilisée sur Amazon.com, Forecast utilise l'apprentissage automatique pour combiner des données de séries chronologiques avec des variables supplémentaires afin de créer des prévisions. Forecast ne nécessite aucune expérience d'apprentissage automatique pour démarrer. Il vous suffit de fournir des données historiques, ainsi que toute donnée supplémentaire susceptible, selon vous, d'avoir un impact sur vos prévisions. Par exemple, la demande pour une couleur particulière de chemise peut changer en fonction des saisons et de l'emplacement du magasin. Cette relation complexe est difficile à déterminer seule, mais l'apprentissage automatique est idéal pour la reconnaître. Une fois que vous avez fourni vos données, Forecast les examine automatiquement, identifie ce qui est significatif et produit un modèle de prévision capable de faire des prédictions jusqu'à 50 % plus précises que si vous examiniez uniquement des données de séries chronologiques.

Pour en savoir plus, consultez [Amazon Forecast](#).

FAQ sur Amazon Forecast dans AWS Managed Services

Q : Comment puis-je demander l'accès à Forecast dans mon compte AMS ?

Demandez l'accès à AWS Firewall Manager en soumettant une RFC avec le type de modification Management | AWS Service | Self-provisioned Service | Add (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_forecast_admin_role` Une fois configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation de Forecast dans mon compte AMS ?

L'accès au compartiment S3 par défaut vous permet uniquement d'accéder aux compartiments portant le modèle de dénomination « `customer-forecast-*` ». Si vous avez votre propre convention de dénomination pour les compartiments de données, discutez de la dénomination des compartiments et de la configuration des accès associés avec votre architecte cloud (CA). Exemples :

- Vous pouvez définir votre rôle spécifique dans le service Amazon Forecast avec un nom tel que « `AmazonForecast - ExecutionRole - *` » et un accès approprié au compartiment S3 associé. Consultez le rôle de service `AmazonForecast-ExecutionRole-Admin` et la politique IAM `customer_forecast_default_s3_access_policy` dans la console IAM.
- Vous devrez peut-être associer l'accès aux compartiments S3 associés au rôle de fédération IAM. Consultez la politique IAM - `customer_forecast_default_s3_access_policy`, dans la console IAM.

Q : Quels sont les prérequis ou les dépendances pour utiliser Forecast dans mon compte AMS ?

- Un ou plusieurs compartiments Amazon S3 appropriés doivent être créés avant d'utiliser Forecast. En particulier, l'accès par défaut aux compartiments S3 se fait avec le modèle de dénomination « `customer-forecast-*` »
- Si vous souhaitez utiliser des modèles de dénomination sur les compartiments S3 autres que « `customer-forecast-*` », vous devez créer un nouveau rôle de service avec des autorisations d'accès S3 sur les compartiments :
 1. Un nouveau rôle de service à créer avec le nom « `AmazonForecast - ExecutionRole - {suffix}` ».
 2. Une nouvelle politique IAM à créer, similaire à `customer_forecast_default_s3_access_policy`, à associer au nouveau rôle de service et au rôle d'administrateur de fédération associé (par exemple « `customer_forecast_admin_role` »)

Q : Comment puis-je améliorer la sécurité des données lors de l'utilisation d'Amazon Forecast ?

- Pour le chiffrement des données au repos, vous pouvez utiliser AWS KMS une clé CMK gérée par le client afin de protéger le stockage des données sur le service Amazon S3 :

- Activez le chiffrement par défaut sur le compartiment à l'aide de la clé de provision et configurez une politique de compartiment pour accepter le chiffrement AWS KMS des données lors de leur saisie.
- Activez le rôle de service Amazon Forecast « AmazonForecast - ExecutionRole - * » et le rôle d'administrateur de fédération (par exemple « customer_forecast_admin_role ») en tant qu'utilisateur clé. AWS KMS
- Pour le chiffrement des données en transit, vous pouvez configurer le protocole HTTPS, qui est requis lors du transfert d'objets dans le cadre de la politique de compartiment Amazon S3.
- Restrictions supplémentaires en matière de contrôle d'accès : activez une politique de compartiment pour l'accès approuvé pour le rôle de service Amazon Forecast « AmazonForecast - ExecutionRole - * » et le rôle d'administrateur (par exemple « customer_forecast_admin_role »).

Q : Quelles sont les meilleures pratiques en matière d'utilisation d'Amazon Forecast ?

- Vous devez avoir une bonne connaissance de vos pratiques de classification des données et définir les besoins en matière de sécurité des données associés lorsque vous utilisez des compartiments S3 avec Amazon Forecast.
- Pour la configuration du compartiment Amazon S3, nous vous conseillons vivement d'activer l'application du protocole HTTPS dans votre politique de compartiment S3.
- Vous devez savoir que le rôle d'administrateur « customer_forecast_admin_role » prend en charge l'accès permissif (objets Get/Delete/Put S3) sur les compartiments Amazon S3 sous le nom de « customer-forecast-* ». REMARQUE : Si vous avez besoin d'un contrôle d'accès précis pour plusieurs équipes, suivez les pratiques suivantes :
 - Définissez votre identité IAM d'accès basée sur l'équipe (rôle/utilisateur) avec un accès de moindre privilège aux compartiments Amazon S3 associés.
 - team/project Sur la base de la création, AWS KMS CMKs accordez un accès approprié aux identités IAM correspondantes. (accès utilisateur et « AmazonForecast - ExecutionRole - {équipe/projet} »).
 - Configurez le chiffrement par défaut du compartiment S3 avec le code créé AWS KMS CMKs.
 - Appliquez le trafic de l'API S3 à l'aide du protocole HTTPS sur la politique des compartiments S3.
 - Appliquez la configuration des compartiments S3 pour obtenir un accès approuvé pour les identités IAM associées (accès utilisateur et « AmazonForecast - ExecutionRole - {team/project} ») aux compartiments.

- Si vous souhaitez utiliser le « `customer_forecast_admin_role` » à des fins générales, tenez compte des points répertoriés précédemment pour protéger les compartiments S3.

Q : Où se trouvent les informations de conformité concernant Amazon Forecast ?

Consultez le [programme AWS de conformité des services](#).

Utilisez AMS SSP pour approvisionner Amazon sur FSx votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux FSx fonctionnalités d'Amazon directement depuis votre compte géré par AMS. Amazon FSx fournit des systèmes de fichiers tiers entièrement gérés. Amazon vous FSx fournit la compatibilité native des systèmes de fichiers tiers avec des ensembles de fonctionnalités pour les charges de travail telles que le stockage sous Windows, le calcul haute performance (HPC), l'apprentissage automatique et l'automatisation de la conception électronique (EDA). Amazon FSx automatise les tâches administratives fastidieuses telles que le provisionnement du matériel, la configuration logicielle, les correctifs et les sauvegardes. Amazon FSx intègre les systèmes de fichiers à des AWS services cloud natifs, ce qui les rend encore plus utiles pour un ensemble plus large de charges de travail.

Amazon vous FSx propose deux systèmes de fichiers : Amazon FSx pour Windows File Server pour les applications Windows et Amazon pour Lustre FSx pour les charges de travail gourmandes en ressources informatiques. Pour en savoir plus, consultez [Amazon FSx](#).

FAQ sur Amazon FSx dans AWS Managed Services

Q : Comment puis-je demander l'accès FSx à Amazon via mon compte AMS ?

Demandez l'accès à Amazon FSx en soumettant une RFC avec le type de modification Management | AWS service | Self-provisioned Service | Add (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_fsx_admin_role` Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon sur FSx mon compte AMS ?

Il n'y a aucune restriction. Toutes les fonctionnalités du service sont disponibles.

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon FSx dans mon compte AMS ?

Il n'y a aucun prérequis. Toutefois, pour les configurations avancées telles que le mode multi-AZ, vous devez installer et gérer les services de réplication DFS et d'espaces de noms DFS. Pour plus d'informations, consultez la section [Déploiement de systèmes de fichiers multi-AZ](#).

Q : Comment intégrer mon système de FSx fichiers Amazon à ma zone de destination multi-comptes Managed AD ?

Lorsque vous créez un système de FSx fichiers Amazon, vous pouvez spécifier votre compte MALZ Managed AD en tant que « Microsoft Active Directory AWS géré » pour l'authentification Windows. Pour plus d'informations, consultez [Utiliser Amazon FSx avec AWS Directory Service pour Microsoft Active Directory](#)

Vous devez également d'abord partager Managed AD avec le compte de l'application. Pour ce faire, soumettez une RFC avec le type de changement de répertoire Management | Directory Service | Directory | Share (ct-369odosk0pd9w).

Q : Quels utilisateurs appartiennent au groupe des FSx administrateurs délégués AWS ?

Uniquement les administrateurs de serveurs de fichiers informatiques. Ce groupe dispose de privilèges d'accès complet sur tous les partages de fichiers.

Q : Dois-je utiliser le partage de fichiers par défaut, le partage, créé lors du provisionnement du FSx système ?

Non, nous ne recommandons pas d'utiliser le partage de fichiers par défaut, le partage, tel que configuré. Il accorde un accès complet à tous, ce qui viole le principe du moindre privilège. Créez plutôt des partages de fichiers personnalisés plus petits qui répondent aux besoins de votre entreprise.

Q : Comment puis-je créer des partages de fichiers personnalisés pour des organisations spécifiques de mon entreprise ?

Consultez la section [Partages de fichiers](#) pour obtenir des instructions sur la création de partages de fichiers personnalisés. Limitez l'accès à chaque partage de fichiers selon le principe du moindre privilège.

Utilisez AMS SSP pour provisionner Amazon FSx pour OpenZFS sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon FSx pour OpenZFS directement depuis votre compte géré par AMS. FSx for OpenZFS est un service de stockage de fichiers entièrement géré qui facilite le transfert de données résidant dans des serveurs de fichiers ZFS sur site ou sur d'autres serveurs de fichiers basés sur Linux vers AWS sans

modifier le code de votre application ou la façon dont vous gérez les données. Il offre un stockage de fichiers hautement fiable, évolutif, performant et riche en fonctionnalités basé sur le système de fichiers open source OpenZFS, offrant les fonctionnalités habituelles des systèmes de fichiers OpenZFS avec l'agilité, l'évolutivité et la simplicité d'un service entièrement géré. AWS Pour les développeurs qui créent des applications natives pour le cloud, il propose un stockage simple et performant doté de fonctionnalités riches pour travailler avec les données.

FSx pour les systèmes de fichiers OpenZFS sont largement accessibles à partir d'instances de calcul et de conteneurs Linux, Windows et macOS utilisant le protocole NFS standard (v3, v4.0, v4.1, v4.2). Alimenté par des processeurs AWS Graviton et les dernières technologies de AWS disque et de réseau (notamment le réseau AWS Scalable Reliable Datagram et le système AWS Nitro), FSx OpenZFS fournit jusqu'à 1 million d'IOPS avec des latences de plusieurs centaines de microsecondes. Grâce à la prise en charge complète des fonctionnalités d'OpenZFS telles que les point-in-time instantanés et le clonage de données, FSx OpenZFS vous permet de remplacer facilement vos serveurs de fichiers sur site par un AWS stockage qui fournit les fonctionnalités habituelles du système de fichiers et élimine le besoin de procéder à de longues qualifications et de modifier ou de restructurer des applications ou des outils existants. De plus, en associant la puissance des fonctionnalités de gestion des données d'OpenZFS aux performances élevées et à la rentabilité des dernières technologies AWS, OpenZFS vous permet de créer et FSx d'exécuter des applications à hautes performances et gourmandes en données.

En tant que service entièrement géré, FSx OpenZFS facilite le lancement, l'exécution et le dimensionnement de systèmes de fichiers entièrement gérés AWS qui remplacent les serveurs de fichiers que vous exécutez sur site, tout en contribuant à améliorer l'agilité et à réduire les coûts. Avec FSx OpenZFS, vous n'avez plus à vous soucier de la configuration et du provisionnement des serveurs de fichiers et des volumes de stockage, de la réplication des données, de l'installation et de l'application des correctifs du logiciel du serveur de fichiers, de la détection et du traitement des défaillances matérielles et de l'exécution manuelle des sauvegardes. Il fournit également une intégration riche avec d'autres AWS services, tels que AWS Identity and Access Management (IAM), AWS Key Management Service (AWS KMS) CloudWatch, Amazon et AWS CloudTrail.

Amazon vous FSx propose deux systèmes de fichiers parmi lesquels choisir : Amazon FSx pour Windows File Server pour les applications Windows et Amazon for Lustre FSx pour les charges de travail gourmandes en ressources informatiques. Pour en savoir plus, consultez [Amazon FSx](#).

FAQ sur Amazon FSx pour OpenZFS dans AWS Managed Services

Q : Comment puis-je demander l'accès à FSx OpenZFS dans mon compte AMS ?

Demandez l'accès à Amazon FSx OpenZFS en soumettant une RFC avec le type de modification Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_fsx_ontap_admin_role`. Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation FSx d'OpenZFS dans mon compte AMS ?

Le remplacement du groupe de sécurité sur les interfaces réseau Amazon FSx Elastic (ENIs) nécessite que vous soumettiez Management | Other | Other | Update, RFCs car les groupes de sécurité constituent un périmètre critique pour l'environnement AMS. C'est la seule restriction.

Q : Quels sont les prérequis ou les dépendances FSx pour utiliser OpenZFS dans mon compte AMS ?

Il n'y a aucun prérequis. Cependant, vous devez l'avoir [Utilisez AMS SSP pour approvisionner Amazon sur FSx votre compte AMS](#) installé.

Utilisez AMS SSP pour approvisionner Amazon FSx pour NetApp ONTAP sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon FSx for NetApp ONTAP directement depuis votre compte géré par AMS. Amazon FSx for NetApp ONTAP est un service entièrement géré qui fournit un stockage de fichiers hautement fiable, évolutif, performant et riche en fonctionnalités, basé sur le célèbre système NetApp de fichiers ONTAP. Il fournit les fonctionnalités, les performances, les capacités et les capacités habituelles APIs des systèmes de NetApp fichiers avec l'agilité, l'évolutivité et la simplicité d'un système entièrement géré Service AWS.

Amazon FSx for NetApp ONTAP fournit un stockage de fichiers partagé riche en fonctionnalités, rapide et flexible, largement accessible à partir d'instances de calcul Linux, Windows et macOS exécutées sur site AWS ou sur site. FSx for ONTAP propose un stockage SSD hautes performances avec des latences inférieures à la milliseconde, et permet de gérer rapidement et facilement vos données en vous permettant de créer des instantanés, de cloner et de répliquer vos fichiers en un seul clic. Il hiérarchise également automatiquement vos données vers un stockage élastique à moindre coût, éliminant ainsi le besoin de provisionner ou de gérer la capacité et vous permettant d'atteindre les niveaux de performance des SSD pour votre charge de travail tout en ne payant pour le stockage SSD que pour une petite partie de vos données. Il fournit un stockage durable et hautement disponible avec des sauvegardes entièrement gérées et prend en charge la reprise après sinistre entre les régions, et prend en charge les applications antivirus et de sécurité des données les

plus populaires qui facilitent encore la protection et la sécurisation de vos données. Pour les clients qui utilisent NetApp ONTAP sur site, ONTAP est la solution idéale FSx pour migrer, sauvegarder ou transférer en rafale vos applications basées sur des fichiers depuis le site vers le site AWS sans qu'il soit nécessaire de modifier le code de votre application ou la façon dont vous gérez vos données.

En tant que service entièrement géré, Amazon FSx for NetApp ONTAP facilite le lancement et le développement d'un stockage de fichiers partagé fiable, performant et sécurisé dans le cloud. Avec Amazon FSx for NetApp ONTAP, vous n'avez plus à vous soucier de la configuration et du provisionnement des serveurs de fichiers et des volumes de stockage, de la réplication des données, de l'installation et de l'application des correctifs logiciels du serveur de fichiers, de la détection et du traitement des défaillances matérielles, de la gestion du basculement et de l'exécution manuelle des sauvegardes. Il fournit également une intégration riche avec d'autres Services AWS AWS Identity and Access Management, tels que Amazon WorkSpaces AWS Key Management Service, et AWS CloudTrail.

Amazon vous FSx propose deux systèmes de fichiers parmi lesquels choisir : Amazon FSx pour Windows File Server pour les applications Windows et Amazon for Lustre FSx pour les charges de travail gourmandes en ressources informatiques. Pour en savoir plus, consultez [Amazon FSx](#).

FAQ sur Amazon FSx pour NetApp ONTAP dans AWS Managed Services

Q : Comment puis-je demander l'accès à Amazon FSx pour NetApp ONTAP depuis mon compte AMS ?

Demandez l'accès à Amazon FSx pour NetApp ONTAP en soumettant une RFC avec le type de modification Management | AWS service | Self-provisioned Service | Add (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_fsx_ontap_admin_role` Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon FSx pour NetApp ONTAP sur mon compte AMS ?

Le remplacement du groupe de sécurité sur les interfaces réseau élastiques Amazon FSx for NetApp ONTAP (ENIs) nécessite que vous soumettiez Management | Other | Other | Update, RFCs car les groupes de sécurité constituent un périmètre critique pour l'environnement AMS. C'est la seule restriction.

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon FSx for NetApp ONTAP sur mon compte AMS ?

Il n'y a aucun prérequis. Cependant, vous devez l'avoir [Utilisez AMS SSP pour approvisionner Amazon sur FSx votre compte AMS](#) installé.

Utilisez AMS SSP pour approvisionner Amazon Inspector Classic sur votre compte AMS

Note

Avis de fin de support : le 20 mai 2026, le support d'Amazon Inspector Classic AWS prendra fin. Après le 20 mai 2026, vous ne pourrez plus accéder à la console Amazon Inspector Classic ni aux ressources Amazon Inspector Classic. Amazon Inspector Classic ne sera plus disponible pour les nouveaux comptes, ni pour les comptes n'ayant pas fait l'objet d'une évaluation au cours des six derniers mois. Pour tous les autres comptes, l'accès restera valide jusqu'au 20 mai 2026, après quoi vous ne pourrez plus accéder à la console Amazon Inspector Classic ni aux ressources Amazon Inspector Classic. Pour plus d'informations, consultez la page de [fin de support d'Amazon Inspector Classic](#).

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon Inspector Classic directement depuis votre compte géré AMS. Amazon Inspector Classic est un service d'évaluation automatique de la sécurité qui permet d'améliorer la sécurité et la conformité des applications déployées sur AWS. Amazon Inspector Classic évalue automatiquement les applications pour détecter leur exposition, leurs vulnérabilités et les écarts par rapport aux meilleures pratiques. Après avoir effectué une évaluation, Amazon Inspector Classic produit une liste détaillée des résultats de sécurité classés par niveau de gravité. Ces résultats peuvent être examinés directement ou dans le cadre de rapports d'évaluation détaillés, disponibles via la console ou l'API Amazon Inspector Classic. Pour en savoir plus, consultez [Amazon Inspector Classic](#).

FAQ sur Amazon Inspector dans AWS Managed Services

Q : Comment puis-je demander l'accès à Amazon Inspector Classic depuis mon compte AMS ?

Demandez l'accès à Amazon Inspector Classic en soumettant une RFC avec le type de modification Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Cette RFC attribue le rôle `customer_inspector_admin_role` IAM à votre compte. Le rôle inclut la `AmazonInspectorFullAccess` politique AWS gérée. Une fois configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon Inspector Classic dans mon compte AMS ?

Il n'y a aucune restriction. Toutes les fonctionnalités d'Amazon Inspector Classic sont disponibles dans votre compte AMS.

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon Inspector Classic dans mon compte AMS ?

Il n'existe aucune condition préalable ni dépendance pour utiliser Amazon Inspector Classic dans votre compte AMS.

Utiliser le nouvel Amazon Inspector dans AMS

Vous pouvez désormais utiliser le nouvel Amazon Inspector dans votre compte AMS.

Pour Amazon Inspector Classic, les `customer-inspector-admin-role-ssm-inspector-agent-policy` et `AmazonInspectorFullAccess` étaient obligatoires. Cependant, le rôle SSPS a été mis à jour `customer-inspector-admin-role`, qui inclut désormais un rôle supplémentaire. `policyAmazonInspector2FullAccess` Cette nouvelle politique autorise les autorisations d'API pour la nouvelle version d'Amazon Inspector.

Utilisez AMS SSP pour approvisionner Amazon Kendra sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon Kendra directement depuis votre compte géré par AMS. Amazon Kendra est un service de recherche intelligent qui utilise le traitement du langage naturel et des algorithmes d'apprentissage automatique avancés pour renvoyer des réponses spécifiques aux questions de recherche à partir de vos données. Contrairement à la recherche traditionnelle basée sur des mots clés, Amazon Kendra utilise ses capacités de compréhension sémantique et contextuelle pour déterminer si un document est pertinent pour une requête de recherche. Amazon Kendra renvoie des réponses spécifiques aux questions, afin que votre expérience soit proche de celle d'une interaction avec un expert humain. Amazon Kendra est hautement évolutif, capable de répondre aux exigences de performance, est étroitement intégré à d'autres AWS services tels qu'Amazon S3 et Amazon Lex, et offre une sécurité de niveau professionnel. Pour en savoir plus, consultez [Amazon Kendra](#) ;.

FAQ sur Amazon Kendra dans AWS Managed Services

Q : Comment puis-je demander l'accès à Amazon Kendra depuis mon compte AMS ?

Pour demander l'accès à Amazon Inspector Classic, soumettez une RFC avec le type de modification Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny). Cette RFC attribue le rôle `customer_kendra_console_role` IAM à votre compte. Une fois le rôle configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon Kendra sur mon compte AMS ?

Il n'y a aucune restriction. Toutes les fonctionnalités d'Amazon Kendra sont disponibles sur votre compte AMS.

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon Kendra dans mon compte AMS ?

Il n'existe aucun prérequis ni aucune dépendance pour démarrer avec Amazon Kendra. Toutefois, en fonction de votre cas d'utilisation spécifique, il se peut que vous deviez accéder à d'autres AWS services.

Utilisez AMS SSP pour approvisionner Amazon Kinesis Data Streams sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon Kinesis Data Streams (KDS) directement depuis votre compte géré AMS. Amazon Kinesis Data Streams est un service de streaming de données en temps réel hautement évolutif et durable. KDS peut capturer en continu des gigaoctets de données par seconde à partir de centaines de milliers de sources telles que les flux de clics sur les sites Web, les flux d'événements de base de données, les transactions financières, les flux de réseaux sociaux, les journaux informatiques et les événements de géolocalisation. Les données collectées sont disponibles en quelques millisecondes pour permettre des cas d'utilisation d'analyses en temps réel tels que des tableaux de bord en temps réel, la détection des anomalies en temps réel, la tarification dynamique, etc. Pour en savoir plus, consultez [Amazon Kinesis Data Streams](#).

FAQ sur les Kinesis Data Streams dans AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès à Amazon Kinesis Data Streams depuis mon compte AMS ?

Demandez l'accès à Amazon Kinesis Data Streams en soumettant une RFC auprès du service Management | AWS | Self-provisioned Service | Ajouter un type de

modification (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_kinesis_data_streaming_user_role` Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon Kinesis Data Streams sur mon compte AMS ?

Il n'y a aucune restriction. Toutes les fonctionnalités d'Amazon Kinesis Data Streams sont disponibles sur votre compte AMS.

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon Kinesis Data Streams dans mon compte AMS ?

Il n'existe aucune condition préalable ni dépendance pour utiliser Amazon Kinesis Data Streams dans votre compte AMS.

Utilisez AMS SSP pour approvisionner Amazon Kinesis Video Streams sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon Kinesis Video Streams (KVS) directement depuis votre compte géré par AMS. Amazon Kinesis Video Streams vous permet de diffuser des vidéos en toute sécurité à partir d'appareils connectés AWS à des fins d'analyse, d'apprentissage automatique (ML), de lecture et d'autres traitements. Kinesis Video Streams fournit automatiquement et adapte de manière élastique toute l'infrastructure nécessaire pour ingérer les données vidéo en streaming provenant de millions d'appareils. Il stocke, chiffre et indexe également de manière durable les données vidéo dans vos flux, et vous permet d'accéder à vos données par le biais de ce logiciel. easy-to-use APIs Kinesis Video Streams vous permet de visionner des vidéos en direct et à la demande, et de créer rapidement des applications qui tirent parti de la vision par ordinateur et de l'analyse vidéo grâce à l'intégration à Amazon Rekognition Video et aux bibliothèques pour les frameworks ML MxNet tels TensorFlow qu'Apache et OpenCV. Pour en savoir plus, consultez [Amazon Kinesis Video Streams](#).

FAQ sur Amazon Kinesis Video Streams dans AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès à Amazon Kinesis Video Streams depuis mon compte AMS ?

Demandez l'accès à Amazon Kinesis Video Streams en soumettant une RFC auprès du type Management AWS | service | Self-provisioned service | Add change

(ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte :

`customer_kinesis_video_streaming_user_role` Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon Kinesis Video Streams sur mon compte AMS ?

Il n'y a aucune restriction. Toutes les fonctionnalités d'Amazon Kinesis Video Streams sont disponibles sur votre compte AMS.

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon Kinesis Video Streams dans mon compte AMS ?

Il n'existe aucune condition préalable ni dépendance pour utiliser Amazon Kinesis Video Streams dans votre compte AMS.

Utilisez AMS SSP pour approvisionner Amazon Lex sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon Lex directement dans votre compte géré AMS. Amazon Lex est un service permettant de créer des interfaces conversationnelles dans n'importe quelle application utilisant la voix et le texte. Amazon Lex fournit les fonctionnalités avancées d'apprentissage profond que sont la reconnaissance vocale automatique (ASR) pour convertir la parole en texte, et la compréhension du langage naturel (NLU) pour reconnaître l'intention du texte, afin de vous permettre de créer des applications proposant des expériences utilisateur très engageantes et des interactions conversationnelles réalistes.

Avec Amazon Lex, les mêmes technologies d'apprentissage profond qui alimentent Amazon Alexa sont désormais accessibles à tous les développeurs, ce qui vous permet de créer rapidement et facilement des robots conversationnels ou des chatbots sophistiqués en langage naturel. Pour en savoir plus, consultez [Amazon Lex](#).

FAQ sur Amazon Lex dans AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès à Amazon Lex depuis mon compte AMS ?

Demandez l'accès en soumettant un type de gestion | AWS service | Service auto-approvisionné | Ajouter un type de modification (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_lex_author_role` Une fois configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon Lex sur mon compte AMS ?

L'intégration d'Amazon Lex à Lambda est limitée aux fonctions Lambda sans préfixe « AMS- », afin d'empêcher toute modification de l'infrastructure AMS.

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon Lex dans mon compte AMS ?

Il n'existe aucune condition préalable ni dépendance pour utiliser Amazon Lex dans votre compte AMS.

Utilisez AMS SSP pour approvisionner Amazon MQ sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon MQ directement depuis votre compte géré AMS. Amazon MQ est un service de messagerie géré pour Apache ActiveMQ qui vous aide à configurer et à exploiter des courtiers de messages dans le cloud. Les courtiers de messages permettent à différents systèmes logiciels, utilisant souvent différents langages de programmation et sur différentes plateformes, de communiquer et d'échanger des informations. Amazon MQ réduit votre charge opérationnelle en gérant le provisionnement, la configuration et la maintenance d'ActiveMQ, un courtier de messages open source populaire. La connexion de vos applications actuelles à Amazon MQ utilise les normes APIs et protocoles du secteur pour la messagerie, notamment JMS, NMS, AMQP, STOMP, MQTT et WebSocket. L'utilisation de normes signifie que, dans la plupart des cas, il n'est pas nécessaire de réécrire le code de messagerie lors de la migration vers AWS. Pour en savoir plus, consultez [Qu'est-ce qu'Amazon MQ ?](#)

FAQ sur Amazon MQ dans AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès à Amazon MQ depuis mon compte AMS ?

L'utilisation d'Amazon MQ dans votre compte AMS s'effectue en deux étapes :

1. Provisionnez le courtier Amazon MQ. Pour ce faire, soumettez un modèle CFN, avec le courtier Amazon MQ inclus, via une RFC avec le formulaire [Deployment | Ingestion | Stack CloudFormation from Template | Create change type \(ct-36cn2avfrj9v\)](#), ou soumettez une RFC à la direction [| Autre | Autre | Créer un type de modification \(ct-1e1xtak34nx76\)](#) demandant que le courtier Amazon MQ soit provisionné sur votre compte.
2. Accédez à la console Amazon MQ. Une fois le courtier Amazon MQ configuré, accédez à la console Amazon MQ en soumettant une RFC avec le type [Management | AWS service | Self-](#)

provisioned service | Add change (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_mq_console_role`

Une fois le rôle configuré dans votre compte, vous devez l'intégrer à votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon MQ sur mon compte AMS ?

Toutes les fonctionnalités d'Amazon MQ sont disponibles sur votre compte AMS ; toutefois, le provisionnement d'Amazon MQ Broker n'est pas disponible dans le cadre de cette politique en raison de l'autorisation élevée requise. Consultez les informations ci-dessus pour savoir comment ajouter le courtier Amazon MQ à vos comptes.

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon MQ dans mon compte AMS ?

Il n'existe aucun prérequis ni aucune dépendance pour utiliser Amazon MQ dans votre compte AMS.

Utilisez AMS SSP pour provisionner Amazon Managed Service pour Apache Flink sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon Managed Service for Apache Flink directement depuis votre compte géré AMS. Le service géré pour Apache Flink est le moyen le plus simple d'analyser les données de streaming, d'obtenir des informations exploitables et de répondre aux besoins de votre entreprise et de vos clients en temps réel. Amazon Managed Service pour Apache Flink simplifie la création, la gestion et l'intégration d'applications de streaming à d'autres AWS services. Les utilisateurs de SQL peuvent facilement interroger des données de streaming ou créer des applications de streaming complètes à l'aide de modèles et d'un éditeur SQL interactif. Les développeurs Java peuvent rapidement créer des applications de streaming sophistiquées à l'aide de bibliothèques Java open source et d'AWS intégrations pour transformer et analyser les données en temps réel. Amazon Managed Service pour Apache Flink prend en charge tout ce qui est nécessaire pour exécuter vos applications en temps réel en continu et s'adapte automatiquement au volume et au débit de vos données entrantes. Avec Amazon Managed Service pour Apache Flink, vous ne payez que pour les ressources consommées par vos applications de streaming. Il n'y a pas de frais minimum ni de frais d'installation. Pour en savoir plus, consultez [Amazon Managed Service pour Apache Flink](#).

FAQ sur le service géré pour Apache Flink dans AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès à Amazon Managed Service pour Apache Flink depuis mon compte AMS ?

Demandez l'accès en soumettant un type de modification Gestion | AWS service | Service auto-provisionné | Ajouter (révision requise) (ct-3qe6io8t6jtny). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_kinesis_analytics_application_role` Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon Managed Service pour Apache Flink dans mon compte AMS ?

- Les configurations sont limitées aux ressources sans les préfixes « AMS- » ou « MC- » afin d'empêcher toute modification de l'infrastructure AMS.
- L'autorisation de supprimer ou de créer de nouveaux Kinesis Data Streams ou Firehose a été supprimée de la politique. Nous avons une autre politique qui le permet.

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon Kinesis Data Streams dans mon compte AMS ?

Il existe quelques dépendances :

- Amazon Managed Service pour Apache Flink exige que Kinesis Data Streams ou Firehose soient créés avant de configurer une application avec Managed Service for Apache Flink.
- Les autorisations de politique basées sur les ressources doivent indiquer une source de données d'entrée particulière.

Utilisez AMS SSP pour provisionner Amazon Managed Streaming pour Apache Kafka sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon Managed Streaming for Apache Kafka (Amazon MSK) directement depuis votre compte géré AMS. Amazon Managed Streaming for Apache Kafka est un service de données de AWS streaming entièrement géré qui vous permet de créer et d'exécuter facilement des applications qui utilisent Apache Kafka pour traiter des données de streaming sans avoir à devenir un expert en exploitation de clusters Apache Kafka. Amazon MSK gère le provisionnement, la configuration et la maintenance des clusters Apache Kafka et des ZooKeeper nœuds Apache pour vous. Amazon MSK affiche également les indicateurs de performance clés d'Apache Kafka dans la AWS console.

Amazon MSK fournit plusieurs niveaux de sécurité pour vos clusters Apache Kafka, notamment l'isolation du réseau VPC, l' AWS IAM pour l'autorisation des API du plan de contrôle, le chiffrement au repos, le chiffrement TLS en transit, l'authentification par certificat basée sur le TLS, l'authentification sécurisée par. SASL/SCRAM AWS Secrets Manager Pour en savoir plus, consultez [Amazon MSK](#).

FAQ sur Amazon MSK dans AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès à Amazon MSK depuis mon compte AMS ?

Demandez l'accès en soumettant un type de modification Gestion | AWS service | Service auto-approvisionné | Ajouter (révision requise) (ct-3qe6io8t6jtny). Cette RFC fournit les politiques et le rôle IAM suivants à votre compte :

- `customer-msk-admin-policy.json`
- `AmazonMSKFullAccess`
- `customer-msk-admin-role.json`

Une fois configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon MSK ?

Pour qu'Amazon MSK envoie les journaux des courtiers aux destinations que vous configurez, assurez-vous que la `AmazonMSKFullAccess` politique est attachée à votre rôle IAM. Les autorisations d'accès complètes sont donc déjà en place.

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon MSK ?

Avant de créer votre cluster MSK, vous devez disposer d'un VPC et de sous-réseaux au sein de ce VPC. Par défaut, AMS couvre cette question dans le cadre de la création du [VPC AMS](#) par défaut.

Pour en savoir plus sur les limites d'Amazon MSK, consultez [Amazon MSK Limits](#).

Utilisez AMS SSP pour provisionner Amazon Managed Service for Prometheus sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon Managed Service for Prometheus (AMP) directement depuis votre compte géré AMS. Amazon

Managed Service for Prometheus est un service de surveillance sans serveur compatible avec Prometheus pour les métriques de conteneur qui facilite la surveillance sécurisée des environnements de conteneurs à grande échelle. Avec Amazon Managed Service for Prometheus, vous pouvez utiliser le même modèle de données et le même langage de requête open source Prometheus que vous utilisez aujourd'hui pour surveiller les performances de vos charges de travail conteneurisées et bénéficier d'une évolutivité, d'une disponibilité et d'une sécurité améliorées sans avoir à gérer l'infrastructure sous-jacente.

Amazon Managed Service for Prometheus adapte automatiquement l'ingestion, le stockage et l'interrogation des indicateurs opérationnels à mesure que les charges de travail augmentent ou diminuent. Il s'intègre aux services AWS de sécurité pour permettre un accès rapide et sécurisé aux données. Pour plus d'informations, consultez [Qu'est-ce qu'Amazon Managed Service pour Prometheus ?](#)

FAQ sur Amazon Managed Service pour Prometheus dans AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès à Amazon Managed Service for Prometheus depuis mon compte AMS ?

Demandez l'accès en soumettant un type de modification Gestion | AWS service | Service auto-approvisionné | Ajouter (révision requise) (ct-3qe6io8t6jtny). Cette RFC attribue le rôle IAM suivant à votre compte : `customer-prometheus-console-role` Une fois qu'il est configuré dans votre compte, vous devez intégrer le `customer-prometheus-console-role` rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon Managed Service for Prometheus sur mon compte AMS ?

Toutes les fonctionnalités sont prises en charge.

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon Managed Service for Prometheus dans mon compte AMS ?

Il n'existe aucun prérequis ni aucune dépendance pour démarrer avec Amazon Managed Service for Prometheus. Toutefois, en fonction de votre cas d'utilisation spécifique, il se peut que vous deviez accéder à d'autres AWS services.

Utilisez AMS SSP pour configurer Amazon Personalize sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon Personalize directement depuis votre compte géré par AMS. Amazon Personalize est un service d'apprentissage automatique qui permet aux développeurs de créer facilement des recommandations personnalisées pour les clients utilisant leurs applications.

L'apprentissage automatique est de plus en plus utilisé pour améliorer l'engagement des clients en proposant des recommandations de produits et de contenus personnalisées, des résultats de recherche personnalisés et des promotions marketing ciblées. Cependant, le développement des capacités d'apprentissage automatique nécessaires à la production de ces systèmes de recommandation sophistiqués est aujourd'hui hors de portée de la plupart des organisations en raison de leur complexité. Amazon Personalize permet aux développeurs n'ayant aucune expérience préalable en machine learning d'intégrer facilement des fonctionnalités de personnalisation sophistiquées à leurs applications, en utilisant une technologie d'apprentissage automatique perfectionnée grâce à des années d'utilisation sur Amazon.com.

Avec Amazon Personalize, vous fournissez un flux d'activité depuis votre application (clics, pages vues, inscriptions, achats, etc.) ainsi qu'un inventaire des articles que vous souhaitez recommander, tels que des articles, des produits, des vidéos ou de la musique. Vous pouvez également choisir de fournir à Amazon Personalize des informations démographiques supplémentaires concernant vos utilisateurs, telles que leur âge ou leur situation géographique. Amazon Personalize traitera et examinera les données, identifiera ce qui est significatif, sélectionnera les bons algorithmes, puis formera et optimisera un modèle de personnalisation adapté à vos données. Toutes les données analysées par Amazon Personalize restent confidentielles et sécurisées, et ne sont utilisées que pour vos recommandations personnalisées. Vous pouvez commencer à proposer des recommandations personnalisées via un simple appel d'API. Vous ne payez que pour ce que vous utilisez, et il n'y a pas de frais minimum ni d'engagement initial.

Pour en savoir plus, consultez [Amazon Personalize](#).

FAQ sur Amazon Personalize dans AWS Managed Services

Q : Comment puis-je demander l'accès à Amazon Personalize depuis mon compte AMS ?

Demandez l'accès en soumettant un type de modification Management | AWS Service | Self-provisioned Service | Add (révision requise) (ct-3qe6io8t6jtny), et vous devez spécifier quel compartiment S3 contient les données à utiliser par custom pour générer

les recommandations. AWS Cette RFC attribue les rôles IAM suivants à votre compte : `customer_personalize_console_role` et `customer_personalize_service_role`

- Une fois `customer_personalize_console_role` le rôle configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération. Vous pouvez également l'associer `customer_personalize_console_policy` à un autre rôle existant autre que `Customer_ReadOnly_Role`.
- Une fois que le `customer_personalize_service_role` est fourni à votre compte, vous pouvez faire référence à son ARN lors de la création d'un nouveau groupe de données.

À ce stade, AMS Operations déploiera également ce rôle de service dans votre compte : `aws_code_pipeline_service_role_policy`.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon Personalize sur mon compte AMS ?

La configuration d'Amazon Personalize est limitée aux ressources dépourvues des préfixes « `ams-` » ou « `mc-` », afin d'empêcher toute modification de l'infrastructure AMS.

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon Personalize dans mon compte AMS ?

- Si le compartiment S3 dans lequel les données sont stockées est chiffré, l'ID de clé KMS doit être fourni afin que nous puissions autoriser le rôle utilisé par Amazon Personalize à déchiffrer le compartiment.

Amazon Personalize ne prend pas en charge la clé KMS S3 par défaut. Si vous souhaitez utiliser KMS, créez une clé personnalisée et ajoutez-y la politique suivante en ouvrant une RFC avec le type de modification KMS Key | Create (révision requise) :

JSON

```
{
  "Version": "2012-10-17",
  "Id": "key-consolepolicy-3",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
        "Service": "personalize.amazonaws.com"
      },
    },
  ],
}
```



```

        "Action": "kms:*",
        "Resource": "*"
      }
    ]
  }
}

```

- Un compartiment S3 doit être créé avec la politique de compartiment suivante. Pour ce faire, soumettez une RFC avec le type de modification S3 Storage | Create Policy. Cette politique permet à Amazon Personalize d'accéder aux données ; ce compartiment contiendra les données destinées à être utilisées par Amazon Personalize.

JSON

```

{
  "Version": "2012-10-17",
  "Id": "PersonalizeS3BucketAccessPolicy",
  "Statement": [
    {
      "Sid": "PersonalizeS3BucketAccessPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "personalize.amazonaws.com"
      },
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::bucket-name",
        "arn:aws:s3:::bucket-name/*"
      ]
    }
  ]
}

```

Utilisez AMS SSP pour approvisionner Amazon sur QuickSight votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux QuickSight fonctionnalités directement dans votre compte géré AMS. QuickSight est un service de business intelligence rapide, basé sur le cloud, qui fournit des informations à tous les membres de votre organisation. En tant que

service entièrement géré, il vous QuickSight permet de créer et de publier facilement des tableaux de bord interactifs qui incluent des informations sur le machine learning (ML). Pour en savoir plus, consultez [Amazon QuickSight](#).

QuickSight dans la FAQ AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès QuickSight à mon compte AMS ?

Demandez l'accès en soumettant un type de gestion | AWS service | Service auto-approvisionné | Ajouter un type de modification (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_quicksight_console_admin_role` Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions d'utilisation QuickSight sur mon compte AMS ?

- AWS les paramètres de ressources QuickSight activés ne vous seront pas accessibles en raison de la dépendance à la politique IAM. Cependant, l'équipe AMS active chaque ressource pour vous en réponse à votre demande d'activation du service.
- L'accès aux ressources pour les utilisateurs individuels et les groupes n'est pas pris en charge dans ce modèle car cette fonctionnalité permet aux utilisateurs de modifier les autorisations IAM susceptibles de compromettre l'infrastructure AMS.
- La possibilité d'inviter des identités IAM depuis l'intérieur n' QuickSight est pas prise en charge en raison du risque lié à la modification des objets IAM.
- QuickSight le service propose deux éditions : Enterprise et Standard. Les deux proposent une option d'authentification unique (SSO) prise en charge sur AMS. Cependant, l'édition Enterprise propose une option d'intégration QuickSight à Active Directory (AD). QuickSight sur AMS ne prend pas en charge l'intégration avec AD en raison d'incompatibilités entre la structure du compte AMS et les exigences de QuickSight confiance.

Q : Quels sont les prérequis ou les dépendances pour pouvoir l'utiliser QuickSight dans mon compte AMS ?

- Lorsque AMS reçoit cette RFC à ajouter QuickSight, vous recevez une demande de service pour obtenir des informations supplémentaires ; fournissez-leur les informations suivantes :
 - QuickSight nom du compte (par exemple, *CustomerName*-quicksight)
 - QuickSight Édition (Standard ou Enterprise)

- La AWS région dans laquelle le QuickSight service doit être activé (par défaut, votre AWS région AMS).
- Une adresse e-mail de notification pour le QuickSight compte.
- (Facultatif) Le compartiment S3 dans lequel se trouvent les fichiers de données à analyser.
- Le VPC et le sous-réseau IDs qui se connectent prennent en QuickSight charge une fonctionnalité permettant d'ajouter une connexion VPC, qui permet une connectivité privée entre le compte QuickSight et les ressources qu'il contient.

Un opérateur AMS effectue le processus d'inscription en votre nom et configure deux QuickSight fonctionnalités :

- [Découverte automatique](#) des sources de données.
- [Connexions VPC](#).

 Note

Ces actions doivent être effectuées par un opérateur AMS car des autorisations IAM et VPC élevées sont requises pendant le processus de connexion.

Utilisez AMS SSP pour configurer Amazon Rekognition sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon Rekognition directement depuis votre compte géré AMS. Amazon Rekognition permet d'ajouter facilement une analyse d'images et de vidéos à vos applications à l'aide d'une technologie d'apprentissage profond éprouvée et hautement évolutive qui ne nécessite aucune expertise en apprentissage automatique pour être utilisée. Avec Amazon Rekognition, vous pouvez identifier des objets, des personnes, du texte, des scènes et des activités dans des images et des vidéos, ainsi que détecter tout contenu inapproprié. Amazon Rekognition fournit également des fonctionnalités d'analyse faciale et de recherche faciale très précises que vous pouvez utiliser pour détecter, analyser et comparer des visages dans le cadre d'une grande variété de cas de vérification utilisateur, de comptage de personnes et de sécurité publique.

Avec les étiquettes personnalisées Amazon Rekognition, vous pouvez identifier des objets et des scènes spécifiques aux besoins de votre entreprise dans les images. Par exemple, vous pouvez

créer un modèle pour classer des pièces de machine spécifiques sur votre chaîne de montage ou pour détecter des plantes insalubres. Amazon Rekognition Custom Labels prend en charge le gros du développement des modèles à votre place. Aucune expérience en apprentissage automatique n'est donc requise. Il vous suffit de fournir des images des objets ou des scènes que vous souhaitez identifier, et le service s'occupe du reste.

Pour en savoir plus, consultez [Amazon Rekognition](#).

FAQ sur Amazon Rekognition dans AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès à Amazon Rekognition depuis mon compte AMS ?

Demandez l'accès en soumettant un type de modification Gestion | AWS service | Service auto-provisionné | Ajouter (révision requise) (ct-3qe6io8t6jtny). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_rekognition_console_role` & `customer_rekognition_service_role` Une fois configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon Rekognition sur mon compte AMS ?

Toutes les fonctionnalités d'Amazon Rekognition sont disponibles avec le rôle de service auto-provisionné Amazon Rekognition.

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon Rekognition dans mon compte AMS ?

Si vous utilisez Kinesis Video Streams qui fournit la source vidéo en streaming pour un processeur de flux vidéo Amazon Rekognition ou un flux de données comme destination pour écrire des données dans Kinesis Data Streams, veuillez fournir un à AMS lors de la création de la RFC.

`kinesisStreamName`

Utilisez AMS SSP pour configurer Amazon SageMaker AI sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon SageMaker AI directement depuis votre compte géré AMS. SageMaker L'IA permet à chaque développeur et scientifique des données de créer, de former et de déployer rapidement des modèles d'apprentissage automatique. Amazon SageMaker AI est un service entièrement géré qui couvre l'ensemble du flux de travail d'apprentissage automatique pour étiqueter et préparer vos données,

choisir un algorithme, entraîner le modèle, le régler et l'optimiser pour le déploiement, faire des prédictions et prendre des mesures. Vos modèles sont mis en production plus rapidement, avec beaucoup moins d'efforts et à moindre coût. Pour en savoir plus, consultez [Amazon SageMaker AI](#).

SageMaker FAQ sur l'IA dans AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès à l' SageMaker IA dans mon compte AMS ?

Demandez l'accès en soumettant un type de modification Management | AWS Service | Autoprovisionné | Add (ct-1w8z66n899dct). Cette RFC attribue les rôles IAM suivants à votre compte : `customer_sagemaker_admin_role` et le rôle de service. `AmazonSageMaker-ExecutionRole-Admin` Une fois l' SageMaker IA configurée dans votre compte, vous devez intégrer le `customer_sagemaker_admin_role` rôle dans votre solution de fédération. Vous ne pouvez pas accéder directement au rôle de service ; le service d' SageMaker IA l'utilise pour effectuer diverses actions, comme décrit ici : [Transmission de rôles](#).

Q : Quelles sont les restrictions relatives à l'utilisation de l' SageMaker IA dans mon compte AMS ?

- Les cas d'utilisation suivants ne sont pas pris en charge par le rôle IAM AMS Amazon SageMaker AI :
 - SageMaker AI Studio n'est pas pris en charge pour le moment.
 - SageMaker L'IA Ground Truth pour gérer les effectifs privés n'est pas prise en charge car cette fonctionnalité nécessite un accès trop permissif aux ressources Amazon Cognito. Si la gestion d'une main-d'œuvre privée est requise, vous pouvez demander un rôle IAM personnalisé avec des autorisations combinées SageMaker AI et Amazon Cognito. Dans le cas contraire, nous vous recommandons de faire appel à du personnel public (soutenu par Amazon Mechanical Turk) ou à des fournisseurs de AWS Marketplace services pour l'étiquetage des données.
- Création de points de terminaison VPC pour prendre en charge les appels d'API aux services d' SageMaker IA (`aws.sagemaker`). `{region}.notebook`, `com.amazonaws.{region}.sagemaker.api` et `com.amazonaws.{region}.sagemaker.runtime`) n'est pas pris en charge car les autorisations ne peuvent pas être limitées aux seuls services liés à l'IA. SageMaker Pour soutenir ce cas d'utilisation, soumettez une RFC Management | Other | Other pour créer des points de terminaison VPC associés.
- SageMaker La mise à l'échelle automatique des terminaux AI n'est pas prise en charge car l' SageMaker IA nécessite `DeleteAlarm` des autorisations sur n'importe quelle ressource (« * »). Pour prendre en charge le dimensionnement automatique d'un point de terminaison, soumettez

une RFC de gestion | Autre | Autre afin de configurer le dimensionnement automatique pour un point de terminaison basé sur l' SageMaker IA.

Q : Quels sont les prérequis ou les dépendances pour utiliser l' SageMaker IA dans mon compte AMS ?

- Les cas d'utilisation suivants nécessitent une configuration spéciale avant utilisation :
 - Si un compartiment S3 doit être utilisé pour stocker des artefacts et des données du modèle, vous devez demander un compartiment S3 nommé avec les mots clés requis (« SageMaker », « Sagemaker », « sagemaker » ou « aws-glue ») avec un Deployment | Advanced stack components | S3 storage | Create RFC.
 - Si Elastic File Store (EFS) doit être utilisé, le stockage EFS doit être configuré dans le même sous-réseau et autorisé par les groupes de sécurité.
 - Si d'autres ressources nécessitent un accès direct aux services d' SageMaker IA (ordinateurs portables, API, environnement d'exécution, etc.), la configuration doit être demandée par :
 - Soumission d'une RFC pour créer un groupe de sécurité pour le point de terminaison (déploiement | Composants de pile avancés | Groupe de sécurité | Créer (auto)).
 - Soumission d'une RFC de gestion | Autre | Autre | Création d'une RFC pour configurer les points de terminaison VPC associés.

Q : Quelles sont les conventions de dénomination prises en charge pour les ressources auxquelles ils **customer_sagemaker_admin_role** peuvent accéder directement ? (Les informations suivantes concernent les autorisations de mise à jour et de suppression ; si vous avez besoin de conventions de dénomination supplémentaires prises en charge pour vos ressources, contactez un architecte du cloud AMS pour obtenir une consultation.)

- Ressource : `AmazonSageMaker-ExecutionRole-*` role
 - Autorisations : le rôle de service auto-provisionné SageMaker AI vous permet d'utiliser le rôle de service SageMaker AI (`AmazonSageMaker-ExecutionRole-*`) avec AWS Glue AWS RoboMaker, et. AWS Step Functions
- Ressource : Secrets on AWS Secrets Manager
 - Autorisations : décrire, créer, obtenir, mettre à jour des secrets avec un `AmazonSageMaker-*` préfixe.
 - Autorisations : Décrivez, obtenez des secrets lorsque la balise de SageMaker ressource est définie sur `true`.

- Ressource : Référentiels sur AWS CodeCommit
 - Autorisations : créer/supprimer des référentiels avec un AmazonSageMaker - * préfixe.
 - Autorisations : Git Pull/Push sur les référentiels avec les préfixes suivants, *sagemaker**SageMaker*, et. *Sagemaker*
- Ressource : référentiels Amazon ECR (Amazon Elastic Container Registry)
 - Autorisations : autorisations : définissez, supprimez des politiques de référentiel et téléchargez des images de conteneur, lorsque la convention de dénomination des ressources suivante est utilisée, *sagemaker*.
- Ressource : compartiments Amazon S3
 - Autorisations : obtenir, placer, supprimer un objet, abandonner le téléchargement partitionné d'objets S3 lorsque les ressources ont les préfixes suivants : *SageMaker*, et *Sagemaker*.
 - *sagemaker* aws-glue
 - Autorisations : obtenez des objets S3 lorsque la SageMaker balise est définie sur true.
- Ressource : Amazon CloudWatch Log Group
 - Autorisations : créer un groupe de journaux ou un flux, mettre un événement de journal, répertorier, mettre à jour, créer, supprimer la livraison du journal avec le préfixe suivant : /aws/sagemaker/*.
- Ressource : Amazon CloudWatch Metric
 - Autorisations : saisissez les données métriques lorsque les préfixes suivants sont utilisés : AWS/SageMakerAWS/SageMaker/, aws/SageMaker, aws/SageMaker/, aws/sagemakeraws/sagemaker/, et /aws/sagemaker/..
- Ressource : Amazon CloudWatch Dashboard
 - Autorisations : Create/Delete tableaux de bord lorsque les préfixes suivants sont utilisés : customer_*
- Ressource : rubrique Amazon SNS (Simple Notification Service)
 - Autorisations : Subscribe/Create sujet lorsque les préfixes suivants sont utilisés : *sagemaker**SageMaker*, et *Sagemaker*.

Q : Quelle est la différence entre **AmazonSageMakerFullAccess** et **customer_sagemaker_admin_role** ?

Le **customer_sagemaker_admin_role** with **customer_sagemaker_admin_policy** fournit presque les mêmes autorisations que, **AmazonSageMakerFullAccess** sauf que :

- Autorisation de connexion à AWS RoboMaker Amazon Cognito et AWS Glue aux ressources.
- SageMaker Mise à l'échelle automatique des terminaux IA. Vous devez soumettre une RFC avec Management | Advanced stack components | Identity and Access Management (IAM) | Modifier le type d'entité ou de politique (révision requise) (ct-27tuth19k52b4) pour augmenter les autorisations de dimensionnement automatique temporairement ou définitivement, car le dimensionnement automatique nécessite un accès permissif au service. CloudWatch

Q : Comment adopter une clé gérée par AWS KMS le client pour le chiffrement des données au repos ?

Vous devez vous assurer que la politique des clés a été correctement configurée sur les clés gérées par le client afin que les utilisateurs ou rôles IAM associés puissent utiliser les clés. Pour plus d'informations, consultez le [document de politique AWS KMS clé](#).

Utilisez AMS SSP pour configurer Amazon Simple Email Service sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon Simple Email Service (Amazon SES) directement depuis votre compte géré AMS. Amazon Simple Email Service est un service d'envoi d'e-mails basé sur le cloud conçu pour aider les spécialistes du marketing numérique et les développeurs d'applications à envoyer des e-mails marketing, de notification et transactionnels.

Vous pouvez utiliser l'interface SMTP ou l'une des interfaces AWS SDKs pour intégrer Amazon SES directement dans vos applications existantes. Vous pouvez également intégrer les fonctionnalités d'envoi d'e-mails d'Amazon SES dans les logiciels que vous utilisez déjà, tels que les systèmes de billetterie et les clients de messagerie.

Pour en savoir plus, consultez [Amazon Simple Email Service](#).

FAQ sur Amazon SES dans AWS Managed Services

Q : Comment puis-je demander l'accès à Amazon SES depuis mon compte AMS ?

Demandez l'accès à Amazon SES en soumettant une RFC avec le type de modification Management | AWS service | Self-provisioned Service | Add (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_ses_admin_role` Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon SES dans mon compte AMS ?

- Vous devez configurer une politique de compartiment S3 pour permettre à Amazon SES de publier des événements dans le compartiment.
- Vous devez utiliser une clé CMK par défaut (AWS SES) ou configurer une clé CMK pour permettre à Amazon SES de chiffrer les e-mails et de transférer des événements vers d'autres ressources de service telles qu'Amazon S3, Amazon SNS, Lambda et Firehose, appartenant au compte.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon SES sur mon compte AMS ?

Vous devez collecter RFCs pour créer les ressources suivantes :

- Un utilisateur SMTP et un rôle de service IAM PutEvents autorisés à accéder à un flux Kinesis Firehose.
- Vous devez créer de nouvelles AWS ressources telles que le bucket S3, le stream Firehose, le topic SNS en utilisant les types de modification AMS afin que les destinations de vos règles et ensembles de configuration Amazon SES fonctionnent avec ces ressources.
- Informations d'identification SMTP. Pour demander de nouvelles informations d'identification SMTP, utilisez le type de modification (Gestion | Autre | Autre | Création). AMS crée les informations d'identification et les ajoute à Secrets Manager pour vous.

Utilisez AMS SSP pour configurer Amazon Simple Workflow Service sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon Simple Workflow Service (Amazon SWF) directement depuis votre compte géré AMS. Amazon Simple Workflow Service aide les développeurs à créer, exécuter et dimensionner des tâches en arrière-plan comportant des étapes parallèles ou séquentielles. Vous pouvez considérer Amazon SWF comme un outil de suivi d'état entièrement géré et un coordinateur de tâches dans le cloud. Si les étapes de votre application prennent plus de 500 millisecondes, si vous devez suivre l'état du traitement, ou si vous devez effectuer une restauration ou une nouvelle tentative en cas d'échec d'une tâche, Amazon SWF peut vous aider. Pour en savoir plus, consultez [Amazon Simple Workflow Service](#).

FAQ sur Amazon SWF dans AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès à Amazon SWF depuis mon compte AMS ?

Demandez l'accès en soumettant un type de gestion | AWS service | Service auto-approvisionné | Ajouter un type de modification (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_swf_role` Une fois configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon SWF dans mon compte AMS ?

Les `InvokeFunction` autorisations Lambda ont été incluses dans ce service, mais l'AMS ajouté à tous les rôles des clients AMS `customer_deny_policy` refuse explicitement l'accès aux fonctions Lambda d'AMS et aux ressources appartenant à AMS. Pour étiqueter ou débaliser des ressources dans Amazon SWF, soumettez un type de modification Management | Other | Other.

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon SWF dans mon compte AMS ?

Amazon SWF dépend du AWS Lambda service. Par conséquent, les autorisations permettant d'invoquer Lambda ont été fournies dans le cadre de ce rôle et aucune autorisation supplémentaire n'est requise pour appeler Lambda depuis Amazon SWF. Dans le cas contraire, il n'y a aucune condition préalable à l'utilisation d'Amazon SWF.

Utilisez AMS SSP pour approvisionner Amazon Textract sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon Textract directement depuis votre compte géré par AMS. Amazon Textract est un service d'apprentissage automatique entièrement géré qui extrait automatiquement le texte imprimé, l'écriture manuscrite et d'autres données des documents numérisés. Il va au-delà de la simple reconnaissance optique de caractères (OCR) pour identifier, comprendre et extraire les données des formulaires et des tableaux. Pour en savoir plus, consultez [Amazon Textract](#).

FAQ sur Amazon Textract dans AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander à ce qu'Amazon Textract soit configuré dans mon compte AMS ?

Demandez l'accès en soumettant un type de modification Gestion | AWS service | Service auto-approvisionné | Ajouter (révision requise) (ct-3qe6io8t6jtny). Cette RFC fournit les rôles IAM suivants à votre compte : `customer_textract_console_role`, `customer_textract_human_review_execution_role`

et `customer_ec2_textract_instance_profile` Une fois configuré dans votre compte, vous devez intégrer le rôle `customer_textract_console_role` dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon Textract sur mon compte AMS ?

Il n'existe aucune restriction quant à l'utilisation d'Amazon Textract dans votre compte AMS.

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon Textract dans mon compte AMS ?

Vous devez demander la création d'un compartiment S3 en soumettant un déploiement RFC | Composants de pile avancés | Stockage S3 | Création (ct-1a68ck03fn98r).

Utilisez AMS SSP pour approvisionner Amazon Transcribe sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon Transcribe directement depuis votre compte géré AMS. Amazon Transcribe est un service de reconnaissance vocale automatique entièrement géré et formé en continu qui génère automatiquement des transcriptions de texte horodatées à partir de fichiers audio. Amazon Transcribe permet aux développeurs d'ajouter facilement des speech-to-text fonctionnalités à leurs applications. Il est pratiquement impossible pour les ordinateurs de rechercher et d'analyser les données audio. Par conséquent, le discours enregistré doit être converti en texte avant de pouvoir être utilisé dans des applications. Historiquement, les clients devaient travailler avec des fournisseurs de transcription qui les obligeaient à signer des contrats coûteux et étaient difficiles à intégrer dans leurs outils technologiques pour accomplir cette tâche. Nombre de ces fournisseurs utilisent des technologies obsolètes qui ne s'adaptent pas bien aux différents scénarios, comme le son basse fidélité des téléphones, courant dans les centres d'appels, qui se traduit par une faible précision.

Amazon Transcribe utilise un processus d'apprentissage approfondi appelé reconnaissance vocale automatique (ASR) pour convertir la parole en texte, rapidement et avec précision. Amazon Transcribe peut être utilisé pour transcrire les appels du service client, automatiser le sous-titrage et générer des métadonnées pour les ressources multimédias afin de créer une archive entièrement consultable. Vous pouvez utiliser Amazon Transcribe Medical pour ajouter des speech-to-text fonctionnalités médicales aux applications de documentation clinique. Pour en savoir plus, consultez [Amazon Transcribe](#).

FAQ sur Amazon Transcribe dans AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander à ce qu'Amazon Transcribe soit configuré sur mon compte AMS ?

Demandez l'accès en soumettant un type de modification Gestion | AWS service | Service auto-approvisionné | Ajouter (révision requise) (ct-3qe6io8t6jtny). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_transcribe_role` Une fois configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation d'Amazon Transcribe sur mon compte AMS ?

Vous devez utiliser « `customer-transcribe*` » comme préfixe pour vos buckets lorsque vous utilisez Transcribe, sauf indication contraire de RA.

Vous n'êtes pas en mesure de créer un rôle IAM dans Amazon Transcribe.

Vous ne pouvez pas utiliser un compartiment S3 géré par un service pour les données de sortie dans le SSPS par défaut (si cela est nécessaire, contactez l'autorité de certification de votre compte).

Vous devez soumettre une acceptation des risques si vous souhaitez utiliser des clés KMS gérées par le client qui ne relèvent pas de l'espace de noms AMS.

Q : Quels sont les prérequis ou les dépendances pour utiliser Amazon Transcribe dans mon compte AMS ?

S3 doit avoir accès aux compartiments portant le nom « `customer-transcribe*` ». KMS est nécessaire pour utiliser Amazon Transcribe si vos compartiments S3 sont chiffrés à l'aide de clés KMS. Si un bucket n'a pas besoin d'être chiffré, le bouton « `KMStranscribe Autoriser` » peut être supprimé.

Utilisez AMS SSP pour approvisionner Amazon sur WorkSpaces votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux WorkSpaces fonctionnalités directement dans votre compte géré AMS. WorkSpaces vous permet de fournir des bureaux Microsoft Windows ou Amazon Linux virtuels basés sur le cloud à vos utilisateurs, connus sous WorkSpaces le nom de. WorkSpaces élimine le besoin d'acheter et de déployer du matériel ou d'installer des logiciels complexes. Vous pouvez rapidement ajouter ou supprimer des utilisateurs à mesure que vos besoins évoluent. Les utilisateurs y WorkSpaces accèdent à l'aide d'une application cliente à partir d'un appareil compatible ou, pour Windows WorkSpaces, d'un navigateur Web, et ils se connectent à l'aide de leurs informations d'identification Active Directory (AD) locales existantes.

Pour en savoir plus, consultez [Amazon WorkSpaces](#).

WorkSpaces dans la FAQ AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès WorkSpaces à mon compte AMS ?

Demandez l'accès en soumettant un type de modification Gestion | AWS service | Service auto-approvisionné | Ajouter (révision requise) (ct-3qe6io8t6jtny). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_workspaces_console_role` Une fois configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions d'utilisation WorkSpaces sur mon compte AMS ?

Toutes les fonctionnalités de Workspaces sont disponibles avec le rôle de WorkSpaces service auto-approvisionné par Amazon.

Q : Quels sont les prérequis ou les dépendances pour pouvoir utiliser WorkSpaces mon compte AMS ?

- WorkSpaces sont limités par AWS région ; par conséquent, l'AD Connector doit être configuré dans la même AWS région que celle où les WorkSpaces instances sont hébergées.

Les clients peuvent se connecter WorkSpaces à l'AD client en utilisant l'une des deux méthodes suivantes :

1. Utilisation du connecteur AD pour l'authentification par proxy auprès du service Active Directory local (de préférence) :

Configurez le connecteur Active Directory (AD) dans votre compte AMS avant d'intégrer votre WorkSpaces instance à votre service d'annuaire local. L'AD Connector agit comme un proxy permettant à vos utilisateurs AD existants (depuis votre domaine) de se connecter à WorkSpaces l'aide des informations d'identification AD locales existantes. C'est préférable car ils WorkSpaces sont directement liés au domaine sur site du client, qui fait à la fois office de forêt de ressources et de forêt d'utilisateurs, ce qui permet un meilleur contrôle du côté du client.

Pour plus d'informations, consultez les [meilleures pratiques pour le déploiement d'Amazon WorkSpaces \(scénario 1\)](#).

2. Utilisation d'AD Connector avec AWS Microsoft AD, Shared Services VPC et d'une confiance unidirectionnelle sur site :

Vous pouvez également authentifier les utilisateurs auprès de votre annuaire local en établissant d'abord une confiance sortante unidirectionnelle entre AD géré par AMS et votre AD local. WorkSpaces rejoindra AD géré par AMS à l'aide d'un AD Connector. WorkSpaces les autorisations d'accès seront ensuite déléguées aux WorkSpaces instances via l'AD géré par AMS, sans qu'il soit nécessaire d'établir une relation de confiance bidirectionnelle avec votre environnement sur site. Dans ce scénario, la forêt utilisateur se trouvera dans l'AD du client et la forêt de ressources dans l'AD géré par AMS (les modifications apportées à l'AD géré par AMS peuvent être demandées via RFC). Notez que la connectivité entre le WorkSpaces VPC et le VPC MALZ Shared Services exécutant l'AD géré par AMS est établie via Transit Gateway.

Pour plus d'informations, consultez les [meilleures pratiques pour le déploiement d'Amazon WorkSpaces \(scénario 6\)](#).

Note

L'AD Connector peut être configuré en soumettant une RFC de type Management | Other | Other | Create change avec les détails de configuration AD requis ; pour plus d'informations, voir [Créer un AD Connector](#). Si la méthode 2 est utilisée pour créer une forêt de ressources dans AD géré par AMS, soumettez une autre RFC Management | Other | Other | Create change type dans un compte de services partagés AMS en exécutant l'AD géré par AMS.

Utilisez AMS SSP pour fournir des services AMS Code sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités des services AMS Code directement dans votre compte géré AMS. Les services AMS Code sont un ensemble propriétaire de services de gestion de code AWS, comme indiqué ci-dessous. Vous pouvez choisir de déployer tous les services dans AMS avec les services AMS Code, ou vous pouvez les déployer individuellement dans AMS.

Les services AMS Code incluent les services suivants :

- AWS CodeCommit: un service de [contrôle de source](#) entièrement géré qui héberge des référentiels sécurisés basés sur Git. Cela permet aux équipes de collaborer sur le code dans un écosystème sécurisé et hautement évolutif. CodeCommit élimine le besoin d'exploiter votre propre système de

contrôle de source ou de vous soucier de la mise à l'échelle de son infrastructure. Vous pouvez utiliser CodeCommit pour tout stocker en toute sécurité, du code source aux fichiers binaires. En outre, ce service fonctionne sans problème avec vos outils Git existants. Pour en savoir plus, consultez [AWS CodeCommit](#)

Pour le déployer dans votre compte AMS indépendamment des services AMS Code, consultez [Utilisez AMS SSP pour approvisionner AWS CodeCommit votre compte AMS](#).

- AWS CodeBuild: service d'intégration continue entièrement géré qui compile le code source, exécute des tests et produit des progiciels prêts à être déployés. Grâce à CodeBuild cela, vous n'avez pas besoin de provisionner, de gérer et de dimensionner vos propres serveurs de construction. CodeBuild évolue en continu et traite plusieurs versions simultanément, afin que vos versions ne soient pas laissées en attente dans une file d'attente. Vous pouvez démarrer rapidement en utilisant des environnements de génération prépackagés, ou bien, vous pouvez créer vos propres environnements de génération personnalisés, que vous utiliserez avec vos outils de génération. Avec CodeBuild, les ressources informatiques que vous utilisez vous sont facturées à la minute. Pour en savoir plus, consultez [AWS CodeBuild](#)

Pour le déployer dans votre compte AMS indépendamment des services AMS Code, consultez [Utilisez AMS SSP pour approvisionner AWS CodeBuild votre compte AMS](#).

- AWS CodeDeploy: un service de déploiement entièrement géré qui automatise les déploiements de logiciels vers divers services informatiques tels qu'Amazon EC2 et vos serveurs sur site. AWS CodeDeploy vous aide à publier rapidement de nouvelles fonctionnalités, à éviter les temps d'arrêt lors du déploiement des applications et à gérer la complexité de la mise à jour de vos applications. Vous pouvez l'utiliser AWS CodeDeploy pour automatiser les déploiements de logiciels, éliminant ainsi le besoin d'opérations manuelles susceptibles d'entraîner des erreurs. Le service s'adapte à vos besoins de déploiement. Pour en savoir plus, consultez [AWS CodeDeploy](#)

Pour le déployer dans votre compte AMS indépendamment des services AMS Code, consultez [Utilisez AMS SSP pour approvisionner AWS CodeDeploy votre compte AMS](#).

- AWS CodePipeline: un service de [livraison continue](#) entièrement géré qui vous aide à automatiser vos pipelines de publication pour des mises à jour rapides et fiables des applications et de l'infrastructure. CodePipeline automatise les phases de création, de test et de déploiement de votre processus de publication chaque fois qu'un changement de code est effectué, en fonction du modèle de version que vous définissez. Cela vous permet de fournir des fonctionnalités et des mises à jour de manière rapide et fiable. Vous pouvez facilement intégrer AWS CodePipeline des services tiers tels que GitHub ou avec votre propre plugin personnalisé. Avec AWS CodePipeline,

vous ne payez que pour ce que vous utilisez. Vous ne subissez ni frais initiaux ni engagement à long terme. Pour en savoir plus, consultez [AWS CodePipeline](#)

Pour le déployer dans votre compte AMS indépendamment des services AMS Code, consultez [Utilisez AMS SSP pour approvisionner AWS CodePipeline votre compte AMS](#).

FAQ sur les services de code AMS dans AWS Managed Services

Q : Comment puis-je demander l'accès aux services AMS Code sur mon compte AMS ?

Demandez l'accès en soumettant un type de modification Gestion | AWS service | Service auto-approvisionné | Ajouter (révision requise) (ct-3qe6io8t6jtny). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_code_suite_console_role`. Une fois le rôle configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération. À ce stade, AMS Operations déploiera également les rôles de `aws_code_pipeline_service_role` service `customer_codebuild_service_role` `customer_codedeploy_service_role`, dans votre compte pour CodeBuild, CodeDeploy et les CodePipeline services. Si des autorisations IAM supplémentaires sont requises pour le `customer_codebuild_service_role` sont, soumettez une demande de service AMS.

Note

Vous pouvez également ajouter ces services séparément ; pour plus d'informations [Utilisez AMS SSP pour approvisionner AWS CodeBuild votre compte AMS](#), voir [Utilisez AMS SSP pour approvisionner AWS CodeDeploy votre compte AMS](#), et [Utilisez AMS SSP pour approvisionner AWS CodePipeline votre compte AMS](#), respectivement.

Q : Quelles sont les restrictions relatives à l'utilisation des services AMS Code sur mon compte AMS ?

- AWS CodeCommit: La fonctionnalité des déclencheurs CodeCommit est désactivée étant donné les droits associés pour créer des sujets SNS. L'authentification directe auprès de Credential CodeCommit Helper est limitée ; les utilisateurs doivent s'authentifier auprès de Credential Helper. Certaines commandes KMS sont également restreintes : kms: Chiffrer, kms: Déchiffrer, kms:ReEncrypt, kms: GenerateDataKey kms:GenerateDataKeyWithoutPlaintext, et. kms: DescribeKey

- **CodeBuild:** pour l'accès de l'administrateur de la AWS CodeBuild console, les autorisations sont limitées au niveau des ressources ; par exemple, les CloudWatch actions sont limitées sur des ressources spécifiques et l'`iam:PassRole` autorisation est contrôlée.
- **CodeDeploy:** CodeDeploy prend actuellement en charge les déploiements sur EC2 Amazon/on-premises uniquement. Les déploiements sur ECS et Lambda CodeDeploy via ne sont pas pris en charge.
- **CodePipeline:** les CodePipeline fonctionnalités, les étapes et les fournisseurs sont limités aux éléments suivants :
 - Étape de déploiement : Amazon S3 et AWS CodeDeploy
 - Étape source : Amazon S3 AWS CodeCommit, Bit Bucket et GitHub
 - Build Stage : AWS CodeBuild et Jenkins
 - Étape d'approbation : Amazon SNS
 - Étape de test : Jenkins AWS CodeBuild BlazeMeter, test de l'interface utilisateur de Ghost Inspector, Micro Focus StormRunner Load, surveillance de l'API Runscope
 - Invoke Stage : Step Functions et Lambda

Note

AMS Operations le déploie `customer_code_pipeline_lambda_policy` dans votre compte ; il doit être associé au rôle d'exécution Lambda pour la phase d'appel Lambda. Indiquez le nom du service/execution rôle Lambda avec lequel vous souhaitez ajouter cette politique. S'il n'existe aucun service/execution rôle Lambda personnalisé, AMS crée un nouveau rôle nommé `customer_code_pipeline_lambda_execution_role`, qui est une copie de `customer_lambda_basic_execution_role`.

`customer_code_pipeline_lambda_policy`

Q : Quels sont les prérequis ou les dépendances pour utiliser les services AMS Code dans mon compte AMS ?

- **CodeCommit:** Si les compartiments S3 sont chiffrés à l'aide de AWS KMS clés, S3 et AWS KMS B doivent être utilisés AWS CodeCommit.
- **CodeBuild:** Si des autorisations IAM supplémentaires sont requises pour le rôle de AWS CodeBuild service défini, demandez-les par le biais d'une demande de service AMS.
- **CodeDeploy:** Aucune.

- CodePipeline: Aucune. AWS les services pris en charge—AWS CodeCommit AWS CodeBuild,, AWS CodeDeploy—doivent être lancés avant ou en même temps que le lancement de CodePipeline. Cependant, cela est effectué par un ingénieur AMS.

Utilisez AMS SSP pour provisionner AWS Amplify votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS Amplify fonctionnalités directement dans votre compte géré AMS. AWS Amplify Il s'agit d'une solution complète qui permet aux développeurs Web et mobiles frontaux de créer, de connecter et d'héberger facilement des applications fullstack. Amplify offre la flexibilité nécessaire pour tirer parti de l'étendue des AWS services au fur et à mesure de l'évolution de vos cas d'utilisation. Amplify fournit des produits pour créer des applications complètes pour iOS, Android, Flutter, Web et React Native. Pour en savoir plus, veuillez consulter la section [AWS Amplify](#).

AWS Amplify dans la FAQ AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander AWS Amplify à être configuré dans mon compte AMS ?

Demandez l'accès en soumettant un type de modification Gestion | AWS service | Service auto-provisionné | Ajouter (révision requise) (ct-3qe6io8t6jtny). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_amplify_console_role` Après avoir été configuré sur votre compte, vous devez intégrer le rôle dans votre solution de fédération.

En outre, vous devez fournir une acceptation des risques, car AWS Amplify vous disposez d'autorisations permettant de modifier l'infrastructure. Pour ce faire, collaborez avec votre responsable de prestation de services cloud (CSDM).

Q : Quelles sont les restrictions d'utilisation AWS Amplify sur mon compte AMS ?

Vous devez l'utiliser ' `amplify*` ' comme préfixe pour vos buckets lorsque vous travaillez avec Amplify, sauf indication contraire en RA.

Q : Quels sont les prérequis ou les dépendances pour pouvoir l'utiliser AWS Amplify dans mon compte AMS ?

Il n'y a aucune condition préalable à l'utilisation de AWS Amplify dans votre compte AMS.

Environnements Malz uniquement : le rôle intégré par défaut pour Amplify est « `customer_amplify_console_role` ». Pour utiliser un rôle personnalisé, déployez d'abord les

entités IAM. Créez ensuite une RFC supplémentaire pour ajouter votre rôle personnalisé à la liste d'autorisation de la politique de contrôle des services pour les comptes d'applications.

Utiliser AMS SSP pour le provisionnement AWS AppSync

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS AppSync fonctionnalités directement dans votre compte géré AMS. AWS AppSync simplifie le développement d'applications en vous permettant de créer une API flexible pour accéder, manipuler et combiner en toute sécurité les données provenant d'une ou de plusieurs sources de données. AWS AppSync est un service géré qui utilise GraphQL pour permettre aux applications d'obtenir facilement les données dont elles ont besoin.

Vous pouvez ainsi créer des AWS AppSync applications évolutives, y compris celles nécessitant des mises à jour en temps réel, sur une gamme de sources de données telles que les magasins de données NoSQL, les bases de données relationnelles, le protocole HTTP APIs et vos sources de données personnalisées avec. AWS Lambda Pour les applications mobiles et Web, fournit AWS AppSync également un accès aux données locales lorsque les appareils se déconnectent, ainsi que la synchronisation des données avec résolution des conflits personnalisable, lorsqu'ils sont de nouveau en ligne. Pour en savoir plus, veuillez consulter la section [AWS AppSync](#).

AWS AppSync dans la FAQ AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès AWS AppSync à mon compte AMS ?

Demandez l'accès en soumettant un type de gestion | AWS service | Service auto-approvisionné | Ajouter un type de modification (ct-1w8z66n899dct). Cette RFC attribue les rôles IAM suivants à votre compte : `customer_appsync_service_role` et `customer_appsync_author_role` Une fois provisionnée dans votre compte, vous devez l'intégrer `customer_appsync_author_role` à votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation du AWS AppSync ?

- Lorsque vous créez une source de données lorsque AppSync le client doit spécifier le rôle de service créé précédemment, la création d'un nouveau rôle n'est pas autorisée et renverra donc un accès refusé
- AppSync les rôles sont configurés pour restreindre les autorisations aux ressources contenant les préfixes « AMS- » ou « MC- » afin d'empêcher toute modification de l'infrastructure AMS.

Q : Quels sont les prérequis ou les dépendances nécessaires à l'utilisation ? AWS AppSync

Le service permet d'utiliser plusieurs autres services comme source de données. Les autorisations de base pour les utiliser en tant que tels sont incluses dans le rôle de service (`customer_appsync_service_role`), mais vous devez sélectionner manuellement le rôle de service lorsque vous utilisez le service.

Utilisez AMS SSP pour approvisionner AWS App Mesh votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS App Mesh fonctionnalités directement dans votre compte géré AMS. AWS App Mesh fournit un réseau au niveau des applications pour permettre à vos services de communiquer facilement entre eux sur plusieurs types d'infrastructures informatiques. App Mesh normalise la façon dont vos services communiquent, vous donne de la end-to-end visibilité et garantit la haute disponibilité de vos applications.

AWS App Mesh facilite l'exécution des services en fournissant une visibilité et un contrôle du trafic réseau cohérents pour les services basés sur plusieurs types d'infrastructures informatiques. App Mesh élimine le besoin de mettre à jour le code de l'application pour modifier la manière dont les données de surveillance sont collectées ou le trafic est acheminé entre les services. App Mesh configure chaque service pour exporter les données de surveillance et met en œuvre une logique de contrôle des communications cohérente dans l'ensemble de votre application. Cela permet de localiser rapidement l'emplacement exact des erreurs et de rediriger automatiquement le trafic réseau en cas de panne ou lorsque des modifications de code doivent être déployées. Pour en savoir plus, veuillez consulter la section [AWS App Mesh](#).

AWS App Mesh dans la FAQ AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès AWS App Mesh à mon compte AMS ?

Demandez l'accès en soumettant un type de gestion | AWS service | Service auto-approvisionné | Ajouter un type de modification (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_app_mesh_console_role` Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation du AWS App Mesh ?

Toutes les fonctionnalités de AWS App Mesh sont disponibles dans votre compte AMS.

Q : Quels sont les prérequis ou les dépendances nécessaires à l'utilisation ? AWS App Mesh

Il n'y a aucun prérequis ni aucune dépendance à utiliser AWS App Mesh dans votre compte AMS.

Utilisez AMS SSP pour provisionner AWS Audit Manager votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Audit Manager directement dans votre compte géré AMS. Audit Manager vous aide à auditer en permanence votre AWS utilisation afin de simplifier la manière dont vous évaluez les risques et la conformité aux réglementations et aux normes du secteur. Audit Manager automatise la collecte de preuves pour faciliter l'évaluation de l'efficacité de vos politiques, procédures et activités. Au moment d'effectuer un audit, Audit Manager vous aide à gérer les révisions de vos contrôles par les parties prenantes et à créer des rapports prêts pour l'audit en réduisant considérablement les efforts manuels. Pour en savoir plus, consultez [Audit Manager](#).

AWS Audit Manager dans la FAQ AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès AWS Audit Manager à mon compte AMS ?

Vous pouvez demander l'accès en soumettant le service AWS Services RFC Management | AWS | Service auto-provisionné | Ajouter (révision requise) (ct-3qe6io8t6jtny). Cette RFC fournit le rôle IAM suivant dans votre compte : `customer-audit-manager-admin-Role` Une fois le rôle configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions d'utilisation AWS Audit Manager ?

Il n'y a aucune restriction quant à l'utilisation de AWS Audit Manager dans votre compte AMS. Toutes les fonctionnalités de AWS Audit Manager sont fournies.

Q : Quels sont les prérequis ou les dépendances nécessaires à l'utilisation ? AWS Audit Manager

1. Vous devez fournir à AMS le compartiment s3 dans lequel vous reports/assessments souhaitez résider.
2. Si vous souhaitez que le service soit chiffré, vous devez fournir à AMS l'ARN KMS CMK à utiliser.
3. Si vous souhaitez envoyer des notifications SNS à une rubrique, vous devez fournir le nom de la rubrique ou de l'ARN.

4. (Facultatif) Il existe une condition préalable supplémentaire si vous souhaitez activer Organizations dans le cadre de votre zone de landing zone multi-comptes dans Audit Manager et si vous souhaitez un compte administrateur délégué : dans le champ de description de RFC (Management | AWS service | Compatible Service| Add), mentionnez que vous souhaitez utiliser le compte administrateur délégué dans le cadre de la configuration d'Audit Manager et fournissez les informations ci-dessous :

- ARN KMS CMK (initialement utilisé pour configurer Audit Manager)
- ID de compte administrateur délégué à utiliser par Audit Manager dans le cadre de cette zone de landing zone multi-comptes (il peut s'agir d'un compte d'application MALZ)

Utilisez AMS SSP pour approvisionner AWS Batch votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS Batch fonctionnalités directement dans votre compte géré AMS. AWS Batch permet aux développeurs, aux scientifiques et aux ingénieurs d'exécuter facilement et efficacement des centaines de milliers de tâches de calcul par lots AWS. AWS Batch fournit dynamiquement la quantité et le type optimaux de ressources de calcul (telles que les instances optimisées pour le processeur ou la mémoire) en fonction du volume et des besoins en ressources spécifiques des tâches par lots soumises. Ainsi AWS Batch, il n'est pas nécessaire d'installer et de gérer les logiciels de traitement par lots ou les clusters de serveurs que vous utilisez pour exécuter vos tâches, ce qui vous permet de vous concentrer sur l'analyse des résultats et la résolution des problèmes. Pour en savoir plus, veuillez consulter la section [AWS Batch](#).

AWS Batch dans la FAQ AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès AWS Batch à mon compte AMS ?

1. Pour demander l'accès à AWS Batch, soumettez le document RFC Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Cette RFC prévoit les rôles et politiques IAM suivants dans votre compte :

Rôles IAM :

- customer_batch_console_role
- customer_batch_ecs_instance_role
- customer_batch_events_service_role

- `customer_batch_service_role`
- `customer_batch_ecs_task_role`

Stratégies :

- `customer_batch_console_role_policy`
- `customer_batch_service_role_policy`
- `customer_batch_events_service_role_policy`

2. Une fois le rôle configuré dans votre compte, vous devez intégrer le rôle `customer_batch_console_role` dans votre solution de fédération.

Q : Quelles sont les restrictions d'utilisation AWS Batch ?

Lors de la création de l'environnement informatique, vous devez étiqueter EC2 les instances comme « `customer_batch` » ou « `customer-batch` ». Si les instances ne sont pas étiquetées, elles ne seront pas supprimées par lots une fois le travail terminé.

Q : Quels sont les prérequis ou les dépendances nécessaires à l'utilisation ? AWS Batch

Il n'y a aucun prérequis ni aucune dépendance à utiliser AWS Batch dans votre compte AMS.

Utilisez AMS SSP pour approvisionner AWS Certificate Manager votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités AWS Certificate Manager (ACM) directement dans votre compte géré AMS. AWS Certificate Manager est un service qui vous permet de fournir, de gérer et de déployer des certificats Secure Sockets Layer/Transport Layer Security (SSL/TLS) publics et privés à utiliser avec les AWS services et vos ressources connectées internes. SSL/TLS les certificats sont utilisés pour sécuriser les communications réseau et établir l'identité des sites Web sur Internet ainsi que des ressources sur les réseaux privés. AWS Certificate Manager élimine le processus manuel fastidieux d'achat, de téléchargement et de renouvellement SSL/TLS des certificats.

Vous pouvez ainsi demander un certificat, le déployer sur des AWS ressources intégrées à ACM, telles que les Elastic Load Balancers, les CloudFront distributions Amazon et sur API APIs Gateway, et vous laisser AWS Certificate Manager gérer les renouvellements de certificats. AWS Certificate

Manager Il vous permet également de créer des certificats privés pour vos ressources internes et de gérer le cycle de vie des certificats de manière centralisée. Les certificats publics et privés fournis AWS Certificate Manager pour être utilisés avec les services intégrés à ACM sont gratuits. Vous ne payez que pour les AWS ressources que vous créez pour exécuter votre application. Avec [AWS Private Certificate Authority](#), vous payez mensuellement pour le fonctionnement de l'Autorité de certification privée AWS et pour les certificats privés que vous émettez. Pour en savoir plus, consultez la section [AWS Certificate Manager - AWS Documentation](#).

FAQ sur l'ACM dans AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès AWS Certificate Manager à mon compte AMS ?

Demandez l'accès en soumettant un type de gestion | AWS service | Service auto-approvisionné | Ajouter un type de modification (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_acm_create_role` Vous pouvez utiliser ce rôle pour créer et gérer des certificats ACM. Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Les certificats ACM peuvent être créés à l'aide des types de modification suivants, même si vous n'avez pas ajouté le rôle `customer_acm_create_role` IAM :

- [ACM | Créer un certificat public](#)
- [ACM | Créer un certificat privé](#)
- [Certificat ACM avec SANs | Créer supplémentaire](#)

Q : Quelles sont les restrictions relatives à l'utilisation du AWS Certificate Manager ?

Vous devez envoyer une demande de modification (RFC) à AMS pour supprimer ou modifier les certificats existants, car ces actions nécessitent un accès administrateur complet (utilisez le type de modification Gestion | Autre | Autre | Mettre à jour (ct-0xdawir96cy7k). Notez que la politique IAM ne peut pas exclure des droits en fonction des noms de balises (`mc*`, `ams*`, etc.). Les certificats ne sont pas payants. Il n'est donc pas urgent de supprimer les certificats non utilisés.

Q : Quels sont les prérequis ou les dépendances nécessaires à l'utilisation de Certificate Manager ?

Nom DNS public existant et accès pour créer des enregistrements DNS CNAME, mais ceux-ci n'ont pas besoin d'être hébergés dans le compte géré.

Utilisez AMS SSP pour approvisionner AWS Private Certificate Authority votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS Private Certificate Authority fonctionnalités directement dans votre compte géré AMS. Les certificats privés sont utilisés pour identifier et sécuriser les communications entre les ressources connectées sur les réseaux privés, telles que les serveurs, les appareils mobiles et les applications IoT. Autorité de certification privée AWS est un service d'autorité de certification privée géré qui vous aide à gérer facilement et en toute sécurité le cycle de vie de vos certificats privés. Autorité de certification privée AWS vous fournit un service d'autorité de certification privée hautement disponible, sans l'investissement initial et les coûts de maintenance permanents liés à l'exploitation de votre propre autorité de certification privée. Autorité de certification privée AWS étend les fonctionnalités de gestion des certificats d'ACM aux certificats privés, ce qui vous permet de créer et de gérer des certificats publics et privés de manière centralisée. Vous pouvez facilement créer et déployer des certificats privés pour vos AWS ressources à l'aide de la console AWS de gestion ou de l'API ACM. Pour les EC2 instances, les conteneurs, les appareils IoT et les ressources sur site, vous pouvez facilement créer et suivre des certificats privés et utiliser votre propre code d'automatisation côté client pour les déployer. Vous avez également la possibilité de créer des certificats privés et de les gérer vous-même pour les applications qui nécessitent des durées de vie de certificats, des algorithmes clés ou des noms de ressources personnalisés. Pour en savoir plus, consultez [Autorité de certification privée AWS](#).

Autorité de certification privée AWS dans la FAQ AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès Autorité de certification privée AWS à mon compte AMS ?

Demandez l'accès via la soumission de la RFC sur les AWS services (Gestion | AWS service | Service compatible). Grâce à cette RFC, le rôle IAM suivant sera fourni dans votre compte : `customer_acm_pca_role` Une fois configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation du Autorité de certification privée AWS ?

À l'heure actuelle, AWS Resource Access Manager (AWS RAM) ne peut pas être utilisé pour partager vos Autorité de certification privée AWS comptes entre plusieurs comptes.

Q : Quels sont les prérequis ou les dépendances nécessaires à l'utilisation ? Autorité de certification privée AWS

1. Si vous envisagez de créer une CRL, vous avez besoin d'un compartiment S3 pour la stocker. Autorité de certification privée AWS dépose automatiquement la CRL dans le compartiment Amazon S3 que vous désignez et la met à jour régulièrement. Avant de pouvoir configurer une CRL, il est indispensable que le compartiment S3 dispose de la politique de compartiment ci-dessous. Pour traiter cette demande, créez une RFC avec ct-0fpjlx808sh2 (Gestion | Composants de pile avancés | Stockage S3 | Politique de mise à jour) comme suit :

- Indiquez le nom ou l'ARN du compartiment S3.
- Copiez la politique ci-dessous sur RFC et remplacez-la par le nom bucket-name de compartiment S3 de votre choix.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "acm-pca.amazonaws.com"
      },
      "Action": [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::bucket-name/*",
        "arn:aws:s3:::bucket-name"
      ]
    }
  ]
}
```

2. Si le compartiment S3 ci-dessus est chiffré, le principal de service acm-pca.amazonaws.com a besoin d'autorisations pour le déchiffrer. Pour traiter cette demande, créez une RFC avec ct-3ovo7px2vsa6n (Gestion | Composants de pile avancés | clé KMS | Mise à jour) comme suit :

- Indiquez l'ARN de la clé KMS sur laquelle la politique doit être mise à jour.
- Copiez la politique ci-dessous sur RFC et remplacez-la par le nom bucket-name de compartiment S3 de votre choix.

```
{
  "Sid": "Allow ACM-PCA use of the key",
  "Effect": "Allow",
  "Principal": {
    "Service": "acm-pca.amazonaws.com"
  },
  "Action": [
    "kms:GenerateDataKey",
    "kms:Decrypt"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": [
        "arn:aws:s3:::bucket_name/acm-pca-permission-test-key",
        "arn:aws:s3:::bucket_name/acm-pca-permission-test-key-private",
        "arn:aws:s3:::bucket_name/audit-report/*",
        "arn:aws:s3:::bucket_name/crl/*"
      ]
    }
  }
}
```

3. Autorité de certification privée AWS CRLs ne prennent pas en charge le paramètre S3 « Bloquer l'accès public aux compartiments et aux objets accordés par le biais de nouvelles listes de contrôle d'accès (ACLs) ». Vous devez désactiver ce paramètre avec le compte et le compartiment S3 afin de permettre l'Autorité de certification privée AWS écriture, CRLs comme indiqué dans [Comment créer et stocker en toute sécurité votre CRL pour ACM Private CA](#). Si vous souhaitez le désactiver, créez une nouvelle RFC avec ct-0xdawir96cy7k (Management | Other | Other | Update) et joignez une acceptation des risques. Si vous avez des questions sur l'acceptation des risques, contactez votre architecte cloud.

Utilisez AMS SSP pour approvisionner AWS CloudEndure votre compte AMS

Note

Suite au lancement réussi de AWS Application Migration Service, le service de CloudEndure migration est désormais en fin de vie dans toutes les AWS régions. Nous recommandons aux clients de l'utiliser AWS Application Migration Service pour les migrations par ascenseur et par équipes vers GovCloud les régions et les régions commerciales. Pour plus d'informations, voir [Qu'est-ce que c'est AWS Application Migration Service ?](#).

Si vous souhaitez utiliser le AWS Application Migration Service, contactez votre autorité de certification afin qu'elle puisse vous guider.

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS CloudEndure fonctionnalités directement dans votre compte géré AMS. AWS CloudEndure la migration simplifie, accélère et automatise les migrations à grande échelle depuis une infrastructure physique, virtuelle et basée sur le cloud vers. AWS CloudEndure Disaster Recovery (DR) protège contre les interruptions de service et les pertes de données causées par toute menace, y compris les ransomwares et la corruption des serveurs.

AWS CloudEndure dans la FAQ AWS Managed Services

Q : Comment puis-je demander l'accès CloudEndure à mon compte AMS ?

Demandez l'accès en soumettant un type de modification Gestion | AWS service | Service auto-approvisionné | Ajouter (révision requise) (ct-3qe6io8t6jtny). Cette RFC fournit l'utilisateur IAM suivant à votre compte : `customer_cloud_endure_user` Une fois qu'elles sont configurées dans votre compte, la clé d'accès et la clé secrète de l'utilisateur sont partagées dans AWS Secrets Manager.

Ces politiques sont également appliquées au compte : `customer_cloud_endure_policy` et `customer_cloud_endure_deny_policy`.

En outre, vous devez fournir une acceptation des risques, car la solution de reprise après CloudEndure sinistre pour l'intégration des applications dispose d'autorisations permettant de modifier l'infrastructure. Pour ce faire, collaborez avec votre responsable de prestation de services cloud (CSDM).

Q : Quelles sont les restrictions d'utilisation CloudEndure sur mon compte AMS ?

Les instances de réplication et de conversion basées sur le cloud ne peuvent être lancées que dans le sous-réseau que vous indiquez.

Q : Quels sont les prérequis ou les dépendances pour pouvoir l'utiliser CloudEndure dans mon compte AMS ? Partagez les informations suivantes via une correspondance bidirectionnelle RFC :

- Détails du sous-réseau VPC pour les instances de réplication et de conversion à lancer.
- Le nom de ressource Amazon (ARN) de la clé KMS si les volumes EBS sont chiffrés.

Utilisez AMS SSP pour provisionner AWS CloudHSM votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS CloudHSM fonctionnalités directement dans votre compte géré AMS. AWS CloudHSM vous aide à répondre aux exigences de conformité de l'entreprise, contractuelles et réglementaires en matière de sécurité des données en utilisant des instances de module de sécurité matérielle (HSM) dédiées dans le AWS cloud. AWS, et les partenaires de AWS Marketplace, proposent diverses solutions pour protéger les données sensibles au sein de la AWS plateforme, mais pour certaines applications et données soumises à des obligations contractuelles ou réglementaires relatives à la gestion des clés cryptographiques, une protection supplémentaire peut être nécessaire. AWS CloudHSM complète les solutions de protection des données existantes et vous permet de protéger vos clés de chiffrement conçues et validées conformément aux normes gouvernementales pour une gestion sécurisée des clés. HSMs AWS CloudHSM vous permet de générer, de stocker et de gérer en toute sécurité les clés cryptographiques utilisées pour le chiffrement des données de manière à ce que les clés ne soient accessibles que par vous. Pour en savoir plus, veuillez consulter la section [AWS CloudHSM](#).

AWS CloudHSM dans la FAQ AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès AWS CloudHSM à mon compte AMS ?

L'utilisation de dans votre compte AMS se fait en deux étapes :

1. Demandez un AWS CloudHSM cluster. Pour ce faire, soumettez une RFC avec le type de modification Management | Other | Other | Create (ct-1e1xtak34nx76). Incluez les informations suivantes :
 - AWS Région.
 - ID/ARN. Provide a VPC ID/VPCARN VPC qui se trouve dans le même compte que la RFC que vous soumettez.

- Spécifiez au moins deux zones de disponibilité pour le cluster.
 - ID d' EC2 instance Amazon qui se connectera au cluster HSM.
2. Accédez à la AWS CloudHSM console. Pour ce faire, soumettez une RFC avec le type de modification Management | AWS Service | Self-provisioned Service | Add (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_cloudhsm_console_role`

Une fois le rôle configuré dans votre compte, vous devez l'intégrer à votre solution de fédération.

Q : Quelles sont les restrictions d'utilisation AWS CloudHSM sur mon compte AMS ?

L'accès à la AWS CloudHSM console ne vous permet pas de créer, de résilier ou de restaurer votre cluster. Pour ce faire, soumettez un type de modification Management | Other | Other | Create change type (ct-1e1xtak34nx76).

Q : Quels sont les prérequis ou les dépendances pour pouvoir l'utiliser AWS CloudHSM dans mon compte AMS ?

Vous devez autoriser le trafic TCP via le port 2225 via une EC2 instance Amazon cliente au sein d'un VPC, ou utiliser le VPN Direct Connect pour les serveurs sur site qui souhaitent accéder au cluster HSM. AWS CloudHSM dépend d'Amazon EC2 pour les groupes de sécurité et les interfaces réseau. Pour la surveillance ou l'audit des journaux, HSM s'appuie sur CloudTrail (les opérations AWS d'API) et les CloudWatch journaux pour toutes les activités des appareils HSM locaux.

Q : Qui appliquera les mises à jour au AWS CloudHSM client et aux bibliothèques logicielles associées ?

Vous êtes responsable de l'application des mises à jour de la bibliothèque et du client. Vous devez surveiller la page d'historique des versions de [CloudHSM](#) pour connaître les versions, puis appliquer les mises à jour à l'aide de la mise à niveau du client [CloudHSM](#).

 Note

Les correctifs logiciels pour l'appliance HSM sont toujours appliqués automatiquement par le AWS CloudHSM service.

Utilisez AMS SSP pour approvisionner AWS CodeBuild votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS CodeBuild fonctionnalités directement dans votre compte géré AMS. AWS CodeBuild est un service d'intégration continue entièrement géré qui compile le code source, exécute des tests et produit des progiciels prêts à être déployés. Grâce à CodeBuild cela, vous n'avez pas besoin de provisionner, de gérer et de dimensionner vos propres serveurs de construction. CodeBuild évolue en continu et traite plusieurs versions simultanément, afin que vos versions ne soient pas laissées en attente dans une file d'attente. Vous pouvez démarrer rapidement en utilisant des environnements de génération prépackagés, ou bien, vous pouvez créer vos propres environnements de génération personnalisés, que vous utiliserez avec vos outils de génération. Avec CodeBuild, les ressources informatiques que vous utilisez vous sont facturées à la minute. Pour en savoir plus, veuillez consulter la section [AWS CodeBuild](#).

Note

Pour intégrer CodeCommit, CodeBuild CodeDeploy, et CodePipeline avec une seule RFC, soumettez le type de changement Management | AWS Service | Self-provisioned Service | Add (révision requise) (ct-3qe6io8t6jtny) et demandez les trois services :, et. CodeBuild CodeDeploy CodePipeline Ensuite, les trois rôles, `customer_codebuild_service_role`, `customer_codedeploy_service_role`, et `aws_code_pipeline_service_role` sont fournis dans votre compte. Une fois le provisionnement effectué dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

CodeBuild dans la FAQ AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès AWS CodeBuild à mon compte AMS ?

L'utilisation de AWS CodeBuild dans votre compte AMS se fait en deux étapes :

1. Provisionnez le processus CodeBuild Service Role de génération afin de le coordonner avec les buckets AWS S3, Amazon CloudWatch et les groupes Log
2. Demande d'accès à la CodeBuild console

Vous pouvez demander que les deux soient configurés dans votre compte AMS en soumettant une RFC avec le type Management | AWS Service | Self-provisioned Service | Add change (ct-1w8z66n899dct). Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions d'utilisation AWS CodeBuild sur mon compte AMS ?

Pour l'accès de l'administrateur de AWS CodeBuild console, les autorisations sont limitées au niveau des ressources ; par exemple, les CloudWatch actions sont limitées sur des ressources spécifiques et l'iam:PassRole autorisation est contrôlée.

Q : Quels sont les prérequis ou les dépendances pour pouvoir l'utiliser CodeBuild dans mon compte AMS ?

Si des autorisations IAM supplémentaires sont requises pour le rôle de AWS CodeBuild service défini, demandez-les par le biais d'une demande de service AMS.

Utilisez AMS SSP pour approvisionner AWS CodeCommit votre compte AMS

Note

AWS a fermé l'accès des nouveaux clients à AWS CodeCommit, à compter du 25 juillet 2024. AWS CodeCommit les clients existants peuvent continuer à utiliser le service normalement. AWS continue d'investir dans l'amélioration de la sécurité, de la disponibilité et des performances AWS CodeCommit, mais nous ne prévoyons pas d'introduire de nouvelles fonctionnalités.

Pour migrer des référentiels AWS CodeCommit Git vers d'autres fournisseurs Git, contactez votre architecte cloud (CA) pour obtenir des conseils. Pour plus d'informations sur la migration de vos référentiels Git, consultez [Comment migrer votre CodeCommit référentiel AWS vers un autre fournisseur Git](#).

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS CodeCommit fonctionnalités directement dans votre compte géré AMS. AWS CodeCommit est un service de [contrôle de source](#) entièrement géré qui héberge des référentiels sécurisés basés sur Git. Il aide les équipes à collaborer sur le code dans un écosystème sécurisé et hautement évolutif. CodeCommit élimine le besoin d'exploiter votre propre système de contrôle de source ou de vous soucier de la mise à l'échelle de son infrastructure. Vous pouvez l'utiliser CodeCommit pour stocker n'importe quoi

en toute sécurité, du code source aux fichiers binaires, et il fonctionne parfaitement avec vos outils Git existants. Pour en savoir plus, veuillez consulter la section [AWS CodeCommit](#).

Note

Pour intégrer CodeCommit, CodeBuild CodeDeploy, et CodePipeline avec une seule RFC, soumettez le type de changement Management | AWS Service | Self-provisioned Service | Add (révision requise) (ct-3qe6io8t6jtny) et demandez les trois services :, et. CodeBuild CodeDeploy CodePipeline Ensuite, les trois rôles, `customer_codebuild_service_role`, `customer_codedeploy_service_role`, et `aws_code_pipeline_service_role` sont fournis dans votre compte. Une fois le provisionnement effectué dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

CodeCommit dans la FAQ AWS Managed Services

Q : Comment puis-je demander l'accès CodeCommit à mon compte AMS ?

AWS CodeCommit les rôles de console et d'accès aux données peuvent être demandés en soumettant deux AWS services RFCs, l'accès à la console et l'accès aux données :

- Demandez l'accès à AWS CodeCommit en soumettant une RFC avec le type de modification Management | AWS Service | Self-provisioned Service | Add (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_codecommit_console_role` Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Les accès aux données (tels que les listes de formation et d'entités) doivent être séparés CTs pour chaque source de données, en spécifiant la source de données S3 (obligatoire), le compartiment de sortie (obligatoire) et le KMS (facultatif). Il n'y a aucune limite à la création AWS CodeCommit d'emplois tant que des rôles d'accès ont été accordés à toutes les sources de données. Pour demander l'accès aux données, soumettez une RFC à Management | Other | Other | Create (ct-1e1xtak34nx76).

Q : Quelles sont les restrictions d'utilisation AWS CodeCommit sur mon compte AMS ?

La fonctionnalité des CodeCommit déclencheurs est désactivée étant donné les droits associés pour créer des sujets SNS. L'authentification directe CodeCommit est restreinte, les utilisateurs doivent

s'authentifier avec Credential Helper. Certaines commandes KMS sont également restreintes : `kms:Encrypt`, `kms:Decrypt`, `kms:ReEncrypt`, `kms:GenerateDataKey`, `kms:GenerateDataKeyWithoutPlaintext`, `kms:DescribeKey`.

Q : Quels sont les prérequis ou les dépendances pour pouvoir utiliser AWS CodeCommit mon compte AMS ?

Si les compartiments S3 sont chiffrés avec des clés KMS, S3 et KMS doivent être utilisés AWS CodeCommit.

Utilisez AMS SSP pour provisionner AWS CodeDeploy votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS CodeDeploy fonctionnalités directement dans votre compte géré AMS. AWS CodeDeploy est un service de déploiement entièrement géré qui automatise les déploiements de logiciels vers divers services informatiques tels qu'Amazon EC2, AWS Fargate AWS Lambda, et vos serveurs sur site. AWS CodeDeploy vous aide à publier rapidement de nouvelles fonctionnalités, à éviter les temps d'arrêt lors du déploiement des applications et à gérer la complexité de la mise à jour de vos applications. Vous pouvez l'utiliser AWS CodeDeploy pour automatiser les déploiements de logiciels, éliminant ainsi le besoin d'opérations manuelles susceptibles d'entraîner des erreurs. Le service s'adapte à vos besoins de déploiement. Pour en savoir plus, veuillez consulter la section [AWS CodeDeploy](#).

Note

Pour intégrer CodeCommit, CodeBuild CodeDeploy, et CodePipeline avec une seule RFC, soumettez le type de changement Management | AWS Service | Self-provisioned Service | Add (révision requise) (ct-3qe6io8t6jtny) et demandez les trois services :, et. CodeBuild CodeDeploy CodePipeline Ensuite, les trois rôles, `customer_codebuild_service_role`, `customer_codedeploy_service_role`, et `aws_code_pipeline_service_role` sont fournis dans votre compte. Une fois le provisionnement effectué dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

CodeDeploy dans la FAQ AWS Managed Services

Q : Comment puis-je demander l'accès CodeDeploy à mon compte AMS ?

Demandez l'accès à CodeDeploy en soumettant une RFC avec le type de modification Management | AWS service | Self-provisioned Service | Add (ct-1w8z66n899dct). Cette RFC attribue les rôles IAM suivants à votre compte : `customer_codedeploy_console_role` et `customer_codedeploy_service_role`. Une fois qu'il est configuré dans votre compte, vous devez intégrer le `customer_codedeploy_console_role` rôle dans votre solution de fédération.

Q : Quelles sont les restrictions d'utilisation CodeDeploy sur mon compte AMS ?

Actuellement, nous ne prenons en charge que la plate-forme de calcul sous la forme : EC2 Amazon/on-Premises. Blue/Green Les déploiements ne sont pas pris en charge.

Q : Quels sont les prérequis ou les dépendances pour pouvoir utiliser CodeDeploy mon compte AMS ?

Il n'y a aucun prérequis ni aucune dépendance à utiliser CodeDeploy dans votre compte AMS.

Utilisez AMS SSP pour provisionner AWS CodePipeline votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS CodePipeline fonctionnalités directement dans votre compte géré AMS. AWS CodePipeline est un service de [livraison continue](#) entièrement géré qui vous aide à automatiser vos pipelines de publication pour des mises à jour rapides et fiables des applications et de l'infrastructure. CodePipeline automatise les phases de création, de test et de déploiement de votre processus de publication chaque fois qu'un changement de code est effectué, en fonction du modèle de version que vous définissez. Cela vous permet de fournir des fonctionnalités et des mises à jour de manière rapide et fiable. Vous pouvez facilement intégrer AWS CodePipeline des services tiers tels que GitHub ou avec votre propre plugin personnalisé. Avec AWS CodePipeline, vous ne payez que pour ce que vous utilisez. Vous ne subissez ni frais initiaux ni engagement à long terme. Pour en savoir plus, veuillez consulter la section [AWS CodePipeline](#).

Note

Pour intégrer CodeCommit, CodeBuild CodeDeploy, et CodePipeline avec une seule RFC, soumettez le type de changement Management | AWS Service | Self-provisioned Service | Add (révision requise) (ct-3qe6io8t6jtny) et demandez les trois services :, et. CodeBuild CodeDeploy CodePipeline Ensuite, les trois rôles, `customer_codebuild_service_role`, `customer_codedeploy_service_role`, et `aws_code_pipeline_service_role` sont fournis dans votre compte. Une fois le

provisionnement effectué dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

CodePipeline in AMS ne prend pas en charge « Amazon CloudWatch Events » pour Source Stage car il nécessite des autorisations élevées pour créer le rôle et la politique de service, ce qui contourne le modèle des moindres privilèges et le processus de gestion des modifications d'AMS.

CodePipeline dans la FAQ AWS Managed Services

Q : Comment puis-je demander l'accès CodePipeline à mon compte AMS ?

Demandez l'accès à CodePipeline en soumettant une demande de service pour le `customer_code_pipeline_console_role` compte concerné. Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

À ce stade, AMS Operations déploiera également ce rôle de service dans votre compte : `aws_code_pipeline_service_role_policy`.

Q : Quelles sont les restrictions d'utilisation CodePipeline sur mon compte AMS ?

Oui CodePipeline les fonctionnalités, les étapes et les fournisseurs sont limités aux éléments suivants :

1. Étape de déploiement : limitée à Amazon S3, et AWS CodeDeploy
2. Étape source : limitée à Amazon S3 AWS CodeCommit, BitBucket, et GitHub
3. Étape de construction : limitée à AWS CodeBuild, et Jenkins
4. Étape d'approbation : limitée à Amazon SNS
5. Phase de test : limitée à Jenkins AWS CodeBuild, BlazeMeter aux tests de l'interface utilisateur de Ghost Inspector, à Micro Focus StormRunner Load et à la surveillance de l'API Runscope
6. Invoke Stage : limité à Step Functions et Lambda

Note

AMS Operations sera déployé `customer_code_pipeline_lambda_policy` dans votre compte ; il doit être associé au rôle d'exécution Lambda pour la phase d'appel Lambda. Indiquez le nom du service/execution rôle Lambda avec lequel vous souhaitez ajouter cette politique. S'il n'existe aucun service/execution rôle Lambda personnalisé, AMS créera

un nouveau rôle nommé `customer_code_pipeline_lambda_execution_role`, qui sera une copie de `customer_lambda_basic_execution_role`.
`customer_code_pipeline_lambda_policy`

Q : Quels sont les prérequis ou les dépendances pour pouvoir utiliser CodePipeline mon compte AMS ?

AWS les services AWS CodeCommit pris en charge AWS CodeDeploy doivent être lancés avant ou en même temps que le lancement de CodePipeline. AWS CodeBuild

Utilisez AMS SSP pour approvisionner AWS Compute Optimizer votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS Compute Optimizer fonctionnalités directement dans votre compte géré AMS. AWS Compute Optimizer recommande des ressources AWS informatiques optimales pour vos charges de travail afin de réduire les coûts et d'améliorer les performances en utilisant le machine learning pour analyser les indicateurs d'utilisation historiques. Le surprovisionnement du calcul (Amazon EC2 et ASGs) peut entraîner des coûts d'infrastructure inutiles et le sous-provisionnement du calcul peut nuire aux performances des applications. Compute Optimizer vous aide à choisir les types d' EC2 instances Amazon optimaux, y compris celles qui font partie d'un groupe Amazon EC2 Auto Scaling, en fonction de vos données d'utilisation. Pour en savoir plus, veuillez consulter la section [AWS Compute Optimizer](#).

FAQ sur le Compute Optimizer dans AWS Managed Services

Q : Comment puis-je demander l'accès à Compute Optimizer depuis mon compte AMS ?

Demandez l'accès en soumettant un type de modification Gestion | AWS service | Service auto-approvisionné | Ajouter (révision requise) (ct-3qe6io8t6jtny). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_compute_optimizer_readonly_role` Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation de Compute Optimizer dans mon compte AMS ?

Il n'y a aucune restriction. Toutes les fonctionnalités de AWS Compute Optimizer sont disponibles dans votre compte AMS.

Q : Quels sont les prérequis ou les dépendances pour utiliser Compute Optimizer dans mon compte AMS ?

- Vous devez soumettre une RFC (Management | Other | Other | Update) autorisant AMS Ops à activer le service dans le compte. Pendant le déploiement, un rôle lié au service (SLR) est créé pour permettre la collecte de métriques et la génération de rapports. Le réflex est étiqueté « AWSService RoleForComputeOptimizer ». Pour plus d'informations, voir [Utilisation de rôles liés à un service](#) pour AWS Compute Optimizer
- CloudWatch les métriques doivent être activées pour les métriques suivantes :
 - Utilisation du processeur : pourcentage d'unités de EC2 calcul Amazon allouées qui sont utilisées sur l'instance. Cette métrique identifie la puissance de traitement requise pour exécuter une application sur une instance sélectionnée.
 - Utilisation de la mémoire : quantité de mémoire utilisée d'une manière ou d'une autre pendant la période d'échantillonnage. Cette métrique identifie la mémoire requise pour exécuter une application sur une instance sélectionnée. L'utilisation de la mémoire est analysée uniquement pour les ressources sur lesquelles l' CloudWatch agent unifié est installé. Pour plus d'informations, voir Activation de l'utilisation de la mémoire avec l' CloudWatch agent (p. 10).
 - Entrée réseau : nombre d'octets reçus par l'instance sur toutes les interfaces réseau. Cette métrique identifie le volume du trafic réseau entrant vers une seule instance.
 - Sortie réseau : nombre d'octets envoyés sur toutes les interfaces réseau par l'instance. Cette métrique identifie le volume du trafic réseau sortant à partir d'une seule instance.
 - Disque local input/output (E/S) : nombre d' input/output opérations effectuées sur le disque local. Cette métrique identifie les performances du volume racine d'une instance

Utilisez AMS SSP pour approvisionner AWS DataSync votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS DataSync fonctionnalités directement dans votre compte géré AMS. AWS DataSync déplace de grandes quantités de données en ligne entre le stockage sur site et Amazon S3, Amazon Elastic File System (Amazon Elastic File System) ou Amazon FSx. Les tâches manuelles liées aux transferts de données peuvent ralentir les migrations et alourdir les opérations informatiques. DataSync élimine ou gère automatiquement bon nombre de ces tâches, notamment la rédaction de scripts de copie, la planification et le suivi des transferts, la validation des données et l'optimisation de l'utilisation du réseau. L'agent DataSync logiciel se connecte à votre système de fichiers réseau (NFS) et à votre système de stockage SMB (Server Message Block) afin que vous n'ayez pas à modifier vos

applications. DataSync peut transférer des centaines de téraoctets et des millions de fichiers à des vitesses jusqu'à 10 fois supérieures à celles des outils open source, via Internet ou des liens. AWS Direct Connect Vous pouvez l'utiliser DataSync pour migrer des ensembles de données ou des archives actifs AWS, transférer des données vers le cloud pour une analyse et un traitement rapides, ou répliquer des données AWS pour assurer la continuité des activités.

Pour en savoir plus, veuillez consulter la section [AWS DataSync](#).

DataSync dans la FAQ AWS Managed Services

Q : Comment puis-je demander l'accès DataSync à mon compte AMS ?

Demandez l'accès en soumettant un type de modification Gestion | AWS service | Service auto-approvisionné | Ajouter (révision requise) (ct-3qe6io8t6jtny). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_datasync_console_role`

Une fois les rôles configurés dans votre compte, vous devez intégrer les rôles dans votre solution de fédération.

Le groupe de CloudWatch journaux à utiliser pour diffuser les journaux des tâches est « `/aws/datasync` ».

Q : Quelles sont les restrictions d'utilisation DataSync sur mon compte AMS ?

Toutes les fonctionnalités de AWS DataSync sont disponibles dans votre compte AMS.

Q : Quels sont les prérequis ou les dépendances pour pouvoir l'utiliser DataSync dans mon compte AMS ?

- Amazon S3 ARNs (Amazon Resource Names) est requis pour tous les compartiments S3 associés aux DataSync tâches qui seront effectuées à l'aide du rôle `customer_datasync_service_role` de DataSync service.
- Les points de terminaison VPC et les groupes de sécurité pour les DataSync agents doivent être demandés à l'aide d'une RFC avec le type de modification Management | Other | Other | Create (ct-1e1xtak34nx76) avant d'utiliser les points de terminaison VPC.
- AWS DataSync les agents s'exécutent dans AMS en tant qu'appliance. L' AWS DataSync agent est corrigé et mis à jour par le service ; pour plus de détails, consultez la [AWS DataSync FAQ](#).
- Pour lancer un AWS DataSync agent, soumettez une RFC avec le type de modification Management | Other | Other | Create (ct-1e1xtak34nx76), en demandant le déploiement de l'agent.

Fournissez l'identifiant AWS DataSync Amazon EC2 AMI, le type d'instance, le sous-réseau, le groupe de sécurité ; et faites référence à une paire de EC2 clés Amazon existante ou demandez la création d'une nouvelle paire de clés.

 Note

AMS approvisionne l' AWS DataSync agent manuellement pour le compte du client et ne nécessite pas le processus d'ingestion du WIGS sur l' AWS DataSync Amazon EC2 AMI.

Utilisez AMS SSP pour approvisionner AWS Device Farm votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS Device Farm fonctionnalités directement dans votre compte géré AMS. AWS Device Farm est un service de test d'applications qui vous permet d'améliorer la qualité de vos applications Web et mobiles en les testant sur une vaste gamme de navigateurs de bureau et de véritables appareils mobiles, sans avoir à fournir ni à gérer d'infrastructure de test. Le service vous permet d'exécuter vos tests simultanément sur plusieurs navigateurs de bureau ou sur de vrais appareils afin d'accélérer l'exécution de votre suite de tests, et génère des vidéos et des journaux pour vous aider à identifier rapidement les problèmes liés à votre application.

Pour en savoir plus, veuillez consulter la section [AWS Device Farm](#).

AWS Device Farm dans la FAQ AWS Managed Services

Q : Comment puis-je demander l'accès AWS Device Farm à mon compte AMS ?

Demandez l'accès en soumettant un type de modification Gestion | AWS service | Service auto-approvisionné | Ajouter (révision requise) (ct-3qe6io8t6jtny). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_devicefarm_role`

Une fois les rôles configurés dans votre compte, vous devez intégrer les rôles dans votre solution de fédération.

Q : Quelles sont les restrictions d'utilisation AWS Device Farm sur mon compte AMS ?

L'accès complet au AWS Device Farm service est fourni, à l'exception de l'utilisation de l'espace de noms AMS dans la balise « Name ».

Q : Quels sont les prérequis ou les dépendances pour pouvoir l'utiliser AWS Device Farm dans mon compte AMS ?

Aucune.

Utilisez AMS SSP pour approvisionner AWS Elastic Disaster Recovery votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS Elastic Disaster Recovery fonctionnalités directement dans votre compte géré AMS. AWS Elastic Disaster Recovery minimise les temps d'arrêt et les pertes de données grâce à une restauration rapide et fiable des applications sur site et dans le cloud à l'aide d'un stockage abordable, d'un calcul minimal et point-in-time d'une restauration. Vous pouvez améliorer la résilience informatique lorsque vous répliquez AWS Elastic Disaster Recovery des applications sur site ou dans le cloud exécutées sur des systèmes d'exploitation pris en charge. Utilisez le AWS Management Console pour configurer les paramètres de réplication et de lancement, surveiller la réplication des données et lancer des instances à des fins d'analyse ou de restauration.

Pour en savoir plus, veuillez consulter la section [AWS Elastic Disaster Recovery](#).

AWS Elastic Disaster Recovery dans la FAQ AWS Managed Services

Q : Comment puis-je demander l'accès AWS Elastic Disaster Recovery à mon compte AMS ?

Demandez l'accès en soumettant un type de modification Gestion | AWS service | Service auto-approvisionné | Ajouter (révision requise) (ct-3qe6io8t6jtny). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_drs_console_role`

Une fois le rôle configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions d'utilisation AWS Elastic Disaster Recovery sur mon compte AMS ?

Il n'y a aucune restriction d'utilisation AWS Elastic Disaster Recovery dans votre compte AMS.

Q : Quels sont les prérequis ou les dépendances pour pouvoir utiliser AWS Elastic Disaster Recovery mon compte AMS ?

- Une fois que vous avez accès au rôle de console, vous devez initialiser le service Elastic Disaster Recovery pour créer les rôles IAM nécessaires dans le compte.

- Vous devez soumettre le type de modification Gestion | Applications | Profil d'instance IAM | Créer (révision requise) le type de modification ct-0ixp4ch2tiu04 RFC pour créer un clone du profil d'instance et joindre la politique. `customer-mc-ec2-instance-profile` `AWSElasticDisasterRecoveryEc2InstancePolicy` Vous devez spécifier les machines auxquelles vous souhaitez associer la nouvelle politique.
- Si l'instance n'utilise pas le profil d'instance par défaut, AMS peut s'attacher `AWSElasticDisasterRecoveryEc2InstancePolicy` par automatisation.
- Vous devez utiliser une clé KMS appartenant au client pour la restauration entre comptes. La clé KMS du compte source doit être mise à jour conformément à la politique pour autoriser l'accès au compte cible. Pour plus d'informations, voir [Partager la clé de chiffrement EBS avec le compte cible](#).
- La politique des clés KMS doit être mise à jour `customer_drs_console_role` pour autoriser l'affichage de la politique si vous ne souhaitez pas changer de rôle pour l'afficher.
- Pour la reprise après sinistre entre comptes et entre régions, AMS doit configurer les comptes source et cible en tant que comptes fiables et déployer les rôles de [secours et de redimensionnement via AWS](#) . AWS CloudFormation

Utilisez AMS SSP pour approvisionner AWS Elemental MediaConvert votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS Elemental MediaConvert fonctionnalités directement dans votre compte géré AMS. AWS Elemental MediaConvert est un service de transcodage vidéo basé sur des fichiers doté de fonctionnalités adaptées à la diffusion. Il vous permet de créer du contenu video-on-demand (VOD) pour la diffusion et la diffusion sur plusieurs écrans à grande échelle. Le service combine des fonctionnalités vidéo et audio avancées avec une interface de services Web et une pay-as-you-go tarification simples. Vous pouvez ainsi vous concentrer sur la création d'expériences multimédias captivantes sans avoir à vous soucier de la complexité liée à la création et à l'exploitation de votre propre infrastructure de traitement vidéo. AWS Elemental MediaConvert

Pour en savoir plus, veuillez consulter la section [AWS Elemental MediaConvert](#).

MediaConvert dans la FAQ AWS Managed Services

Q : Comment puis-je demander l'accès MediaConvert à mon compte AMS ?

Demandez l'accès en soumettant un type de modification Gestion | AWS service | Service auto-approvisionné | Ajouter (révision requise) (ct-3qe6io8t6jtny). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_mediaconvert_author_role` Une fois configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Un deuxième rôle sera fourni `customer_MediaConvert_Default_Role`, qui sera utilisé pour lire à partir du compartiment S3 source et écrire la sortie MediaConvert dans le compartiment S3 de destination, ainsi que pour appeler la passerelle API au cas où vous auriez besoin d'une gestion des droits numériques (DRM).

Q : Quelles sont les restrictions d'utilisation MediaConvert sur mon compte AMS ?

Il n'y a aucune restriction quant à l'utilisation de MediaConvert dans AMS.

Q : Quels sont les prérequis ou les dépendances pour pouvoir l'utiliser MediaConvert dans mon compte AMS ?

Il n'y a aucun prérequis ni aucune dépendance à utiliser MediaConvert dans votre compte AMS.

Utilisez AMS SSP pour approvisionner AWS Elemental MediaLive votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS Elemental MediaLive fonctionnalités directement dans votre compte géré AMS. AWS Elemental MediaLive est un service de traitement vidéo en direct de qualité télévisuelle. Il vous permet de créer des flux vidéo de haute qualité destinés à être diffusés sur des télévisions et des appareils multi-écrans connectés à Internet, tels que des tablettes TVs, des smartphones et des décodeurs connectés. Le service fonctionne en encodant vos flux vidéo en direct en temps réel, en prenant une source vidéo en direct de plus grande taille et en la compressant en versions plus petites pour la distribuer à vos spectateurs. Avec AWS Elemental MediaLive, vous pouvez facilement configurer des diffusions pour des événements en direct et des chaînes 24 heures sur 24, 7 jours sur 7, grâce à des fonctionnalités de diffusion avancées, à une haute disponibilité et pay-as-you-go à des prix. AWS Elemental MediaLive vous permet de vous concentrer sur la création d'expériences vidéo en direct captivantes pour vos spectateurs, sans la complexité liée à la création et à l'exploitation d'une infrastructure de traitement vidéo adaptée à la diffusion.

Pour en savoir plus, veuillez consulter la section [AWS Elemental MediaLive](#).

MediaLive dans la FAQ AWS Managed Services

Q : Comment puis-je demander l'accès MediaLive à mon compte AMS ?

Demandez l'accès en soumettant un type de modification Gestion | AWS service | Service auto-approvisionné | Ajouter (révision requise) (ct-3qe6io8t6jtny). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_medialive_author_role`

Dans le cadre de cette RFC, un deuxième rôle est déployé dans votre compte ; ce `customer_medialive_service_role` rôle peut être attribué à vos chaînes Media Live et à vos entrées pour interagir avec d'autres services tels qu'Amazon S3 et CloudWatch Logs. MediaStore

Une fois les rôles configurés dans votre compte, vous devez les intégrer dans votre solution de fédération.

Q : Quelles sont les restrictions d'utilisation MediaLive sur mon compte AMS ?

Il n'y a aucune restriction quant à l'utilisation de MediaLive dans AMS.

Q : Quels sont les prérequis ou les dépendances pour pouvoir l'utiliser MediaLive dans mon compte AMS ?

Il n'y a aucun prérequis ni aucune dépendance à utiliser MediaLive dans votre compte AMS.

Utilisez AMS SSP pour approvisionner AWS Elemental MediaPackage votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS Elemental MediaPackage fonctionnalités directement dans votre compte géré AMS. AWS Elemental MediaPackage prépare et protège de manière fiable votre vidéo en vue de sa diffusion sur Internet. À partir d'une seule entrée vidéo, AWS Elemental MediaPackage crée des flux vidéo formatés pour être lus sur des téléphones portables TVs, des ordinateurs, des tablettes et des consoles de jeux connectés. Il permet de mettre en œuvre facilement des fonctionnalités vidéo populaires pour les spectateurs (redémarrage, pause, retour en arrière, etc.), comme celles que l'on trouve couramment sur le site. DVRs AWS Elemental MediaPackage peut également protéger votre contenu à l'aide de la gestion des droits numériques (DRM). AWS Elemental MediaPackage évolue automatiquement en fonction de la charge, de sorte que vos spectateurs bénéficieront toujours d'une expérience exceptionnelle sans que vous ayez à prévoir avec précision à l'avance la capacité dont vous aurez besoin.

Pour en savoir plus, veuillez consulter la section [AWS Elemental MediaPackage](#).

MediaPackage dans la FAQ AWS Managed Services

Q : Comment puis-je demander l'accès AWS Elemental MediaPackage à mon compte AMS ?

Demandez l'accès en soumettant un type de modification Gestion | AWS service | Service auto-approvisionné | Ajouter (révision requise) (ct-3qe6io8t6jtny). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_mediapackage_author_role` Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Un deuxième rôle sera fourni `customer_mediapackage_service_role`, qui pourra être attribué à vos chaînes Media Live et à vos entrées pour interagir avec d'autres services tels que S3 et Secrets Manager.

Q : Quelles sont les restrictions d'utilisation MediaPackage sur mon compte AMS ?

Il n'y a aucune restriction quant à l'utilisation de MediaPackage dans AMS.

Q : Quels sont les prérequis ou les dépendances pour pouvoir utiliser MediaPackage mon compte AMS ?

Il n'y a aucun prérequis ni aucune dépendance à utiliser MediaPackage dans votre compte AMS.

Utilisez AMS SSP pour approvisionner AWS Elemental MediaStore votre compte AMS

Note

Après mûre réflexion, AWS a pris la décision de mettre fin à ses activités MediaStore, à compter du 13 novembre 2025. Si vous êtes un client actif de MediaStore, vous pouvez l'utiliser normalement MediaStore jusqu'au 13 novembre 2025, date à laquelle le support du service prendra fin. Après cette date, vous ne pourrez plus utiliser MediaStore aucune des fonctionnalités fournies par ce service.

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS Elemental MediaStore fonctionnalités directement dans votre compte géré AMS. AWS Elemental MediaStore est un service

AWS de stockage optimisé pour les médias. Il vous offre les performances, la cohérence et la faible latence nécessaires pour diffuser du contenu vidéo en direct. AWS Elemental MediaStore fait office de magasin d'origine dans votre flux de travail vidéo. Ses capacités de haute performance répondent aux besoins des charges de travail de diffusion multimédia les plus exigeantes, associées à un stockage rentable à long terme. Pour en savoir plus, veuillez consulter la section [AWS Elemental MediaStore](#).

MediaStore dans la FAQ AWS Managed Services

Q : Comment puis-je demander l'accès MediaStore à mon compte AMS ?

Demandez l'accès à MediaStore en soumettant une RFC avec le type de modification Management | AWS service | Self-provisioned Service | Add (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_mediastore_author_role`. Dans le cadre de cette RFC, un deuxième rôle est déployé dans votre compte ; `MediaStoreAccessLogs` rôle, qui est utilisé par le MediaStore service pour enregistrer l'activité CloudWatch, si vous choisissez d'activer cette fonctionnalité. Une fois qu'il est configuré dans votre compte, vous devez intégrer les rôles dans votre solution de fédération.

À ce stade, AMS Operations déploiera également ce rôle de service dans votre compte : `aws_code_pipeline_service_role_policy`.

Q : Quelles sont les restrictions d'utilisation MediaStore sur mon compte AMS ?

Il n'y a aucune restriction quant à l'utilisation de MediaStore dans AMS.

Q : Quels sont les prérequis ou les dépendances pour pouvoir l'utiliser MediaStore dans mon compte AMS ?

Il n'y a aucun prérequis ni aucune dépendance à utiliser MediaStore dans votre compte AMS.

Utilisez AMS SSP pour approvisionner AWS Elemental MediaTailor votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS Elemental MediaTailor fonctionnalités directement dans votre compte géré AMS. AWS Elemental MediaTailor permet aux fournisseurs de vidéos d'insérer des publicités ciblées individuellement dans leurs flux vidéo sans sacrifier le niveau de diffusion quality-of-service. Ainsi AWS Elemental MediaTailor, les spectateurs de votre vidéo en direct ou à la demande reçoivent chacun un flux qui combine votre contenu

avec des publicités personnalisées pour eux. Mais contrairement aux autres solutions publicitaires personnalisées, l'intégralité de AWS Elemental MediaTailor votre flux (vidéo et publicités) est diffusée avec une qualité vidéo de qualité supérieure afin d'améliorer l'expérience de vos spectateurs. AWS Elemental MediaTailor fournit des rapports automatisés basés à la fois sur les indicateurs de diffusion des publicités côté client et côté serveur, afin de mesurer avec précision les impressions publicitaires et le comportement des spectateurs. Vous pouvez facilement monétiser les événements de visionnage inattendus et très demandés, sans frais initiaux. AWS Elemental MediaTailor II améliore également les taux de diffusion des publicités, vous aidant à gagner plus d'argent avec chaque vidéo, et il fonctionne avec une plus grande variété de réseaux de diffusion de contenu, de serveurs de décision publicitaire et d'appareils clients.

Pour en savoir plus, veuillez consulter la section [AWS Elemental MediaTailor](#).

MediaTailor dans la FAQ AWS Managed Services

Q : Comment puis-je demander l'accès MediaTailor à mon compte AMS ?

Demandez l'accès à MediaTailor en soumettant une RFC avec le type de modification Management | AWS service | Self-provisioned Service | Add (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte : `customer-mediatailor-role` Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions d'utilisation MediaTailor sur mon compte AMS ?

Il n'y a aucune restriction quant à l'utilisation de MediaTailor dans AMS.

Q : Quels sont les prérequis ou les dépendances pour pouvoir utiliser MediaTailor mon compte AMS ?

Il n'y a aucun prérequis ni aucune dépendance à utiliser MediaTailor dans votre compte AMS.

Utilisez AMS SSP pour approvisionner AWS Global Accelerator votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités de Global Accelerator directement dans votre compte géré AMS. Global Accelerator est un service de couche réseau dans lequel vous créez des accélérateurs pour améliorer la disponibilité et les performances des applications Internet utilisées par un public mondial. Pour en savoir plus, consultez [Global Accelerator](#).

FAQ sur l'accélérateur mondial dans AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander la configuration de Global Accelerator sur mon compte AMS ?

Demandez l'accès via la soumission de la RFC sur les AWS services (Management | AWS service | Self-provisioned Service). Grâce à cette RFC, les rôles IAM suivants seront fournis dans votre compte : `customer_global_accelerator_console_role` Une fois le provisionnement effectué dans votre compte, vous devez intégrer le rôle de console dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation de Global Accelerator sur mon compte AMS ?

Global Accelerator est un service mondial qui prend en charge les points de terminaison situés dans plusieurs AWS régions, qui sont répertoriées dans le [tableau des AWS régions](#).

Q : Quelles sont les conditions préalables ou les dépendances pour utiliser Global Accelerator dans mon compte AMS ?

Lorsque vous configurez votre accélérateur avec Global Accelerator, vous associez les adresses IP statiques à des points de terminaison régionaux dans une ou plusieurs AWS régions. Pour les accélérateurs standard, les points de terminaison sont les équilibreurs de charge réseau, les équilibreurs de charge d'application, les instances EC2 Amazon ou les adresses IP élastiques. Pour les accélérateurs de routage personnalisés, les points de terminaison sont des sous-réseaux de cloud privé virtuel (VPC) dotés d'une ou de plusieurs instances. EC2

Utilisez AMS SSP pour approvisionner AWS Glue votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS Glue fonctionnalités directement dans votre compte géré AMS. AWS Glue est un service d'extraction, de transformation et de chargement (ETL) entièrement géré qui vous aide à préparer et à charger vos données à des fins d'analyse. Vous pouvez créer et exécuter une tâche ETL en quelques clics dans le AWS Management Console. Vous AWS Glue pointez sur vos données stockées sur AWS, vous découvrez AWS Glue vos données et vous stockez les métadonnées associées (par exemple, définition de table et schéma) dans le AWS Glue Data Catalog. Une fois cataloguées, vos données sont immédiatement consultables, interrogeables et disponibles pour les actions ETL. Pour en savoir plus, veuillez consulter la section [AWS Glue](#).

AWS Glue dans la FAQ AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander AWS Glue à être configuré dans mon compte AMS ?

Demandez l'accès à AWS Glue en soumettant une RFC auprès du service Management | AWS | Service auto-provisionné | Ajouter un type de modification (ct-1w8z66n899dct). Cette RFC attribue les rôles IAM suivants à votre compte :

- `customer_glue_console_role`
- `customer_glue_service_role`

Les rôles précédents incluent les politiques jointes suivantes :

- `customer_glue_secrets_manager_policy`
- `customer_glue_deny_policy`

Une fois les rôles configurés dans votre compte, vous devez les intégrer à votre solution de fédération.

Pour accéder aux crawlers, aux jobs et aux points de terminaison de développement (rôles nécessaires pour des cas d'utilisation spécifiques), soumettez une RFC avec le formulaire Deployment | Advanced stack components | Identity and Access Management (IAM) | Create entity or policy (ct-3dpd8mdd9jn1r).

Q : Quelles sont les restrictions d'utilisation AWS Glue sur mon compte AMS ?

Il n'y a aucune restriction. Toutes les fonctionnalités de AWS Glue sont disponibles dans votre compte AMS. Pour un environnement interactif dans lequel vous pouvez créer et tester des scripts ETL, utilisez Notebooks on AWS Glue Studio. AWS Glue Les sessions interactives et les carnets de tâches sont des fonctionnalités sans serveur AWS Glue que vous pouvez utiliser AWS Glue et qui utilisent le rôle de AWS Glue service.

AWS Glue avant la version 2.0 : les AWS Glue blocs-notes sont une ressource non gérée qui lance des EC2 instances Amazon dans un compte. Il est recommandé de lancer vos propres EC2 instances Amazon et d'installer le logiciel nécessaire pour prendre en charge l'environnement et le développement d'un ordinateur portable. Pour plus d'informations, consultez [Tutoriel : Configuration d'un bloc-notes Apache Zeppelin local pour tester et déboguer des scripts ETL et Utilisation de points de terminaison de développement pour le développement de scripts](#).

Q : Quels sont les prérequis ou les dépendances pour pouvoir utiliser AWS Glue mon compte AMS ?

AWS Glue dépend d'Amazon S3 et CloudWatch de CloudWatch Logs. Les dépendances transitives varient en fonction des sources de données, et d'autres fonctionnalités du AWS Glue service peuvent interagir avec elles (par exemple : Amazon Redshift, Amazon RDS, Athena).

Utilisez AMS SSP pour approvisionner AWS Lake Formation votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS Lake Formation fonctionnalités directement dans votre compte géré AMS. AWS Lake Formation est un service qui permet de configurer facilement un lac de données sécurisé en quelques jours. Un lac de données est un référentiel centralisé, organisé et sécurisé qui stocke toutes vos données, à la fois sous leur forme originale et préparée pour l'analyse. Un lac de données vous permet de décomposer des silos de données et de combiner différents types d'analyses pour obtenir des informations afin de prendre des décisions éclairées.

Créer un lac de données avec Lake Formation est aussi simple que définir des sources de données et les politiques d'accès aux données et de sécurité que vous souhaitez appliquer. Lake Formation vous aide ensuite à collecter et à cataloguer des données à partir de bases de données et de stockage d'objets, à les déplacer vers votre nouveau lac de données Amazon S3, à nettoyer et à classer vos données à l'aide d'algorithmes d'apprentissage automatique, ainsi qu'à sécuriser l'accès à vos données sensibles. Vos utilisateurs peuvent accéder à un catalogue de données centralisé (pour plus de détails, voir [AWS Glue FAQ](#)) qui décrit les ensembles de données disponibles et leur utilisation appropriée. Vos utilisateurs exploitent ensuite ces ensembles de données avec les services d'analyse et d'apprentissage automatique de leur choix, tels qu'[Amazon Redshift](#), [Amazon Athena](#) et (en version bêta) [Amazon EMR](#) pour Apache Spark. Lake Formation s'appuie sur les capacités disponibles dans [AWS Glue](#).

Pour en savoir plus, veuillez consulter la section [AWS Lake Formation](#).

FAQ sur la formation des lacs dans AWS Managed Services

Q : Comment puis-je demander l'accès AWS Lake Formation à mon compte AMS ?

Demandez l'accès en soumettant un type de modification Gestion | AWS service | Service auto-approvisionné | Ajouter (révision requise) (ct-3qe6io8t6jtny). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_lakeformation_data_analyst_role` Une fois qu'il est configuré dans votre compte, vous devez intégrer les rôles dans votre solution de fédération.

En outre, les deux rôles suivants sont facultatifs :

- `customer_lakeformation_admin_role`
- `customer_lakeformation_workflow_role`

Pour les autorisations d'administrateur, vous pouvez choisir d'intégrer le rôle dans le `customer_lakeformation_admin_role` cadre du même type de modification SSPS (ct-3qe6io8t6jtny).

Si vous souhaitez créer des plans dans la AWS Lake Formation console, vous devez soumettre une RFC Management | Other | Other (ct-1e1xtak34nx76) pour déployer le `customer_lakeformation_workflow_role`. Dans la RFC, vous devez fournir le nom du compartiment S3 si le compartiment est une source lors de la création des Blueprints. Le bucket S3 est applicable si le type de Blueprint est AWS CloudTrail Classic Load Balancer Logs ou Application Load Balancer Logs.

Q : Quelles sont les restrictions d'utilisation AWS Lake Formation sur mon compte AMS ?

Toutes les fonctionnalités de Lake Formation sont disponibles dans AMS.

Q : Quels sont les prérequis ou les dépendances pour pouvoir l'utiliser AWS Lake Formation dans mon compte AMS ?

Lake Formation s'intègre au AWS Glue service, AWS Glue les utilisateurs ne peuvent donc accéder qu'aux bases de données et aux tables sur lesquelles ils ont des autorisations Lake Formation. En outre, les utilisateurs d' AWS Athena et d'Amazon Redshift peuvent uniquement interroger les bases de données et AWS Glue les tables sur lesquelles ils disposent des autorisations Lake Formation.

Utilisez AMS SSP pour approvisionner AWS Lambda votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS Lambda fonctionnalités directement dans votre compte géré AMS. AWS Lambda vous permet d'exécuter du code sans provisionner ni gérer de serveurs. Vous ne payez que pour le temps de calcul que vous consommez, il n'y a aucun frais lorsque votre code n'est pas en cours d'exécution. Avec Lambda, vous pouvez exécuter du code pour pratiquement n'importe quel type d'application ou de service principal, le tout sans aucune administration. Téléchargez votre code et Lambda se charge de tout ce qui est nécessaire pour exécuter et faire évoluer votre code avec une haute disponibilité. Vous pouvez configurer votre code pour qu'il se déclenche automatiquement à partir d'autres AWS services, ou l'appeler directement depuis n'importe quelle application Web ou mobile. Pour en savoir plus, veuillez consulter la section [AWS Lambda](#).

FAQ sur Lambda dans AWS Managed Services

Q : Comment puis-je demander l'accès AWS Lambda à mon compte AMS ?

Demandez l'accès en soumettant un type de modification Gestion | AWS service | Service auto-provisionné | Ajouter (révision requise) (ct-3qe6io8t6jtny). Cette RFC attribue les rôles IAM suivants à votre compte : `customer_lambda_admin_role` et `customer_lambda_basic_execution_role`. Une fois qu'il est configuré dans votre compte, vous devez intégrer les rôles dans votre solution de fédération.

Q : Quelles sont les restrictions d'utilisation AWS Lambda sur mon compte AMS ?

- Une fonction Lambda est conçue pour être invoquée par des sources d'événements. Pour obtenir la liste des services pouvant être utilisés comme source d'événements Lambda, consultez la section [Utilisation AWS Lambda avec d'autres services](#). Tous ces services ne sont actuellement pas disponibles dans les comptes AMS. Si vous avez besoin d'un service qui n'est pas disponible, utilisez votre AMS CSDM pour signaler une exception.
- Par défaut, AMS vous fournit un rôle d'initiation Lambda de base contenant les `AWSXrayWriteOnlyAccess` autorisations `AWSLambdaBasicExecutionRole` et ; pour plus d'informations, voir Rôle [AWS Lambda d'initiation](#). Si vous avez besoin d'autorisations supplémentaires, telles que la possibilité de fournir des fonctions Lambda au sein de votre VPC AMS, soumettez une RFC avec le type de modification Management | AWS service | Self-provisioned Service | Add (révision requise) (ct-3qe6io8t6jtny).

Q : Quels sont les prérequis ou les dépendances pour pouvoir utiliser AWS Lambda mon compte AMS ?

Il n'existe aucun prérequis ni aucune dépendance pour commencer AWS Lambda ; toutefois, selon votre cas d'utilisation spécifique, vous pouvez avoir besoin d'accéder à d'autres AWS services pour créer des sources d'événements, ou d'autorisations supplémentaires pour que votre fonction puisse effectuer diverses actions. Si des autorisations supplémentaires sont nécessaires, soumettez une RFC avec le type de modification Management | AWS service | Self-provisioned Service | Add (révision requise) (ct-3qe6io8t6jtny).

Q : Que dois-je faire pour exécuter une fonction Lambda dans l'un de mes comptes ?

Pour déployer une fonction Lambda dans un compte principal, suivez les instructions suivantes :

- Assurez-vous que SSPS for AWS Lambda est intégré.

- Aucune restriction spécifique n'interdit ce déploiement sous la responsabilité d'AMS, tant que vos ressources AMS sont protégées et conformes.
- Si vous souhaitez qu'AMS crée la fonction Lambda, vous devez d'abord utiliser le rôle SSPS fourni. AWS Lambda Ensuite, si vous souhaitez toujours bénéficier de l'assistance AMS pour déployer ou prendre en charge la fonction, contactez votre autorité de certification et lancez le processus hors champ (OOS).

Utilisez AMS SSP pour approvisionner AWS License Manager votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS License Manager fonctionnalités directement dans votre compte géré AMS. AWS License Manager s'intègre aux AWS services pour simplifier la gestion des licences sur plusieurs AWS comptes, catalogues informatiques et sur site, via un seul AWS compte. AWS License Manager permet aux administrateurs de créer des règles de licence personnalisées qui imitent les termes de leurs contrats de licence, puis d'appliquer ces règles lorsqu'une instance d'Amazon EC2 est lancée. Les règles de cette AWS License Manager section vous permettent de limiter une violation de licence en empêchant physiquement le lancement de l'instance ou en informant les administrateurs de cette violation. Pour en savoir plus, veuillez consulter la section [AWS License Manager](#).

FAQ sur le License Manager dans AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander AWS License Manager à être configuré dans mon compte AMS ?

Demandez l'accès à AWS License Manager en soumettant une RFC avec le type de modification Management | AWS Service | Self-provisioned Service | Add (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_license_manager_role` Une fois que le rôle License Manager IAM est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions d'utilisation AWS License Manager sur mon compte AMS ?

Vous pouvez associer des AWS License Manager règles aux AMIs vôtres (filtrées sous « Je suis propriétaire »). Si vous choisissez d'appliquer une association de limites à une AMI (exemple : cette AMI ne peut prendre en charge que 100 vCPU) et que vous dépassez la limite, les futurs lancements avec cette AMI sont bloqués et renvoient un message d'erreur indiquant « Aucune

licence disponible ». C'est le comportement prévu de ce service (ne pas autoriser l'épuisement des licences). Si vous avez dépassé la limite mais que vous devez relancer l'AMI, vous devez modifier la règle configurée dans AWS License Manager.

Q : Quels sont les prérequis ou les dépendances pour pouvoir utiliser AWS License Manager mon compte AMS ?

Il n'y a aucun prérequis ni aucune dépendance à utiliser AWS License Manager dans votre compte AMS.

Utilisez AMS SSP pour approvisionner AWS Migration Hub votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS Migration Hub fonctionnalités directement dans votre compte géré AMS. AWS Migration Hub fournit un emplacement unique où vous pouvez suivre la progression des migrations d'applications entre plusieurs AWS solutions partenaires. L'utilisation de Migration Hub vous permet de choisir les outils de migration AWS et les outils de migration partenaires qui répondent le mieux à vos besoins, tout en offrant une visibilité sur l'état des migrations dans l'ensemble de votre portefeuille d'applications. Migration Hub fournit également des indicateurs clés et la progression des applications individuelles, quels que soient les outils utilisés pour les migrer. Cela vous permet d'obtenir rapidement des mises à jour sur l'état d'avancement de toutes vos migrations, d'identifier et de résoudre facilement les problèmes, et de réduire le temps et les efforts globaux consacrés à vos projets de migration. Pour en savoir plus, veuillez consulter la section [AWS Migration Hub](#).

FAQ sur le Hub de migration dans AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès à Migration Hub depuis mon compte AMS ?

Demandez l'accès à Migration Hub en soumettant une RFC avec le type de modification Management | AWS Service | Self-provisioned Service | Add (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_migrationhub_author_role` Une fois configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions applicables à Migration Hub ?

Aucune.

Q : Quels sont les prérequis pour activer Migration Hub ?

Il n'y a aucune condition préalable pour commencer à utiliser Migration Hub dans votre compte AMS. Cependant, des autorisations extérieures à Migration Hub peuvent être requises lors de la gestion du service, par exemple pour écrire des autorisations sur Amazon S3 pour télécharger les informations du serveur.

Utilisez AMS SSP pour approvisionner AWS Outposts votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS Outposts fonctionnalités directement dans votre compte géré AMS. AWS Outposts est un service entièrement géré qui étend AWS l'infrastructure, les AWS services et les outils à pratiquement tous les centres de données, espaces de colocation ou installations sur site pour une expérience hybride cohérente. APIs AWS Outposts convient aux charges de travail qui nécessitent un accès à faible latence aux systèmes sur site, un traitement de données local ou un stockage de données local. Pour en savoir plus, veuillez consulter la section [AWS Outposts](#).

AWS Outposts dans la FAQ AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander AWS Outposts à être configuré dans mon compte AMS ?

Demandez l'accès à AWS Outposts en soumettant une RFC avec le type de modification Management | AWS Service | Self-provisioned Service | Add (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_outposts_role` Une fois le rôle configuré dans votre compte, vous devez l'intégrer à votre solution de fédération.

Q : Quelles sont les restrictions d'utilisation AWS Outposts sur mon compte AMS ?

Il n'y a aucune restriction quant à l'utilisation de AWS Outposts dans votre compte AMS.

Q : Quels sont les prérequis ou les dépendances pour pouvoir utiliser AWS Outposts mon compte AMS ?

Il n'y a aucun prérequis ni aucune dépendance à utiliser AWS Outposts dans votre compte AMS.

Utilisez AMS SSP pour approvisionner AWS Resilience Hub votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS Resilience Hub fonctionnalités directement dans votre compte géré AMS. AWS Resilience Hub vous aide à préparer

et à protéger vos AWS applications de manière proactive contre les perturbations. Le Resilience Hub propose une évaluation et une validation de la résilience qui s'intègrent au cycle de vie de votre développement logiciel afin de détecter les faiblesses en matière de résilience. Resilience Hub vous aide à estimer si vos applications peuvent atteindre les objectifs de temps de restauration (RTO) et de point de reprise (RPO), et vous aide à résoudre les problèmes avant leur mise en production. Après avoir déployé une AWS application en production, vous pouvez utiliser Resilience Hub pour continuer à suivre le niveau de résilience de votre application. En cas de panne, Resilience Hub envoie une notification à l'opérateur pour lancer le processus de reprise associé.

AWS Resilience Hub dans la FAQ AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès AWS Resilience Hub à mon compte AMS ?

Demandez l'accès à Resilience Hub en soumettant une RFC avec le type de modification Management | AWS Service | Self-provisioned Service | Add (ct-1w8z66n899dct). Cette RFC fournit les rôles et politiques IAM suivants à votre compte :

Rôles IAM

- `customer_resiliencehub_console_role`
- `customer_resiliencehub_service_role`

Stratégies

- `customer_resiliencehub_console_policy`
- `customer_resiliencehub_service_policy`

Une fois le rôle configuré dans votre compte, vous devez l'intégrer `customer_resiliencehub_console_role` dans votre solution de fédération.

Q : Quelles sont les restrictions d'utilisation AWS Resilience Hub sur mon compte AMS ?

Il n'y a aucune restriction. Toutes les fonctionnalités de Resilience Hub sont disponibles sur votre compte AMS.

Q : Quels sont les prérequis ou les dépendances pour pouvoir utiliser AWS Resilience Hub mon compte AMS ?

Il n'existe aucune condition préalable ni dépendance pour utiliser Resilience Hub dans votre compte AMS.

Utilisez AMS SSP pour approvisionner AWS Secrets Manager votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS Secrets Manager fonctionnalités directement dans votre compte géré AMS. AWS Secrets Manager vous aide à protéger les secrets nécessaires pour accéder à vos applications, services et ressources informatiques. Le service vous permet de faire pivoter, de gérer et de récupérer facilement les informations d'identification de base de données, les clés d'API et autres secrets tout au long de leur cycle de vie. Les utilisateurs et les applications récupèrent les secrets en appelant le Secrets Manager APIs, ce qui élimine le besoin de coder en dur les informations sensibles en texte brut. Secrets Manager propose une rotation secrète avec intégration intégrée à Amazon RDS, Amazon Redshift et Amazon DocumentDB. En outre, le service est extensible à d'autres types de secrets, notamment les clés d'API et les OAuth jetons. Pour en savoir plus, veuillez consulter la section [AWS Secrets Manager](#).

Note

Par défaut, les opérateurs AMS peuvent accéder aux secrets chiffrés à AWS Secrets Manager l'aide de la AWS KMS clé par défaut du compte (CMK). Si vous souhaitez que vos secrets ne soient pas accessibles à AMS Operations, utilisez une clé CMK personnalisée, avec une politique de clé AWS Key Management Service (AWS KMS) qui définit les autorisations appropriées aux données stockées dans le secret.

FAQ sur le gestionnaire des Secrets Manager dans AWS Managed Services

Q : Comment puis-je demander l'accès AWS Secrets Manager à mon compte AMS ?

Demandez l'accès à Secrets Manager en soumettant une RFC avec le type de modification Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny). Cette RFC attribue les rôles IAM suivants à votre compte : `customer_secrets_manager_console_role` et `customer-rotate-secrets-lambda-role` `customer_secrets_manager_console_role` est utilisé comme rôle d'administrateur pour fournir et gérer les secrets, et `customer-rotate-secrets-lambda-role` est utilisé comme rôle d'exécution Lambda pour les fonctions Lambda

qui font pivoter les secrets. Une fois qu'il est configuré dans votre compte, vous devez intégrer le `customer_secrets_manager_console_role` rôle dans votre solution de fédération.

Q : Quelles sont les restrictions d'utilisation AWS Secrets Manager sur mon compte AMS ?

Toutes les fonctionnalités de AWS Secrets Manager sont disponibles dans votre compte AMS, ainsi que la fonctionnalité de rotation automatique des secrets. Notez toutefois que la configuration de votre rotation à l'aide de « Créer une nouvelle fonction Lambda pour effectuer une rotation » n'est pas prise en charge car elle nécessite des autorisations élevées pour créer AWS CloudFormation la pile (création d'un rôle IAM et d'une fonction Lambda), ce qui contourne le processus de gestion des modifications. AMS Advanced prend uniquement en charge la fonction « Utiliser une fonction Lambda existante pour effectuer une rotation », dans laquelle vous gérez vos fonctions Lambda pour faire pivoter les secrets à l'aide du AWS rôle d'administrateur Lambda SSPS. AMS Advanced ne crée ni ne gère Lambda pour alterner les secrets.

Q : Quels sont les prérequis ou les dépendances pour pouvoir utiliser AWS Secrets Manager mon compte AMS ?

Les espaces de noms suivants sont réservés à l'usage d'AMS et ne sont pas disponibles dans le cadre de l'accès direct à AWS Secrets Manager :

- `arn:aws:secretsmanager :*:secret:ams-shared/*`
- `arn:aws:secretsmanager :*:secret:customer-shared/*`
- `arn:aws:secretsmanager :*:secret:ams/*`

Partage de clés à l'aide de Secrets Manager (AMS SSPS)

Le partage de secrets avec AMS dans le texte brut d'une RFC, d'une demande de service ou d'un rapport d'incident entraîne un incident de divulgation d'informations et AMS expédie ces informations du dossier et vous demande de régénérer les clés.

Vous pouvez utiliser [AWS Secrets Manager](#) (Secrets Manager) sous cet espace de noms, `customer-shared`.

FAQ sur le partage de clés à l'aide de Secrets Manager

Q : Quels types de secrets doivent être partagés à l'aide de Secrets Manager ?

Quelques exemples sont les clés pré-partagées pour la création d'un VPN, les clés confidentielles telles que les clés d'authentification (IAM, SSH), les clés de licence et les mots de passe.

Q : Comment puis-je partager les clés avec AMS à l'aide de Secrets Manager ?

1. Connectez-vous à la console AWS de gestion à l'aide de votre accès fédéré et du rôle approprié :

pour SALZ, le `Customer_ReadOnly_Role`

pour MALZ, `AWSSecretsManagerSharedPolicy`.
2. Accédez à la [AWS Secrets Manager console](#) et cliquez sur Enregistrer un nouveau secret.
3. Sélectionnez Other type of secrets (Autres types de secrets).
4. Entrez la valeur secrète sous forme de texte brut et utilisez le chiffrement KMS par défaut. Cliquez sur Next (Suivant).
5. Entrez le nom et la description du secret, le nom commence toujours par customer-shared/. Par exemple customer-shared/mykey2022. Cliquez sur Next (Suivant).
6. Laissez la rotation automatique désactivée, cliquez sur Suivant.
7. Vérifiez et cliquez sur Store pour enregistrer le secret.
8. Répondez-nous en indiquant le nom secret par le biais de la demande de service, du RFC ou du rapport d'incident, afin que nous puissions identifier et récupérer le secret.

Q : Quelles sont les autorisations requises pour partager les clés à l'aide de Secrets Manager ?

SALZ : recherchez la politique IAM `customer_secrets_manager_shared_policy` gérée et vérifiez que le document de politique est le même que celui joint dans les étapes de création ci-dessous. Vérifiez que la politique est attachée aux rôles IAM suivants : `Customer_ReadOnly_Role`.

MALZ : Vérifiez que le `AWSSecretsManagerSharedPolicy`, est attaché au `AWSSecretsManagerSharedPolicy` rôle qui vous autorise à effectuer l'`GetSecretValue` action dans l'espace de `ams-shared` noms.

Exemple :

```
{
  "Action": "secretsmanager:*",
  "Resource": [
```

```
"arn:aws:secretsmanager:*:*:secret:ams-shared/*",
"arn:aws:secretsmanager:*:*:secret:customer-shared/*"
],
"Effect": "Allow",
"Sid": "AllowAccessToSharedNameSpaces"
}
```

Note

Les autorisations requises sont accordées lors de l'ajout en AWS Secrets Manager tant que service provisionné en libre-service.

Utilisez AMS SSP pour approvisionner AWS Security Hub votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS Security Hub fonctionnalités directement dans votre compte géré AMS. AWS Security Hub vous fournit une vue complète de l'état de votre sécurité interne AWS et de votre conformité aux normes et aux meilleures pratiques du secteur de la sécurité. Security Hub centralise et hiérarchise les résultats de sécurité et de conformité provenant de l'ensemble des AWS comptes, des services et des partenaires tiers pris en charge pour vous aider à analyser vos tendances en matière de sécurité et à identifier les problèmes de sécurité les plus prioritaires. Pour en savoir plus, veuillez consulter la section [AWS Security Hub](#).

FAQ sur le Security Hub dans AWS Managed Services

Q : Comment puis-je demander l'accès AWS Security Hub à mon compte AMS ?

Demandez l'accès à Security Hub en soumettant une RFC avec le type de modification Management | AWS service | Self-provisioned Service | Add (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_securityhub_role` Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation de Security Hub sur mon compte AMS ?

La fonctionnalité d'archivage a été considérée comme un risque potentiel en matière de sécurité et d'exploitation et a été limitée dans le cadre du rôle de sécurité du service auto-approvisionné.

Q : Quels sont les prérequis ou les dépendances pour pouvoir utiliser AWS Security Hub mon compte AMS ?

Il n'y a aucun prérequis ni aucune dépendance à utiliser AWS Security Hub dans votre compte AMS.

Utilisez AMS SSP pour approvisionner AWS Service Catalog AppRegistry votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AppRegistry fonctionnalités directement dans votre compte géré AMS. AppRegistry permet de rechercher des applications, de créer des rapports et de gérer des actions à partir d'un emplacement central. Les créateurs créent rarement des applications dans un seul AWS compte. Ils séparent généralement les ressources des applications par phases du cycle de vie, telles que le développement, les tests et la production. AppRegistry vous permet de regrouper et de visualiser toutes vos collections de ressources sur les AWS comptes que vous définissez.

Vous pouvez y stocker vos AWS applications, l'ensemble des ressources associées à vos applications et les groupes d'attributs d'applications. AppRegistry Pour en savoir plus, consultez la section [Qu'est-ce que c'est AppRegistry](#).

FAQ : AWS Service Catalog AppRegistry dans AMS

Q : Comment puis-je demander l'accès AWS Service Catalog AppRegistry à mon compte AMS ?

Demandez l'accès à AppRegistry en soumettant une RFC avec le type de modification Management | AWS Service | Self-provisioned Service | Ajouter (révision requise) (ct-3qe6io8t6jtny). Cette RFC attribue le rôle IAM suivant à votre compte : `customer-appregistry-console-role` Une fois le rôle configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions d'utilisation AWS Service Catalog AppRegistry sur mon compte AMS ?

L'accès complet au AppRegistry service est fourni, à l'exception de l'utilisation de l'espace de noms AMS dans la 'Name' balise.

Q : Quels sont les prérequis ou les dépendances pour pouvoir l'utiliser AWS Service Catalog AppRegistry dans mon compte AMS ?

Il n'y a aucun prérequis ni aucune dépendance à utiliser AppRegistry dans votre compte AMS.

Utilisez AMS SSP pour approvisionner AWS Shield Advanced votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS Shield Advanced fonctionnalités directement dans votre compte géré AMS. AWS Shield Advanced est un service géré de protection par déni de service (DDoS) distribué qui protège les applications qui s'exécutent sur AWS. Shield Advanced fournit une détection permanente et des mesures d'atténuation automatiques en ligne qui minimisent les temps d'arrêt et la latence des applications. Il n'est donc pas nécessaire de contacter le AWS Support pour bénéficier de la protection S. DDo Il existe deux niveaux AWS Shield : Standard et Advanced ; AMS propose Shield Advanced. Pour en savoir plus, consultez [Shield Advanced](#).

Tous les AWS clients bénéficient des protections automatiques de AWS Shield Standard, sans frais supplémentaires. AWS Shield Standard protège contre les attaques de couche DDo S les plus courantes et fréquentes qui ciblent votre site Web ou vos applications. Lorsque vous utilisez AWS Shield Standard Amazon CloudFront et Amazon Route 53, vous bénéficiez d'une protection de disponibilité complète contre toutes les attaques d'infrastructure connues (couches 3 et 4).

Pour bénéficier de niveaux de protection supérieurs contre les attaques ciblant vos applications exécutées sur les ressources Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing (ELB) CloudFront AWS Global Accelerator, Amazon et Amazon Route 53, vous pouvez vous abonner à AWS Shield Advanced.

Outre les protections associées au réseau et à la couche de transport AWS Shield Standard, il AWS Shield Advanced fournit une détection et une atténuation supplémentaires contre les attaques DDo S sophistiquées et de grande envergure, une visibilité en temps quasi réel sur les attaques et une intégration à AWS WAF un pare-feu d'applications Web. AWS Shield Advanced vous donne également accès à l'équipe d' AWS Shield intervention (SRT) 24 heures sur 24, 7 jours sur 7 et vous protège contre les pics liés au DDo S dans vos frais Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing (Elastic Load Balancing) CloudFront AWS Global Accelerator, Amazon et Amazon Route 53.

FAQ sur Shield Advanced dans AWS Managed Services

Q : Comment puis-je demander l'accès à Shield Advanced depuis mon compte AMS ?

Demandez l'accès à Shield Advanced en soumettant une RFC avec le type de modification Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Cette RFC attribue

les rôles IAM suivants à votre compte : `customer_shield_role` et `aws_drt_shield_role`
Une fois les rôles configurés dans votre compte, vous devez intégrer les rôles dans votre solution de fédération.

Une fois les rôles déployés dans votre compte, vous pouvez utiliser le `customer_shield_role` pour confirmer votre abonnement AWS Shield Advanced à votre compte.

 Note

Notez que des frais mensuels et un engagement d'un an sont associés à l'utilisation de AWS Shield Advanced. En outre, l'utilisation AWS Shield Advanced dans AMS autorise AMS à passer à la AWS Shield (SRT), qui peut modifier les règles de votre pare-feu d'application Web (AWS WAF) lors d'incidents de déni de service (DDoS) distribués intensifiés. Ces modifications seront effectuées en coordination avec AMS.

Q : Quelles sont les restrictions relatives à l'utilisation de Shield Advanced sur mon compte AMS ?

Bien qu'il ne s'agisse pas d'une restriction, vous devez comprendre que l'utilisation de Shield Advanced déploie `aws_drt_shield_role`, ce qui permet aux AWS Shield équipes (SRT) d'apporter des modifications d'urgence aux AWS WAF règles des comptes AMS lors d'incidents S intensifiés DDoS. Cela est recommandé par AMS pour remédier le plus rapidement possible aux attaques DDoS, et cela se produirait après une escalade de l'AMS vers le SRT.

Q : Quels sont les prérequis ou les dépendances pour utiliser Shield Advanced dans mon compte AMS ?

Il n'existe aucune condition préalable ni dépendance pour utiliser Shield Advanced dans votre compte AMS.

Utilisez AMS SSP pour approvisionner AWS Snowball Edge votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités de Snowball Edge directement dans votre compte géré par AMS. Snowball Edge est une solution de transport de données à l'échelle du pétaoctet qui utilise des appareils conçus pour être sécurisés, afin de transférer de grandes quantités de données vers et depuis le cloud. AWS Snowball Edge répond aux défis courants liés aux transferts de données à grande échelle, notamment les coûts de réseau

élevés, les longs délais de transfert et les problèmes de sécurité. Vous pouvez utiliser Snowball Edge pour migrer des données analytiques, des données génomiques, des vidéothèques, des référentiels d'images, des sauvegardes et pour archiver une partie des fermetures de centres de données, du remplacement de bandes magnétiques ou des projets de migration d'applications. Le transfert de données à l'aide de Snowball Edge est simple, rapide, plus sécurisé et ne coûte que cinq fois moins cher que le transfert de données via Internet haut débit.

Avec Snowball Edge, vous n'avez pas besoin d'écrire de code ni d'acheter de matériel pour transférer vos données. Commencez par utiliser la console AWS de gestion pour [créer un Job d'importation](#) pour Snowball, et un appareil Snowball vous sera automatiquement expédié. Une fois arrivé, connectez l'appareil à votre réseau local, téléchargez et exécutez le client Snowball (« Client ») pour établir une connexion, puis utilisez le client pour sélectionner les répertoires de fichiers que vous souhaitez transférer vers l'appareil. Le client chiffre et transfère ensuite les fichiers sur l'appareil à grande vitesse. Une fois le transfert terminé et l'appareil prêt à être retourné, l'étiquette d'expédition E Ink est automatiquement mise à jour et vous pouvez suivre l'état de la tâche avec Amazon Simple Notification Service (Amazon SNS), par SMS ou directement dans la console. Pour en savoir plus, veuillez consulter la section [AWS Snowball Edge](#).

FAQ sur Snowball Edge dans AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès AWS Snowball Edge à mon compte AMS ?

La mise en œuvre de Snowball Edge dans AMS se fait en deux étapes :

1. Soumettez un type de modification Management | Other | Other | Create (ct-1e1xtak34nx76) et demandez un rôle de service pour Snowball Edge pour votre compte AMS.
2. Demandez l'accès utilisateur en soumettant un type de gestion | AWS service | service auto-approvisionné | Ajouter un type de modification (ct-1w8z66n899dct). Cette RFC fournit les rôles IAM suivants à votre compte : `customer_snowball_console_role`, `customer_snowball_export_role`, et `customer_snowball_import_role`. Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions d'utilisation AWS Snowball Edge sur mon compte AMS ?

Toutes les fonctionnalités du AWS Snowball Edge sont disponibles dans votre compte AMS.

Q : Quels sont les prérequis ou les dépendances pour pouvoir utiliser AWS Snowball Edge mon compte AMS ?

Vous devez disposer du compte de rôle de service comme indiqué ci-dessus.

Utilisez AMS SSP pour approvisionner AWS Step Functions votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS Step Functions fonctionnalités directement dans votre compte géré AMS. AWS Step Functions est un service Web qui vous permet de coordonner les composants des applications distribuées et des microservices à l'aide de flux de travail visuels. Vous développez les applications à partir de composants individuels qui exécutent chacun une fonction discrète, ou tâche, vous permettant de mettre à l'échelle et de modifier les applications rapidement. Step Functions fournit un moyen fiable de coordonner les composants et de parcourir les fonctions de votre application. Step Functions propose une console graphique permettant de visualiser les composants de votre application sous forme d'une série d'étapes. Il déclenche et suit automatiquement chaque étape, et réessaie en cas d'erreur, afin que votre application s'exécute dans l'ordre et comme prévu, à chaque fois. Step Functions enregistre l'état de chaque étape. Ainsi, en cas de problème, vous pouvez diagnostiquer et corriger rapidement les problèmes. Pour en savoir plus, veuillez consulter la section [AWS Step Functions](#).

FAQ sur les Step Functions dans AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès AWS Step Functions à mon compte AMS ?

Demandez l'accès à AWS Step Functions en soumettant une RFC auprès de Management | AWS Service | Service auto-approvisionné | Ajouter un type de modification (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_step_functions_role` Une fois configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions d'utilisation AWS Step Functions sur mon compte AMS ?

Toutes les fonctionnalités du AWS Step Functions sont disponibles dans votre compte AMS.

Q : Quels sont les prérequis ou les dépendances pour pouvoir l'utiliser AWS Step Functions dans mon compte AMS ?

Au moment de l'exécution, le rôle utilisé par Step Functions doit avoir accès aux services utilisés par la fonction step. Par exemple, une fonction d'étape peut dépendre des fonctions Lambda. Une

personne qui crée une fonction d'étape est susceptible de créer des fonctions Lambda en même temps et devra également demander l'accès à ce service.

Utilisez AMS SSP pour approvisionner le AWS Systems Manager Parameter Store sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités du AWS Systems Manager Parameter Store directement dans votre compte géré AMS. AWS Systems Manager Parameter Store fournit un stockage hiérarchique sécurisé pour la gestion des données de configuration et la gestion des secrets. Vous pouvez stocker des données telles que des mots de passe, des chaînes de base de données et des codes de licence en tant que valeurs de paramètres. Vous pouvez stocker ces valeurs sous forme de texte brut ou de données chiffrées. Vous pouvez ensuite faire référence à ces valeurs en utilisant le nom unique que vous avez spécifié lors de la création du paramètre. Hautement évolutif, disponible et durable, Parameter Store est soutenu par le AWS cloud. Pour en savoir plus, consultez [AWS Systems Manager Parameter Store](#).

Note

Si vous souhaitez un magasin de secrets dédié avec gestion du cycle de vie, [Utilisez AMS SSP pour approvisionner AWS Secrets Manager votre compte AMS](#) utilisez-le plutôt que Parameter Store. Secrets Manager vous aide à répondre à vos exigences de sécurité et de conformité en vous permettant de transférer automatiquement les secrets. Secrets Manager propose une intégration intégrée pour MySQL, PostgreSQL et Amazon Aurora sur Amazon RDS, qui est extensible à d'autres types de secrets en personnalisant les fonctions Lambda.

AWS Systems Manager FAQ sur le stockage des paramètres dans AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès à Systems Manager Parameter Store depuis mon compte AMS ?

Demandez l'accès au magasin de AWS Systems Manager paramètres en soumettant une RFC à l'adresse Management | AWS service | Self-provisioned service | Ajouter un type de modification (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte .:

`customer_systemsmanager_parameterstore_console_role` Une fois configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions relatives à l'utilisation de AWS Systems Manager Parameter Store dans mon compte AMS ?

Vous devez utiliser des clés AWS gérées ; l'accès est limité à la création de clés KMS personnalisées. Toutefois, si une clé personnalisée est requise, soumettez une RFC pour créer une clé gérée par le client (CMK) en utilisant le type Deployment | Advanced Stack Components | KMS Key | Create change (ct-1d84keiri1jhg) avec ce rôle IAM comme valeur pour les paramètres et. `customer_systemsmanager_parameterstore_console_role`
`IAMPrincipalsRequiringDecryptPermissions`
`IAMPrincipalsRequiringEncryptPermissionsPrincipal` Une fois la clé KMS créée, vous pouvez créer une chaîne sécurisée à l'aide de celle-ci.

Q : Quels sont les prérequis ou les dépendances pour utiliser AWS Systems Manager Parameter Store dans mon compte AMS ?

Il n'y a aucune condition préalable ; toutefois, le magasin de paramètres SSM dépend de KMS pour créer une chaîne sécurisée afin que vous puissiez chiffrer et déchiffrer leurs valeurs stockées dans le magasin de paramètres.

Utilisez AMS SSP pour provisionner AWS Systems Manager l'automatisation dans votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités AWS Systems Manager d'automatisation directement dans votre compte géré AMS. AWS Systems Manager L'automatisation simplifie les tâches courantes de maintenance et de déploiement des instances Amazon Elastic Compute Cloud et d'autres AWS ressources à l'aide de runbooks, d'actions et de quotas de service. Il vous permet de créer, d'exécuter et de surveiller des automatisations à grande échelle. Un Systems Manager Automation est un type de document Systems Manager qui définit les actions que Systems Manager exécute sur vos instances gérées. Un runbook que vous utilisez pour effectuer des tâches de maintenance et de déploiement courantes, telles que l'exécution de commandes ou de scripts d'automatisation au sein de vos instances gérées. Systems Manager inclut des fonctionnalités qui vous aident à cibler de grands groupes d'instances à l'aide des balises Amazon Elastic Compute Cloud et des contrôles de vitesse qui vous aident à déployer les modifications conformément aux limites que vous définissez. Les runbooks sont écrits en utilisant la notation JavaScript d'objet (JSON) ou YAML. Toutefois, l'outil Document Builder de la console Systems Manager Automation permet de créer un runbook sans avoir à utiliser JSON ou YAML. Vous

pouvez également utiliser les runbooks fournis par Systems Manager avec des étapes prédéfinies adaptées à vos besoins. Pour en savoir plus, consultez la section [Utilisation des runbooks](#) dans AWS Systems Manager la documentation.

Note

Bien que Systems Manager Automation prenne en charge 20 types d'actions pouvant être utilisés dans le runbook, vous pouvez utiliser un nombre limité d'actions lors de la création du runbook dans votre compte AMS Advanced. De même, un nombre limité de runbooks fournis par Systems Manager peuvent être utilisés soit directement, soit depuis votre propre runbook. Pour plus de détails, consultez les restrictions dans la FAQ suivante.

AWS Systems Manager FAQ sur l'automatisation dans AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès à Systems Manager Automation depuis mon compte AMS ?

Demandez l'accès à AWS Systems Manager l'automatisation en soumettant une RFC à l'adresse [Management | AWS service | Self-provisioned Service | Ajouter un type de modification \(ct-1w8z66n899dct\)](#). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_systemsmanager_automation_console_role` Une fois configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les limites de l'utilisation de l' AWS Systems Manager automatisation dans mon compte AMS ?

Vous devez créer votre runbook, avec un ensemble limité d'actions prises en charge par Systems Manager à des fins d'automatisation, uniquement pour exécuter des and/or scripts de commandes dans vos instances gérées. Les actions qui s'offrent à vous ainsi que les restrictions éventuelles sont décrites ci-dessous.

AWS Systems Manager Limites de l'automatisation

Action	Description	Limitation
lois : <code>assertAwsResource</code> Propriété —	Affirmer un état de AWS ressource ou un état d'événement	EC2 Instances uniquement

Action	Description	Limitation
aws:aws:branche —	Exécuter des étapes d'automatisation conditionnelles	Aucune limitation
AWS : CreateTags —	Création de balises pour les AWS ressources	Uniquement pour les runbooks d'automatisation SSM dont vous êtes l'auteur
AWS : Exécuter l'automatisation —	Exécuter une autre automatisation	Uniquement le runbook d'automatisation que vous avez créé
AWS : ExecuteScript —	Exécuter un script	Seul script qui n'effectue aucun appel d'API vers aucun service
aws:pause —	Suspendre une automatisation	Aucune limitation
AWS : Exécuter une commande —	Exécuter une commande sur une instance gérée	En utilisant uniquement le document fourni par System Manager - AWS- RunShellScript et AWS- RunPowerShellScript
aws:sleep —	Retarder une automatisation	Aucune limitation
lois : waitForAws ResourceProperty —	Attendre sur une propriété AWS de ressource	EC2 Instances uniquement

Vous pouvez également choisir d'exécuter une commande ou un script directement avec les runbooks AWS RunShellScript et AWS fournis par Systems Manager RunPowerShellScript en utilisant la fonctionnalité « Run Command » depuis la console Systems Manager. Vous pouvez également imbriquer ces runbooks dans votre runbook, ce qui permet une validation préalable and/or supplémentaire ou toute logique d'automatisation complexe.

Le rôle respecte le principe du moindre privilège et fournit uniquement l'autorisation requise pour créer, exécuter et récupérer les détails d'exécution des runbooks destinés à exécuter des and/or scripts de commande dans vos instances gérées. Il ne fournit aucune autorisation pour les autres fonctionnalités fournies par le AWS Systems Manager service. Bien que cette fonctionnalité vous permette de créer des runbooks automatisés, l'exécution des runbooks ne peut pas être ciblée pour les ressources détenues par AMS.

Q : Quels sont les prérequis ou les dépendances pour utiliser AWS Systems Manager Automation dans mon compte AMS ?

Il n'y a aucune condition préalable ; toutefois, vous devez vous assurer que les contrôles de and/or conformité de vos processus internes sont respectés lors de la création de runbooks. Nous recommandons également de tester minutieusement les runbooks avant de les exécuter par rapport aux ressources de production.

Q : La politique Systems Manager peut-elle **customer_systemsmanager_automation_policy** être associée à d'autres rôles IAM ?

Non, contrairement aux autres services activés par l'auto-provisionnement, cette politique ne peut être attribuée qu'au rôle par défaut provisionné.
`customer_systemsmanager_automation_console_role`

Contrairement aux politiques des autres rôles SSPS, cette politique SSPS SSM ne peut pas être partagée avec d'autres rôles IAM personnalisés, car ce service AMS sert uniquement à exécuter des commandes ou des scripts d'automatisation au sein de vos instances gérées. Si ces autorisations étaient autorisées à être associées à d'autres rôles IAM personnalisés, éventuellement avec des autorisations sur d'autres services, la portée des actions autorisées pourrait s'étendre aux services gérés et potentiellement réduire le niveau de sécurité de votre compte.

Pour évaluer toute demande de modification (RFCs) par rapport à nos normes techniques AMS, contactez votre architecte cloud ou votre responsable de prestation de services respectif, consultez les [revues de sécurité RFC](#).

Note

AWS Systems Manager vous permet d'utiliser des runbooks partagés avec votre compte. Nous vous recommandons de faire preuve de prudence et de faire preuve de diligence raisonnable lorsque vous utilisez des runbooks partagés et de vérifier le contenu pour comprendre comment command/scripts ils s'exécutent avant d'exécuter les runbooks. Pour

plus de détails, reportez-vous à la section [Meilleures pratiques pour les documents SSM partagés](#).

Utilisez AMS SSP pour approvisionner AWS Transfer Family votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités (Transfer AWS Transfer Family Family) directement dans votre compte géré AMS. AWS Transfer Family est un AWS service entièrement géré qui vous permet de transférer des fichiers via le protocole SFTP (Secure File Transfer Protocol), vers et depuis le stockage Amazon Simple Storage Service (Amazon S3). SFTP est également connu sous le nom de Secure Shell (SSH) File Transfer Protocol. Le protocole SFTP est utilisé dans les flux de travail d'échange de données dans différents secteurs d'activité, comme les services financiers, la santé, la publicité et la vente au détail.

Avec AWS SFTP, vous avez accès à un serveur SFTP AWS sans avoir à exécuter d'infrastructure de serveur. Vous pouvez utiliser ce service pour migrer vos flux de travail basés sur SFTP AWS tout en conservant les clients et les configurations de vos utilisateurs finaux tels quels. Vous associez d'abord votre nom d'hôte au point de terminaison du serveur SFTP, puis vous ajoutez vos utilisateurs et leur attribuez le niveau d'accès approprié. Ensuite, les demandes de transfert de vos utilisateurs sont traitées directement depuis le point de terminaison de votre serveur AWS SFTP. Pour en savoir plus [AWS Transfer for SFTP](#), voir également [Créer un serveur compatible SFTP](#).

AWS Transfer for SFTP dans la FAQ AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès AWS Transfer for SFTP à mon compte AMS ?

Demandez l'accès à AWS Transfer for SFTP en soumettant une RFC auprès de Management | AWS Service | Service auto-approvisionné | Ajouter un type de modification (ct-1w8z66n899dct). Grâce à cette RFC, les rôles IAM suivants, ainsi qu'une politique, sont fournis dans votre compte :

- `customer_transfer_author_role`. Ce rôle est conçu pour vous permettre de gérer le service SFTP via la console.
- `customer_transfer_sftp_server_logging_role`. Ce rôle est conçu pour être attaché au serveur SFTP. Il permet au serveur SFTP d'y extraire les journaux. CloudWatch

- `customer_transfer_sftp_user_role`. Ce rôle est conçu pour être attaché aux utilisateurs SFTP. Il permet aux utilisateurs SFTP d'interagir avec le compartiment S3.
- `policy_customer_transfer_scope_down_policy`. Cette politique est une politique de portée réduite qui peut être appliquée à l'utilisateur SFTP pour limiter son accès au compartiment S3 à ses dossiers personnels.
- `customer_transfer_sftp_efs_user_role`. Ce rôle est conçu pour être attaché aux utilisateurs SFTP. Il permet aux utilisateurs du SFTP d'interagir avec le système de fichiers EFS.

Une fois qu'il est configuré dans votre compte, vous devez intégrer les rôles dans votre solution de fédération.

Q : Quelles sont les restrictions d'utilisation AWS Transfer for SFTP sur mon compte AMS ?

AWS Le transfert pour la configuration SFTP est limité aux ressources sans les préfixes « AMS- » ou « MC- » afin d'empêcher toute modification de l'infrastructure AMS.

Q : Quels sont les prérequis ou les dépendances pour pouvoir utiliser AWS Transfer for SFTP mon compte AMS ?

- Vous devez disposer d'un compartiment Amazon S3 dont le nom contient le mot clé « transfer » avant de créer le AWS Transfer for SFTP serveur et les utilisateurs.
- Pour utiliser un « Customer Identify Provider », vous devez déployer l'API Gateway, la fonction Lambda et votre référentiel utilisateur (AD, Secrets Manager, etc.). Pour plus d'informations, voir [Activer l'authentification par mot de passe pour AWS Transfer for SFTP l'utilisation AWS Secrets Manager et l'utilisation des fournisseurs d'identité](#).

Utilisez AMS SSP pour approvisionner AWS Transit Gateway votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS Transit Gateway fonctionnalités directement dans votre compte géré AMS. AWS Transit Gateway est un service qui vous permet de connecter votre Amazon Virtual Private Cloud (VPCs) et vos réseaux locaux à une passerelle unique. Au fur et à mesure que vous augmentez le nombre de charges de travail exécutées AWS, vous devez être en mesure de faire évoluer vos réseaux sur plusieurs comptes et sur Amazon VPCs pour suivre le rythme de cette croissance. Aujourd'hui, vous pouvez connecter des paires d'Amazon VPCs en utilisant le peering. Cependant, la gestion de la point-to-point connectivité sur de nombreux Amazon VPCs, sans la possibilité de gérer de manière centralisée les politiques de

connectivité, peut s'avérer coûteuse et fastidieuse sur le plan opérationnel. Pour la connectivité sur site, vous devez connecter votre AWS VPN à chaque Amazon VPC individuel. La création de cette solution peut prendre beaucoup de temps et être difficile à gérer lorsque le nombre VPCs atteint des centaines. Pour en savoir plus, veuillez consulter la section [AWS Transit Gateway](#).

AWS Transit Gateway dans la FAQ AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès AWS Transit Gateway à mon compte AMS ?

Demandez l'accès à AWS Transit Gateway en soumettant une RFC auprès de Management | AWS Service | Service auto-approvisionné | Ajouter un type de modification (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_tgw_console_role`. Une fois configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions d'utilisation AWS Transit Gateway sur mon compte AMS ?

Toutes les fonctionnalités de AWS Transit Gateway sont disponibles sur votre compte de zone d'atterrissage à compte unique AMS, à l'exception des modifications des tables de routage pour le routage Transit Gateway. Demandez des modifications de table de routage en soumettant un type Management | Other | Other | Create change (ct-1e1xtak34nx76).

Note

Ce service n'est pris en charge que pour les zones d'atterrissage à compte unique (SALZ), et non pour les zones d'atterrissage multicomptes (MALZ).

Q : Quels sont les prérequis ou les dépendances pour pouvoir utiliser AWS Transit Gateway mon compte AMS ?

Il n'y a aucun prérequis ni aucune dépendance à utiliser AWS Transit Gateway dans votre compte AMS.

Utilisez AMS SSP pour configurer le AWS WAF Web Application Firewall dans votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS WAF fonctionnalités directement dans votre compte géré AMS. AWS WAF est un pare-feu pour applications Web (AWS

WAF) qui aide à protéger vos applications Web contre les exploits Web courants susceptibles d'affecter la disponibilité des applications, de compromettre la sécurité ou de consommer des ressources excessives. AWS WAF vous permet de contrôler le trafic à autoriser ou à bloquer vers vos applications Web en définissant des règles de sécurité Web personnalisables. Vous pouvez les utiliser AWS WAF pour créer des règles personnalisées qui bloquent les modèles d'attaque courants, tels que l'injection SQL ou les scripts intersites, ainsi que des règles conçues pour votre application spécifique.

Pour en savoir plus, voir [AWS WAF - Web Application Firewall](#).

AMS ne prend pas en charge la surveillance (CloudWatch alarmes/événements/alertes MMS) pour AWS WAF. En raison de la nature de AWS WAF, vous devez créer des règles personnalisées pour vos applications ; AMS ne peut pas quantifier et créer des alarmes pour vous, sans le contexte de votre application. Pour en savoir plus, voir [AWS WAF - Web Application Firewall](#).

AWS WAF dans la FAQ AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander AWS WAF à être configuré dans mon compte AMS ?

Demandez l'accès à AWS WAF en soumettant une RFC auprès du service Management | AWS | Service auto-provisionné | Ajouter un type de modification (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_waf_role` Une fois le rôle AWS WAF IAM configuré dans votre compte, vous devez l'intégrer dans votre solution de fédération.

Q : Quelles sont les restrictions d'utilisation AWS WAF ?

Une fois les autorisations accordées, vous disposez de toutes les fonctionnalités de AWS WAF.

Q : Quels sont les prérequis ou les dépendances nécessaires à l'utilisation ? AWS WAF

Il n'y a aucun prérequis ni aucune dépendance à utiliser AWS WAF dans votre compte AMS.

Utilisez AMS SSP pour approvisionner AWS Well-Architected Tool votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS Well-Architected Tool fonctionnalités directement dans votre compte géré AMS. AWS Well-Architected Tool Cela vous aide à examiner l'état de vos charges de travail et à les comparer aux meilleures pratiques

AWS architecturales les plus récentes. L'outil est basé sur le [AWS Well-Architected Framework](#), développé pour aider les architectes du cloud à créer une infrastructure d'applications sécurisée, performante, résiliente et efficace. Ce framework fournit une approche cohérente pour évaluer les architectures, a été utilisé dans des dizaines de milliers d'exams de charge de travail menés par l'équipe d'architecture AWS des solutions et fournit des conseils pour aider à mettre en œuvre des conceptions qui s'adaptent aux besoins des applications au fil du temps. Pour en savoir plus, veuillez consulter la section [AWS Well-Architected Tool](#).

AWS WA Tool dans la FAQ AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès AWS Well-Architected Tool à mon compte AMS ?

Demandez l'accès à AWS Well-Architected Tool en soumettant une RFC auprès du service Management | AWS | Service auto-provisionné | Ajouter un type de modification (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_well_architected_tool_console_admin_role` Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Q : Quelles sont les restrictions d'utilisation AWS Well-Architected Tool sur mon compte AMS ?

Toutes les fonctionnalités du AWS Well-Architected Tool sont disponibles dans votre compte AMS.

Q : Quels sont les prérequis ou les dépendances pour pouvoir l'utiliser AWS Well-Architected Tool dans mon compte AMS ?

Il n'y a aucun prérequis ni aucune dépendance à utiliser AWS Well-Architected Tool dans votre compte AMS.

Utilisez AMS SSP pour approvisionner AWS X-Ray votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités (AWS X-Ray X-Ray) directement dans votre compte géré AMS. AWS X-Ray aide les développeurs à analyser et à déboguer les applications distribuées de production, telles que celles créées à l'aide d'une architecture de microservices. Avec X-Ray, vous pouvez comprendre les performances de votre application et de ses services sous-jacents, afin d'identifier et de résoudre les causes profondes des problèmes et des erreurs de performance. X-Ray fournit une end-to-end vue des demandes au fur et à mesure qu'elles transitent dans votre application et affiche une carte des composants sous-

jacents de votre application. Vous pouvez utiliser X-Ray pour analyser à la fois des applications en développement et en production, qu'il s'agisse d'applications simples à trois niveaux ou d'applications de microservices complexes comprenant des milliers de services. Pour en savoir plus, veuillez consulter la section [AWS X-Ray](#).

FAQ sur X-Ray dans AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès AWS X-Ray à mon compte AMS ?

Demandez l'accès en soumettant un type de modification Management | AWS Service | Autoprovisionné | Add (ct-1w8z66n899dct). Cette RFC attribue le rôle IAM suivant à votre compte : `customer_xray_console_role`. Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération. De plus, vous devez être en mesure `customer_xray_daemon_write_instance_profile` de transférer les données de vos EC2 instances Amazon vers X-Ray. Ce profil d'instance est créé lorsque vous recevez le `customer_xray_console_role`.

Vous pouvez envoyer une demande de service à AMS Operations pour l'attribuer `customer_xray_daemon_write_policy` au profil d'instance existant, ou vous pouvez utiliser le profil d'instance créé lorsque AMS Operations active X-Ray pour vous.

Q : Quelles sont les restrictions d'utilisation AWS X-Ray sur mon compte AMS ?

Toutes les fonctionnalités de AWS X-Ray sont disponibles dans votre compte AMS, à l'exception du chiffrement avec la clé AWS KMS (clé KMS). AWS X-Ray chiffre toutes les données de trace par défaut. Par défaut, X-Ray chiffre les traces et les données associées au repos. Si vous devez chiffrer des données au repos avec une clé, vous pouvez choisir une clé KMS AWS gérée (aws/xray) ou une clé KMS gérée par le client. Pour la clé KMS gérée par le client pour le chiffrement X-Ray, soumettez un type de modification Management | Other | Other | Create (ct-1e1xtak34nx76).

Q : Quels sont les prérequis ou les dépendances pour pouvoir utiliser AWS X-Ray mon compte AMS ?

AWS X-Ray dépend d'Amazon S3 et de CloudWatch Logs CloudWatch, qui sont déjà implémentés dans les comptes AMS. Les dépendances transitives varient en fonction des sources de données et des autres AWS services avec AWS X-Ray lesquels les fonctionnalités peuvent interagir (par exemple, Amazon Redshift, Amazon RDS, Athena).

Utilisez AMS SSP pour provisionner une machine virtuelle Import/Export dans votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder à la machine virtuelle Import/Export capabilities directement depuis votre compte géré AMS. Import/Export La machine virtuelle vous permet d'importer facilement des images de machines virtuelles de votre environnement existant vers des EC2 instances Amazon et de les réexporter vers votre environnement sur site. Cette offre vous permet de tirer parti de vos investissements existants dans les machines virtuelles que vous avez créées pour répondre à vos exigences en matière de sécurité informatique, de gestion des configurations et de conformité en intégrant ces machines virtuelles dans Amazon EC2 sous forme d' ready-to-use instances. Vous pouvez également réexporter les instances importées vers votre infrastructure de virtualisation sur site, ce qui vous permet de déployer des charges de travail sur l'ensemble de votre infrastructure informatique. Pour en savoir plus, consultez [VM Import/Export](#).

FAQ Import/Export sur les machines virtuelles dans AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès à la machine virtuelle Import/Export dans mon compte AMS ?

Demandez l'accès à la machine virtuelle Import/Export en soumettant une RFC à l'adresse Management | AWS Service | Self-provisioned Service | Ajouter un type de modification (ct-1w8z66n899dct). Cette RFC fournit la politique IAM suivante à votre compte .:

customer_vmimport_policy Une fois qu'il est configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.

Un rôle supplémentaire, le rôle VM Import/Export Service, est requis pour que le service puisse effectuer des actions sur votre compte.

Q : Quelles sont les restrictions relatives à l'utilisation de VM Import/Export dans mon compte AMS ?

- Les fonctionnalités permettant d'importer des images de machine et des volumes de données personnalisés sont toutes deux disponibles dans AMS VM Import/Export. Cependant, les autorisations accordées à S3 ont été limitées afin de limiter les actions aux compartiments correspondant au nom customer-vmimport-* afin de limiter l'accès aux informations du compte.
- L'importation d'images et de clichés est prise en charge dans AMS VM Import/Export. Cependant, les fonctionnalités d'importation et d'exportation d'instances ne sont pas disponibles en raison de mesures de sécurité.

- En outre, la fonctionnalité d'exportation a été désactivée afin d'atténuer le risque lié à l'exportation de données sensibles et restreintes.

Q : Quels sont les prérequis ou les dépendances pour utiliser VM Import/Export dans mon compte AMS ?

- Vous devez fournir une image disque compatible à importer dans l' AWS environnement. Pour plus d'informations, consultez la section [Import/Export Exigences relatives aux machines virtuelles](#).
- La machine virtuelle Import/Export n'est pas accessible via la AWS console. Vous devez accéder à ce service via le AWS CLI Outils AWS pour PowerShell, ou le AWS SDKs. Vous pouvez également demander un profil d'instance en soumettant le type de modification ct-117rmp64d5mvpb :
Deployment | Advanced stack components | Identity and Access Management (IAM) | Create instance profile. EC2 Ce profil d'instance permet aux outils d'exécuter des commandes à partir d'une instance.

Mode géré par le client

Le mode géré par le client d'AWS Managed Services (AMS) fournit un modèle de gouvernance flexible qui peut être adapté à vos besoins. Cela peut être considéré comme une option de secours pour les services et applications qu'AMS n'est pas en mesure de gérer pour vous. AMS n'exploite pas d'infrastructure hébergée dans des comptes créés selon ce mode. Toutefois, vous pouvez tirer parti de la gestion centralisée de plusieurs comptes dans ce mode. Les fonctionnalités de la zone d'atterrissage multi-comptes suivantes peuvent être exploitées dans ce mode :

- Déploiement automatique du compte
- Connectivité via Transit Gateway dans un compte réseau
- Bibliothèque de règles de configuration AMS
- Stocker des copies des journaux dans le compte de connexion
- Agrégation des alertes Guard Duty gérées par le client sur le compte Security
- Facturation consolidée
- Activation de politiques de contrôle des services personnalisées.

Par exemple : si vous souhaitez exécuter des charges de travail sur Ubuntu Pro, qui n'est pas un système d'exploitation géré par AMS, vous pouvez utiliser un compte géré par le client pour l'héberger. Vous pouvez également consolider les charges de travail par le biais de comptes gérés

par les clients, afin de bénéficier de la réduction globale sur les Instances/Sharing plans réservés disponible grâce au partage au sein d'une organisation AWS.

Commencer à utiliser le mode géré par le client

Le mode AMS Customer Managed est disponible via un compte spécial d'application de zone d'atterrissage multi-comptes.

Pour plus de détails, notamment sur la façon de créer un compte d'application géré par le client, consultez la section [Comptes d'applications gérés par le client](#).

AMS et AWS Service Catalog

Service Catalog in AWS Managed Services (AMS) permet aux entreprises de créer et de gérer des catalogues de services informatiques AWS et aux administrateurs informatiques de créer, gérer et distribuer des catalogues de produits approuvés aux utilisateurs finaux de leurs comptes, qui peuvent ensuite accéder aux produits dont ils ont besoin sur un portail de services personnalisé. Les administrateurs peuvent contrôler quels utilisateurs ont accès à chaque produit afin de garantir le respect des politiques commerciales de l'organisation. Les administrateurs peuvent également configurer des rôles afin que les utilisateurs finaux aient uniquement besoin d'un accès IAM à Service Catalog pour déployer des ressources approuvées. Service Catalog permet à votre entreprise de bénéficier d'une agilité accrue et de coûts réduits, car les utilisateurs finaux peuvent trouver et lancer uniquement les produits dont ils ont besoin à partir d'un catalogue que vous contrôlez.

Service Catalog vous propose une alternative au processus de demande de modification (RFC) AMS pour le provisionnement et la mise à jour des ressources dans vos comptes gérés par AMS. AMS gère toutes les tâches opérationnelles d'infrastructure nécessaires pour exécuter AWS à grande échelle pour toutes les ressources d'infrastructure mises en service via Service Catalog, notamment la sécurité, la conformité, le provisionnement, la disponibilité, les correctifs, la surveillance, les alertes, les rapports, la réponse aux incidents et l'optimisation des coûts. L'utilisation de Service Catalog dans votre compte géré AMS vous fournit un mécanisme permettant de gérer de manière centralisée les services informatiques couramment déployés et vous aide à obtenir une gouvernance cohérente tout en permettant aux utilisateurs de déployer rapidement uniquement les services informatiques approuvés dont ils ont besoin dans leurs environnements gérés.

Commencer à utiliser Service Catalog

Pour commencer à utiliser Service Catalog dans AMS, soumettez une demande de service via la console AMS pour demander l'accès à Service Catalog. Lors de la soumission de la

demande, trois rôles IAM seront déployés sur votre/vos compte (s) ainsi qu'une pile gérée par AMS contenant la CloudFormation macro qui invoque l'AMS Transform (décrite précédemment) afin que nous puissions enregistrer les produits dans nos systèmes et effectuer des opérations sur l'infrastructure fournie via Service Catalog. Les trois rôles IAM déployés incluent un rôle permettant aux administrateurs informatiques de gérer les produits en tant qu'administrateurs de Service Catalog ; un rôle permettant aux propriétaires d'applications et aux utilisateurs finaux de configurer, lancer et gérer les produits ; et un rôle qui sera utilisé comme contrainte de lancement, qui définit les autorisations que Service Catalog utilisera lors du lancement ou de la mise à jour de votre produit.

Service Catalog dans AMS avant de commencer

Service Catalog remplace-t-il le processus de demande de modification (RFC) AMS existant ?

Dans les comptes où Service Catalog est activé, il servira de système de gestion des modifications dans lequel vous fournirez et mettrez à jour les services informatiques de votre compte AMS via votre catalogue de produits prédéfini ; AMS fournira un portfolio/product catalogue par défaut, et vos administrateurs informatiques pourront créer et configurer le vôtre. Service Catalog n'accusera réception que des piles fournies via Service Catalog. De même, les services fournis via Service Catalog ne seront pas modifiables par le biais du processus AMS RFC, car toute modification en dehors de Service Catalog dérivera la pile de la configuration du produit approuvée.

Puis-je voir les piles fournies via le catalogue de services dans la console AMS ?

Oui. Vous pouvez consulter toutes les piles fournies via le catalogue de services dans la console AMS. Les piles fournies via le catalogue de services sont facilement identifiables grâce à l'ID de pile « SC- ». Bien que les piles soient visibles dans la console AMS, vous ne pourrez pas les mettre à jour via le processus AMS RFC. L'accès au système de gestion des modifications AMS (RFCs) est limité aux demandes d'accès, à l'orchestration des correctifs et à la sauvegarde RFCs uniquement.

Si je mets à and/or jour une pile via Service Catalog, y aura-t-il une RFC correspondante dans la console AMS ?

La seule RFC qui s'affichera dans la console AMS est une RFC pour enregistrer la pile auprès d'AMS lorsqu'une pile est initialement provisionnée. Cette RFC est déposée automatiquement par le processus de validation AMS qui est déclenché lorsqu'une pile est lancée via Service Catalog. Tous les autres approvisionnements et modifications sont suivis directement dans Service Catalog et sont consultables dans la console Service Catalog. En outre, vous pouvez utiliser la fonctionnalité Provisioned Product Plan de Service Catalog pour consulter la liste des

modifications qui seront apportées aux ressources avant le provisionnement ou la mise à jour du produit.

Dois-je faire quelque chose de spécifique pour approvisionner des produits sur mon compte géré par AMS ?

Oui. Tous les produits Service Catalog fournis dans les comptes AMS doivent contenir cette ligne de JSON dans le modèle CFN qui définit ce produit :

```
"Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":  
{"Ref":"AWS::StackId"}}}
```

Cet extrait de CloudFormation code déclenche les validations AMS requises avant que la ressource puisse être provisionnée dans votre compte géré AMS. Il est de votre responsabilité d'inclure cette ligne de code dans la définition du produit. S'il n'est pas inclus, le provisionnement échouera et le message d'erreur suivant s'affichera : « Impossible de créer le produit. Ce compte est géré par AMS. Tous les produits des comptes AMS doivent comporter le Transform code AMS dans le modèle. »

Existe-t-il des fonctionnalités du Service Catalog non disponibles et and/or limitées pour les clients AMS au moment du lancement ?

Oui, les fonctionnalités SC suivantes ne sont pas disponibles pour les clients AMS lors du lancement initial :

- Création de compte via Service Catalog
- Possibilité de lancer tous les services AWS via Service Catalog sur un compte géré par AMS. La disponibilité des services AWS est limitée aux services pris en charge par AMS (gérés et auto-provisionnés). Pour plus d'informations sur les services pris en charge par AMS, consultez la description du service AMS.
- Les connecteurs ITSM (Service Catalog IT Service Manager) de Service Catalog ne communiqueront pas avec les rapports d'incidents et les demandes de service d'AMS.
- Possibilité de tirer parti des démarrages rapides et des architectures de référence de Service Catalog sans modification. N'oubliez pas que les produits Service Catalog pour les comptes AMS doivent contenir cette ligne de code JSON :

```
"Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":  
{"Ref":"AWS::StackId"}}}
```

dans le modèle CNF. Notez que cette ligne ne fait pas partie d'un CloudFormation modèle AWS classique et doit être ajoutée de manière explicite.

- Terraform n'est actuellement pas pris en charge par AMS pour le provisionnement des produits Service Catalog.
- Les stacksets AWS CFN ne sont pas pris en charge dans AMS.
- Vous ne pouvez pas créer de rôles IAM personnalisés.
- Les actions de service sont limitées à :
 - [AWS- RebootRdsInstance](#)
 - [Instance AWS Restart EC2](#)
 - [Instance AWS Start EC2](#)
 - [AWS- StartRdsInstance](#)
 - [Instance AWS Stop EC2](#)
 - [AWS- StopRdsInstance](#)
 - [AWS- CreateImage](#)
 - [AWS- CreateRdsSnapshot](#)
 - [AWS- CreateSnapshot](#)

 Note

Lorsque vous créez des actions de service, vous pouvez configurer le rôle d'exécution comme étant les autorisations de l'utilisateur final, le rôle de lancement ou un rôle IAM personnalisé de votre choix. Le rôle d'exécution sélectionné doit disposer des autorisations suffisantes pour effectuer l'action de service et disposer d'une autorisation TrustPolicy permettant à Service Catalog de l'assumer, sinon cette action de service échouera au moment de l'exécution. Nous vous recommandons d'utiliser le `AWSManagedServicesServiceCatalogLaunchRole`, qui dispose des autorisations et de la politique de confiance appropriées pour être utilisé en tant qu'action de service.

Pourquoi aurai-je encore besoin pour utiliser le système AMS RFC ?

Lors de la disponibilité générale (GA), vous devrez toujours utiliser le RFCS pour exécuter les actions suivantes :

- Configuration de Patch Orchestrator
- Configuration des politiques de sauvegarde

- Demande d'accès à une instance
- Création et attribution de groupes de sécurité non conformes aux directives AMS.
- Réalisation de l'ingestion de la charge de travail (WIGS)
- Création de rôles IAM

Puis-je utiliser la CLI Service Catalog pour accéder à Service Catalog depuis mon compte géré AMS ?

Oui, les Service Catalog APIs sont disponibles et activés via la CLI. Des actions allant de la gestion des artefacts du Service Catalog à la mise en service et à la résiliation de ces artefacts sont disponibles. Pour plus d'informations, consultez les [ressources AWS Service Catalog](#) ou téléchargez le dernier SDK ou CLI AWS.

Qui crée, gère et distribue les catalogues de produits approuvés par les clients ?

L'administrateur du catalogue du client (administrateur and/or informatique), ou ressource désignée, est responsable de la gestion de vos catalogues Service Catalog et des produits approuvés.

Puis-je utiliser AMS AMIs ?

L'AMS AMIs vendu après mars 2020 peut être déployé via AWS Service Catalog.

Comment migrer vers AMS à l'aide de Service Catalog ?

Pour migrer votre charge de travail vers AMS à l'aide de Service Catalog, vous devez commencer par suivre le processus [Workload Ingest](#) (WIGs) pour créer une AMI dans AMS. Vous utilisez l'AMI produite par WIGS pour créer un produit dans Service Catalog. La procédure à suivre est décrite dans [AWS Service Catalog - Getting Started](#).

Trouver les données dont vous avez besoin (SKMS), AMS

Pour trouver les données dont vous avez besoin lorsque vous utilisez vos comptes AWS Managed Services (AMS), vous devez faire appel au système de gestion des connaissances des services AMS, ou SKMS. BRAS.

SKMS est l'abréviation de Service Knowledge Management System et fait référence à toutes les informations relatives au service AWS Managed Services (AMS) destiné à un client. AMS dispose d'une API SKMS pour rechercher des données.

Rubriques

- [Qu'est-ce que la gestion des connaissances liées aux services ?](#)
- [Trouver un VPC IDs dans AMS](#)
- [Recherche d'un sous-réseau IDs dans AMS](#)
- [Trouvez AMI IDs, AMS](#)
- [Rechercher un groupe de sécurité \(SG\) IDs, AMS](#)
- [Rechercher des entités IAM dans AMS](#)
- [Trouver une pile IDs dans AMS](#)
- [Rechercher une instance IDs ou une adresse IP dans AMS](#)
- [Trouvez les noms de ressources Amazon \(ARNs\) dans AMS](#)
- [Trouver des ressources par ARN dans AMS](#)
- [Rechercher les paramètres du compte AMS](#)

Qu'est-ce que la gestion des connaissances liées aux services ?

La gestion des connaissances des services est le stockage de toutes les informations de votre compte AMS. Les informations suivantes sont obtenues à partir du système de gestion des connaissances des services (SKMS) AMS, via l'API AMS SKMS ou via la console AMS :

- VPCs
- Sous-réseaux gérés
- Des piles et des composants de pile, y compris des EC2 instances Amazon et d'autres ressources
- Images de machines Amazon (AMIs)

Vous pouvez utiliser les informations du SKMS pour comprendre l'infrastructure sous gestion et comme contribution à la gestion des modifications et aux demandes de service pour créer, modifier ou supprimer une infrastructure.

 Note

Tous les appels d'API AMS SKMS sont enregistrés dans AWS CloudTrail.

Accédez au SKMS via l'API AMS SKMS, qui fournit des opérations permettant de découvrir des informations sur un environnement (VPCs et ses sous-réseaux) et les ressources de l'application (piles, instances EC2 Amazon et images d'instance AMIs ou) qui peuvent y être déployées.

VPCs et les images d'instance sont configurées dans un compte, avec les autorisations d'accès nécessaires, lors de l'intégration. Une fois qu'ils ont été établis, vous pouvez utiliser le système de gestion des modifications pour les remplir VPCs avec des piles de travail.

Trouver un VPC IDs dans AMS

Un cloud privé virtuel (VPC) possède un ou plusieurs sous-réseaux. Dans AMS, votre VPC se trouve dans un Région AWS et vous avez des sous-réseaux privés et publics.

Voir aussi [Recherche d'un sous-réseau IDs dans AMS](#).

Certains CTs nécessitent le VpcId. Pour trouver un ID VPC, vous pouvez utiliser la console AMS ou l'API/CLI.

Console AMS :

Dans le volet de navigation, sélectionnez VPCset le VPC approprié. La page de détails du VPC pour le VPC sélectionné s'ouvre avec des informations telles que l'ID du VPC.

API ListVpcSummaries ou CLI AMS SKMS :

 Note

L'AMS CLI doit être installée pour que ces commandes fonctionnent. Pour installer l'API ou la CLI AMS, rendez-vous sur la page Ressources pour développeurs de la console AMS. Pour des informations de référence sur l'API AMS CM ou l'API AMS SKMS, consultez la section Ressources d'information AMS du guide de l'utilisateur. Vous devrez peut-être ajouter une

--profile option d'authentification ; par exemple, `aws amsskms ams-cli-command --profile SAML`. Vous devrez peut-être également ajouter --region cette option car toutes les commandes AMS sont exécutées à partir de us-east-1, par exemple. `aws amscm ams-cli-command --region=us-east-1`

Note

Les points de terminaison AMS API/CLI (amscm et amsskms) se trouvent dans la région AWS de Virginie du Nord, us-east-1. En fonction de la configuration de votre authentification et de la région AWS dans laquelle se trouvent votre compte et vos ressources, vous devrez peut-être en ajouter --region us-east-1 lors de l'émission de commandes. Vous devrez peut-être également ajouter --profile saml, s'il s'agit de votre méthode d'authentification.

1. Dans les exemples suivants, la première commande demande une liste de résumés pour tous les éléments VPCs du compte. La deuxième commande demande la liste des VPCs, avec un filtre de requête pour ne répertorier que celles VPCs créées en 2016, et affiche le CreatedTime VpcId, et le nom.

Note

Vous pouvez obtenir la CLI AMS SKMS via la page Ressources du développeur de la console AMS.

```
aws amsskms list-vpc-summaries --output table
```

```
-----
|                               |
|               ListVPCSummaries               |
|-----+-----+
|                               |
|               VPCSummaries                   |
|+-----+-----+
| CreatedTime | 2016-01-15T18:50:11Z |
| VpcId       | vpc-01234567890abcdef |
| LastModifiedTime | 2016-01-15T18:50:11Z |
| Name        | 952444781316-initial-vpc |
|-----+-----+
|                               |
```

Visibility	
Id	PrivateAndPublic
Name	PrivateAndPublic

2. Cette fois, avec une requête :

```
aws amsskms list-VPC-summaries --query "VPCSummaries[?
starts_with(@.CreatedTime,to_string(`2016`))].[CreatedTime, VpcId, Name]" --output
table
```

ListVPCSummaries		
2016-01-15T18:50:11Z	vpc-01234567890abcdef	952444781316-initial-VPC

Recherche d'un sous-réseau IDs dans AMS

Plusieurs ressources nécessitent que vous spécifiez un sous-réseau, ou une liste de sous-réseaux, au moment de la configuration. Pour rechercher des sous-réseaux, vous pouvez utiliser la console AMS ou AMS SKMS API/CLI. Note that the AMS SKMS API/CLI est privé et doit être installé avant de pouvoir l'utiliser.

Console AMS :

1. Dans le volet de navigation, sélectionnez VPCset le VPC approprié. La page de détails du VPC sélectionné s'ouvre avec une table des sous-réseaux. Cliquez sur un ID de sous-réseau pour ouvrir la page de détails et trouver l'ID.

API ListSubnetSummaries ou CLI AMS SKMS :

Note

L'AMS CLI doit être installée pour que ces commandes fonctionnent. Pour installer l'API ou la CLI AMS, rendez-vous sur la page Ressources pour développeurs de la console AMS. Pour des informations de référence sur l'API AMS CM ou l'API AMS SKMS, consultez la section

Ressources d'information AMS du guide de l'utilisateur. Vous devrez peut-être ajouter une `--profile` option d'authentification ; par exemple, `aws amsskms ams-cli-command --profile SAML`. Vous devrez peut-être également ajouter `--region` cette option car toutes les commandes AMS sont exécutées à partir de `us-east-1`, par exemple. `aws amscm ams-cli-command --region=us-east-1`

Note

Les points de terminaison AMS API/CLI (amscm et amsskms) se trouvent dans la région AWS de Virginie du Nord, `us-east-1`. En fonction de la configuration de votre authentification et de la région AWS dans laquelle se trouvent votre compte et vos ressources, vous devrez peut-être en ajouter `--region us-east-1` lors de l'émission de commandes. Vous devrez peut-être également ajouter `--profile saml`, s'il s'agit de votre méthode d'authentification.

Pour trouver les sous-réseaux de votre VPC, vous pouvez effectuer une recherche à l'aide de `list-subnet-summaries` la commande comme indiqué.

Note

Si vous recherchez des sous-réseaux qui ne figurent pas dans un compte AMS, vous pouvez essayer `aws ec2 describe-subnets --region us-west-2`.

1. L' API/CLI ListSubnetSummaries opération SKMS :

Une liste simple :

```
aws amsskms list-subnet-summaries
```

Sortie vers une table :

```
aws amsskms list-subnet-summaries --output table
```

2. Le ListSubnetSummaries fonctionnement de l'API SKMS comporte des paramètres permettant d'affiner les résultats en fonction de la visibilité. En outre, vous pouvez [filtrer](#) les résultats en

fonction du nom. Si vous utilisez la CLI, vous pouvez également utiliser l'option `--query` pour affiner la sortie ou rechercher une partie d'une valeur. Par exemple, pour rechercher tous les sous-réseaux d'un VPC en particulier, vous pouvez utiliser cette commande :

```
aws amsskms list-subnet-summaries --query
  "SubnetSummaries.sort_by(@,&Visibility.Name)[].[Visibility.Name,SubnetId,Name]" --
  output table
```

Ce qui renvoie quelque chose comme ceci :

```
-----
|                               ListSubnetSummaries                               |
+-----+-----+-----+-----+
| Private| subnet-01234567890abcdef | Demo Deployment Zone #1 |
| Private| subnet-01234567890abcdef | Demo Deployment Zone #1 |
| Public | subnet-01234567890abcdef | Demo DMZ #1             |
| Public | subnet-01234567890abcdef | Demo DMZ #1             |
+-----+-----+-----+-----+
```

Pour plus d'informations sur l'utilisation des requêtes CLI, consultez [Comment filtrer la sortie avec l'option --query](#) et la référence du langage de requête, [JMESPath Spécification](#).

3. Si vous en avez plusieurs VPCs, incluez un filtre VPC dans la commande, puis exécutez la commande pour chaque VPC. Exemples :

```
list-subnet-summaries --filter Attribute=VpcId,Value=vpc-xxxxxxx --query
  "SubnetSummaries.sort_by(@,&Visibility.Name)[].[Visibility.Name,SubnetId,Name]" --
  output table
```

4. Dans AWS, utilisez [describe-subnets](#).

Pour plus d'informations sur l'utilisation des requêtes CLI, consultez [Comment filtrer la sortie avec l'option --query](#) et la référence du langage de requête, [JMESPath Spécification](#).

Noms de sous-réseaux

Vos sous-réseaux AMS sont créés automatiquement une fois que les entrées ont été recueillies auprès de vous et ajoutées au système. AMS utilise une formule pour créer les noms de vos sous-réseaux : A **ACCOUNT_ID** - **SUBNET-TYPE** - **AZ** - **IDENTIFIER**. Le type de sous-réseau serait soit `dmzshared-services`, soit `customer-application`. Si vous avez plusieurs sous-réseaux

d'applications clients, un identifiant facultatif peut être ajouté au nom du sous-réseau, après l'ID de compte, pour indiquer qu'il s'agit d'un sous-réseau « supplémentaire » ou « réservé ».

Trouvez AMI IDs, AMS

Une Amazon Machine Image, ou AMI, est un modèle pour les EC2 instances Amazon, créé à partir d'une EC2 instance Amazon. AWS fournit des mises à jour AMIs (avec des correctifs, par exemple) tous les mois ; cependant, AWS Managed Services (AMS) exige AMIs qu'elles aient été modifiées pour pouvoir être utilisées par AMS. AMS publie chaque mois une nouvelle version AMIs que vous pouvez utiliser peu après le Patch Tuesday.

Amazon Machine Images (AMIs) sont des modèles de configuration d'instance utilisés pour créer des EC2 instances dans AWS. AMS exige que des informations spécifiques AMIs soient utilisées pour les ressources gérées par AMS. Les types de modification pour créer EC2 des instances et des groupes EC2 Auto Scaling nécessitent que vous spécifiez une AMI qu'AMS utilisera comme base pour les instances créées par le type de modification. AMS vous recommande de toujours sélectionner l'AMI la plus récente à votre disposition.

Pour en savoir plus AWS AMIs, consultez [AWS AMI Design](#).

Lorsque vous créez une EC2 pile Amazon ou un groupe Amazon EC2 Auto Scaling pour votre compte AMS, vous devez spécifier une AMI par Amild. Vous êtes limité à AMIs ce qui commence par « client » et nous vous recommandons de toujours choisir l'AMI la plus récente.

Pour trouver l'AMI la plus récente pour votre compte, vous pouvez effectuer une recherche à l'aide d'une commande CLI AMS SKMS ou utiliser la page de détails de la console AMS pour le VPC correspondant :

- Utiliser la console AMS : AMIs les options disponibles sont répertoriées sur la page AMI de la console AMS. Choisissez parmi AMIs des noms commençant par « client- ».
- Utilisez l' API/CLI ListAmis opération AMS SKMS.

Note

L'AMS CLI doit être installée pour que ces commandes fonctionnent. Pour installer l'API ou la CLI AMS, rendez-vous sur la page Ressources pour développeurs de la console AMS. Pour des informations de référence sur l'API AMS CM ou l'API AMS SKMS, consultez la section Ressources d'information AMS du guide de l'utilisateur. Vous devrez peut-être

ajouter une `--profile` option d'authentification ; par exemple, `aws amsskms ams-cli-command --profile SAML`. Vous devrez peut-être également ajouter `--region` cette option car toutes les commandes AMS sont exécutées à partir de `us-east-1`, par exemple.

```
aws amscm ams-cli-command --region=us-east-1
```

Voici un exemple de CLI avec une `query` option qui limite les résultats au client AMIs :

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?starts_with(Name,'customer')].[Name,AmiId]" --output table
```

Cet exemple utilise l'`filter` option `query` permettant de rechercher AMIs les fenêtres commençant par « client » :

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?starts_with(Name,'customer')].[Name,AmiId]" --filter Attribute=Platform,Value=windows --output table
```

- Pour plus d'informations sur l'utilisation des requêtes CLI, consultez [Comment filtrer la sortie avec l'option --query](#) et la référence du langage de requête, [JMESPath Spécification](#).

Rechercher un groupe de sécurité (SG) IDs, AMS

Les domaines Amazon EC2 OpenSearch Create et Create CTs nécessitent un ID de groupe de sécurité. Ce sera dans le formulaire `sg-02ce123456e7893c7`. Votre compte possède au moins deux groupes de sécurité par défaut ; voir [Groupes de sécurité](#). En outre, vous pouvez avoir des groupes de sécurité que vous avez créés à des fins spécifiques. Pour découvrir vos groupes de sécurité :

- Console AWS : utilisez la console EC2 ou VPC pour afficher tous les groupes de sécurité pour le VPC sélectionné.
- API/CLI (lorsque vous êtes connecté à votre compte AMS) :

Répertoriez vos groupes de sécurité :

```
aws ec2 describe-security-groups
```

Rechercher des entités IAM dans AMS

Votre compte possède des rôles et des politiques IAM par défaut ; voir [Rôle d'utilisateur IAM dans AMS](#) et les profils d'instance IAM par défaut ; voir [EC2 Profil d'instance IAM](#) avec des politiques par défaut. Pour découvrir vos rôles et politiques IAM :

- Console : utilisez la console IAM pour consulter toutes les politiques et tous les rôles IAM associés à votre compte.
- API/CLI (lorsque vous êtes connecté à votre compte AMS) :

Note

L'AMS CLI doit être installée pour que ces commandes fonctionnent. Pour installer l'API ou la CLI AMS, rendez-vous sur la page Ressources pour développeurs de la console AMS. Pour des informations de référence sur l'API AMS CM ou l'API AMS SKMS, consultez la section Ressources d'information AMS du guide de l'utilisateur. Vous devrez peut-être ajouter une `--profile` option d'authentification ; par exemple, `aws amsskms ams-cli-command --profile SAML`. Vous devrez peut-être également ajouter `--region` cette option car toutes les commandes AMS sont exécutées à partir de `us-east-1`, par exemple. `aws amscm ams-cli-command --region=us-east-1`

Répertoriez vos rôles :

```
aws --profile saml iam list-roles
```

Répertoriez vos politiques :

```
aws --profile saml iam list-role-policies --role-name ROLE_NAME
```

Trouver une pile IDs dans AMS

Pour trouver un Stack ID, vous pouvez utiliser la EC2 console Amazon, la console AMS ou l'API/CLI AMS SKMS.

Console AMS :

- Dans le volet de navigation, sélectionnez RFCs, puis cliquez sur le RFC qui a créé la pile. Utilisez l'option de filtre en haut pour réduire la liste. La page de détails de la RFC s'ouvre et inclut la sortie d'exécution avec l'ID de pile.
- Vous pouvez également sélectionner Stacks dans le volet de navigation pour ouvrir la page de liste des piles, puis parcourir la liste des piles jusqu'à la pile qui vous intéresse. Cette méthode est plus utile si vous connaissez le sujet de la pile que vous recherchez.

EC2 Console Amazon :

Dans le volet de navigation, sélectionnez Instances ou Load Balancers ou Auto Scaling Groups.

API ListStackSummaries ou CLI AMS SKMS :

Note

L'AMS CLI doit être installée pour que ces commandes fonctionnent. Pour installer l'API ou la CLI AMS, rendez-vous sur la page Ressources pour développeurs de la console AMS. Pour des informations de référence sur l'API AMS CM ou l'API AMS SKMS, consultez la section Ressources d'information AMS du guide de l'utilisateur. Vous devrez peut-être ajouter une `--profile` option d'authentification ; par exemple, `aws amsskms ams-cli-command --profile SAML`. Vous devrez peut-être également ajouter `--region` cette option car toutes les commandes AMS sont exécutées à partir de `us-east-1`, par exemple. `aws amscm ams-cli-command --region=us-east-1`

Note

Les points de terminaison AMS API/CLI (`amscm` et `amsskms`) se trouvent dans la région AWS de Virginie du Nord, `us-east-1`. En fonction de la configuration de votre authentification et de la région AWS dans laquelle se trouvent votre compte et vos ressources, vous devrez peut-être en ajouter `--region us-east-1` lors de l'émission de commandes. Vous devrez peut-être également ajouter `--profile saml`, s'il s'agit de votre méthode d'authentification.

Pour afficher la liste des piles du compte courant, exécutez l' `ListStackSummaries` API SKMS (CLI :`list-stack-summaries`). Pour obtenir des informations complètes sur une instance de stack particulière `StackId`, exécutez `GetStack`.

- Dans les exemples suivants, la première commande demande une liste de résumés pour toutes les instances de pile du compte. La deuxième commande demande la liste des instances de pile, avec un filtre de requête pour répertorier uniquement celles d'un modèle de pile spécifique, et affiche les `VpcId` valeurs, `Name` et `StackId`.

```
aws amsskms list-stack-summaries --output table
```

```
-----
|                                     ListStackSummaries                                     |
|                                     StackSummaries                                       |
+-----+-----+-----+-----+
| VpcId | StackId | StackTemplateId | Name |
+-----+-----+-----+-----+
| vpc-0123abcd | stack-1fb7fe2212345678 | stm-sdhopvbb123456789 | Test ELB |
| vpc-0123abcd | stack-8323cc0e12345678 | stm-s2b72beb123456789 | S3 store |
| vpc-0123abcd | stack-2309fa0712345678 | stm-sdhopvbb123456789 | ELB      |
| vpc-0123abcd | stack-5e61a70512345678 | stm-sdpabqbb123456789 | PatchSim |
| vpc-0123abcd | stack-bd0e080d12345678 | stm-s2b72beb123456789 | CLI demo |
+-----+-----+-----+-----+
```

Pour plus d'informations sur l'utilisation des requêtes CLI, consultez [Comment filtrer la sortie avec l'option --query](#) et la référence du langage de requête, [JMESPath Spécification](#).

Note

Pour plus d'informations sur l'utilisation de l'instance IDs pour l'accès, consultez également [Accès aux instances à l'aide de bastions](#).

Rechercher une instance IDs ou une adresse IP dans AMS

- Pour demander l'accès à une instance, pour vous connecter à une instance ou pour créer une AMI, vous devez disposer de l'ID de l'instance. Pour une EC2 instance (instance autonome

ou partie d'une pile) ou pour une instance de base de données, vous pouvez trouver l'ID de différentes manières :

- La console AMS pour une instance dans une pile ASG : recherchez sur la page détaillée de la RFC la RFC qui a créé la pile. Dans la section Execution Output, vous trouverez l'ID de pile pour la pile ASG. Vous pouvez ensuite accéder à la page EC2 Console Auto Scaling Groups, rechercher cet ID de pile et trouver des instances pour celui-ci. Lorsque vous trouvez l'instance, sélectionnez-la et une zone s'ouvre au bas de la page avec des détails, notamment l'adresse IP.
- La console AMS pour une instance autonome EC2 ou de base de données (DB) : recherchez sur la page détaillée de la RFC la RFC qui a créé la EC2 pile ou l'instance de base de données. Dans la section Execution Output, vous trouverez l'ID et l'adresse IP de l'instance.
- EC2 Console AWS :
 1. Dans le panneau de navigation, sélectionnez Instances. La page Instances s'ouvre.
 2. Cliquez sur l'instance pour laquelle vous souhaitez obtenir l'ID. La page des détails de l'instance s'ouvre et affiche l'ID et l'adresse IP.
- Console de base de données AWS :
 1. Sur la page d'accueil, sélectionnez DB Instances. La page Instances s'ouvre.
 2. Filtrez l'instance de base de données pour laquelle vous souhaitez obtenir l'ID. La page des détails de l'instance s'ouvre et affiche l'ID.
- CLI/API CAMS.

 Note

L'AMS CLI doit être installée pour que ces commandes fonctionnent. Pour installer l'API ou la CLI AMS, rendez-vous sur la page Ressources pour développeurs de la console AMS. Pour des informations de référence sur l'API AMS CM ou l'API AMS SKMS, consultez la section Ressources d'information AMS du guide de l'utilisateur. Vous devrez peut-être ajouter une `--profile` option d'authentification ; par exemple, `aws amsskms ams-cli-command --profile SAML`. Vous devrez peut-être également ajouter `--region` cette option car toutes les commandes AMS sont exécutées à partir de `us-east-1`, par exemple. `aws amscm ams-cli-command --region=us-east-1`

 Note

Les points de terminaison AMS API/CLI (amscm et amsskms) se trouvent dans la région AWS de Virginie du Nord, `us-east-1`. En fonction de la configuration de votre authentification et de la région AWS dans laquelle se trouvent votre compte et vos ressources, vous devrez peut-être en ajouter `--region us-east-1` lors de l'émission de commandes. Vous devrez peut-être également ajouter `--profile sam1`, s'il s'agit de votre méthode d'authentification.

Exécutez la commande suivante pour obtenir les détails de la sortie d'exécution de la pile :

```
aws amsskms get-stack --stack-id STACK_ID
```

La sortie ressemble à ceci, avec le message `InstanceId` apparaissant en bas, sous `Outputs` (les valeurs indiquées sont des exemples) :

```
{
  "Stack": {
    "StackId": "stack-7fa52bd5eb8240123",
    "Status": {
      "Id": "CreateCompleted",
      "Name": "CreateCompleted"
    },
    "VpcId": "vpc-01234567890abcdef",
    "Description": "Amazon",
    "Parameters": [
      {
        "Value": "sg-01234567890abcdef,sg-01234567890abcdef",
        "Key": "SecurityGroups"
      },
      {
        "Value": "subnet-01234567890abcdef",
        "Key": "InstanceSubnetId"
      },
      {
        "Value": "t2.large",
        "Key": "InstanceType"
      }
    ]
  }
}
```



```
{
  {
    "Value": "ami-01234567890abcdef",
    "Key": "InstanceAmiId"
  },
  "Tags": [],
  "Outputs": [
    {
      "Value": "i-0b22a22eec53b9321",
      "Key": "InstanceId"
    },
    {
      "Value": "10.0.5.000",
      "Key": "InstancePrivateIP"
    }
  ],
  "StackTemplateId": "stm-s6xvs0000000000000",
  "CreatedTime": "1486584508416",
  "Name": "Amazon"
}
```

Trouvez les noms de ressources Amazon (ARNs) dans AMS

Un Amazon Resource Name (ARN) est une chaîne qui identifie de manière unique une AWS ressource, telle que des EC2 instances, des compartiments S3, des comptes, des fonctions Lambda, etc. AWS nécessite un ARN lorsque vous souhaitez spécifier une ressource sans ambiguïté dans l'ensemble, par exemple dans les politiques IAM AWS, les balises Amazon Relational Database Service (Amazon RDS) et les appels d'API. ARNs sont construits à partir d'identifiants qui spécifient le service, la région, le compte et d'autres informations. Il existe trois formats d'ARN :

```
arn:aws:service:region:account-id:resource-id
arn:aws:service:region:account-id:resource-type/resource-id
arn:aws:service:region:account-id:resource-type:resource-id
```

Note

Le format exact d'un ARN dépend du service et du type de ressource. Pour en savoir plus ARNs, consultez [Amazon Resource Names \(ARNs\) et Espaces de noms de AWS service](#) et [formats ARN](#).

Pour des exemples de format ARN par ressource, consultez le [tableau des types de ressources](#) de référence d'autorisation de AWS service.

Il peut être difficile de trouver l'ARN d'un objet AWS. Voici trois façons d'essayer :

- Console de service AWS : accédez à la console de service AWS appropriée, localisez la ressource et recherchez l'ARN dans les détails de la ressource.
- AWS API/CLI (vous devez d'abord installer l'AWS CLI) : recherchez le service approprié dans la [référence de commande de l'AWS CLI](#), puis, selon le service AWS, recherchez l'opération appropriée `describe`, telle que `get`, ou, etc. Par exemple, pour tous les rôles, politiques et utilisateurs IAM, vous pouvez obtenir l'ARN dans la sortie de la CLI avec :

```
aws iam get-role --role-name EMR_DefaultRole
```

- Construisez l'ARN en fonction du format approprié : recherchez le format ARN de la ressource en consultant la page [Actions, ressources et clés de condition pour les services AWS](#), en recherchant le service pertinent, puis l'action appropriée, puis en explorant le format ARN de la ressource. Une fois le format défini, remplacez les variables par les paramètres appropriés.

Vous pouvez créer vous-même l'ARN en suivant le format approprié (les formats changent en fonction du service et du type de ressource) et en remplissant les informations. Voici quelques exemples d'ARN :

- La syntaxe d'un Compte AWS ARN est la suivante :

```
arn:aws:iam::ACCOUNT-ID:root
```

- Un ARN S3 possède une hiérarchie plate de buckets et d'objets associés :

```
arn:aws:s3:::ams-bucket
```

- Un EC2 ARN possède des sous-types de ressources tels que l'image, les groupes de sécurité, les instances, etc. Cet exemple inclut l'ID de l'instance à la fin :

```
arn:aws:ec2:us-east-1:123456789012:instance/i-012abcd34efghi56
```

- Un ARN Lambda possède le nom de fonction pour la partie identifiant de ressource, et vous devrez peut-être inclure le numéro de version à la fin, comme indiqué dans cet exemple :

```
arn:aws:lambda:us-east-1:123456789012:function:api-function:1
```

Le AWS Key Management Service service fournit les informations suivantes : [Recherche de l'ID et de l'ARN de la clé](#).

[Pour trouver l'ARN d'une table DynamoDB, utilisez l'interface de ligne de commande de la table de description DynamoDB.](#)

Pour un aperçu externe de la recherche AWS ARNs, consultez [AWS ARN Explained : Amazon Resource Name Guide](#).

Trouver des ressources par ARN dans AMS

Amazon Resource Names (ARNs) identifie les AWS ressources de manière unique. Pour en savoir plus sur ARNs les formats ARN, consultez [Amazon Resource Names \(ARNs\) et les espaces de noms de AWS service](#) et [formats ARN](#).

Note

Pour obtenir des informations sur une ressource à partir de son ARN, vous devez avoir accès au compte qui a créé la ressource.

Il n'existe aucun chemin direct AWS permettant de rechercher tous les détails des ressources à partir de l'ARN de la ressource, car les services ont plusieurs types de ressources avec diverses informations connexes. Si vous disposez de l'ARN d'une ressource, vous pouvez déterminer :

- Le AWS service associé (le troisième segment ARN) vous indique la console AWS à consulter pour trouver la ressource
- L'ID de ressource (le sixième ou septième segment d'ARN) confirme que vous avez trouvé la bonne ressource

Vous pouvez également rechercher les commandes AWS CLI disponibles pour ce service dans la [référence des commandes de la AWS CLI](#) pour obtenir des informations sur l'obtention de détails sur la ressource.

Par exemple, à partir de l'ARN suivant, vous pouvez déterminer que le service est `lambda123456789012`, le compte `function`, le type de ressource et le nom de la fonction `TestFunction`.

```
arn:aws:lambda:us-east-1:123456789012:function:TestFunction
```

À partir de là, vous pouvez consulter la [documentation de la AWS CLI du service Lambda pour](#) savoir comment obtenir plus de détails à l'aide de différentes commandes, telles que `get-function` et `get-function-configuration`.

Par exemple, vous pouvez utiliser les commandes suivantes pour obtenir plus d'informations sur une fonction Lambda si vous connaissez son nom ou son ARN :

```
aws lambda get-function-configuration --function-name TestFunction
```

```
aws lambda get-function-configuration --function-name arn:aws:lambda:us-east-1:123456789012:function:TestFunction
```

Rechercher les paramètres du compte AMS

Paramètres de compte utilisés pour créer AMS RFCs, définir les horaires et déterminer qui reçoit les notifications.

Certains paramètres sont créés lors de l'intégration et nécessitent une demande de service pour être modifiés. Vous devez prendre note de ces informations de compte, car vous les utiliserez lorsque vous communiquerez avec AMS :

- Informations d'identification : si vous avez besoin de récupérer votre nom d'utilisateur ou votre mot de passe AMS, contactez votre administrateur informatique local. AMS utilise l'Active Directory de votre entreprise.
- Cloud Service Delivery Manager (CSDM) : cette personne est votre agent de liaison avec AMS et est disponible pour répondre aux questions de service. Les coordonnées de cette personne vous sont communiquées lors de l'intégration et vous devez les garder accessibles à tous les membres de votre organisation qui interagissent avec AMS. Vous pouvez vous attendre à recevoir des rapports mensuels sur votre service AMS de la part de cette personne.
- Accès à la console : vous accédez à la console AMS via une URL configurée spécifiquement pour votre compte. Vous pouvez obtenir l'URL à partir de votre CSDM.

- CLI AMS : vous pouvez obtenir l'interface de ligne de commande AMS via la page des ressources du développeur de la console AMS ou via le package distribuables fourni par votre CSDM. Une fois que vous avez le package distribuables, suivez les étapes décrites dans [Installation ou mise à niveau de l'AMS CLI](#).
- Fenêtre de maintenance : votre fenêtre de maintenance détermine le moment où les correctifs sont appliqués à vos EC2 instances. La fenêtre de maintenance (ou fenêtre de maintenance) AWS Managed Services (ou fenêtre de maintenance) exécute les activités de maintenance d'AWS Managed Services (AMS) et a lieu le deuxième jeudi de chaque mois de 15 h 00 à 16 h 00, heure du Pacifique. AMS peut modifier le créneau de maintenance avec un préavis de 48 heures. Vous avez peut-être choisi une autre fenêtre lors de l'intégration. Conservez une trace de la fenêtre de maintenance que vous avez choisie.
- Surveillance : AMS fournit un ensemble de CloudWatch métriques par défaut, mais vous pouvez également demander des métriques supplémentaires. Si c'est le cas, gardez-en une trace.
- Journaux : Par défaut, vos journaux sont stockés dans `ams-a-ACCOUNT_ID-log-management-`, où `REGION` trouve la région `REGION` où le journal a été généré.
- Atténuation : lors de l'intégration, AMS enregistre l'action d'atténuation de votre choix en cas d'identification d'une attaque malveillante contre vos ressources. Par exemple, contactez certaines personnes. Mettez ces informations à la disposition de tous les membres de votre organisation qui interagissent avec AMS.
- Région : vous pouvez consulter la page de détails du VPC dans la console AMS. Vous pouvez également exécuter cette commande après avoir installé la CLI AMS SKMS (cette commande utilise un profil SAML, à supprimer si votre méthode d'authentification est différente) :

```
aws --profile saml amsskms get-vpc --vpc-id VPC_ID
```

Important

Note

Les points de terminaison AMS API/CLI (`amscm` et `amsskms`) se trouvent dans la région AWS de Virginie du Nord, `us-east-1`. En fonction de la configuration de votre authentification et de la région AWS dans laquelle se trouvent votre compte et vos ressources, vous devrez peut-être en ajouter `--region us-east-1` lors

de l'émission de commandes. Vous devrez peut-être également ajouter `--profile sam1`, s'il s'agit de votre méthode d'authentification.

Rechercher FQDNs dans AMS

Les types de modification d'accès à AWS Managed Services (AMSCTs) () nécessitent le nom de domaine complet, ou FQDN, de votre domaine approuvé par AMS, sous la forme de. C844273800838 . amazonaws . com Pour découvrir votre AWS FQDN, effectuez l'une des opérations suivantes :

- Console AWS : recherchez dans la console AWS Directory Service, dans la colonne Nom du répertoire.
- CLI : utilisez ces commandes lorsque vous êtes connecté à votre domaine :

Windows (renvoie l'utilisateur et le FQDN) :

```
whoami /upn
```

ou (DC+DC+DC=FQDN)

```
whoami /fqdn
```

Linux :

```
hostname --fqdn
```

Note

Les points de terminaison AMS API/CLI (amscm et amsskms) se trouvent dans la région AWS de Virginie du Nord, `us-east-1`. En fonction de la configuration de votre authentification et de la région AWS dans laquelle se trouvent votre compte et vos ressources, vous devrez peut-être en ajouter `--region us-east-1` lors de l'émission de commandes. Vous devrez peut-être également ajouter `--profile sam1`, s'il s'agit de votre méthode d'authentification.

Trouver les zones de disponibilité (AZs) dans AMS

Zone de disponibilité : tous les comptes ont au moins deux zones de disponibilité. Pour trouver avec précision les noms de vos zones de disponibilité, vous devez d'abord connaître l'ID de sous-réseau associé.

- Console AMS : dans le volet de navigation VPCs, cliquez, puis sur le VPC approprié, si nécessaire. Sur la page de VPCs détails, sélectionnez le sous-réseau approprié dans le tableau des sous-réseaux pour ouvrir la page de détails du sous-réseau avec le nom de la zone de disponibilité associée.
- API/CLI AMS SIMS :

```
aws amsskms list-subnet-summaries --output table
```

```
aws amsskms get-subnet --subnet-id SUBNET_ID
```

Note

Les points de terminaison AMS API/CLI (amscm et amsskms) se trouvent dans la région AWS de Virginie du Nord, `us-east-1`. En fonction de la configuration de votre authentification et de la région AWS dans laquelle se trouvent votre compte et vos ressources, vous devrez peut-être en ajouter `--region us-east-1` lors de l'émission de commandes. Vous devrez peut-être également ajouter `--profile sam1`, s'il s'agit de votre méthode d'authentification.

Rechercher des sujets SNS dans AMS

Vos rubriques SNS déterminent qui est averti dans différentes circonstances. AMS fournit des rubriques SNS pour les notifications AMI (voir [Notifications AMI AMS avec SNS](#)), les CloudWatch alarmes et les EC2 ressources (voir [Réception d'alertes générées par AMS](#)) et plus encore. Pour découvrir vos rubriques SNS existantes, procédez comme suit :

- Console AWS : utilisez la console SNS pour afficher tous les sujets, applications et abonnements, ainsi qu'un graphique des messages. Créez, supprimez, abonnez-vous à des rubriques et publiez-les également sur celles-ci.

- API/CLI (une fois connecté à votre compte AMS, nécessite l'interface de ligne de commande AWS) :

Répertoriez vos sujets SNS :

```
aws sns list-topics
```

Répertoriez vos abonnements SNS :

```
aws sns list-subscriptions
```

Note

Les points de terminaison AMS API/CLI (amscm et amsskms) se trouvent dans la région AWS de Virginie du Nord, `us-east-1`. En fonction de la configuration de votre authentification et de la région AWS dans laquelle se trouvent votre compte et vos ressources, vous devrez peut-être en ajouter `--region us-east-1` lors de l'émission de commandes. Vous devrez peut-être également ajouter `--profile sam1`, s'il s'agit de votre méthode d'authentification.

Rechercher les paramètres de sauvegarde dans AMS

Les sauvegardes et les instantanés sont gérés par AMS via le [AWS Backup](#) service natif.

La configuration est gérée par le biais AWS Backup de plans. Vous pouvez avoir plusieurs AWS Backup plans qui associent des ressources balisées à des plannings de sauvegarde et à des politiques de rétention. Pour trouver les AWS Backup paramètres de votre compte AMS, utilisez la console <https://console.aws.amazon.com/backup> ou la référence de commande de l'AWS CLI pour les commandes [de sauvegarde](#).

Pour plus d'informations sur AMS et AWS Backup consultez la section [Gestion de la continuité](#).

Gestion des accès dans AMS

Découvrez comment accéder aux ressources à l'aide du protocole SSH, ou protocole RDP (Remote Desktop Protocol), et comment utiliser les bastions.

Le système de gestion des accès AWS Managed Services (AMS) est configuré lors de l'intégration. Seuls les utilisateurs dotés du rôle d'utilisateur AMS IAM, fédérés via AMS, peuvent accéder aux ressources AMS du compte.

Outre la confiance fédérée, décrite ci-dessous, les groupes de sécurité AMS constituent un élément important de l'accès aux applications privées et publiques. Pour plus d'informations sur les groupes de sécurité AMS et sur la manière de les modifier, consultez [Groupes de sécurité](#).

Rubriques

- [Qu'est-ce que la gestion des accès ?](#)
- [Comment et quand utiliser le compte utilisateur root dans AMS](#)
- [Console AMS Advanced et Amazon EC2 Access](#)
- [Accès à la console AWS de gestion et à la console AMS](#)
- [Accès aux instances à l'aide de bastions](#)

Qu'est-ce que la gestion des accès ?

La gestion des accès permet à AMS de protéger vos ressources en n'autorisant que les accès autorisés et authentifiés. AMS utilise un rôle d'utilisateur et un profil d'instance IAM par défaut, ainsi qu'une authentification multifactorielle, des groupes de sécurité, des noms de bastions compatibles avec le DNS, etc. pour protéger vos ressources.

AMS se concentre sur trois types d'accès nécessitant une gestion :

- Accès à la console : grâce à la fédération, les utilisateurs de l'Active Directory du compte peuvent accéder à la console à l'aide de l'authentification unique (SSO). Si l'authentification multifactorielle est configurée pour ces comptes, vous pouvez continuer à avoir besoin de l'authentification MFA pour accéder à la console.
- Accès aux instances via RDP ou SSH : en s'appuyant sur une approbation Active Directory, les utilisateurs de l'Active Directory existant du compte peuvent demander l'accès à une instance, puis s'authentifier avec succès auprès d'un bastion et de l'instance en utilisant leurs informations

d'identification d'entreprise existantes. Si l'authentification multifactorielle est configurée pour ces comptes, vous pouvez continuer à avoir besoin de la MFA pour demander l'accès à une instance. AMS utilise sa propre solution MFA pour restreindre l'accès des ingénieurs AMS aux instances.

- Accès aux applications : varie selon les cas d'utilisation.

Rubriques

- [Pourquoi et quand AMS accède à votre compte](#)

Pourquoi et quand AMS accède à votre compte

AWS Managed Services (AMS) gère votre infrastructure AWS et parfois, pour des raisons spécifiques, les opérateurs et administrateurs AMS accèdent à votre compte. Ces événements d'accès sont documentés dans vos journaux AWS CloudTrail (CloudTrail).

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
Déploiements d'infrastructures	AMS	Problème de déploiement
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
Exécution manuelle des RFC	Vous	Problème de demande de modification (RFC). (La non-automatisation RFCs peut nécessiter un accès AMS à vos ressources)
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

Lorsqu'il est déclenché, AMS accède aux comptes clients à l'aide de AWS Identity and Access Management rôles (IAM). Comme pour toutes les activités de votre compte, les rôles et leur utilisation sont connectés CloudTrail.

 Important

Ne modifiez ni ne supprimez ces rôles.

Rôles IAM pour l'accès AMS aux comptes clients

Nom du rôle	Type de compte (SALZ, gestion MALZ, application MALZ, etc.)	Description
ams-service-admin	SEL, MALZ	Accès automatisé aux services AMS et déploiements d'infrastructures automatisés, par

Nom du rôle	Type de compte (SALZ, gestion MALZ, applicati on MALZ, etc.)	Description
		exemple Patch, Backup, Automated Remediation.
ams-application-infra-read-uniquelement	SALZ, applicati on MALZ, application d'outils MALZ	Accès en lecture seule par l'opérateur
ams-application-infra-operations		Accès de l'opérateur pour les incidents/service demandes
ams-application-infra-admin		Accès AD Admin
ams-primary-read-only	Gestion du MALZ	Accès en lecture seule par l'opérateur
ams-primary-operations		Accès de l'opérateur pour les incidents/service demandes
ams-primary-admin		Accès AD Admin
ams-logging-read-only	Journalisation MALZ	Accès en lecture seule par l'opérateur
ams-logging-operations		Accès de l'opérateur pour les incidents/service demandes
ams-logging-admin		Accès AD Admin
ams-networking-read-only	Réseau MALZ	Accès en lecture seule par l'opérateur
ams-networking-operations		Accès de l'opérateur pour les incidents/service demandes
ams-networking-admin		Accès AD Admin
ams-shared-services-read-uniquelement	Services partagés MALZ	Accès en lecture seule par l'opérateur

Nom du rôle	Type de compte (SALZ, gestion MALZ, applicati on MALZ, etc.)	Description
ams-shared-services- operations		Accès de l'opérateur pour les incidents/service demandes
ams-shared-services- admin		Accès AD Admin
ams-security-read-only	Sécurité MALZ	Accès en lecture seule par l'opérateur
ams-security-operations		Accès de l'opérateur pour les incidents/service demandes
ams-security-admin		Accès AD Admin
ams-access-security- analyst	SALZ, applicati on MALZ, application d'outils MALZ, noyau MALZ	Accès à la sécurité AMS
ams-access-security- analyst-lecture seule		AMS Security, accès en lecture seule
Sentinel_ AdminUser _Role_ 0 MBhe PXHaz RQadu PVc CDc	SALZ	[BreakGlassRole] Utilisé pour introduire du verre dans les comptes clients
Sentinel_ PowerUser _Role_ S0 0 wZuPu ROOI IazDb RI9	SEL, MALZ	Accès des utilisateurs avancés aux comptes clients pour l'exécution des RFC
Sentinelle _ _Role_PD4 L6RW9RD0LNLKD5 ReadOnlyUser JOo		ReadOnly accès aux comptes clients pour l'exécution des RFC
ams_admin_role		Accès administrateur aux comptes clients pour l'exécution des RFC

Nom du rôle	Type de compte (SALZ, gestion MALZ, applicati on MALZ, etc.)	Description
AWSManagedServices _Provisioning_Cust omerStacksRole		Utilisé pour lancer et mettre à jour les piles CFN pour le compte des clients via Ingest CloudFormation
rôle_automation_client		Rôle transmis par les exécutions CT à SSM Automation pour l'exécution du runbook
ams_ssm_automation_role	SALZ, applicati on MALZ, noyau MALZ	Rôle transmis par les services AMS à SSM Automation pour l'exécution du runbook
ams_ssm_iam_deploy ment_role	Application MALZ	Rôle utilisé par le catalogue IAM
ams_ssm_shared_svc s_intermediary_role	Services partagés MALZ	Rôle utilisé par l'application ams_ssm_a utomation_role pour exécuter des documents SSM spécifiques dans un compte Shared Services
AmsOpsCenterRole		Utilisé pour créer et mettre OpsItems à jour des comptes clients
AMSOpsItemAutoExec utionRole	SEL, MALZ	Utilisé pour obtenir des documents SSM, décrire les balises de ressources OpsItems, mettre à jour et démarrer l'automatisation
customer-mc-ecprofil à 2 instances		Profil d' EC2 instance client par défaut (rôle)

Demande d'accès à une instance

Pour accéder à une ressource, vous devez d'abord soumettre une demande de modification (RFC) pour cet accès. Vous pouvez demander deux types d'accès : administrateur (autorisations de lecture/

écriture) et lecture seule (accès utilisateur standard). L'accès dure huit heures, par défaut. Ces informations sont obligatoires :

- ID de pile, ou ensemble de piles IDs, pour l'instance ou les instances auxquelles vous souhaitez accéder.
- Le nom de domaine complet de votre domaine approuvé par AMS.
- Le nom d'utilisateur Active Directory de la personne qui souhaite y accéder.
- L'ID du VPC où se trouvent les piles auxquelles vous souhaitez accéder.

Une fois que l'accès vous a été accordé, vous pouvez mettre à jour la demande selon vos besoins.

Pour des exemples de demande d'accès, voir [Stack Admin Access | Grant](#) ou [Stack Read-only Access | Grant](#).

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.

Note

La MFA est activée lors de l'intégration d'AMS Advanced pour interdire spécifiquement l'accès des utilisateurs root. L'accès root dans les comptes gérés par AMS est différent de celui des autres AWS comptes et est essentiel à la sécurité de l'ensemble de votre environnement géré par AMS. Le MFA configuré est un MFA virtuel exécuté à l'aide d'un appareil appartenant à AMS. Une fois le MFA virtuel configuré avec l'assistance d'AMS, le jeton virtuel est immédiatement supprimé. Cela garantit que ni vous ni AMS ne pouvez vous connecter au compte en tant qu'utilisateur root. La connexion root ne peut être réactivée que sur demande spéciale (expliquée ci-dessous) et AMS s'attend à ce que ces accès ne soient utilisés qu'en cas d'absolue nécessité. Pour plus d'informations sur l'authentification multifactorielle, voir [Sécuriser un nouveau compte grâce à l'authentification multifactorielle](#).

L'accès root déclenche toujours une réponse de l'équipe chargée de la sécurité et des opérations d'AMS. AMS surveille les appels d'API pour l'accès root, et des alarmes sont déclenchées si un tel accès est détecté.

La demande d'accès root est légèrement différente selon les types de comptes AMS.

Accès root avec la zone de landing à compte unique AMS Advanced :

Si vous disposez d'une zone de landing zone à compte unique, contactez votre responsable de prestation de services cloud (CSDM) et vos architectes cloud (CAs) pour les informer du travail d'accès root dont vous avez besoin. Il est préférable de donner un préavis de vingt-quatre heures avant l'activité proposée.

Accès root avec la zone de landing multi-comptes AMS Advanced :

Pour les comptes d'application de zone d'atterrissage multicomptes, de services partagés, de sécurité ou de mise en réseau, utilisez le type de changement Management | Other | Other (ct-1e1xtak34nx76). Incluez la date, l'heure et le but de l'utilisation des informations d'identification de l'utilisateur root et planifiez le RFC pour vous assurer de donner un préavis de vingt-quatre heures avant l'activité proposée. Utilisez votre compte de gestion de zone d'atterrissage multi-comptes pour soumettre le RFC.

De plus, contactez votre CSDM CAs 24 heures à l'avance pour l'informer du travail d'accès root dont vous avez besoin.

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.

Console AMS Advanced et Amazon EC2 Access

Accès à la console AMS Advanced.

Accès à vos EC2 instances Amazon.

Soumettre une demande d'accès :

Connexion à vos EC2 instances Amazon AMS :

Accès à la console AWS de gestion et à la console AMS

Lors de l'intégration, vous êtes connecté à la console de AWS gestion (avec des privilèges limités : vous pouvez écrire sur la console AMS et dans certains champs de votre page d'informations client). Vous pouvez accéder à la console AMS en sélectionnant le lien Managed Services dans la console AWS de gestion. L'accès fédéré ou les informations d'identification partagées (nom d'utilisateur/mot de passe) sont préparés comme convenu avec votre équipe d'administration informatique. Pour créer un compte ou un groupe ultérieurement, envoyez une demande de service à AMS.

Pour plus d'informations sur l'accès à la console AWS de gestion, consultez la section [Utilisation de la console AWS de gestion](#).

Pour obtenir des conseils sur l'utilisation de la console AMS, consultez la section [Utilisation de la console AMS](#).

Accès temporaire à la console AMS

Si vous n'avez pas encore configuré de fournisseur d'identité (par exemple, SAML) pour vous authentifier auprès d'AMS, vous pouvez obtenir un accès temporaire à la console AMS. Contactez votre CSDM pour qu'une demande de déploiement | Advanced stack components | Identity and Access Management (IAM) | Créer une demande de modification d'entité ou de politique (ct-3dpd8mdd9jn1r) soit soumise en votre nom avec les valeurs suivantes :

- Username: nom de l'entité utilisateur IAM que vous créez
- AccessType: « Accès à la console »
- UserPermissions: « Accès temporaire à la console AMS pour **USERNAME** (la personne à laquelle vous souhaitez avoir un accès temporaire) »
- Notifications par e-mail : votre adresse e-mail, afin que vous puissiez approuver la demande lorsqu'AMS vous demande

Note

Cette RFC pour l'accès temporaire à la console AMS nécessite un examen de sécurité et son acceptation à la fois par votre équipe de sécurité interne et par AMS Global Security.

Une fois cette demande terminée et que vous êtes en mesure de vous connecter, vous devez approuver le RFC créé, suivre l'approbation et permettre à l'équipe AMS de terminer le travail. Pour approuver le RFC, recherchez-le dans la page de liste du RFC (il y aura un indicateur en attente d'approbation à côté), sélectionnez-le pour ouvrir la page de détails du RFC correspondant à ce RFC, puis choisissez Approuver. Notez que vous ne pourrez pas utiliser AMS tant que le RFC n'aura pas été approuvé.

Lorsque la RFC est terminée avec succès, AMS operations vous fournit le nouvel utilisateur IAM et un mot de passe. Suivez ensuite les étapes suivantes :

1. Accédez à la console AWS de gestion et connectez-vous à l'aide des informations d'identification fournies. Il vous sera demandé de créer un nouveau mot de passe. Vous devez également, lors de votre connexion, configurer l'authentification multifactorielle (MFA) ; pour en savoir plus à ce sujet, [voir Using Multi-Factor Authentication \(MFA\)](#) dans. AWS
2. Dans la console AWS de gestion, passez au rôle IAM fourni (customer_ *CustomerCode* _readonly_user_role).
3. Ouvrez la console AMS Managed Services.

Note

L'accès temporaire est par défaut de soixante jours ; toutefois, vous pouvez demander une prolongation de trente jours en contactant votre CSDM.

Accès aux instances à l'aide de bastions

Tous les accès aux ressources des comptes gérés par AMS, tant pour les clients que pour les opérateurs AMS, sont limités par l'utilisation d'hôtes bastion. Nous maintenons des bastions RDP Linux et Windows pour l'accès aux comptes AMS Advanced de zone d'atterrissage à comptes multiples (MALZ) et de zone d'atterrissage à compte unique (SALZ).

Vos bastions ne sont accessibles que via votre connexion privée (VPN ou AWS Direct Connect) DX. Outre le pare-feu destiné à empêcher le trafic entrant, les bastions sont régulièrement réapprovisionnés (avec les informations d'identification existantes) selon un calendrier fixe.

 Note

Pour plus d'informations sur le déplacement de fichiers vers une EC2 instance, voir [Transfert de fichiers : PC Windows ou MAC local vers Linux Amazon EC2](#).

MALZ

Vous accédez aux instances de votre compte en vous connectant à une instance Bastion avec vos informations d'identification Active Directory (AD). Amazon utilise des bastions situés dans le VPC (compte réseau) du réseau de périmètre, et vous utilisez les bastions de vos clients, situés dans votre sous-réseau Customer Bastions du compte de services partagés.

Lorsque votre environnement AMS est initialement intégré, vous disposez de deux bastions SSH et de deux bastions RDP selon votre choix.

SALZ

Vous accédez aux instances de votre compte en vous connectant à une instance Bastion avec vos informations d'identification Active Directory (AD). AMS utilise des bastions situés dans les sous-réseaux du réseau périmétrique, et vous utilisez des bastions situés dans vos sous-réseaux privés.

Lorsque votre compte est initialement intégré, vous disposez par défaut de deux bastions RDP et de deux bastions SSH.

 Note

Dans le cadre de la zone de landing zone à compte unique, AMS fournit à la fois des bastions RDP (Windows) et SSH (Linux) pour accéder à vos piles ; vous pouvez toutefois choisir de ne choisir que des bastions RDP ou uniquement des bastions SSH. Pour demander que seuls les bastions RDP ou SSH soient maintenus, soumettez une demande de service.

Pour accéder à une instance, vous devez :

- Accès accordé à la pile. Pour obtenir l'accès accordé à une pile, voir [Stack Admin Access | Accorder ou Stack Read-Only Access | Grant](#).

- L'ID de pile auquel vous souhaitez accéder afin de pouvoir accéder à l'instance. Pour trouver un identifiant de pile, consultez [Trouver une pile IDs dans AMS](#).
- L'adresse IP de l'instance à laquelle vous souhaitez accéder. Pour trouver l'adresse IP d'une instance, consultez [Rechercher une instance IDs ou une adresse IP dans AMS](#).
- Le nom du bastion convivial pour le DNS ou l'adresse IP du bastion. Comment utiliser des noms de bastion compatibles avec le DNS et comment trouver une adresse IP de bastion sont décrits ci-dessous.

Noms de bastion compatibles avec le DNS

AWS Managed Services (AMS) utilise des noms de bastions compatibles avec le DNS.

MALZ

Pour la zone de landing zone multi-comptes (MALZ), des enregistrements DNS sont créés pour les bastions dans le FQDN de l'Active Directory géré par AMS. AMS remplace les bastions Linux et Windows selon les besoins. Par exemple, si une nouvelle AMI bastion doit être déployée, les enregistrements DNS du bastion sont mis à jour dynamiquement pour pointer vers de nouveaux bastions valides.

1. Pour accéder aux bastions SSH (Linux), utilisez des enregistrements DNS comme celui-ci :
`sshbastion(1-4).Your_Domain.com`

Par exemple, lorsque le domaine est Your_Domain :

- `sshbastion1.Your_Domain.com`
- `sshbastion2.Your_Domain.com`
- `sshbastion3.Your_Domain.com`
- `sshbastion4.Your_Domain.com`

2. Pour accéder aux bastions RDP (Windows), utilisez des enregistrements DNS comme celui-ci : `rdp-Username.Your_Domain.com`

Par exemple, lorsque le nom d'utilisateur est alextest,demo, oubob, et le domaine est `Your_Domain.com` :

- `rdp-alex.Your_Domain.com`
- `rdp-test.Your_Domain.com`

- `rdp-demo.Your_Domain.com`
- `rdp-bob.Your_Domain.com`

SALZ

La zone de landing zone à compte unique (SALZ) remplace les bastions Linux et Windows selon les besoins. Par exemple, si une nouvelle AMI bastion doit être déployée, les enregistrements DNS du bastion sont mis à jour dynamiquement pour pointer vers de nouveaux bastions valides.

1. Pour accéder aux bastions SSH (Linux), utilisez des enregistrements DNS comme celui-ci : `sshbastion(1-4).AccountNumber.amazonaws.com`.

Par exemple, où se 123456789012 trouve le numéro de compte :

- `sshbastion1.A123456789012.amazonaws.com`
- `sshbastion2.A123456789012.amazonaws.com`
- `sshbastion3.A123456789012.amazonaws.com`
- `sshbastion4.A123456789012.amazonaws.com`

2. Pour accéder aux bastions RDP (Windows), utilisez des enregistrements DNS comme celui-ci : `rdpbastion(1-4).ACCOUNT_NUMBER.amazonaws.com`

Par exemple, où se 123456789012 trouve le numéro de compte :

- `rdpbastion1.A123456789012.amazonaws.com`
- `rdpbastion2.A123456789012.amazonaws.com`
- `rdpbastion3.A123456789012.amazonaws.com`
- `rdpbastion4.A123456789012.amazonaws.com`

Réduction des coûts sur les bastions de la zone d'atterrissage à compte unique (SALZ)

AMS fournit deux bastions SSH et deux bastions RDP dans la configuration par défaut pour vous permettre de vous connecter à vos EC2 instances Amazon, et déploie également deux bastions DMZ dans la configuration par défaut pour les opérations de service. Les bastions utilisent par défaut des EC2 instances Amazon de grande taille m4. Vous avez la possibilité de remplacer les EC2 instances Amazon utilisées pour les bastions par t3.small et de réduire les coûts.

Si vous utilisez des instances à la demande, des instances ponctuelles ou un plan d'épargne, vous devez envisager cette fonctionnalité et réduire les coûts. Si vous utilisez des instances réservées, déterminez si l'utilisation d'instances t3.small peut réduire vos coûts. Pour modifier le type d'instance, soumettez une RFC avec Management | Advanced stack components | EC2 instance stack | Resize (ct-15mazjj88xc69) CT depuis votre compte AMS.

Contactez votre responsable de prestation de services cloud (CSDM) pour toute question supplémentaire ou pour vérifier si vous pouvez bénéficier de cette fonctionnalité.

Utilisation des adresses IP bastions

Les clients AMS peuvent utiliser les bastions SSH et RDP, soit ceux [Noms de bastion compatibles avec le DNS](#) décrits précédemment, soit les adresses IP des bastions.

Pour trouver les adresses IP de Bastion, SSH et RDP, pour votre compte :

1. Pour la zone de landing zone multi-comptes uniquement : connectez-vous au compte Shared Services.
2. Ouvrez la EC2 console et choisissez Running Instances.

La page Instances s'ouvre.

3. Dans la zone de filtre en haut, entrez ssh-bastion ou rdp-bastion.

Dans le champ de filtre en haut, entrez customer-ssh ou customer-rdp.

Les bastions SSH and/or RDP pour l'affichage de votre compte.

Notez qu'en plus de vos bastions SSH, vous pouvez voir des bastions du réseau de périmètre AMS dans la liste, qui ne sont pas disponibles pour cela.

4. Sélectionnez un bastion SSH ou RDP. Si vous utilisez un ordinateur Windows et que vous souhaitez vous connecter à une instance Linux, vous devez utiliser un bastion SSH. Si vous souhaitez vous connecter à une instance Windows, vous devez utiliser un bastion RDP. Si vous utilisez un système d'exploitation Linux et que vous souhaitez vous connecter à une instance Windows, vous utilisez un bastion SSH via un tunnel RDP (cela vous permet d'accéder au bureau Windows). Pour accéder à une instance Linux depuis un système d'exploitation Linux, vous devez utiliser un bastion SSH.

Exemples d'accès aux instances dans AMS

Ces exemples montrent comment vous connecter à une instance dans votre compte AMS en utilisant un bastion après avoir obtenu l'accès via une RFC. Pour plus d'informations sur l'obtention de l'accès, consultez [Demande d'accès à une instance](#).

Note

Pour plus d'informations sur le déplacement de fichiers vers une EC2 instance, voir [Transfert de fichiers : PC Windows ou MAC local vers Linux Amazon EC2](#).

Données requises :

- Nom ou adresse IP convivial pour le DNS de Bastion : utilisez un nom convivial pour le DNS comme décrit dans [Noms de bastion compatibles avec le DNS](#) ou recherchez les adresses IP de Bastion comme décrit dans [Utilisation des adresses IP bastions](#)

Note

Une EC2 instance Amazon créée par le biais d'un groupe Amazon EC2 Auto Scaling aura une adresse IP qui entre et sort et vous devrez utiliser votre EC2 console Amazon pour trouver cette adresse IP.

- Nom d'utilisateur (par exemple `DOMAIN_FQDN\USERNAME`) et mot de passe : informations d'identification du compte. `USERNAME` Il doit s'agir de votre nom d'utilisateur Active Directory.

Notez qu'un nom d'utilisateur au format `username@customerdomain.com` peut être utilisé mais peut entraîner des problèmes avec votre configuration PBIS.

- Adresse IP de la pile : recherchez-la en consultant le résultat d'exécution de la RFC que vous avez soumise pour lancer la pile, ou recherchez l'adresse IP de l' EC2 instance Amazon dans la EC2 console Amazon. Pour une seule EC2 instance Amazon, vous pouvez également utiliser la commande AMS SKMS `ListStackSummaries` pour trouver l'ID de pile, puis `GetStack` pour trouver l'adresse IP de la pile. Pour la référence de l'API AMS SKMS, consultez l'onglet Rapports de la console AWS Artifact.

Accédez à l'adresse IP du bastion, SSH ou RDP, selon le cas, et connectez-vous à l'aide de l'une des procédures suivantes.

 Note

Les bastions RDP n'autorisent que deux connexions simultanées. Ainsi, dans le meilleur des cas, seuls 4 administrateurs peuvent se connecter à Windows Stacks en même temps. Si vous avez besoin de davantage de connexions pour RDP, consultez les [options d'AMS Bastion lors de la migration/de l'intégration des applications dans le guide d'intégration d'AMS](#).

Ordinateur Linux vers instance Linux

Utilisez SSH pour vous connecter au bastion SSH, puis à l'instance Linux.

MALZ

Pour plus d'informations sur les noms de bastions conviviaux, consultez la section [Bastions DNS](#).

Pour vous connecter à l'instance Linux, vous devez d'abord vous connecter à un bastion SSH.

1. Ouvrez une fenêtre shell et entrez :

```
ssh Domain_FQDN\\Username@SSH_bastion_name  
or SSH_bastion_IP
```

Ce qui ressemblerait à ceci si votre domain_FQDN est « corp.domain.com », votre numéro de compte est « 123456789123 », votre domaine est « amazonaws.com », vous choisissez le bastion « 4 » et votre nom d'utilisateur est « » : JoeSmith

```
ssh corp.domain.com\\JoeSmith sshbastion4.A123456789123.amazonaws.com
```

2. Connectez-vous à l'aide des informations d'identification Active Directory de votre entreprise.
3. Lorsque vous recevez une invite Bash, connectez-vous à l'instance en SSH, puis entrez :

```
ssh Domain_FQDN\\Username@Instance_IP
```

Vous pouvez également utiliser l'indicateur de connexion (-l) :

```
ssh -l Domain_FQDN\\Username@Instance_IP
```


SALZ

Pour plus d'informations sur les noms de bastions conviviaux, consultez la section [Bastions DNS](#).

Pour vous connecter à l'instance Linux, vous devez d'abord vous connecter à un bastion SSH.

1. Ouvrez une fenêtre shell et entrez :

```
ssh DOMAIN_FQDN\\USERNAME@SSH_BASTION_name  
or SSH_BASTION_IP
```

Cela ressemblerait à ceci si votre numéro de compte est 123456789123, que vous choisissiez le bastion 4 et que votre nom d'utilisateur est : JoeSmith

```
ssh corp.domain.com\\JoeSmith sshbastion1.A123456789123.amazonaws.com
```

2. Connectez-vous à l'aide des informations d'identification Active Directory de votre entreprise.
3. Lorsque vous recevez une invite Bash, connectez-vous à l'instance en SSH, puis entrez :

```
ssh DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

Vous pouvez également utiliser l'indicateur de connexion (-l) :

```
ssh -l DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

Ordinateur Linux vers instance Windows

Utilisez un tunnel SSH et un client RDP pour vous connecter à une instance Windows depuis votre ordinateur Linux.

MALZ

Cette procédure nécessite un client Remote Desktop Connection pour Linux ; l'exemple utilise Microsoft Remote Desktop (un client UNIX open source pour la connexion aux services Windows Remote Desktop). Rdesktop est une alternative.

 Note

La façon dont vous vous connectez aux instances Windows peut changer en fonction du client de bureau à distance utilisé.

Vous établissez d'abord un tunnel SSH, puis vous vous connectez.

Pour plus d'informations sur les noms sympathiques des bastions, consultez [Noms de bastion compatibles avec le DNS](#).

Avant de commencer :

- Demandez l'accès à l'instance à laquelle vous souhaitez vous connecter ; pour plus d'informations, consultez la section [Demandes d'accès](#).
- Choisissez un nom de bastion DNS SSH convivial auquel vous connecter ; par exemple :

```
sshbastion(1-4).Your_Domain
```

Ce qui ressemblerait à ceci si votre domain_FQDN est « corp.domain.com », votre domaine Your_Domain géré par AMS est « amazonaws.com », vous choisissez le bastion « 4 » et votre nom d'utilisateur est « » : JoeSmith

```
ssh corp.domain.com\\JoeSmith sshbastion4.amazonaws.com
```

- Trouvez l'adresse IP de l'instance à laquelle vous souhaitez vous connecter ; pour plus d'informations, consultez la section [Recherche d'un ID ou d'une adresse IP d'instance](#).
1. Configurez le protocole RDP via un tunnel SSH entre un poste de travail Linux et une instance Windows. Pour émettre la ssh commande avec les bonnes valeurs, vous pouvez procéder de plusieurs manières :
 - Dans le shell Linux, définissez les variables, puis entrez la commande de connexion SSH :

```
BASTION="sshbastion(1-4).Your_Domain"  
WINDOWS="Windows_Instance_Private_IP"  
AD="AD_Account_Number"  
USER="AD_Username"  
ssh -L 3389:$WINDOWS:3389 A$AD\\\\$USER@$BASTION
```

Par exemple, si les valeurs suivantes sont utilisées :

```
BASTION="sshbastion4.A123456789123.amazonaws.com"
```

```
WINDOWS="172.16.3.254"
```

```
AD="ACORP_example"
```

```
USER="john.doe"
```

- Ajoutez les valeurs des variables directement à la ssh commande.

Dans les deux cas, voici ce que serait la demande rendue (en supposant le même ensemble de valeurs de variables) :

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\\john.doe@myamsadomain.com
```

2. Soit : ouvrez votre client Remote Desktop, entrez l'adresse et le port de boucle, 127.0.0.1:3389, puis ouvrez la connexion.

Vous pouvez également vous connecter à l'instance Windows à partir d'un nouveau shell de bureau Linux. Si vous l'utilisez RDesktop, la commande ressemble à ceci :

```
rdesktop 127.0.0.1:3389
```

Une fenêtre de bureau à distance pour l'instance Windows apparaît sur votre bureau Linux.

 Tip

Si la session de bureau à distance ne démarre pas, vérifiez que la connectivité réseau à l'instance Windows depuis le bastion SSH est autorisée sur le port 3389 du shell à l'étape 1 (remplacez `private_ip_address_of_windows_instance` de manière appropriée) :

```
nc private_ip_address_of_windows_instance 3389 -v -z
```

Succès :

```
nc 172.16.0.83 3389 -v -z
```

```
Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
netstat -anvp | grep 3389
tcp    0      0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
```

SALZ

Cette procédure pour une zone d'atterrissage à compte unique nécessite un client Remote Desktop Connection pour Linux ; l'exemple utilise Microsoft Remote Desktop (un client UNIX open source pour la connexion aux services Windows Remote Desktop). Rdesktop est une alternative.

Note

La façon dont vous vous connectez aux instances Windows peut changer en fonction du client de bureau à distance utilisé.

Vous établissez d'abord un tunnel SSH, puis vous vous connectez.

Pour plus d'informations sur les noms sympatiques des bastions, consultez [Noms de bastion compatibles avec le DNS](#).

Avant de commencer :

- Demandez l'accès à l'instance à laquelle vous souhaitez vous connecter ; pour plus d'informations, consultez la section [Demandes d'accès](#).
- Choisissez un nom de bastion DNS SSH convivial auquel vous connecter ; par exemple :

```
sshbastion(1-4).AMSAccountNumber.amazonaws.com
```

Ce qui ressemblerait à ceci si votre numéro de compte est 123456789123 et que vous choisissez le bastion 4 :

```
sshbastion4.A123456789123.amazonaws.com
```

- Trouvez l'adresse IP de l'instance à laquelle vous souhaitez vous connecter ; pour plus d'informations, consultez la section [Recherche d'un ID ou d'une adresse IP d'instance](#).

1. Configurez le protocole RDP via un tunnel SSH entre un poste de travail Linux et une instance Windows. Pour émettre la `ssh` commande avec les bonnes valeurs, vous pouvez procéder de plusieurs manières :
 - Dans le shell Linux, définissez les variables, puis entrez la commande de connexion SSH :

```
BASTION="sshbastion(1-4).AMSAccountNumber.amazonaws.com"
WINDOWS="WINDOWS_INSTANCE_PRIVATE_IP"
AD="AD_ACCOUNT_NUMBER"
USER="AD_USERNAME"
ssh -L 3389:$WINDOWS:3389 A$AD\\\\"$USER@$BASTION
```

Par exemple, si les valeurs suivantes sont utilisées :

```
BASTION="sshbastion4.A123456789123.amazonaws.com"
```

```
WINDOWS="172.16.3.254"
```

```
AD="ACORP_example"
```

```
USER="john.doe"
```

- Ajoutez les valeurs des variables directement à la `ssh` commande.

Dans les deux cas, voici ce que serait la demande rendue (en supposant le même ensemble de valeurs de variables) :

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\\"
\\john.doe@sshbastion4.A123456789123.amazonaws.com
```

2. Soit : ouvrez votre client Remote Desktop, entrez l'adresse et le port de boucle, 127.0.0.1:3389, puis ouvrez la connexion.

Vous pouvez également vous connecter à l'instance Windows à partir d'un nouveau shell de bureau Linux. Si vous l'utilisez RDesktop, la commande ressemble à ceci :

```
rdesktop 127.0.0.1:3389
```

Une fenêtre de bureau à distance pour l'instance Windows apparaît sur votre bureau Linux.

 Tip

Si la session de bureau à distance ne démarre pas, vérifiez que la connectivité réseau à l'instance Windows depuis le bastion SSH est autorisée sur le port 3389 du shell à l'étape 1 (remplacez `private_ip_address_of_windows_instance` de manière appropriée) :

```
nc private_ip_address_of_windows_instance 3389 -v -z
```

Succès :

```
nc 172.16.0.83 3389 -v -z
    Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
netstat -anvp | grep 3389
tcp      0      0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
```

Ordinateur Windows vers instance Windows

Utilisez le client Windows Remote Desktop Connection pour vous connecter à une instance Windows depuis votre ordinateur Windows.

MALZ

Pour plus d'informations sur les noms sympatiques des bastions, consultez [Noms de bastion compatibles avec le DNS](#).

1. Ouvrez le programme Remote Desktop Connection, un programme Windows standard, et entrez le nom DNS convivial du bastion Windows dans le champ du nom d'hôte.
2. Choisissez Se connecter. La connexion Remote Desktop tente d'établir une connexion RDP avec le bastion.

En cas de succès, une boîte de dialogue d'identification s'ouvre. Pour y accéder, utilisez les informations d'identification Active Directory de votre entreprise, comme vous le feriez avec l'instance Windows.

3. Ouvrez le programme Remote Desktop Connection sur le bastion et entrez l'adresse IP de l'instance Windows à laquelle vous souhaitez vous connecter (par exemple, 10.0.0.100), puis choisissez Connect. Les informations d'identification Active Directory de votre entreprise sont à nouveau requises avant de vous connecter à l'instance Windows.

SALZ

Pour plus d'informations sur les noms sympathiques des bastions, consultez [Noms de bastion compatibles avec le DNS](#).

1. Ouvrez le programme Remote Desktop Connection, un programme Windows standard, et entrez le nom DNS convivial du bastion Windows dans le champ du nom d'hôte ; par exemple `rdpbastion(1-4).AMSAccountNumber.amazonaws.com`, ce qui ressemblerait à ceci si votre numéro de compte est 123456789123 et que vous choisissiez le bastion 4, `rdpbastion4.A123456789123.amazonaws.com`
2. Choisissez Se connecter. La connexion Remote Desktop tente d'établir une connexion RDP avec le bastion.

En cas de succès, une boîte de dialogue d'identification s'ouvre. Pour y accéder, utilisez les informations d'identification Active Directory de votre entreprise, comme vous le feriez avec l'instance Windows.

3. Ouvrez le programme Remote Desktop Connection sur le bastion et entrez l'adresse IP de l'instance Windows à laquelle vous souhaitez vous connecter (par exemple, 10.0.0.100), puis choisissez Connect. Les informations d'identification Active Directory de votre entreprise sont à nouveau requises avant de vous connecter à l'instance Windows.

Ordinateur Windows vers instance Linux

Pour utiliser le protocole RDP vers un bastion SSH depuis un environnement Windows, procédez comme suit.

MALZ

Avant de commencer :

- Demandez l'accès à l'instance à laquelle vous souhaitez vous connecter ; pour plus d'informations, consultez la section [Demandes d'accès](#).
- Choisissez un nom de bastion DNS SSH convivial auquel vous connecter ; par exemple :

```
sshbastion(1-4).YOUR_DOMAIN
```

Ce qui ressemblerait à ceci si « YOUR_DOMAIN » était « myamsaddomain.com » et que vous choisissiez le bastion 4 :

```
sshbastion4.myamsaddomain.com
```

- Trouvez l'adresse IP de l'instance à laquelle vous souhaitez vous connecter ; pour plus d'informations, consultez la section [Recherche d'un ID ou d'une adresse IP d'instance](#).

Pour vous connecter à l'instance Linux depuis votre machine Windows, vous devez d'abord vous connecter à un bastion SSH.

Utilisez le client Windows [OpenSSH](#) natif ou installez [PuTTY](#) sur votre machine locale. Pour en savoir plus sur OpenSSH, consultez [OpenSSH](#) sous Windows.

1. Utilisez le système Windows natif ou ouvrez PuTTY et entrez le nom d'hôte du bastion SSH ou l'adresse IP du bastion SSH. Par exemple, 10.65.2.214 (22 est le port utilisé pour SSH ; il sera défini par défaut).
2. OpenSSH ou PuTTY tente d'établir une connexion SSH avec le bastion et ouvre une fenêtre shell.
3. Utilisez les informations d'identification Active Directory de votre entreprise comme vous le feriez avec les hôtes RDP pour y accéder.
4. Lorsque vous recevez une invite Bash, connectez-vous à l'instance en SSH. Entrez :

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```


SALZ

Avant de commencer :

- Demandez l'accès à l'instance à laquelle vous souhaitez vous connecter ; pour plus d'informations, consultez la section [Demandes d'accès](#).
- Choisissez un nom de bastion DNS SSH convivial auquel vous connecter ; par exemple :

```
sshbastion(1-4).AMSAccountNumber.amazonaws.com
```

Ce qui ressemblerait à ceci si votre numéro de compte est 123456789123 et que vous choisissiez le bastion 4 :

```
sshbastion4.A123456789123.amazonaws.com
```

- Trouvez l'adresse IP de l'instance à laquelle vous souhaitez vous connecter ; pour plus d'informations, consultez la section [Recherche d'un ID ou d'une adresse IP d'instance](#).

Pour vous connecter à l'instance Linux depuis votre machine Windows, vous devez d'abord vous connecter à un bastion SSH.

Utilisez le client Windows [OpenSSH](#) natif ou installez [PuTTY](#) sur votre machine locale. Pour en savoir plus sur OpenSSH, consultez [OpenSSH](#) sous Windows.

1. Utilisez le système Windows natif ou ouvrez PuTTY et entrez le nom d'hôte du bastion SSH ou l'adresse IP du bastion SSH. Par exemple, 10.65.2.214 (22 est le port utilisé pour SSH ; il sera défini par défaut).
2. OpenSSH ou PuTTY tente d'établir une connexion SSH avec le bastion et ouvre une fenêtre shell.
3. Utilisez les informations d'identification Active Directory de votre entreprise comme vous le feriez avec les hôtes RDP pour y accéder.
4. Lorsque vous recevez une invite Bash, connectez-vous à l'instance en SSH. Entrez :

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

Contrôle d'accès basé sur l'équipe ou le rôle dans un compte AMS

Scénario : deux équipes d'application A et B utilisent un seul compte AMS pour leurs applications « AA » et « BB », respectivement. L'équipe A souhaite accéder uniquement aux ressources de l'application « AA », et l'équipe B souhaite accéder uniquement aux ressources de l'application « BB ». Comment puis-je le configurer ?

Utilisez les outils de leur ITSM pour mettre en œuvre des contrôles d'accès basés sur l'équipe (TBAC). Par exemple, vous pouvez utiliser l'application AMS ServiceNow Connector pour l'intégration à AMS APIs. Contactez votre CSDM pour obtenir des conseils de haut niveau sur cette mise en œuvre.

Configuration d'instance automatisée dans AMS Advanced

Le service de configuration automatique des instances AMS Advanced s'exécute quotidiennement et analyse et met à jour automatiquement le SSM, les CloudWatch agents et les fichiers de configuration sur vos EC2 instances gérées. Les mises à jour s'appliquent, le cas échéant, à :

- SSM et agents CloudWatch
- CloudWatch fichiers de configuration

Ces mises à jour permettent à AMS d'accéder à vos EC2 instances gérées par AMS et de configurer vos instances pour qu'elles émettent des [journaux et des métriques](#) appropriés.

Rubriques

- [Conditions préalables à la configuration automatique des instances](#)
- [Installation automatique de l'agent SSM](#)
- [Modifications automatisées](#)

Conditions préalables à la configuration automatique des instances

Pour les clients AMS Advanced qui déploient des instances avec Change Management, les conditions préalables suivantes doivent être remplies :

- L'agent SSM est installé et est géré.
- L'instance est étiquetée en tant qu'instance gérée. (La valeur de la `aws:cloudformation:stack-name` balise commence par `stack-` ou `sc-`.)

Si l'agent SSM n'est pas déjà installé sur votre instance, vous pouvez l'installer à l'aide de la fonction d'installation automatique de l'agent AMS SSM. Pour de plus amples informations, veuillez consulter [Installation automatique de l'agent SSM](#).

Vous pouvez également installer l'agent SSM manuellement. Pour plus d'informations, consultez les ressources suivantes :

- Linux : [installation manuelle de l'agent SSM sur EC2 les instances pour Linux - AWS Systems Manager](#)

- Windows : [installation manuelle de l'agent SSM sur EC2 les instances pour Windows Server - AWS Systems Manager](#)

Pour plus d'informations sur l'agent SSM, consultez la documentation AWS [Working with SSM](#) Agent.

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

- 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.
- La fonctionnalité d'installation automatique de l'agent AMS SSM est désactivée par défaut. Pour l'activer, contactez votre autorité de certification ou votre CSDM.

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 SSMManged EC2 InstanceDefaultPolicy
 - Amazon SSMManged 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 automatisées

Le service de configuration d'instance automatique AMS Advanced apporte les modifications nécessaires à vos EC2 instances.

Quels sont les changements :

- [Mettre à jour automatiquement le code sur les instances Linux](#)
- [Mettre à jour automatiquement le PBIS sur les instances Linux](#)
- [Mettre à jour automatiquement la version minimale de SSM et des agents CloudWatch](#)
- [CloudWatch fichiers de configuration, détails des mises à jour](#)
- [Logs configurés automatiquement](#)

Mettre à jour automatiquement le code sur les instances Linux

AMS met automatiquement à jour le code d'instance sur les instances Linux. Cela permet d'améliorer la stabilité opérationnelle et la sécurité des composants et de l'environnement AMS dans leur ensemble.

FAQ :

Qu'est-ce qui est inclus dans le code On Instance (OIC) sous Linux ?

L'OIC inclut le package ams-toolkit ainsi que des fichiers de configuration et des tâches cron. AMS a besoin de ces fichiers et packages pour l'intégration (Active Directory CloudFormation et autres dépendances). Nous préinstallons ces fichiers dans l'instance fournie par AMS AMIs ou nous les installons sur votre instance lors de l'ingestion de la charge de travail.

Quand AMS mettra-t-il à jour l'OCI ?

AMS met à jour OIC lorsque nous publions une nouvelle version contenant des corrections de bogues ou d'autres améliorations. Le flux de travail pour vérifier la version et la mise à jour de l'OCI s'exécute quotidiennement.

Mettre à jour automatiquement le PBIS sur les instances Linux

AMS utilise le module Power Broker Identity Service (PBIS) pour joindre des instances Linux à Active Directory géré par AMS.

AMS met automatiquement à jour le PBIS sur les instances Linux.

FAQ :

Quand est-ce qu'AMS mettra à jour le PBIS ?

AMS active la mise à jour du PBIS au redémarrage. Si une nouvelle version de PBIS est disponible, AMS tente de l'installer lors du prochain redémarrage de l'instance.

La mise à jour du PBIS peut-elle être désactivée ?

Vous pouvez désactiver la mise à jour du PBIS au niveau de l'instance ou du compte :

- Niveau du compte : créez un paramètre dans le magasin de paramètres SSM : Nom : `/ams/skip-pbis-update`, Valeur : `true` (dans tous les cas).

Note

Le profil d'instance doit être autorisé à lire les paramètres SSM. Si l'indicateur est absent, le comportement par défaut consiste à exécuter la mise à jour.

- Niveau de l'instance :
 - Basé sur des balises : ajoutez la balise suivante à l'instance : Key : `skip_pbis_update`, Value : `true` (dans tous les cas).
 - Fichier de configuration : ajoutez l'indicateur suivant au `/opt/aws/ams/etc/ams.conf.d/state.ini` fichier : `skip_pbis_update = true`.

 Note

La balise a une priorité plus élevée que le paramètre SSM. Vous pouvez désactiver la mise à jour du PBIS au niveau du compte via le paramètre, mais l'activer pour une (ou plusieurs) instance (s) en ajoutant une `baliseKey: skip_pbis_update, Value: false`.

Pour configurer l'une des options décrites, suivez le processus de gestion des modifications standard dans votre environnement AMS.

Mettre à jour automatiquement la version minimale de SSM et des agents CloudWatch

La version minimale AMS Advanced (du SSM ou des CloudWatch agents) est la version qui a été testée par l'équipe de service AMS et préapprouvée pour votre système d'exploitation. Nous essayons de rester proactifs et d'utiliser la dernière version stable et compatible, de sorte que le numéro de version change au fil du temps. Vous pouvez trouver la version minimale actuelle en soumettant une demande de service à AMS.

- Gestion des agents SSM

L'agent Amazon 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.

- Gestion des agents Cloudwatch

L' CloudWatch agent Amazon est responsable de l'émission des journaux et des métriques du système d'exploitation. La configuration automatique des instances effectue les opérations suivantes :

- Si nécessaire, désactive l'ancien agent CloudWatch Log et migre la configuration vers le nouvel agent unifié CloudWatch
- Si votre instance exécute l'ancien CloudWatch Log Agent, la configuration automatique de l'instance désactive l'ancien service CloudWatch Log Agent et migre sa configuration vers l'agent unifié CloudWatch .
- Personnalise votre CloudWatch configuration pour émettre des journaux et des métriques appropriés.

Fichiers et répertoires concernés :

- Windows
 - % ProgramData % \ Amazon \ AmazonCloudWatchAgent \
 - % ProgramData % \ Amazon \ AmazonCloudWatchAgent \ Configurations \
- Linux
 - /opt/aws/amazon-cloudwatch-agent/etc/
 - /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/
 - /opt/aws/ams/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json

CloudWatch fichiers de configuration, détails des mises à jour

Nous lisons vos CloudWatch configurations personnalisées (JSON uniquement) dans les CloudWatch répertoires suivants (voir les [répertoires recommandés](#)) et les fusionnons avec la CloudWatch configuration AMS standard :

- CloudWatch Dossiers
 - Sur l'instance :
 - Windows
 - % ProgramData % \ Amazon \ AmazonCloudWatchAgent \ Configurations \
 - % ProgramFiles % \ \ Modules WindowsPowerShell \ AWSManaged Services.Logging.Utilities \ Files \ Config.json
 - Linux
 - /opt/aws/ams/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json
 - Sur Amazon S3 :
 - Windows :
 - [https://ams-configuration-artifacts-*REGION_NAME*.s3.*REGION_NAME*.amazonaws.com/configurations/cloudwatch/latest/windows-cloudwatch-config.json](https://ams-configuration-artifacts-<i>REGION_NAME</i>.s3.<i>REGION_NAME</i>.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](https://ams-configuration-artifacts-<i>REGION_NAME</i>.s3.<i>REGION_NAME</i>.amazonaws.com/configurations/cloudwatch/latest/linux-cloudwatch-config.json)

Logs configurés automatiquement

Nous configurons votre instance pour écrire les journaux suivants.

- 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

Surveillance et gestion des événements dans AMS

Rubriques

- [Qu'est-ce que le monitoring ?](#)
- [Qu'est-ce que le système de surveillance AMS surveille ?](#)
- [Fonctionnement de la surveillance](#)
- [Affichage de la configuration de surveillance pour un compte AMS](#)
- [Modification de la configuration de surveillance d'un compte AMS](#)
- [Notifications d'incidents liées aux applications dans AMS](#)
- [Utilisation OpsCenter dans AMS](#)
- [Notifications d'alerte d'AMS](#)
- [Création d' CloudWatch alarmes supplémentaires dans AMS](#)
- [Création de CloudWatch métriques et d'alarmes personnalisées dans AMS](#)
- [Utilisation CloudWatch d'Application Insights pour .Net et SQL Server dans AMS](#)
- [Utilisation des règles EventBridge gérées par Amazon dans AMS](#)
- [Remédiateur fiable dans AMS](#)

Le système de surveillance AWS Managed Services (AMS) surveille vos ressources AMS pour détecter les défaillances, les dégradations de performances et les problèmes de sécurité. Le système de surveillance AMS repose sur des services AWS tels qu'Amazon CloudWatch (CloudWatch), Amazon GuardDuty, Amazon Macie et. AWS Health Outre le système de surveillance, AMS déploie également des dispositifs de protection contre TrendMicro DeepSecurity les malwares sur les instances Amazon Elastic Compute Cloud (Amazon EC2). Pour plus d'informations sur les paramètres de sécurité des terminaux (EPS) par défaut, voir. [Sécurité des terminaux \(EPS\)](#)

La surveillance AMS offre les avantages suivants :

- 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 plus d'informations, consultez [Alertes issues de la surveillance de base dans AMS](#).
- Alertes d'investigation pour déterminer l'action appropriée. Par exemple, s'il GuardDuty détecte une activité indiquant des tentatives de force brute contre une EC2 instance Amazon, AMS analyse les journaux de flux VPC pour comprendre l'origine et le contexte de l'activité.

- Corriger les alertes, 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 bilan de santé du système, AMS tente de récupérer l'instance en l'arrêtant puis en la redémarrant. Pour de plus amples informations, veuillez consulter [Correction automatique des alertes par AMS](#).
- Transparence des alertes actives et précédemment résolues à l'aide de OpsCenter. Par exemple, si vous constatez une utilisation élevée du processeur inattendue sur une EC2 instance Amazon, vous pouvez demander l'accès à la console AWS Systems Manager (y compris l'accès à la OpsCenter console) et le consulter OpsItem directement dans la OpsCenter console.

Qu'est-ce que le monitoring ?

Le système de surveillance AMS surveille vos AWS ressources pour détecter les défaillances, la dégradation des performances et les problèmes de sécurité. En tant que compte géré, AMS configure et déploie des alarmes pour les AWS ressources applicables, les surveille et effectue des corrections le cas échéant.

Le système de surveillance AMS génère des alertes en fonction de la configuration de surveillance de votre compte. La configuration de surveillance d'un compte fait référence à tous les paramètres de ressources du compte qui créent une alerte ; pour plus d'informations sur les paramètres des ressources, consultez [Alertes issues de la surveillance de base dans AMS](#). La configuration de surveillance d'un compte inclut les définitions CloudWatch d'alarme et les règles d' CloudWatch événement qui génèrent l'alerte (alarme ou événement).

La configuration de surveillance de base est l'ensemble de définitions d'alarmes ([Alertes issues de la surveillance de base dans AMS](#)) créé par AMS pour surveiller les ressources de votre compte géré. La configuration de surveillance d'un compte peut différer de la configuration de base en raison des modifications que vous avez demandées.

Une notification signalant des défaillances imminentes, en cours, en cours ou potentielles, une dégradation des performances ou des problèmes de sécurité générés par la surveillance de base configurée dans un compte est appelée alerte. Des exemples d'alertes sont une CloudWatch alarme Amazon, un CloudWatch événement Amazon, un événement ou un résultat d'un service AWS tel qu'Amazon GuardDuty, et un événement, ou une alerte, provenant de Trend Micro Deep Security.

Les alertes provenant de services AWS liés à la sécurité tels qu'Amazon GuardDuty, Amazon Macie ou Trend Micro Deep Security sont appelées alertes de sécurité afin de les différencier des autres types d'alertes.

La surveillance AMS offre les avantages suivants :

- Possibilité de personnaliser les alarmes relatives aux ressources de base en fonction de vos besoins.
- Correction automatique des alertes, 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](#).
- Transparence 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.
- 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, consultez [Alertes 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). Les alertes incluent par exemple une CloudWatch alarme, un événement ou une découverte provenant d'un service AWS, tel que GuardDuty ou AWS Health.

Qu'est-ce que le système de surveillance AMS surveille ?

Conformément au modèle de responsabilité des services partagés d'AWS Managed Services (AMS), le système de surveillance AMS surveille votre infrastructure AWS. Pour plus de détails sur la surveillance de base dans AMS, y compris les ressources AWS surveillées et le type d'alertes pour chaque ressource, consultez [Alertes issues de la surveillance de base dans AMS](#). Pour les EC2 instances Amazon, AMS surveille le système d'exploitation et fournit une surveillance de base basée sur des indicateurs du système d'exploitation tels que l'utilisation du processeur et l'utilisation du volume racine.

Nous vous recommandons de compléter la surveillance AMS par une surveillance supplémentaire à l'aide des services AWS adaptés à votre application. Pour obtenir des conseils sur la surveillance de la disponibilité, consultez la section « Surveillance et alarme » de ce livre blanc sur le pilier de [la fiabilité](#). Vous pouvez configurer votre propre surveillance en fonction de vos besoins opérationnels ; la procédure à suivre est expliquée dans [Création d' CloudWatch alarmes supplémentaires dans AMS](#) et [Création de CloudWatch métriques et d'alarmes personnalisées dans AMS](#).

Surveillance proactive d'Active Directory Trust dans AMS via une zone d'atterrissage à compte unique

La zone de landing zone à compte unique (SALZ) AMS surveille l'état des relations de confiance unidirectionnelles entre le Managed Active Directory (AD) de votre compte géré AMS et le domaine de votre entreprise. La confiance unidirectionnelle avec Managed AD est essentielle pour les demandes d'accès et les demandes d'ouverture de session d'instance. Grâce à cette nouvelle surveillance, AMS répond désormais de manière proactive aux problèmes liés à la confiance et réduit le temps moyen de détection des incidents liés à l'accès.

Cette fonctionnalité est automatiquement activée dans vos comptes AWS Managed Services (AMS).

L'impact sur les coûts est faible. La fonctionnalité utilise quatre CloudWatch métriques AWS et deux CloudWatch alarmes AWS pour une confiance.

Fonctionnement de la surveillance

Consultez les graphiques suivants sur l'architecture de surveillance dans AWS Managed Services (AMS).

Le schéma suivant fournit une vue d'ensemble du flux de travail de surveillance des zones d'atterrissage multi-comptes AMS et des zones d'atterrissage monocomptes 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** :

- Zone d'accueil multi-comptes : les alertes sont générées par vos ressources au sein des comptes de l'application et de l'unité organisationnelle principale et envoyées au système de surveillance AMS en les dirigeant via le compte Security.
- Zone d'accueil à compte unique : 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. 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. Cela fonctionne de la même manière, que vous utilisiez une zone d'atterrissage multi-comptes ou une zone d'atterrissage à compte unique.
- 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 ; pour plus d'informations sur la gestion des incidents, voir [Réponse aux incidents AMS](#).

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 dans [Fonctionnement 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

Affichage de la configuration de surveillance pour un compte AMS

La configuration de surveillance d'un compte comporte deux éléments essentiels que vous pouvez consulter :

- CloudWatch Alarmes : vous pouvez afficher toutes les alarmes CW du compte en accédant à la CloudWatch console et en sélectionnant les différents services qui vous intéressent.
- CloudWatch Événements :
 - Zone d'accueil multi-comptes : les CloudWatch événements surveillés dans le compte peuvent être trouvés en filtrant toutes les règles relatives aux événements CW à l'aide de la chaîne.
"ams - "

- Zone d'accueil à compte unique : les CloudWatch événements surveillés dans le compte peuvent être trouvés en filtrant toutes les règles relatives aux événements CW à l'aide de la chaîne.
"mc - "

Modification de la configuration de surveillance d'un compte AMS

Vous pouvez modifier votre configuration de surveillance de base pour les EC2 ressources Amazon. Pour les alertes qui peuvent être configurées, consultez [Alertes issues de la surveillance de base dans AMS](#). Vous pouvez modifier la définition de l'alarme, la destination de l'alarme ou désactiver la notification d'alarme pour les moniteurs de base afin que les alertes répondent aux exigences opérationnelles de votre application. Vous pouvez demander tout ou partie des modifications mentionnées précédemment en soumettant un CT de gestion | Autre | Autre | Mise à jour (ct-0xdawir96cy7k) avec les détails suivants.

- Instance IDs [facultatif, si ce n'est pas mentionné, toutes les instances du compte sont incluses]
- CloudWatch nom de la métrique, par exemple, utilisation du processeur/swap free/ IOwait
- Cible : adresse e-mail, numéro de téléphone pour le sujet SMS ou SNS

Pour en savoir plus sur le type de modifications que vous pouvez demander dans la configuration de surveillance de base, consultez la [CloudWatch documentation Amazon](#).

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 AppRegistry](#) afin 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 le provisionner AWS Service Catalog AppRegistry dans votre compte AMS.

Pour en savoir plus sur les paramètres de surveillance par défaut d'AMS, consultez [Surveillance et gestion des événements dans AMS](#).

Fournissez AppRegistry des informations sur votre compte AMS et créez des applications

Le AppRegistry service est disponible en mode Self-service Provisioning (SSP) pour votre compte AMS. Pour obtenir des instructions sur la façon de demander l'accès, voir [Utiliser le SSP AMS pour le provisionnement AWS Service Catalog AppRegistry de votre compte AMS](#).

Après le provisionnement AppRegistry, 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 console AWS, 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 .

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.

Clé de balise	Valeur de balise
géré par des tiers	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 [SeverityLevel](#) la 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-*
```

Utilisation OpsCenter dans AMS

L'équipe opérationnelle d'AWS Managed Services (AMS) utilise [AWS Systems Manager OpsCenter](#) pour diagnostiquer et corriger de nombreuses alertes liées à vos ressources.

L'utilisation OpsCenter réduit le temps moyen de résolution (MTTR), tout en offrant une vue transparente des files d'attente opérationnelles des équipes opérationnelles d'AMS.

AMS vous fournit une vue transparente des éléments de travail opérationnels, également appelés « tâches sur [OpsItems](#) » auxquelles travaillent activement les équipes AMS », en plus des solutions automatisées. OpsCenter

Pour en savoir plus sur OpsCenter et OpsItems, voir [AWS Systems Manager OpsCenter](#). Pour plus d'informations sur l'accès à la console AWS de gestion, consultez la section [Utilisation de la console de gestion AWS](#). Depuis l'AWS Management Console, vous pouvez accéder à la console AWS Systems Manager et OpsCenter, pour en savoir plus, consultez [AWS Systems Manager Session Manager](#). OpsCenter fournit également une API que vous pouvez utiliser ; pour plus d'informations, voir [En savoir plus sur OpsCenter](#).

OpsCenter est une fonctionnalité payante d'environ 1 000€ OpsItems qui coûte moins de 10\$. Pour obtenir des informations, veuillez consulter [Tarification AWS Systems Manager](#).

Notifications d'alerte d'AMS

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 ; consultez le schéma de l'architecture de surveillance AMS pour le processus de gestion des alertes dans [Fonctionnement de la surveillance](#).

Réception d'alertes générées par AMS

AWS Managed Services (AMS) vous permet de recevoir directement des notifications d'alerte pour les EC2 ressources Amazon afin de réduire les délais de communication. Pour recevoir directement des EC2 alertes Amazon, inscrivez votre cible (e-mail préféré) à la rubrique Amazon SNS Direct-Customer-Alerts en utilisant le type de modification Gestion | Surveillance et notification | SNS | Abonnement (ct-3rc19u1k017wu).

Note

Toutes les alertes de base ne sont pas envoyées par défaut à la rubrique Direct-Customer-Alerts. Pour voir toutes les alertes générées par le système de surveillance AMS, abonnez-vous à la rubrique Amazon SNS relative au système de surveillance AMS. Dans la demande, demandez le « sujet de surveillance AMS », spécifiez un canal d'abonnement pour recevoir les alertes (Lambda, Amazon SQS, HTTP/S, e-mail ou SMS) et spécifiez les points de terminaison (par exemple, les adresses e-mail, si vous choisissez le protocole e-mail) qui recevront les alertes.

La rubrique de surveillance AMS reçoit des alertes utilisées par les services partagés AMS. Elle peut donc être bruyante.

Pour en savoir plus, consultez la section [Subscribe](#) de la référence de l'API d'abonnement d'Amazon Simple Notification Service.

Pour obtenir la liste des alertes de base fournies par AMS, consultez [Alertes issues de la surveillance de base dans AMS](#).

Notifications d'alerte basées sur des balises dans AMS

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.

Important

Les notifications d'alerte basées sur des balises ne fonctionnent que pour les notifications relatives à Amazon EC2, Amazon EBS, Elastic Load Balancing, Network Load Balancer, Application Load Balancer, Amazon RDS, Amazon Redshift et. OpenSearch
N'ajoutez pas d'informations personnelles identifiables (PII) dans vos tags.

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 `lekey = 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 donnant votre accord pour activer la notification automatique 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.

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 [Utilisation des balises](#). Pour baliser une ressource existante, soumettez une RFC avec le type de modification Deployment | Advanced stack components | Tag | Create (auto) (ct-3cx7we852p3af).

Note

Il n'est *OwnerTeamEmail* pas nécessaire que la valeur clé soit dans un étui à chameau. Toutefois, les balises font la distinction majuscules/majuscules et il est recommandé d'utiliser le format recommandé.

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
Canal sécurisé cassé	L'alarme Broken Secure Channel est déclenchée sur les EC2 instances Windows lorsque l'instance perd la connexion avec le contrôleur de domaine AD.	Le seuil est supérieur à la valeur définie 10 fois au cours des 15 dernières minutes.	La correction automatique AMS valide que l'instance est en ligne dans SSM, que le nom d'hôte n'est pas dupliqué et que l'objet informatique AD est aligné sur la pile. CloudFormation La correction répare la connexion au canal sécurisé afin de rétablir l'accès à l'instance.
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

Nom de l'alerte	Description	Seuils	Action
			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) sur votre EC2 instance est pleine.	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 d'espace disque, cela augmente le volume afin d'éviter toute interruption de service en cas de saturation du volume.
AMSWindowsDiskUsage	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 automatique 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 interruption 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: <code>ams:rt:ams-rds-max-allocated-storage-policy</code>, Value: <code>ams-opt-out</code>".

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: <code>ams:rt:ams-rds-max-allocated-storage-policy</code>, Value: <code>ams-opt-out</code>".

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: <code>ams:rt:ams-rds-max-allocated-storage-policy</code>, Value: <code>ams-opt-out</code>".

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: <code>ams:rt:ams-rds-max-allocated-storage-policy</code>, Value: <code>ams-opt-out</code>".

Amazon EC2 Broken Secure Channel : note sur l'automatisation des mesures correctives

Avant que la correction automatique d'AWS Managed Services (AMS) ne corrige les problèmes liés à Amazon EC2 Windows Broken Secure Channel, l'automatisation effectue les vérifications préalables suivantes et crée un rapport d'incident pour une enquête plus approfondie :

- Valide que le statut SSM de l' EC2 instance Amazon est « En ligne ».
- Valide si l' EC2 instance Amazon fait partie d'un groupe Auto Scaling et si toutes les instances du groupe Auto Scaling ont le même nom d'hôte.
- Vérifie si l' EC2 instance Amazon fait partie de la CloudFormation pile qui a été utilisée pour la provisionner. Si l'instance a été supprimée de la CloudFormation pile, l'automatisation vérifie si l'unité organisationnelle (UO) Active Directory associée fait toujours référence à la pile.

Une fois les validations ci-dessus passées, l'automatisation procède à la correction du canal Broken Secure.

Étapes de correction :

- La correction automatique tente de réparer le canal sécurisé entre l' EC2 instance et le domaine AD, en rétablissant l'accès à l'instance.
- Après la correction, l'automatisation vérifie que le canal sécurisé est établi. En cas d'échec, AMS crée un incident et engage les opérations AMS pour enquêter.

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 automatisé 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'un 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.

Création d' CloudWatch alarmes supplémentaires dans AMS

Vous pouvez créer de nouvelles CloudWatch alarmes à l'aide du type de changement AWS Managed Services (AMS) [Deployment | Monitoring and notification CloudWatch | | Create alarmes](#).

Important

AMS ne surveille pas les CloudWatch alarmes que vous avez créées.

Utilisation de CloudWatch métriques et d'alarmes personnalisées pour les EC2 instances Amazon (fonctionne uniquement pour les déploiements mutables qui ne reposent pas sur des mises à jour AMIs déployées sur des groupes Auto Scaling) :

1. 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 Amazon pour les EC2 instances Amazon Linux montrent comment produire et utiliser des métriques CloudWatch personnalisées Amazon. 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.
2. Téléchargez votre script de surveillance. Pour télécharger le script de surveillance dans la configuration de votre groupe Auto Scaling ou de votre EC2 instance Amazon, vous pouvez l'utiliser UserData lors de la configuration de votre groupe Auto Scaling ou de votre EC2 instance Amazon, ou, si votre application a été déployée avec CodeDeploy, vous pouvez modifier la configuration avec Deployment | Applications | CodeDeploy application | Deploy CT (ct-2edc3sd1sqmrb).
3. Publiez votre métrique personnalisée sur CloudWatch (la première fois que vous publiez un point de données pour une nouvelle métrique personnalisée, il est créé), voir [Publication de métriques personnalisées](#).
4. Créez l' CloudWatch alarme, voir [Création d'une CloudWatch alarme pour une instance](#).

 Important

Les données de surveillance doivent être envoyées vers ce chemin [infra/INSTANCE_ID/YOUR_CUSTOM_METRIC]

Pour modifier ou supprimer une CloudWatch alarme, soumettez une RFC avec le type Management | Other | Other | Create change (ct-1e1xtak34nx76) avec les paramètres requis pour effectuer l'action, comme décrit dans la référence de l'API Amazon. CloudWatch [PutMetricAlarm](#)

Vous pouvez utiliser le flux CloudWatch d'événements. AMS est intégré à CloudWatch et vous pouvez demander que tout appel d'API AWS déclenche un CloudWatch événement.

Pour ce faire, soumettez un CT de gestion | Autre | Autre | Mise à jour (ct-0xdawir96cy7k) avec les appels d'API qui vous intéressent. Un opérateur AMS vous contactera pour recueillir les exigences. Pour en savoir plus, consultez la [CloudWatch documentation Amazon](#).

Pour accéder au flux d' CloudWatch événements, soumettez un CT de gestion | Autre | Autre | Mise à jour (ct-0xdawir96cy7k) pour ajouter une partie à la rubrique de notification SNS. Un opérateur AMS vous contactera pour recueillir les exigences.

Création de CloudWatch métriques et d'alarmes personnalisées dans AMS

Vous pouvez stocker les statistiques de votre activité et de vos applications sur Amazon CloudWatch. Vous pouvez consulter des graphiques et définir des alarmes en fonction de ces métriques, comme vous le pouvez pour les métriques CloudWatch déjà stockées pour vos ressources AWS Managed Services (AMS). Pour en savoir plus CloudWatch, consultez [Amazon CloudWatch Concepts](#).

Amazon SNS permet aux applications d'envoyer des messages urgents à plusieurs abonnés par le biais d'un mécanisme « push » à l'encontre du système de surveillance géré AMS ou MMS, rubrique Amazon SNS (SNS) sur laquelle les alarmes sont publiées ; dans ce cas, les MMS et vos files d'attente SQS. Vous pouvez les utiliser CloudWatch pour créer des métriques personnalisées et, par le biais d'une rubrique SNS, demander à AMS de vous avertir de manière appropriée. Pour ce faire, suivez les étapes suivantes.

Note

Ce processus ne fonctionne pas pour les déploiements immuables qui reposent sur des mises à jour AMIs déployées dans des groupes Auto Scaling. Il convient aux déploiements d'applications mutables (et non d'ASG).

La configuration d'une métrique personnalisée dans les limites d'AMS Advanced est une tâche complexe. Pour un exemple tiré de CloudWatch, voir [Exemple : compter les occurrences d'un terme](#).

1. Produisez votre script de surveillance des applications et une métrique personnalisée (comme l'exemple du nombre d'occurrences). 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](#).
2. Téléchargez votre script de surveillance. Pour télécharger le script de surveillance dans la configuration de votre groupe Auto Scaling ou de votre EC2 instance Amazon, vous pouvez l'utiliser UserData lors de la configuration de votre groupe Auto Scaling ou de votre EC2 instance Amazon, ou, si votre application a été déployée avec CodeDeploy, vous pouvez

- modifier la configuration avec Deployment | Applications | CodeDeploy application | Deploy CT (ct-2edc3sd1sqmrb).
3. Publiez votre métrique personnalisée sur CloudWatch (la première fois que vous publiez un point de données pour une nouvelle métrique personnalisée, il est créé), voir [Publier des métriques personnalisées](#).
 4. Pour intégrer votre métrique client à votre système de surveillance des applications, demandez à AMS de créer une rubrique SNS pour la métrique en soumettant une RFC avec le type Deployment | Monitoring and notification | SNS | Create change (ct-3dfnglm4ombbs).
 5. Créez l' CloudWatch alarme, consultez [Création d' CloudWatch alarmes Amazon](#).

 Important

Les données de surveillance doivent être envoyées sur ce chemin [infra/*INSTANCE_ID/YOUR_CUSTOM_METRIC*].

Utilisation CloudWatch d'Application Insights pour .Net et SQL Server dans AMS

Vous pouvez utiliser Amazon CloudWatch Application Insights pour configurer les moniteurs des ressources de votre application AWS Managed Services (AMS) afin d'analyser en permanence les données afin de détecter tout signe de problème avec vos applications et de réduire le temps moyen de réparation (MTTR) lors de la résolution des problèmes liés aux applications. Pour plus de détails sur CloudWatch Application Insights, consultez [CloudWatch Application Insights pour .NET et SQL Server](#).

 Important

AMS ne surveille pas les problèmes à partir d' CloudWatch Application Insights, car ils concernent le code d'application que vous contrôlez.

Pour utiliser CloudWatch Application Insights, soumettez une RFC avec le type de modification Deployment | Advanced stack components | Identity and Access Management (IAM) | Create entity or policy (révision requise) (ct-3dpd8mdd9jn1r) avec une demande de création d'un rôle IAM vous autorisant à configurer Application Insights. CloudWatch Il existe deux options pour

recevoir les problèmes identifiés : via un sujet SNS ou avec une cible dans les règles de CloudWatch l'événement. Dans le RFC, spécifiez ce que vous voulez. Si vous prévoyez d'utiliser les règles relatives aux CloudWatch événements, spécifiez également la définition de la règle dans la RFC. Une fois que vous avez configuré CloudWatch Application Insights, vous êtes informé des problèmes potentiels, notamment des informations indiquant leur cause première possible.

Pour savoir comment assumer ce rôle, consultez le guide d'intégration AMS [Federate your Active Directory with the AMS IAM Roles](#).

Utilisation des règles EventBridge gérées par Amazon dans AMS

AMS Advanced 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 sont liées au principal du `events.managedservices.amazonaws.com` 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
AMSAdvancedCoreRule	Cette règle transmet les CloudWatch alarmes Amazon à AMS Monitorin	<pre>{ { "source": ["aws.cloudwatch"], "detail-type": ["CloudWatch Alarm State Change"], } }</pre>

Nom de règle	Description	Définition
	g. Les CloudWatch événements s Amazon surveillent les CloudWatch alarmes.	}

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 Advisor](#)[AWS 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 passé en revue, vous pouvez créer une RFC automatisée, [Trusted Remediator | Finding | Remediate](#), modifier le type pour corriger la ressource. Pour plus d'informations sur les étapes de correction manuelles, voir [Exécuter des corrections manuelles dans Trusted Remediator](#).

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.

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 Advisor](#) vérifications et [AWS Compute Optimizer](#) les 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.
- 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-mail, 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 AMS Advanced.
- 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.

- Région AWS: l' Région 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. 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](#).

Configurez Trusted Remediator dans votre Comptes AWS

Lorsque l'intégration est terminée, votre CA ou votre CDSM vous en informe et les configurations par défaut sont créées dans votre administrateur délégué. Compte AWS La configuration est stockée dans l' AWS AppConfig application Trusted Remediator. Vous pouvez utiliser le RFC [Management | Trusted Remediator | Configuration de correction | Mise à jour pour demander des mises à jour de configuration](#). Pour de plus amples informations, veuillez consulter [Configurer Trusted Advisor la correction des chèques dans Trusted Remediator](#).

Pour consulter les configurations par défaut de Trusted Remediator, procédez comme suit :

1. Ouvrez la AWS Systems Manager console à l'adresse <https://console.aws.amazon.com/systems-manager/>.

 Note

Assurez-vous que vous êtes connecté au compte d'administrateur délégué.

2. Choisissez Gestion des applications, AppConfig.
3. Sélectionnez Trusted Remediator dans la liste des applications.

Voici un exemple de AWS AppConfig console présentant les configurations de 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. Soumettez une demande [de gestion | Remédiateur fiable | Configuration de correction | Mise à jour](#) pour mettre à jour la configuration des contrôles sélectionnés Trusted Advisor . Pour obtenir des instructions sur la manière de sélectionner les chèques, consultez [Configurer 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 à l'aide d'une RFC automatisée. Lorsque vous choisissez la correction manuelle, Trusted Remediator crée une exécution manuelle. OpsItem 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 Mb/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 fonctionne 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-TerminateEC2 InstanceStoppedForPeriodOfTime - 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 <code>true</code>. Pour ne pas créer de sauvegarde avant de terminer, choisissez <code>false</code>. L'argument par défaut est <code>true</code>. - 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 <code>true</code>, 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 <code>true</code>. Les valeurs valides sont <code>true</code> et <code>false</code> (distinction majuscules et minuscules). • <code>MinimumUnattachedDays</code>: 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 est 7. 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 <code>true</code> pour forcer l'arrêt des instances à l'aide du stockage d'instances. Sinon, définissez sur <code>false</code> . La valeur par défaut de <code>false</code> 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 préconfigurés pris en charge
QCH7DWOuX1 EC2 Instances Amazon à faible taux d'utilisation	AWSManagedServices-ResizeInstanceByOneLevel L' EC2 instance Amazon est redimensionnée selon un type d'instance inférieur dans le même type de famille d'instances. L'instance 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 redimensionnement des instances qui se trouvent dans un Auto Scaling Group.	• MinimumDaysSinceLastChange: nombre minimum de jours écoulés depuis le dernier changement 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 AMI Before redimensionnement : pour créer l'AMI de l'instance en tant que sauvegarde avant le redimensionnement, choisissez <code>true</code> Pour ne pas créer de sauvegarde, choisissez <code>false</code>. L'argument par défaut est <code>false</code>. Les valeurs valides sont <code>true</code> et <code>false</code> (distinction majuscules et minuscules). • ResizeIfStopped: Pour procéder au changement de taille de l'instance, même si l'instance est dans un état arrêté, choisissez <code>true</code>. Pour ne pas redimensionner automatiquement l'instance en cas d'arrêt, choisissez <code>false</code>. Les valeurs valides sont <code>true</code> et <code>false</code> (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 AMI Before résiliation : définissez cette option sur <code>true</code> ou pour <code>false</code> créer une AMI d'instance en tant que sauvegarde avant de mettre fin à l'EC2 instance. L'argument par défaut est <code>true</code> . Les valeurs valides sont <code>true</code> et <code>false</code> (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 from Recommandations 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 de Recommandations 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-TrustedRoleEnableAutoScalingGroupELBHealthCheck 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-TrustedRolemediatorEnableCloudTrailLogValidation 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-TrustedRolemediatorEnableCodeBuildLoggingConfig 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-TrustedRolemediatorDisablePublicAccessOnDocumentDBSnapshot 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-TrustedRolemediatorEnableDocumentDBClusterDeletionProtection 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-TrustedRolemediatorEnableDynamoDBTableDeletionProtection 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-TrustedRolemediatorDisablePublicAccessOnEBSSnapshot 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 <code>true</code>. Pour ne pas créer de sauvegarde avant de terminer, choisissez <code>false</code>. L'argument par défaut est <code>true</code>. 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 <code>true</code>. Pour ne pas créer de sauvegarde avant de terminer, choisissez <code>false</code>. L'argument par défaut est <code>true</code>. Aucune contrainte
Hs4Ma3G121 - Le cryptage par défaut EBS doit être activé AWS Security Hub Contrôle correspondant : 7 EC2.	AWSManagedServices-EncryptEBSDefault 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-TrustedRolemediatorActiver 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'immutabilité des balises doit être configurée dans les référentiels privés ECR AWS Security Hub Contrôle correspondant : ECR.2	AWSManagedServices-TrustedR emediatorSetImageTagImmutability 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-TrustedR emediatorEnableEKSAuditLog 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 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-EnableELBLoggingV2 La journalisation entre Application Load Balancer et Classic Load Balancer est activée.	• TargetBucketTagKey: nom du tag (distinguant majuscules et minuscules) utilisé pour identifier le compartiment Amazon S3 cible. Utilisez-le avec TargetBucketTagValue 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 identifier le compartiment Amazon S3 cible. Utilisez-le avec TargetBucketTagKey pour étiqueter le compartiment qui servira de compartiment de destination pour la journalisation des accès. • S3 BucketPrefix : préfixe (hiérarchie logique) du compartiment Amazon S3. Le préfixe que vous spécifiez ne doit pas inclure la chaîne AWSLogs. Pour plus d'informations, consultez Organisation 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-TrustedRoleMediatorEnableEMRBlockPublicAccess 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-TrustedRolemediatorEnableNeptuneDBClusterDeletionProtection 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 Network Firewall.	AWSManagedServices-TrustedRolemediatorEnableNetworkFirewallDeletionProtection- 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 préconfigurés 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 surveillance 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 <code>rdsmonitoringrole</code> est utilisé ou créé, s'il n'existe pas. Si la surveillance améliorée est activée avant l'exécution de l'automatisation, 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-TrustedR emediatorEnableRDSDeletionP rotection 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-TrustedR emediatorEnableRDSDeletionP rotection 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-TrustedR emediatorEnableRDSLogExports 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-UpdateRD SIAMDatabaseAuthentication 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. <code>true</code> Pour planifier le changement pour la prochaine fenêtre de maintenance, choisissez <code>false</code>. 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 <code>true</code>. Pour planifier le changement pour la prochaine fenêtre de maintenance, choisissez <code>false</code>. 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 <code>available</code> 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-UpdateRDS CopyTagsToSnapshots CopyTagstosnapshot 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-UpdateRDS CopyTagsToSnapshots 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-TrustedRedshiftClusterAuditLogging 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-TrustedRedshiftClusterEnhancedVPCRouting 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-TrustedResourceBlockS3BucketPublicAccess 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 préconfigurés pris en charge
Hs4Ma3G230 - La journalisation des accès au serveur de compartiment S3 doit être activée AWS Security Hub Contrôle correspondant : S3.9	AWSManagedServices-EnableBucketAccessLogging(document SSM par défaut pour les modes d'exécution automatique et manuel) La journalisation des accès au serveur 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 du journal (les valeurs distinguant les majuscules et minuscules). Pour utiliser le format simple des clés S3 pour les objets du journal, choisissezSimplePrefix . 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 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 préconfigurés pris en charge
Hs4Ma3G230 — La journalisation des accès au serveur de compartiments S3 doit être activée AWS Security Hub Contrôle correspondant : S3.9	AWSManagedServices-TrustedRoleMediatorEnableBucketAccessLoggingV2 - La journalisation des compartiments Amazon S3 est activée.	• TargetBucketTagKey: nom du tag (distinguant majuscules et minuscules) permettant d'identifier le compartiment cible. Utilisez-le et TargetBucketTagValue pour étiqueter le compartiment à utiliser comme compartiment de destination pour la journalisation des accès. • 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 de journal (les valeurs distinguent majuscules et minuscules) : Pour utiliser le format simple des clés S3 pour les objets de 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

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 RwgBli 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-TrustedRolemediatorDisableSageMakerNotebookInstanceRootAccess 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 <code>alias/aws/sns</code>. 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-TrustedRolemediatorDisableSSMDocPublicSharing- 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 préconfigurés pris en charge
Hs4Ma3G13 6 - Les files d'attente Amazon SQS doivent être chiffrées au repos AWS Security Hub Chèque correspondant : SQS.1	AWSManagedServices-EnableSQSEncryptionAtRest Les messages dans Amazon SQS sont chiffrés.	• SqsManagedSseEnabled: défini sur <code>true</code> pour activer le chiffrement des files d'attente côté serveur à l'aide des clés de chiffrement détenues par Amazon SQS, défini sur <code>false</code> pour activer le chiffrement des files d'attente côté serveur 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, <code>alias/aws/sqs</code> est utilisé. • KmsDataKeyReusePeriodSeconds: 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 <code>SqsManagedSseEnabled</code> est défini sur <code>true</code>. 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-TrustedRolemediatorEnableDDBPITR Permet point-in-time la restauration des tables DynamoDB.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
R365S2QDDF Amazon S3 Bucket Versioning	AWSManagedServices-TrustedRolemediatorEnableBucketVersioning 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-000000000000).
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, choisissezSimplePre

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 z. PartitionedPrefixEventTime Pour utiliser la clé S3 partitionnée pour les objets du journal et DeliveryTime pour le préfixe partitionné, choisissez z. PartitionedPrefixDeliveryTime L'argument par défaut est PartitionedPrefixEventTime . Les valeurs valides sontSimplePrefix , 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-TrustedR emediatorEnableRDSMultiAZ Le déploiement de zones de disponibilité multiple est activé.	Aucun paramètre préconfiguré n'est autorisé. Une dégradation des performances est possible lors de cette modifcat ion.
H7 IgTzj TYb Instantanés Amazon EBS	AWSManagedServices-TrustedR emediatorCreateEBSSnapshot 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 <code>true</code> d'appliquer la modification immédiatement ou <code>false</code> de la planifier pour la fenêtre de maintenance suivante. Si le <code>ApplyImmediately</code> paramètre est défini sur <code>true</code>, les modifications en attente sur la base de données sont appliquées avec le paramètre de <code>RDSBackup</code> rétention.

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés 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 KIUw 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 préconfigurés 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 synchrono us_commit paramètre Amazon RDS est désactivé	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Le paramètre synchrono us_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-TrustedRemediatorRemediateRDSParmeterGroupParameter 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-TrustedRemediatorRemediateRDSParmeterGroupParameter 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-TrustedRemediatorRemediateRDSParmeterGroupParameter 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 préconfigurés pris en charge
COr6dfpM06 AWS Lambda fonctions sous-provisionnées pour ce qui est de la taille de la mémoire	AWSManagedServices-ResizeLambdaMemory La taille de mémoire des fonctions Lambda 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 est modifiée avant l'exécution de l'automatisation, cette automatisation peut remplacer les paramètres par la valeur recommandée par. Trusted Advisor
ZRxQIPsb6c EC2 Instances Amazon à haut taux d'utilisation	AWSManagedServices-ResizeInstanceByOneLevel 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 redimensionnement 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 changement de type d'instance. Si le type d'instance a été modifié dans le 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 AMI Before redimensionnement : pour créer l'AMI de l'instance en tant que sauvegarde avant le redimensionnement, choisissez. true Pour ne pas créer de sauvegarde, choisissez false. 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
		• <code>ResizeStopped</code>: Pour procéder au changement de taille de l'instance, même si l'instance est dans un état arrêté, choisissez <code>true</code>. Pour ne pas redimensionner automatiquement l'instance en cas d'arrêt, choisissez <code>false</code>. Les valeurs valides sont <code>true</code> et <code>false</code> (distinction majuscules et minuscules). Aucune contrainte
c1qf5bt021 innodb_buffering Paramètre Amazon RDS utilisant une valeur inférieure à la valeur optimale	AWSManagedServices-TrustedRemediatorRemediateRDSParmeterGroupParameter La valeur du <code>innodb_buffering</code> paramètre est définie sur <code>NONE</code> Amazon RDS.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
c1qf5bt025 Le <code>autovacuum</code> paramètre Amazon RDS est désactivé	AWSManagedServices-TrustedRemediatorRemediateRDSParmeterGroupParameter Le paramètre <code>autovacuum</code> 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_in dexonlyscan paramètre Amazon RDS est désactivé	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Le paramètre enable_in dexonlyscan est activé pour Amazon RDS.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
c1qf5bt029 Le enable_in dexscan 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-Increase ServiceQuota 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-Increase ServiceQuota 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-Increase ServiceQuota 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 préconfigurés pris en charge
8 WiQ K YSt25 Dispositifs d'équilibrage de charge de réseau ELB	AWSManagedServices-IncreaseServiceQuota Une nouvelle limite pour les équilibres 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 OK 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 préconfigurés pris en charge
c18d2gz125 Amazon API Gateway ne consigne pas les journaux d'exécution	AWSManagedServices-TrustedRemediatorEnableAPIGatewayExecutionLogging 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 protection contre la suppression d'Elastic Load	AWSManagedServices-TrustedRemediatorEnableELBDeletionProtection- 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 préconfigurés pris en charge
Balancing n'est pas activée pour les équilibres de charge		
c1qf5bt012 Amazon RDS Performance Insights est désactivé	AWSManagedServices-TrustedR emediatorEnableRDSPerformanceInsights Performance Insights est activé pour Amazon RDS.	- PerformanceInsightsRetentionPeriod: 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) ou 731. - 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
c1fd6b9614 Journaux d'accès Amazon S3 activés	AWSManagedServices-TrustedRolemediatorEnableBucketAccessLoggingV2 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, choisissezSimplePrefix . 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 préconfigurés 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 demander à configurer les corrections 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-percentage** Pourcentage 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 OpsItem et exécutez la correction à l'aide de la RFC automatisée. Pour de plus amples informations, veuillez consulter [Travailler avec des corrections dans Trusted Remediator](#).
 - **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](#) et [Personnalisez 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'attribut `alternative-automation-document` 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 dans [Trusted Advisor contrôles pris en charge par Trusted Remediator](#).

Par exemple, pour le contrôle `Qch7DwouX1`, trois documents SSM sont associés : `AWSManagedServices-StopEC2Instance`, `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 attributs `manual-for-tagged-only` et `automated-for-tagged-only` 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 charge [Trusted Advisor contrôles pris en charge par Trusted Remediator](#).
3. Ajoutez une balise aux ressources avec la clé et la valeur suivantes à l'aide du type de modification [Tag | Update](#) ou [Tag | Bulk Update](#) :
 - 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 à l'aide du système automatisé. Pour de plus amples informations, veuillez consulter [Travailler avec des corrections dans Trusted Remediator](#).
 - 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. Utilisez le paramètre Configuration|Mise à jour, modifiez le type pour demander la mise à jour de la configuration.
2. Entrez les paramètres suivants :
 - CheckIds: DAv U99Dc4C
 - ExecutionMode: Manuel

Note

Plusieurs contrôles peuvent être configurés en une seule demande. Pour les vérifications qui nécessitent la même configuration, incluez plusieurs vérifications IDs dans le CheckIdsparamètre. Pour les vérifications qui nécessitent une configuration différente, créez un nouvel RemediationConfigurationobjet.

3. Soumettez le RFC.

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. Ignorez la correction automatique pour certains volumes Amazon EBS :

[Utilisez le type de modification Tag | Update ou Tag | Bulk Update pour appliquer la balise suivante aux volumes à exclure de la correction automatique :](#)

- Clé : DAv TR-U99Dc4C-Mode d'exécution
 - Valeur : Inactive
2. Utilisez le type de modification Configuration|Update pour demander la mise à jour de la configuration.
 3. Entrez les paramètres suivants :
 - CheckIds: DAv U99Dc4C
 - ExecutionMode: Automatisé
 4. Soumettez le RFC.

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. Utilisez le menu [Configuration de correction | Mise à jour](#), changez de type pour demander la mise à jour de la configuration.
2. Entrez les paramètres suivants :

- CheckIds: DAv U99Dc4C
- ExecutionMode: Conditionnel
- AutomatedForTaggedOnly: {"Étape » : » NonProd « }

Note

La valeur spécifiée pour le AutomatedForTaggedOnlyparamètre remplace la valeur précédemment configurée. Pour conserver les balises existantes, incluez-les dans la nouvelle valeur.

3. Soumettez le RFC.

Rétablir la configuration par défaut

Cet exemple supprime la automated-for-tagged-onlyconfiguration existante pour le check Hs4Ma3G104. Pour supprimer la configuration de balise précédemment appliquée, définissez la valeur du AutomatedForTaggedOnlyparamètre sur {}.

Réinitialiser la configuration par défaut pour vérifier Hs4Ma3G104

1. Utilisez le type de modification [Configuration de correction | Mise à jour](#) pour demander la mise à jour de la configuration.
2. Entrez les paramètres suivants :
 - CheckIds: Hs4Ma3G104
 - ExecutionMode: Entrez la valeur actuellement utilisée
 - AutomatedForTaggedOnly: {}
3. Soumettez le RFC.

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.
- **trustedAdvisorCheckManualRemediation**: données personnalisées qui fournissent des informations de référence pour la correction manuelle.
- **ManualExecutionInput**: objet qui définit les paramètres dont vous pouvez modifier les valeurs lors de l'exécution d'une correction manuelle.
 - **DocumentName**: nom du runbook (document SSM).
 - **CustomizableParameters**: noms de paramètres que vous pouvez modifier.
- **DefaultInput**: objet qui définit les noms et les valeurs des paramètres à utiliser pour la correction manuelle. Les valeurs sont renseignées en fonction de paramètres préconfigurés.

6. Pour y remédier manuellement OpsItem, procédez comme suit :

- Utiliser un [correcteur fiable | Trouver | Corriger le type de modification ct-1c7ch8z5phrjp](#)
- Entrez des valeurs pour les paramètres suivants :
 - **DocumentName**: Ça doit être le casAWSManagedServices-RemediateTrustedRemediatorFinding.
 - **Région** : La Région AWS, sous la forme us-east-1.
 - **Paramètres** : Entrez les paramètres de correction manuelle :
 - **OpsItemId**: ID de l'objet Ops.
 - **RemediationDocumentName**: nom du document d'automatisation SSM à utiliser. Le document doit être associé à l'élément Ops. Si plusieurs documents sont associés à l'élément Ops, ils DocumentNamedoivent être spécifiés.
 - **RemediationParameters**: Une key/value carte des paramètres pour l'exécution de l'automatisation, sous la forme : `{"ParameterName1\":[\"ParameterValue1\"],\"ParameterName2\":[\"ParameterValue2\"]}`. Vous ne pouvez utiliser que les paramètres présents dans l'élément Ops **trustedAdvisorCheckManualRemediation CustomizableParameters**. S'ils ne sont pas spécifiés, les paramètres et les valeurs sont extraits de l'élément Ops.
- Cliquez sur Exécuter. S'il n'y a aucune erreur, la page RFC créée avec succès s'affiche avec les détails de la RFC soumise et le résultat d'exécution initial.

- e. Une fois l'exécution terminée, le problème OpsItem est résolu. Si le RFC a échoué, suivez les étapes décrites dans [Résoudre les problèmes liés aux mesures correctives dans Trusted Remediator](#). Pour obtenir une assistance supplémentaire en matière de dépannage, contactez AMS.

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 DocumentName et 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, corrigez manuellement le OpsItem. Pour les étapes de correction, voir [Exécutez des corrections manuelles dans Trusted Remediator](#).
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.

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"}
```

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 également contacter AMS pour les modifications de configuration, l'assistance, les 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 AMS Advanced. 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 ?

Utilisez le type de modification [Management | Trusted Remediator | State | Activer ou désactiver](#) pour arrêter le service Trusted Remediator. Utilisez le même type de modification pour réactiver Trusted Remediator.

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](#).

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 nommé `ams-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.

Gestion des journaux

Rubriques

- [Qu'est-ce que la gestion des journaux ?](#)
- [Comment fonctionne la journalisation AMS](#)
- [Accès à vos journaux](#)
- [Personnalisation de la configuration de votre journal](#)

La gestion des journaux AMS collecte, agrège et contrôle la conservation des journaux du compte géré. AWS la gestion des journaux regroupe les journaux des EC2 instances Amazon et des AWS ressources déployées au sein de votre compte dans CloudWatch Logs. La liste complète des services à partir desquels les journaux sont actuellement agrégés se trouve dans [Journaux de service agrégés AMS](#).

Qu'est-ce que la gestion des journaux ?

La gestion des journaux est le processus qui consiste à traiter les événements des journaux générés par les instances, les applications et les services AWS. Cette fonctionnalité définit la manière dont AMS traite, stocke et fait pivoter les événements du journal générés dans votre compte AWS géré. Les journaux d'infrastructure sont utilisés lors de la résolution des incidents et pour soutenir les audits des systèmes.

Comment fonctionne la journalisation AMS

La gestion des journaux de la zone d'atterrissage à compte unique (SALZ) AMS utilise divers agents et outils préinstallés qui sont mis en œuvre lors de l'intégration ou du provisionnement d'instances et d'applications.

La journalisation est configurée lors du processus d'intégration du compte et lors du lancement d'une pile.

Les journaux de zone d'atterrissage multi-comptes (MALZ) AMS produits par les instances et les services AWS sont disponibles dans CloudWatch Logs ou Amazon Simple Storage Service (Amazon S3), au sein de chaque compte géré par AMS. La zone de landing multi-comptes AMS fournit un

compte de journalisation central qui sert d'emplacement d'agrégation central pour certains journaux produits par des comptes d'application individuels.

Les tableaux des [Accès à vos journaux](#) sous-sections décrivent les journaux disponibles dans les comptes individuels et ceux disponibles dans le compte de journalisation central.

Accès à vos journaux

Pour accéder à vos journaux, assurez-vous que vous possédez l'un des rôles IAM requis et que vous êtes connecté à votre compte AMS. Naviguez ensuite vers le répertoire affiché.

Multi-Account Landing Zone (MALZ)

Fournit cinq rôles IAM par défaut, chacun permettant d'accéder à tous les journaux de votre compte (tous sont précédés par `AWSManagedServices`) :

- AdminRole
- CaseRole
- ChangeManagementRole
- ReadOnlyRole
- SecurityOpsRole

L'accès à ces rôles est configuré par fédération, chaque rôle étant mappé à un groupe au sein de votre domaine Active Directory.

Pour en savoir plus sur ces rôles, consultez [Rôle d'utilisateur IAM dans AMS](#).

Single-Account Landing Zone (SALZ)

La zone `Customer_ReadOnly_Role` de landing compte unique par défaut d'AMS vous permet d'accéder à tous les journaux de votre compte. L'accès aux journaux est contrôlé à l'aide de rôles AWS Identity and Access Management (IAM) mappés à des groupes Active Directory.

Journaux de service agrégés AMS

Chaque AWS service se connecte soit à CloudWatch Logs, soit à un emplacement spécifique dans un compartiment Amazon S3.

 Note

Sauf indication contraire, tous les emplacements des journaux sont locaux sur le compte qui a généré les journaux et ne sont pas agrégés dans le compte de journalisation central. Pour trouver les noms des CloudTrail pistes AMS par défaut dans les comptes SALZ et MALZ, accédez à la console AWS pour CloudTrail puis à la page des pistes et recherchez AMS. Les ressources AMS étant dotées de balises, vous pouvez trouver les sentiers de cette façon. Exemple de CloudTrail balise AMS :

```
Environment    AMSInfrastructure
```

Pour accéder à vos journaux, assurez-vous que vous possédez l'un des rôles IAM requis et que vous êtes connecté à votre compte AMS. Naviguez ensuite vers le répertoire affiché.

Multi-Account Landing Zone

Journaux de service agrégés de la zone d'atterrissage multi-comptes AMS

	Nom du service	Détails du journal	Emplacement du journal
1	Amazon Aurora	Journaux généraux, de requêtes lentes et d'erreurs.	CloudWatch LogGroup: /aws/rds/cluster/{ <i>database_name</i> }/{ <i>log_name</i> }
2	AWS CloudFormation (CFN)	Journalisation des appels d'API uniquement.	AWS CloudFormation Les appels d'API sont documentés via CloudTrail, qui envoie ses journaux au compartiment S3, CloudWatch LogGroup puis les synchronise dans un compartiment S3. Les journaux sont conservés pendant 14 jours par défaut dans le CloudWatch LogGroup compartiment S3 et sont conservés indéfiniment dans le compartiment S3.

	Nom du service	Détails du journal	Emplacement du journal
			CloudWatch LogGroup:/CloudTrail/Journaux des zones d'atterrissage Compartiment S3 [dans le compte de journalisation central] : aws-landing-zone-logs -ams-a {<i>account_ID</i>} -log-management- {} <i>region</i> Chemin :/AWSLogs/{<i>account_ID</i>}/CloudTrail/
3	Amazon CloudFront (CloudFront)	Enregistrement des demandes des utilisateurs. CloudFront la journalisation doit être explicitement activée. Pour plus d'informations, consultez Activer la journalisation pour les services pris en charge .	Compartiment S3 : ams-a {<i>account_ID</i>} -log-management- {} <i>region</i> Chemin : AWS/RedShift/{} <i>CloudFront distribution ID</i>
4	Amazon CloudWatch (CloudWatch)	Journalisation des appels d'API uniquement.	CloudWatch LogGroup:/CloudTrail/Journaux des zones d'atterrissage Compartiment S3 [dans le compte de journalisation central] : aws-landing-zone-logs - {<i>account_ID</i>} - {} <i>region</i> Chemin :/AWSLogs/{<i>account_ID</i>}/CloudTrail/
5	Amazon Elastic Block Store (Amazon EBS)	Aucun journal n'est produit par le service EBS.	Ne s'applique pas

	Nom du service	Détails du journal	Emplacement du journal
6	Amazon Elastic Compute Cloud (Amazon EC2)	Journaux du système et des applications. Pour plus d'informations, consultez Amazon Elastic Compute Cloud (Amazon EC2) : journaux au niveau du système.	CloudWatch Journaux :/ <i>{instance ID}</i>
7	Amazon Elastic File System (Amazon EFS)	Journalisation des appels d'API uniquement.	CloudWatch LogGroup:/CloudTrail/Journaux des zones d'atterrissage Compartiment S3 [dans le compte de journalisation central] : aws-landing-zone-logs - <i>{account_ID}</i> - <i>{region}</i> Chemin :/AWSLogs/<i>{account_ID}</i>/CloudTrail/

	Nom du service	Détails du journal	Emplacement du journal
8	Elastic Load Balancing (ELB)	Entrées du journal des accès et des erreurs. Les équilibres de charge élastiques enregistrent toutes les demandes qui leur sont envoyées, y compris les demandes qui ne sont pas acheminées vers les instances principales. Par exemple, si un client envoie une demande mal formée ou s'il n'y a aucune instance saine à laquelle répondre, la demande est toujours enregistrée. Pour plus d'informations sur les entrées du journal Elastic Load Balancing, voir - Équilibreurs de charge classiques : accédez aux entrées du journal. - Équilibreurs de charge des applications : accédez aux entrées du journal. - Équilibreurs de charge réseau : accès aux entrées du journal.	Journaux d'appels de l'API : CloudWatch LogGroup:/CloudTrail/Journaux des zones d'atterrissage Compartiment S3 [dans le compte de journalisation central] : aws-landing-zone-logs - {<i>account_ID</i>} - {<i>region</i>} Chemin :/AWSLogs/{<i>account_ID</i>}/CloudTrail/ Journaux d'accès : Compartiment S3 : mc-a {<i>account_ID</i>} -logs {} <i>region</i> Chemin : aws/elbaccess

	Nom du service	Détails du journal	Emplacement du journal
9	Amazon OpenSearch Service (OpenSearch Service)	Journaux d'erreurs de service. Vous devez activer explicitement la OpenSearch journalisation. Pour plus d'informations, veuillez consulter Activer la journalisation pour les services pris en charge	CloudWatch LogGroup:/CloudTrail/Journaux des zones d'atterrissage Compartiment S3 [dans le compte de journalisation central] : aws-landing-zone-logs - {account_ID} - {region} Chemin :/AWSLogs/{account_ID}/CloudTrail/
10	Amazon ElastiCache	Journalisation des appels d'API uniquement.	CloudWatch LogGroup://CloudTrail/Logs des zones d'atterrissage
11	Amazon GuardDuty		Compartiment S3 [dans le compte de journalisation central] : aws-landing-zone-logs - {account_ID} - {region}
12	Amazon Inspector		Chemin :/AWSLogs/{ account_ID }/CloudTrail/
13	Amazon Macie		
14	Amazon Redshift	Journaux de connexion, d'utilisateur et d'activité. La journalisation est activée par défaut lorsque vous créez votre cluster Redshift en invoquant le cluster Create Redshift CT (ct-1malj7snzxrkr). Pour plus d'informations, consultez la section Journalisation des audits de base de données.	Compartiment S3 : ams-a {account_ID} -log-management- {region} Chemin : /AWS/RedShift/{CloudFront Distribution ID}

	Nom du service	Détails du journal	Emplacement du journal
15	Amazon Relational Database Service (RDS)	Journaux spécifiques au type de base de données. Vous devez activer explicitement la journalisation RDS. Pour plus d'informations, veuillez consulter Activer la journalisation pour les services pris en charge Vous ne pouvez accéder aux journaux MSSQL que par le biais d'une procédure stockée ; pour plus d'informations, consultez la section Archivage des fichiers journaux.	CloudWatch LogGroup: /aws/rds/ (<i>instance</i>ou<i>cluster</i>)/ {}/{ <i>database_name</i> <i>log_name</i>

	Nom du service	Détails du journal	Emplacement du journal
16	Amazon S3 (S3)	Journaux d'accès aux compartiments. Chaque enregistrement du journal d'accès fournit des détails sur une seule demande d'accès, tels que le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et le code d'erreur (le cas échéant). Les informations des journaux d'accès peuvent s'avérer utiles en cas d'audit de sécurité ou d'audit des accès. Cela peut également vous aider à en savoir plus sur votre base de clients et à comprendre votre facture Amazon S3. Pour plus d'informations sur les entrées du journal d'accès S3, consultez Format du journal d'accès au serveur S3.	Compartiment S3 : mc-a- {<i>account_ID</i>} -log-manage-ment- {<i>region</i> Chemin : /aws/s3access/ { <i>bucket_name</i> Compartiment S3 [dans le compte de journalisation central] : aws-landing-zone-s 3-access-logs- {<i>account_ID</i>} - {<i>region</i> Trajectoire :/
17	Amazon Simple Email Service (SES)	Appels de service d'API SES.	CloudWatch LogGroup:/CloudTrail/Journaux des zones d'atterrissage Compartiment S3 [dans le compte de journalisation central] : aws-landing-zone-logs - {<i>account_ID</i>} - {<i>region</i>} Chemin :/AWSLogs/{<i>account_ID</i>} /CloudTrail/

	Nom du service	Détails du journal	Emplacement du journal
18	Amazon Virtual Private Cloud (VPC)	Données de flux VPC (informations sur le trafic IP à destination et en provenance des interfaces réseau de votre VPC).	CloudWatch LogGroup: /aws/vpcflow/ {} <i>VPC_ID</i>
19	Auto Scaling	Journalisation des appels d'API uniquement.	CloudWatch LogGroup:/CloudTrail/Journaux des zones d'atterrissage
20	AWS Certificate Manager		Compartiment S3 [dans le compte de journalisation central] : aws-landing-zone-logs - { <i>account_ID</i> } - { <i>region</i> } Chemin :/AWSLogs/{ <i>account_ID</i> }/CloudTrail/
21	AWS CodeDeploy	Journaux de déploiement spécifiques à l'instance.	Sur instance
22	AWS Config	Appels de service d'API AWS Config.	CloudWatch LogGroup:/CloudTrail/Journaux des zones d'atterrissage Compartiment S3 [dans le compte de journalisation central] : aws-landing-zone-logs - { <i>account_ID</i> } - { <i>region</i> } Chemin :/AWSLogs/{ <i>account_ID</i> }/CloudTrail/

	Nom du service	Détails du journal	Emplacement du journal
		Modifications de configuration des ressources, telles qu'elles sont suivies par AWS Config.	Compartiment S3 [dans le compte de journalisation central] : aws-landing-zone-logs - {<i>account_ID</i> } - {<i>region</i>} Chemin :/AWSLogs/ {<i>account_ID</i> } /Config/
23	AWS Database Migration Service	Journaux de migration de base de données. Pour plus d'informations, consultez Présentation de la gestion des journaux dans AWS Database Migration Service .	Console de migration de base de données
24	AWS Direct Connect (DX)	Journalisation des appels d'API uniquement.	CloudWatch LogGroup:/CloudTrail/Journaux des zones d'atterrissage
25	AWS Glacier		
26	AWS IAM (IAM)		Compartiment S3 [dans le compte de journalisation central] : aws-landing-zone-logs - {<i>account_ID</i> } - {<i>region</i>}
27	AWS Key Management Service		Chemin :/AWSLogs/ {<i>account_ID</i> } /CloudTrail/
28	Console de gestion AWS (console ou console AWS)		
29	Service de notification simple (SNS) AWS		

	Nom du service	Détails du journal	Emplacement du journal
30	Service de mise en file d'attente simple (SQS) AWS		

Single-Account Landing Zone

Journaux de service agrégés de la zone d'atterrissage à compte unique AMS

	Nom du service	Détails du journal	Emplacement du journal
1	Amazon Aurora	Journaux généraux, de requêtes lentes et d'erreurs.	CloudWatch LogGroup: /aws/rds/cluster/{ <i>database_name</i> }/ { <i>log_name</i> }
2	Amazon CloudFormation (CloudFormation ou CFN)	Journalisation des appels d'API uniquement.	CloudFormation Les appels d'API sont documentés via CloudTrail, qui envoie ses journaux au compartiment S3, CloudWatch LogGroup puis les synchronise dans un compartiment S3. CloudWatch LogGroup: /aws/ams/cloudtrail Compartiment S3 : ams-a { <i>account_ID</i> } -log-management- { <i>region</i> }
3	Amazon CloudFront (CloudFront)	Enregistrement des demandes des utilisateurs. Vous devez activer explicitement la CloudFront journalisation. Pour plus d'informations, veuillez	Compartiment S3 : ams-a { <i>account_ID</i> } -log-management- { <i>region</i> } Chemin : AWS/RedShift/{ <i>CloudFront_distribution_ID</i> }

	Nom du service	Détails du journal	Emplacement du journal
		consulter Activer la journalisation pour les services pris en charge	
4	Amazon CloudWatch (CloudWatch)	Journalisation des appels d'API uniquement.	CloudWatch LogGroup: /aws/ams/cloudtrail
5	Amazon Elastic Block Store (EBS)	Aucun journal n'est produit par le service EBS.	Ne s'applique pas
6	Amazon Elastic Compute Cloud (EC2)	Journaux du système et des applications. Pour plus d'informations, consultez Amazon Elastic Compute Cloud (Amazon EC2) : journaux au niveau du système.	CloudWatch Journaux : / { <i>instance_ID</i> }
7	Amazon Elastic File System (Amazon EFS)	Journalisation des appels d'API uniquement.	CloudWatch LogGroup: /aws/ams/cloudtrail

	Nom du service	Détails du journal	Emplacement du journal
8	Elastic Load Balancing (ELB)	Entrées du journal des accès et des erreurs. Les équilibres de charge élastiques enregistrent toutes les demandes qui leur sont envoyées, y compris les demandes qui ne sont pas acheminées vers les instances principales. Par exemple, si un client envoie une demande mal formée ou s'il n'y a aucune instance saine à laquelle répondre, la demande est toujours enregistrée. Pour plus d'informations sur les entrées du journal Elastic Load Balancer, voir - Équilibreurs de charge classiques : accédez aux entrées du journal. - Équilibreurs de charge des applications : accédez aux entrées du journal. - Équilibreurs de charge réseau : accès aux entrées du journal.	CloudWatch LogGroup: /aws/ams/cloudtrail Compartiment S3 : mc-a {<i>account_ID</i> } -logs- { } <i>region</i> Chemin : aws/elbaccess
9	Amazon OpenSearch Service (OpenSearch Service)	Journaux d'erreurs de service. Vous devez activer explicitement la OpenSearch journalisation. Pour plus d'informations, veuillez consulter Activer la journalisation pour les services pris en charge	CloudWatch LogGroup: /aws/ams/cloudtrail

	Nom du service	Détails du journal	Emplacement du journal
10	Amazon ElastiCache	Journalisation des appels d'API uniquement.	CloudWatch LogGroup: /aws/ams/cloudtrail
11	Amazon GuardDuty		
12	Amazon Inspector		
13	Amazon Macie		
14	Amazon Redshift	Journaux de connexion, d'utilisateur et d'activité. La journalisation est activée par défaut lorsque vous créez votre cluster Redshift en invoquant le cluster Create Redshift CT (ct-1malj7snzxrkr). Pour plus d'informations, consultez la section Journalisation des audits de base de données.	Compartiment S3 : ams-a {<i>account_ID</i>} -log-management- {} <i>region</i> Chemin : /AWS/RedShift/{} <i>CloudFront_Distribution_ID</i>

	Nom du service	Détails du journal	Emplacement du journal
15	Amazon Relational Database Service (RDS)	Journaux spécifiques au type de base de données. La journalisation RDS doit être explicitement activée. Pour plus d'informations, veuillez consulter Activer la journalisation pour les services pris en charge Vous ne pouvez accéder aux journaux MSSQL que par le biais d'une procédure stockée ; pour plus d'informations, consultez la section Archivage des fichiers journaux.	CloudWatch LogGroup: /aws/rds/(instance cluster)/{nom de la base de données}/{nom du journal}

	Nom du service	Détails du journal	Emplacement du journal
16	Amazon S3 (S3)	Journaux d'accès aux compartiments. Chaque enregistrement du journal d'accès fournit des détails sur une seule demande d'accès, tels que : le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et le code d'erreur (le cas échéant). Les informations du journal d'accès peuvent être utiles pour les audits de sécurité et d'accès ; elles peuvent également vous aider à mieux connaître votre clientèle et à comprendre votre facture Amazon S3. Pour plus d'informations sur les entrées du journal d'accès S3, voir Format du journal d'accès au serveur S3.	Compartiment S3 : mc-a {<i>account_ID</i>} -log-management- {} <i>region</i> Chemin : /aws/s3access/ {} <i>bucket_name</i>
17	Amazon Simple Email Service (SES)	Appels de service d'API SES.	CloudWatch LogGroup: /aws/ams/cloudtrail Compartiment S3 : ams-a {<i>account_ID</i>} -log-management- {} <i>region</i> Chemin : AWS/CloudTrail/AWSLogs/{<i>account_ID</i>}/CloudTrail/{<i>region</i>}

	Nom du service	Détails du journal	Emplacement du journal
18	Amazon Virtual Private Cloud (VPC)	Données de flux VPC (informations sur le trafic IP à destination et en provenance des interfaces réseau de votre VPC).	CloudWatch LogGroup: /aws/vpcflow/ {vpc_id}
19	Auto Scaling	Journalisation des appels d'API uniquement.	CloudWatch LogGroup: /aws/ams/cloudtrail
20	AWS Certificate Manager		
21	AWS CodeDeploy	Journaux de déploiement spécifiques à l'instance.	Sur une instance
22	AWS Config	Appels de service d'API AWS Config.	CloudWatch LogGroup: /aws/ams/cloudtrail Compartiment S3 : <code>ams-a</code> <code>{account_ID}</code> -log-management- <code>{region}</code> Chemin : <code>AWS/CloudTrail/AWSLogs/{account_ID}/CloudTrail/{region}</code>
23	AWS Database Migration Service	Journaux de migration de base de données. Pour plus d'informations, consultez Présentation de la gestion des journaux dans AWS Database Migration Service .	Console de migration de base de données
24	AWS Direct Connect (DX)	Journalisation des appels d'API uniquement.	CloudWatch LogGroup: /aws/ams/cloudtrail
25	AWS Glacier		

	Nom du service	Détails du journal	Emplacement du journal
26	AWS IAM (IAM)		
27	AWS Key Management Service		
28	Console de gestion AWS (console ou console AWS)		
29	Service de notification simple (SNS) AWS		
30	Service de mise en file d'attente simple (SQS) AWS		

Journaux des services partagés AMS

Le tableau suivant décrit les journaux et leur emplacement pour les services partagés AMS de votre compte.

Pour accéder à vos journaux, assurez-vous que vous possédez l'un des rôles IAM requis et que vous êtes connecté à votre compte AMS. Naviguez ensuite vers le répertoire affiché.

Enregistrement des services partagés dans la zone d'atterrissage à compte unique AMS

	Nom du service partagé	Détails du journal	Emplacement du journal
1	Hôtes bastions	Informations concernant les utilisateurs accédant à l'hôte Bastion.	Bastions Linux : CloudWatch Journaux :/{identifiant d'instance}/var/log/secure

	Nom du service partagé	Détails du journal	Emplacement du journal
			CloudWatch Journaux :/{identifiant d'instance}/var/log/audit/audit.log Bastions Windows : CloudWatch Journaux :/{identifiant d'instance}/SecurityEventLog
2	Hôtes de gestion	Sortie de scripts, qui aident à automatiser les actions de gestion des accès au sein du compte.	CloudWatch Journaux :/{identifiant d'instance}/ApplicationEventLog
4	Hôtes EPS (DSM)	Informations concernant l'inscription des instances sur la plateforme Deep Security Management.	CloudWatch Journaux :/{identifiant d'instance}/var/log/DSM.log
5	Services d'annuaire	Informations concernant la connexion au compte, la gestion du compte, le suivi détaillé, l'accès aux objets, le changement de politique et l'utilisation des privilèges dans le répertoire du compte. Vous devez activer explicitement la journalisation des services d'annuaire. Pour plus d'informations, consultez Activer la journalisation pour les services pris en charge.	CloudWatch Journaux : /aws/directoryservice/ {identifiant du répertoire} - {nom DNS du répertoire}

	Nom du service partagé	Détails du journal	Emplacement du journal
6	Lambdas	Sortie de différents lambdas, qui facilitent les actions opérationnelles automatisées au sein du compte.	CloudWatch Journaux : /aws/lambda/{nom lambda}

Enregistrement des services partagés dans la zone de landing zone multi-comptes AMS

	Nom du service partagé	Détails du journal	Emplacement du journal
1	Bastions	Résultat des connexions aux instances et des échecs d'authentification.	CloudWatch Journaux des bastions Linux :/{ <i>instance_ID</i> }/var/log/secure.log CloudWatch Journaux de Windows Bastions :/{ <i>instance_ID</i> }/SecurityEventLog
2	Hôtes de gestion	Sortie de scripts, qui aident à automatiser les actions de gestion des accès au sein du compte.	CloudWatch Journaux :/{ <i>instance_ID</i> }/ApplicationEventLog
3	Hôtes EPS (DSM)	Informations concernant l'inscription des instances sur la plateforme Deep Security Management.	CloudWatch Journaux :/{ <i>instance_ID</i> }/var/log/DSM.log
4	Services d'annuaire	Informations concernant la connexion au compte, la gestion du compte, le suivi détaillé, l'accès aux objets, le changement de politique et l'utilisation des	CloudWatch Journaux : /aws/directoryservice/ {} - {} <i>directory_ID</i> <i>directory_DNS_name</i>

	Nom du service partagé	Détails du journal	Emplacement du journal
		privilèges dans le répertoire du compte. Vous devez activer explicitement la journalisation des services d'annuaire. Pour plus d'informations, consultez Activer la journalisation pour les services pris en charge.	
5	Lambdas	Sortie de différents lambdas, qui facilitent les actions opérationnelles automatisées au sein du compte.	CloudWatch Journaux : /aws/lambda/ { } <i>Lambda_name</i>

Amazon Elastic Compute Cloud (Amazon EC2) : journaux au niveau du système

Les journaux d'instance sont collectés par un agent CloudWatch Logs exécuté sur l'instance et sont accessibles via un groupe de CloudWatch journaux portant le même nom que l'instance. Par exemple, si l'ID d'instance est i-0123456789abcdef0 et que le nom du fichier journal est /var/log/messages, the Log Group would be i-0123456789abcdef0 and the Log Stream /var/log/messages

Voir aussi [Journaux de service agrégés AMS](#).

Pour accéder à vos journaux, assurez-vous que vous possédez l'un des rôles IAM requis et que vous êtes connecté à votre compte AMS. Naviguez ensuite vers le répertoire affiché.

Note

Les journaux suivants sont collectés par défaut.

Amazon Linux/Red Hat Linux/Centos Linux/Ubuntu /SUSE Linux

Fichier journal/Flux de journal

```
/var/log/amazon/ssm/amazon-ssm-agent.log
/var/log/amazon/ssm/errors.log
/var/log/audit/audit.log
/var/log/cloud-init-output.log
/var/log/cfn-init.log
/var/log/cfn-init-cmd.log
/var/log/cloud-init.log (Amazon Linux 1 / Amazon Linux 2 only)
/var/log/cron
/var/log/dnf.log
/var/log/maillog
/var/log/messages
/var/log/secure
/var/log/spooler
/var/log/yum.log
/var/log/aws/ams/bootstrap.log
/var/log/aws/ams/build.log
/var/log/syslog
/var/log/dpkg.log
/var/log/auth.log
/var/log/zypper.log
```

Note

Pour plus d'informations sur l'accès aux journaux pour Amazon Linux 2023, consultez [Pourquoi le répertoire /var/log manque-t-il des journaux dans mon instance EC2 Amazon Linux 2023 ?](#)

Windows

Fichier journal/Flux de journal

```
SecurityEventLog
SystemEventLog
AmazonSSMAgentLog
MicrosoftWindowsAppLockerMSIAndScriptEventLog
MicrosoftWindowsAppLockerEXEAndDLLEventLog
AmazonCloudWatchAgentLog
EC2ConfigServiceEventLog (Windows Server 2012 R2 Only)
ApplicationEventLog
```

```
AmazonCloudFormationLog
MicrosoftWindowsGroupPolicyOperationalEventLog
AmazonSSMErrorLog
```

Intégration à Splunk

AMS prend en charge les services d'analyse des journaux clients basés sur AWS Lambda, tels que Splunk.

AMS utilise le module complémentaire Splunk pour Amazon Web Services, qui permet de diffuser les données AWS vers Splunk. Consultez la section Configuration [matérielle et logicielle requise](#).

Reportez-vous à ce billet de blog de Splunk [intitulé Comment diffuser CloudWatch des journaux AWS vers Splunk \(Conseil : c'est plus facile que vous ne le pensez\)](#). Étant donné que le streaming des CloudWatch journaux est activé par défaut pour les clients AMS et qu'AMS configure la fonction AWS Lambda pour vous, vous devez toutefois configurer l'entrée Splunk HTTP Event Collector (HEC) et envoyer une demande à AMS pour bénéficier des fonctionnalités supplémentaires.

Voici à quoi peuvent ressembler les paramètres de saisie des données :

Personnalisation de la configuration de votre journal

Vous pouvez modifier la conservation des données des CloudWatch journaux et activer la journalisation pour des services AWS supplémentaires.

Modification de la conservation des CloudWatch journaux

Vous pouvez modifier le paramètre de conservation des données des CloudWatch journaux pour les journaux. Par défaut, les journaux sont conservés indéfiniment et n'expirent jamais. Vous pouvez ajuster la stratégie de conservation pour chaque groupe de journaux. Elle peut être indéfinie ou comprise entre 10 ans et un jour. Pour connaître la période de conservation minimale autorisée dans AMS, consultez le document sur les normes techniques AMS disponible via AWS Artifact. Pour accéder à AWS Artifact, contactez votre CSDM pour obtenir des instructions ou consultez [Getting Started with AWS](#) Artifact.

La fonctionnalité de conservation des CloudWatch journaux supprime les événements du journal dans un flux en fonction de la politique de rétention. Il ne supprime pas les flux de journaux ni les

groupes de journaux. Pour obtenir des informations générales, consultez le guide de l'utilisateur d'Amazon CloudWatch Logs [Qu'est-ce qu'Amazon CloudWatch Logs ?](#) .

Pour plus d'informations sur la personnalisation d'une période de conservation des journaux et pour en savoir plus, consultez la section [Conservation des données des journaux des modifications dans CloudWatch les journaux](#).

Activer la journalisation pour les services pris en charge

Certains services n'ont pas activé la journalisation par défaut et nécessitent une activation explicite.

Pour activer la journalisation pour Amazon RDS et Route53 CloudFront OpenSearch, soumettez une RFC avec le type Management | Other | Other | Create change (ct-1e1xtak34nx76) avec les valeurs suivantes, en les remplaçant le cas échéant : *variables*

Subject: Enable logging for *SERVICE_NAME*
Description: Service ARN: *SERVICE_ARN*

Gestion de la sécurité

La gestion de la sécurité d'AWS Managed Services (AMS) est le processus par lequel AMS identifie les actifs d'une organisation et met en œuvre des politiques et des procédures pour protéger ces actifs.

Note

AMS dispose désormais d'un type de modification (CT), Deployment | Advanced stack components | ACM avec un certificat supplémentaire SANs | Create (ct-3l14e139i5p50), que vous pouvez utiliser pour soumettre une demande de certificat. AWS Certificate Manager
Pour plus d'informations, consultez [AWS::CertificateManager::Certificate](#). Ce CT prévoit la création d'un nom alternatif de sujet (SAN) supplémentaire.

Pour mieux comprendre AWS la sécurité générale, consultez les [meilleures pratiques en matière de sécurité, d'identité et de conformité](#).

AMS classe les risques de sécurité comme suit :

- Risques connus détectés par l'anti-malware, que le processus d'atténuation des malwares gère.
- Les événements de sécurité, y compris les violations d'accès, gérés par le processus de gestion des événements de sécurité.

Rubriques

- [Protection des données dans AMS](#)
- [Identity and Access Management](#)
- [Réponse aux incidents de sécurité dans AMS](#)
- [Examens de sécurité des demandes de modification dans AMS Advanced](#)

Protection des données dans AMS

AMS surveille en permanence vos comptes gérés en tirant parti de AWS services natifs tels qu'Amazon GuardDuty, Amazon Macie (en option) et d'autres outils et processus internes propriétaires. Après le déclenchement d'une alarme, AMS assume la responsabilité du triage initial et de la réponse à l'alarme. Nos processus de réponse sont basés sur les normes du NIST. AMS

teste régulièrement ses 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 pour les clients.

Lorsqu'AMS détecte une violation, ou une menace imminente de violation, de vos politiques de AWS sécurité, nous collectons des informations, y compris les ressources concernées et les modifications liées à la configuration. AMS fournit une follow-the-sun assistance 24 heures sur 24, 7 jours sur 7 et 365 jours par an grâce à des opérateurs dédiés qui examinent et étudient activement les tableaux de bord de surveillance, la file d'attente des incidents et les demandes de service sur tous vos comptes gérés. AMS examine les résultats avec nos experts en sécurité 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 de nos résultats, AMS interagit avec vous de manière proactive. Si vous pensez 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'AMS ne puisse prendre 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.

Amazon Macie

AWS Managed Services vous recommande d'utiliser Macie pour détecter une liste importante et complète de données sensibles, telles que des informations médicales personnelles (PHI), des informations personnelles identifiables (PII) et des données financières.

Macie peut être configuré pour s'exécuter régulièrement sur n'importe quel compartiment Amazon S3, automatisant ainsi l'évaluation de tout objet nouveau ou modifié dans un compartiment au fil du temps. Au fur et à mesure que des résultats de sécurité sont générés, AMS vous en informera et travaillera avec vous pour y remédier si nécessaire.

Pour plus d'informations, consultez [Analyser les résultats d'Amazon Macie](#).

Sécurité Amazon Macie

Macie est un service de sécurité intelligence/AI artificiel qui vous aide à prévenir les pertes de données en découvrant, en classant et en protégeant automatiquement les données sensibles stockées sur AWS. Macie utilise l'apprentissage automatique pour reconnaître les données sensibles telles que les informations personnelles identifiables (PII) ou la propriété intellectuelle, attribuer une valeur commerciale et fournir une visibilité sur l'endroit où ces données sont stockées et sur la

manière dont elles sont utilisées dans votre organisation. Macie surveille en permanence les activités d'accès aux données pour détecter les anomalies et émet des alertes lorsqu'il détecte un risque d'accès non autorisé ou de fuite de données par inadvertance. Le service Macie prend en charge Amazon S3 et les sources AWS CloudTrail de données.

AMS surveille en permanence les alertes provenant de Macie et, en cas d'alerte, prend des mesures rapides pour protéger vos ressources et votre compte. Avec l'ajout de Macie à la liste des services pris en charge par AMS, nous sommes également désormais responsables de l'activation et de la configuration de Macie dans tous vos comptes, conformément à vos instructions. Vous pouvez consulter les alertes Macie et nos actions au fur et à mesure qu'elles se déroulent dans la console AWS ou dans les intégrations prises en charge. Lors de l'enregistrement du compte, vous pouvez indiquer les comptes que vous utilisez pour stocker des informations personnelles. Pour tous les nouveaux comptes dotés d'informations personnelles, nous vous recommandons d'utiliser Macie. Pour les comptes existants avec des informations personnelles, contactez-nous et nous les activerons dans votre compte. Ainsi, vous pouvez bénéficier d'une couche de protection supplémentaire et profiter de tous les avantages de Macie dans votre environnement AWS géré par AMS.

AMS Macie FAQs

- Pourquoi ai-je besoin de Macie alors que Trend Micro est GuardDuty activé sur tous les comptes AMS ?

Macie vous aide à protéger vos données dans Amazon S3 en vous aidant à classer les données dont vous disposez, leur valeur pour l'entreprise et le comportement associé à l'accès à ces données. Amazon GuardDuty fournit une protection étendue de vos comptes, de vos charges de travail et de vos données AWS en vous aidant à identifier les menaces telles que la reconnaissance des acteurs malveillants, les problèmes d'instance et les activités problématiques du compte. Les deux services intègrent l'analyse du comportement des utilisateurs, l'apprentissage automatique et la détection des anomalies pour détecter les menaces dans leurs catégories respectives. Trend Micro ne se concentre pas sur l'identification des informations personnelles et des menaces qui en découlent.

- Comment activer Macie sur mon compte AMS ?

Si vous avez PII/PHI enregistré des données dans vos comptes ou si vous envisagez de les stocker, contactez votre CSDM ou soumettez une demande de service pour activer Macie pour vos comptes nouveaux ou existants gérés par AMS.

- Quelles sont les implications financières liées à l'activation de Macie sur mon compte AMS ?

La tarification Macie fonctionne pour AMS de la même manière que pour d'autres services tels qu'Amazon Elastic Compute Cloud (Amazon EC2). Vous payez pour Amazon Macie en fonction de votre utilisation et pour un AMS Uplift en fonction de votre SLA. Les frais Macie sont basés sur l'utilisation, voir la tarification d'[Amazon Macie](#), mesurée en AWS CloudTrail fonction des événements et du stockage Amazon S3. Notez que les frais de Macie ont tendance à s'aplatir à partir du deuxième mois suivant son activation, car ils sont facturés en fonction des données incrémentielles ajoutées aux compartiments Amazon S3.

Pour en savoir plus sur Macie, consultez [Amazon Macie](#).

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 environnement AWS. 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 également le comportement d'accès aux comptes Amazon Web Services pour détecter les signes de compromission, tels que les déploiements d'infrastructure non autorisés, tels que le déploiement d'instances dans une région qui n'a jamais été utilisée, ou les appels d'API inhabituels, tels que la modification d'une politique de mot de passe visant à réduire la solidité du mot de passe. Pour plus d'informations, consultez le [guide de GuardDuty l'utilisateur](#).

Pour consulter et analyser vos GuardDuty résultats, procédez comme suit.

1. Ouvrez la [GuardDuty console](#).
2. Choisissez Conclusions, puis choisissez 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](#).

GuardDuty sécurité

Amazon GuardDuty propose une solution de détection des menaces qui vous permet de surveiller et de protéger en permanence vos comptes et charges de travail AWS. Amazon GuardDuty analyse les flux continus de métadonnées générés par votre compte et l'activité du réseau trouvés dans les AWS CloudTrail événements, les journaux de flux Amazon VPC et les journaux DNS (Domain Name System). Il utilise également des informations intégrées sur les menaces, telles que les adresses IP malveillantes connues, la détection des anomalies et l'apprentissage automatique pour identifier les menaces avec plus de précision. GuardDuty est un service AMS surveillé. Pour en savoir plus sur la GuardDuty surveillance d'Amazon, consultez [GuardDuty surveillance](#). Pour en savoir plus GuardDuty, consultez [Amazon GuardDuty](#).

Tous les nouveaux comptes AMS sont GuardDuty activés par défaut. AMS se configure GuardDuty lors de l'intégration du compte. Vous pouvez soumettre des demandes de modification pour modifier les paramètres à tout moment. GuardDuty la tarification fonctionne pour AMS de la même manière que pour d'autres services tels qu'Amazon Elastic Compute Cloud (Amazon EC2). Vous payez GuardDuty en fonction de votre utilisation et une augmentation de l'AMS en fonction de votre. SLAs GuardDuty les frais sont basés sur l'utilisation ([Amazon GuardDuty Pricing](#)), mesurés en fonction AWS CloudTrail des événements et du volume de votre journal Amazon VPC Flow.

GuardDuty Dans AMS, les principales catégories de détection suivantes sont activées :

- Reconnaissance : activité suggérant une reconnaissance par un acteur malveillant, telle qu'une activité inhabituelle d'API, une analyse des ports intra-VPC, des modèles inhabituels de demandes de connexion échouées ou une analyse de port débloquée à partir d'une adresse IP défectueuse connue.
- Problème lié à l'instance : activité problématique de l'instance, telle que le minage de cryptomonnaies, les logiciels malveillants utilisant des algorithmes de génération de domaines (DGA), le déni de service sortant, le volume anormalement élevé de trafic réseau, les protocoles réseau inhabituels, les communications d'instance sortantes avec une adresse IP malveillante connue, les EC2 informations d'identification Amazon temporaires utilisées par une adresse IP externe et l'exfiltration de données à l'aide du DNS.
- Activité du compte : les modèles courants indiquant l'activité du compte incluent les appels d'API provenant d'un proxy de géolocalisation ou d'anonymisation inhabituel, les tentatives de désactivation de la AWS CloudTrail journalisation, les lancements d'instances ou d'infrastructures inhabituels, les déploiements d'infrastructure dans une région AWS inhabituelle et les appels d'API provenant d'adresses IP malveillantes connues.

AMS les utilise GuardDuty dans vos comptes gérés pour surveiller en permanence les résultats et les alertes GuardDuty et, en cas d'alerte, AMS Operations prend des mesures proactives pour protéger vos ressources et votre compte. Vous pouvez consulter GuardDuty les résultats et nos actions au fur et à mesure de leur évolution dans la console AWS ou dans les intégrations prises en charge.

GuardDuty fonctionne avec Trend Micro Deep Security Manager dans votre compte. Trend Micro Deep Security Manager fournit des services de détection et de prévention des intrusions basés sur l'hôte. Les services de réputation Web de Trend Micro se recoupent GuardDuty dans une certaine mesure en termes de capacité à détecter lorsqu'un hôte tente de communiquer avec un hôte ou un service Web connu pour constituer une menace. Il GuardDuty fournit toutefois des catégories de détection de menaces supplémentaires et y parvient en surveillant le trafic réseau, une méthode complémentaire de la détection basée sur l'hôte de Trend Micro. La détection des menaces basée sur le réseau permet de renforcer la sécurité en empêchant les contrôles d'échouer si l'hôte présente un comportement problématique. AMS recommande de l'utiliser GuardDuty dans tous vos comptes AMS.

Pour en savoir plus sur Trend Micro, consultez le [centre d'aide de Trend Micro Deep Security](#) ; notez que les liens n'appartenant pas à Amazon peuvent être modifiés sans préavis.

GuardDuty surveillance

GuardDuty vous informe de l'état de votre environnement AWS en produisant des [résultats de sécurité](#) qu'AMS capture et sur lesquels il peut émettre des alertes.

Amazon GuardDuty surveille la sécurité de votre environnement AWS en analysant et en traitant les journaux de flux VPC, les journaux d' AWS CloudTrail événements et les journaux du système de noms de domaine. Vous pouvez étendre cette portée de surveillance en configurant GuardDuty de manière à utiliser également vos propres listes d'adresses IP fiables et listes de menaces personnalisées.

- Les listes d'adresses IP fiables sont constituées d'adresses IP que vous avez autorisées à communiquer de manière sécurisée avec votre infrastructure et vos applications AWS. GuardDuty ne génère pas de résultats pour les adresses IP figurant sur des listes d'adresses IP fiables. À tout moment, vous pouvez avoir seulement une liste d'adresses IP approuvées chargée par compte AWS et par région.
- Les listes de menaces sont constituées d'adresses IP malveillantes connues. GuardDuty génère des résultats basés sur des listes de menaces. À tout moment, vous pouvez avoir jusqu'à six listes de menaces chargées par compte AWS et par région.

Pour la mise en œuvre GuardDuty, utilisez le logiciel AMS CT Deployment | Monitoring and notification | GuardDuty IP set | Create (ct-08avsj2e9mc7g) pour créer un ensemble d'adresses IP approuvées. Vous pouvez également utiliser l'outil AMS CT Deployment | Monitoring and notification | GuardDuty Threat Intel Set | Create (ct-25v6r7t8gvkq5) pour créer un ensemble d'adresses IP refusées.

Pour obtenir la liste des services surveillés par AMS, consultez [Qu'est-ce que le système de surveillance AMS surveille ?](#).

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 modification (RFC) en utilisant [Management | Other | Other | Create CT \(ct-1e1xtak34nx76\)](#).
- Créez une demande de service.

Si votre compte est géré en mode développeur ou en mode changement direct, vous pouvez effectuer les modifications vous-même.

AWS Certificate Manager certificat (ACM)

AMS dispose d'un certificat CT, Deployment | Advanced stack components | ACM avec SANs | Create (ct-3l14e139i5p50) supplémentaire, que vous pouvez utiliser pour soumettre une demande de certificat AWS Certificate Manager, avec jusqu'à cinq noms alternatifs de sujet (SAN) supplémentaires (tels que example.com, example.net et example.org). Pour plus de détails, voir [Qu'est-ce que c'est AWS Certificate Manager ?](#) et [caractéristique du certificat ACM](#).

Note

Ce paramètre de délai d'expiration ne concerne pas uniquement l'exécution, mais également votre validation du certificat ACM par le biais de la validation par e-mail. Sans votre validation, le RFC échoue.

Chiffrement des données dans AMS

AMS utilise plusieurs AWS services pour le chiffrement des données, notamment Amazon Simple Storage Service AWS Key Management Service (AWS KMS), Amazon Elastic Block Store, Amazon Relational Database Service Amazon Redshift, Amazon ElastiCache, AWS Lambda, et OpenSearch Amazon Service.

Amazon S3

Amazon S3 offre plusieurs options de chiffrement d'objet 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](#).

Amazon EBS

Avec le chiffrement Amazon EBS, vous n'avez pas besoin de créer, de maintenir et de sécuriser votre propre infrastructure de gestion des clés. Le chiffrement Amazon EBS utilise des AWS KMS clés lors de la création de volumes chiffrés et de snapshots. Les opérations de chiffrement ont lieu sur les serveurs qui hébergent EC2 les instances Amazon. Ceci est fait pour garantir la sécurité à la fois data-at-rest data-in-transit entre une instance et son stockage Amazon EBS attaché. Vous pouvez

attacher simultanément des volumes chiffrés et des volumes non chiffrés à une instance. Pour en savoir plus, consultez la page [Chiffrement Amazon EBS](#).

Amazon RDS

Amazon RDS peut chiffrer vos instances de base de données Amazon RDS. Les données chiffrées au repos incluent le stockage sous-jacent pour les instances de base de données, ses sauvegardes automatisées, ses répliques de lecture et ses instantanés. Les instances de base de données cryptées Amazon RDS utilisent l'algorithme de chiffrement standard AES-256 pour chiffrer vos données sur le serveur qui héberge vos instances de base de données Amazon RDS. Une fois vos données chiffrées, Amazon RDS gère l'authentification de l'accès et le déchiffrement de vos données de manière transparente avec un impact minimal sur les performances. Vous n'avez pas besoin de modifier vos applications clientes de base de données pour utiliser le chiffrement. Pour plus d'informations, veuillez consulter [Chiffrer des ressources Amazon RDS](#).

Amazon Simple Queue Service

Outre l'option de chiffrement côté serveur (SSE) géré par Amazon SQS par défaut, le SSE géré par Amazon SQS (SSE-SQS) vous permet de créer un chiffrement géré personnalisé côté serveur qui utilise des clés de chiffrement gérées par Amazon SQS pour protéger les données sensibles envoyées via des files d'attente de messages. Le chiffrement côté serveur (SSE) vous permet de transmettre des données sensibles dans des files d'attente cryptées. SSE protège le contenu des messages dans les files d'attente à l'aide de clés de chiffrement gérées par Amazon SQS (SSE-SQS) ou de clés gérées dans (SSE-KMS). AWS KMS Pour plus d'informations sur la gestion de SSE à l'aide de AWS Management Console, consultez la section [Chiffrement au repos](#).

Chiffrement des données au repos

OpenSearch Les domaines de service offrent le chiffrement des données au repos, une fonctionnalité de sécurité qui permet d'empêcher tout accès non autorisé à vos données. La fonctionnalité utilise AWS Key Management Service (AWS KMS) pour stocker et gérer vos clés de chiffrement et l'algorithme Advanced Encryption Standard avec des clés de 256 bits (AES-256) pour effectuer le chiffrement. Pour plus d'informations, consultez la section [Chiffrement des données au repos pour Amazon OpenSearch Service](#).

Gestion des clés

AWS KMS est un service géré qui vous permet de créer et de contrôler facilement les clés principales du client (CMKs), les clés de chiffrement utilisées pour chiffrer vos données. AWS KMS CMKs sont protégés par des modules de sécurité matériels (HSMs) validés par le programme de validation des

modules cryptographiques FIPS 140-2, sauf dans les régions de Chine (Pékin) et de Chine (Ningxia). Pour plus d'informations, consultez [Qu'est-ce qu'AWS Key Management Service ?](#)

Identity and Access Management

AWS Identity and Access Management (IAM) 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, vous êtes chargé de créer des rôles d'administrateur IAM entre comptes au sein de chacun de vos comptes gérés.

Mesures de protection IAM pour les zones d'atterrissage multicomptes (MALZ)

La zone de landing zone multi-comptes (MALZ) d'AMS nécessite une confiance Active Directory (AD) comme objectif de conception principal de la gestion des accès AMS afin de permettre à chaque organisation (AMS et client) de gérer le cycle de vie de ses propres identités. Cela évite d'avoir des informations d'identification dans le répertoire de l'autre. La confiance unidirectionnelle est configurée de telle sorte que le répertoire Active Directory géré au sein du client Compte AWS approuve l'AD détenu ou géré par le client pour authentifier les utilisateurs. Comme la confiance n'est qu'à sens unique, cela ne signifie pas que le client Active Directory fait confiance à Managed AD.

Dans cette configuration, le répertoire des clients qui gère les identités des utilisateurs est appelé User Forest, et le Managed AD auquel les EC2 instances Amazon sont attachées est connu sous le nom de Resource Forest. Il s'agit d'un modèle de conception Microsoft couramment utilisé pour l'authentification Windows ; pour plus d'informations, [voir Modèles de conception forestière](#).

Ce modèle permet aux deux organisations d'automatiser leurs cycles de vie respectifs et permet à AMS et à vous-même de révoquer rapidement l'accès si un employé quitte l'organisation. Sans ce modèle, si les deux organisations utilisaient un répertoire commun (ou si elles étaient créées users/groups dans les annuaires de l'autre), elles devraient mettre en place des flux de travail supplémentaires, ainsi que des synchronisations d'utilisateurs, pour tenir compte du départ et du départ des employés. Cela présente un risque car ce processus présente une latence et peut être sujet aux erreurs.

Conditions préalables à l'accès au MALZ

Intégration du fournisseur d'identité MALZ pour accéder à la console AWS/AMS, à la CLI et au SDK.

Confiance unidirectionnelle pour les EC2 instances Amazon de votre compte AMS.

Authentification par des identités

AMS utilise des rôles IAM, qui sont un type d'identité IAM. Un rôle IAM est très similaire à celui d'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 est destiné à 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.

Rôle d'utilisateur IAM dans AMS

Un rôle IAM est similaire à un utilisateur IAM, dans la mesure où il s'agit d'une AWS identité dotée de politiques d'autorisation qui déterminent ce que l'identité peut et ne peut pas faire. AWS En revanche, au lieu d'être associé de manière unique à une personne, un rôle est conçu pour être assumé par tout utilisateur qui en a besoin.

Il existe actuellement un rôle utilisateur AMS par défaut pour `Customer_ReadOnly_Role` les comptes AMS standard et un rôle supplémentaire `customer_managed_ad_user_role` pour les comptes AMS avec Managed Active Directory.

Les politiques de rôle définissent les autorisations CloudWatch et les actions de journalisation d'Amazon S3, l'accès à la console AMS, les restrictions en lecture seule pour la plupart Services AWS, l'accès restreint à la console S3 du compte et l'accès au type de changement de type AMS.

En outre, il `Customer_ReadOnly_Role` dispose d'autorisations mutatives sur les instances réservées qui vous permettent de réserver des instances. Cela permet de réaliser des économies. Par conséquent, si vous savez que vous aurez besoin d'un certain nombre d' EC2 instances Amazon pendant une longue période, vous pouvez les APIs appeler. Pour en savoir plus, consultez [Amazon EC2 Reserved Instances](#).

Note

L'objectif de niveau de service (SLO) AMS pour créer des politiques IAM personnalisées pour les utilisateurs IAM est de quatre jours ouvrables, sauf si une politique existante doit

être réutilisée. Si vous souhaitez modifier le rôle d'utilisateur IAM existant ou en ajouter un nouveau, soumettez une RFC [IAM : Update Entity](#) ou [IAM : Create Entity](#), respectivement.

Si les rôles Amazon IAM ne vous sont pas familiers, consultez la section Rôles [IAM pour obtenir des informations importantes](#).

Zone d'atterrissage multi-comptes (MALZ) : pour voir les politiques de rôle utilisateur par défaut et non personnalisées de la zone d'atterrissage multi-comptes AMS, reportez-vous à la section suivante. [MALZ : Rôles utilisateur IAM par défaut](#)

MALZ : Rôles utilisateur IAM par défaut

Déclarations de politique JSON pour les rôles utilisateur par défaut de la zone de landing zone multi-comptes AMS multi-comptes.

 Note

Les rôles des utilisateurs sont personnalisables et peuvent varier d'un compte à l'autre. Des instructions pour trouver votre rôle sont fournies.

Voici des exemples des rôles utilisateur MALZ par défaut. Pour vous assurer que vous avez défini les politiques dont vous avez besoin, exécutez la commande AWS [get-role](#) ou connectez-vous à la [console AWS Management -> IAM](#) et choisissez Rôles dans le volet de navigation.

Rôles principaux du compte UO

Un compte principal est un compte d'infrastructure géré par Malz. Les comptes principaux de la zone de landing zone multi-comptes AMS incluent un compte de gestion et un compte réseau.

Compte Core UO : rôles et politiques communs

Rôle	Politique ou politiques
AWSManagedServicesReadOnlyRole	ReadOnlyAccess (Politique publique gérée par AWS).
AWSManagedServicesCaseRole	ReadOnlyAccess

Rôle	Politique ou politiques
	AWSSupportAccès (politique publique gérée par AWS).
AWSManagedServicesChangeManagementRole (Version du compte principal)	ReadOnlyAccess AWSSupportAccès AMSChangeManagementReadOnlyPolicy AMSChangeManagementInfrastructurePolicy

Compte UO principal : rôles et politiques du compte de gestion

Rôle	Politique ou politiques
AWSManagedServicesBillingRole	AMSBillingPolitique (AMSBillingPolitique).
AWSManagedServicesReadOnlyRole	ReadOnlyAccess (Politique publique gérée par AWS).
AWSManagedServicesCaseRole	ReadOnlyAccess AWSSupportAccès (politique publique gérée par AWS).
AWSManagedServicesChangeManagementRole (Version du compte de gestion)	ReadOnlyAccess AWSSupportAccès AMSChangeManagementReadOnlyPolicy AMSChangeManagementInfrastructurePolicy AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

Compte UO principal : rôles et politiques du compte réseau

Rôle	Politique ou politiques
AWSManagedServicesReadOnlyRole	ReadOnlyAccess (Politique publique gérée par AWS).
AWSManagedServicesCaseRole	ReadOnlyAccess AWSSupportAccès (politique publique gérée par AWS).
AWSManagedServicesChangeManagementRole (Version du compte réseau)	ReadOnlyAccess AWSSupportAccès AMSChangeManagementReadOnlyPolicy AMSChangeManagementInfrastructurePolicy AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

Rôles des comptes d'applications

Les rôles de compte d'application sont appliqués à vos comptes spécifiques à l'application.

Compte d'application : rôles et politiques

Rôle	Politique ou politiques
AWSManagedServicesReadOnlyRole	ReadOnlyAccess (Politique publique gérée par AWS).
AWSManagedServicesCaseRole	ReadOnlyAccess AWSSupportAccès (politique publique gérée par AWS). Cette politique donne accès à toutes les opérations et ressources de support. Pour plus

Rôle	Politique ou politiques
	d'informations, consultez Getting Started with AWS Support .
AWSManagedServicesSecurityOpsRole	ReadOnlyAccess AWSsupport Exemple d'accès Cette politique donne accès à toutes les opérations et ressources de support. AWSCertificateManagerFullAccess informations, (politique publique gérée par AWS) AWSWAFFullAccess informations, (politique publique gérée par AWS). Cette politique accorde un accès complet aux ressources AWS WAF. AMSSecretsManagerSharedPolicy
AWSManagedServicesChangeManagementRole (Version du compte de l'application)	ReadOnlyAccess AWSsupportAccès (politique publique gérée par AWS). Cette politique donne accès à toutes les opérations et ressources de support. Pour plus d'informations, consultez Getting Started with AWS Support . AMSSecretsManagerSharedPolicy AMSChangeManagementPolicy AMSReservedInstancesPolicy AMSS3Stratégie

Rôle	Politique ou politiques
AWSManagedServicesAdminRole	ReadOnlyAccess
	AWSSupportAccès
	AMSChangeManagementInfrastructurePolicy
	AWSMarketplaceManageSubscriptions
	AMSSecretsManagerSharedPolicy
	AMSChangeManagementPolicy
	AWSCertificateManagerFullAccess
	AWSWAFFullAccès
	AMSS3Stratégie
	AMSReservedInstancesPolicy

Exemples de stratégies

Des exemples sont fournis pour la plupart des politiques utilisées. Pour consulter la [ReadOnlyAccess](#) politique (longue de plusieurs pages car elle fournit un accès en lecture seule à tous les AWS services), vous pouvez utiliser ce lien, si vous avez un compte AWS actif : [ReadOnlyAccess](#) Une version condensée est également incluse ici.

AMSBillingPolitique

AMSBillingPolicy

Le nouveau rôle de facturation peut être utilisé par votre service de comptabilité pour consulter et modifier les informations de facturation ou les paramètres du compte dans le compte de gestion. Pour accéder à des informations telles que les contacts alternatifs, consulter l'utilisation des ressources du compte, suivre votre facturation ou même modifier vos méthodes de paiement, vous utilisez ce rôle. Ce nouveau rôle comprend toutes les autorisations répertoriées sur la [page Web des actions IAM d'AWS Billing](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "aws-portal:ViewBilling",
        "aws-portal:ModifyBilling"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "AllowAccessToBilling"
    },
    {
      "Action": [
        "aws-portal:ViewAccount",
        "aws-portal:ModifyAccount"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "AllowAccessToAccountSettings"
    },
    {
      "Action": [
        "budgets:ViewBudget",
        "budgets:ModifyBudget"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "AllowAccessToAccountBudget"
    },
    {
      "Action": [
        "aws-portal:ViewPaymentMethods",
        "aws-portal:ModifyPaymentMethods"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "AllowAccessToPaymentMethods"
    },
    {
      "Action": [
```

```

        "aws-portal:ViewUsage"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToUsage"
},
{
    "Action": [
        "cur:DescribeReportDefinitions",
        "cur:PutReportDefinition",
        "cur>DeleteReportDefinition",
        "cur:ModifyReportDefinition"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToCostAndUsageReport"
},
{
    "Action": [
        "pricing:DescribeServices",
        "pricing:GetAttributeValues",
        "pricing:GetProducts"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToPricing"
},
{
    "Action": [
        "ce:*",
        "compute-optimizer:*"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToCostExplorerComputeOptimizer"
},
{
    "Action": [
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ModifyPurchaseOrders"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToPurchaseOrders"
}

```

```

    },
    {
      "Action": [
        "redshift:AcceptReservedNodeExchange",
        "redshift:PurchaseReservedNodeOffering"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "AllowAccessToRedshiftAction"
    },
    {
      "Action": "savingsplans:*",
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "AWSSavingsPlansFullAccess"
    }
  ]
}

```

AMSChangeManagementReadOnlyPolicy

AMSChangeManagementReadOnlyPolicy

Autorisations permettant de voir tous les types de modifications AMS et l'historique des types de modifications demandés.

AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

Autorisations permettant de demander le type de changement de type Déploiement | Zone d'atterrissage gérée | Compte de gestion | Créer un compte d'application (avec VPC).

AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

Autorisations permettant de demander le type de changement de type Déploiement | Zone d'atterrissage gérée | Compte réseau | Créer une table de routage de l'application.

AMSChangeManagementInfrastructurePolicy

AMSChangeManagementInfrastructurePolicy(pour la gestion | Autre | Autre CTs)

Autorisations permettant de demander les types de modification Gestion | Autre | Autre | Création et gestion | Autre | Autre | Mettre à jour.

AMSSecretsManagerSharedPolicy

AMSSecretsManagerSharedPolicy

Autorisations permettant de consulter le secret passwords/hasches partagé par AMS AWS Secrets Manager (par exemple, les mots de passe de l'infrastructure à des fins d'audit).

Autorisations permettant de créer un secret password/hasches à partager avec AMS. (par exemple, les clés de licence pour les produits qui doivent être déployés).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowAccessToSharedNameSpaces",
    "Effect": "Allow",
    "Action": "secretsmanager:*",
    "Resource": [
      "arn:aws:secretsmanager:*:secret:ams-shared/*",
      "arn:aws:secretsmanager:*:secret:customer-shared/*"
    ]
  },
  {
    "Sid": "DenyGetSecretOnCustomerNamespace",
    "Effect": "Deny",
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "arn:aws:secretsmanager:*:secret:customer-shared/*"
  },
  {
    "Sid": "AllowReadAccessToAMSNameSpace",
    "Effect": "Deny",
    "NotAction": [
      "secretsmanager:Describe*",
      "secretsmanager:Get*",
      "secretsmanager:List*"
    ],
    "Resource": "arn:aws:secretsmanager:*:secret:ams-shared/*"
  }
]
```

```
]
}
```

AMSCChangeManagementPolicy

AMSCChangeManagementPolicy

Autorisations permettant de demander et de consulter tous les types de modifications AMS, ainsi que l'historique des types de modifications demandés.

AMSReservedInstancesPolicy

AMSReservedInstancesPolicy

Autorisations pour gérer les instances EC2 réservées Amazon ; pour plus d'informations sur les tarifs, consultez [Amazon EC2 Reserved Instances](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowReservedInstancesManagement",
    "Effect": "Allow",
    "Action": [
      "ec2:ModifyReservedInstances",
      "ec2:PurchaseReservedInstancesOffering"
    ],
    "Resource": [
      "*"
    ]
  }]
}
```

AMSS3Politique

AMSS3Policy

Autorisations permettant de créer et de supprimer des fichiers à partir de compartiments Amazon S3 existants.

 Note

Ces autorisations ne permettent pas de créer des compartiments S3 ; cela doit être fait avec le type de modification Deployment | Advanced stack components | S3 storage | Create change.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:PutObject"
      ],
      "Resource": "*"
    }
  ]
}
```

AWSSupportAccès

AWSSupportAccess

Accès complet à Support. Pour plus d'informations, consultez [Getting Started with Support](#). Pour plus d'informations sur le Support Premium, consultez [Support](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "support:*"
    ]
  }]
}
```

```
],  
  "Resource": "*"   
}]  
}
```

AWSMarketplaceManageSubscriptions

AWSMarketplaceManageSubscriptions(Politique AWS gérée par le public)

Autorisations de s'abonner, de se désabonner et de consulter AWS Marketplace les abonnements.

JSON

```
{  
  "Version":"2012-10-17",  
  "Statement": [{  
    "Action": [  
      "aws-marketplace:ViewSubscriptions",  
      "aws-marketplace:Subscribe",  
      "aws-marketplace:Unsubscribe"  
    ],  
    "Effect": "Allow",  
    "Resource": "*"   
  }]  
}
```

AWSCertificateManagerFullAccess

AWSCertificateManagerFullAccess

Accès complet à AWS Certificate Manager. Pour de plus amples informations, veuillez consulter [AWS Certificate Manager](#).

[AWSCertificateManagerFullAccess](#) informations, (politique publique gérée par AWS).

JSON

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



```
"Effect": "Allow",
"Action": [
  "acm:*"
],
"Resource": "*"
}]
}
```

AWSWAFFullAccès

AWSWAFFullAccess

Accès complet à AWS WAF. Pour plus d'informations, voir [AWS WAF - Web Application Firewall](#).

[AWSWAFFullAccess](#) information, (politique AWS gérée par le public). Cette politique accorde un accès complet aux AWS WAF ressources.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "waf:*",
      "waf-regional:*",
      "elasticloadbalancing:SetWebACL"
    ],
    "Effect": "Allow",
    "Resource": "*"
  }]
}
```

ReadOnlyAccess

ReadOnlyAccess

Accès en lecture seule à tous les AWS services et ressources de la AWS console. Lors du AWS lancement d'un nouveau service, AMS met à jour la ReadOnlyAccess politique afin d'ajouter des autorisations en lecture seule pour le nouveau service. Les autorisations mises à jour s'appliquent à toutes les entités du principal auxquelles la politique est attachée.

Cela ne permet pas de se connecter à des EC2 hôtes ou à des hôtes de base de données.

Si vous avez une politique active Compte AWS, vous pouvez utiliser ce lien [ReadOnlyAccess](#) pour consulter l'intégralité de la ReadOnlyAccess politique. L'ensemble ReadOnlyAccess de la politique est très long car il fournit un accès en lecture seule à tous. Services AWS Ce qui suit est un extrait partiel de la ReadOnlyAccess politique.

Zone d'atterrissage à compte unique (SALZ) : pour voir les politiques de rôle utilisateur par défaut et non personnalisées de la zone d'atterrissage à compte unique AMS, reportez-vous à la section suivante. [SALZ : rôle d'utilisateur IAM par défaut](#)

SALZ : rôle d'utilisateur IAM par défaut

Déclarations de politique JSON pour le rôle utilisateur par défaut de la zone de landing zone à compte unique AMS.

 Note

Le rôle d'utilisateur par défaut de SALZ est personnalisable et peut varier d'un compte à l'autre. Des instructions pour trouver votre rôle sont fournies.

Voici un exemple du rôle utilisateur SALZ par défaut. Pour vous assurer que les politiques sont définies pour vous, exécutez la [get-role](#) commande. Vous pouvez également vous connecter à la AWS Identity and Access Management console à l'<https://console.aws.amazon.com/iam/> adresse, puis sélectionner Rôles.

Le rôle client en lecture seule est une combinaison de plusieurs politiques. Le détail du rôle (JSON) suit.

Politique d'audit des Managed Services :

Politique IAM ReadOnly de Managed Services

Politique relative aux utilisateurs de Managed Services

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

```

    "Effect": "Allow",
    "Action": [
        "s3:ListBucket"
    ],
    "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
    ],
    "Condition": {
        "StringLike": {
            "s3:prefix": [
                "aws/*",
                "app/*",
                "encrypted",
                "encrypted/",
                "encrypted/app/*"
            ]
        }
    }
},
{
    "Sid": "BasicAccessRequiredByS3Console",
    "Effect": "Allow",
    "Action": [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
    ],
    "Resource": [
        "arn:aws:s3:::*"
    ]
},
{
    "Sid": "AllowCustomerToGetLogs",
    "Effect": "Allow",
    "Action": [
        "s3:GetObject*"
    ],
    "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/aws/*",
        "arn:aws:s3:::mc-a*-logs-*/encrypted/app/*"
    ]
},
{
    "Sid": "AllowAccessToOtherObjects",
    "Effect": "Allow",

```

```

    "Action": [
      "s3:DeleteObject*",
      "s3:Get*",
      "s3:List*",
      "s3:PutObject*"
    ],
    "Resource": [
      "*"
    ]
  },
  {
    "Sid": "AllowCustomerToListTheLogBucketRoot",
    "Effect": "Allow",
    "Action": [
      "s3:ListBucket"
    ],
    "Resource": [
      "arn:aws:s3:::mc-a*-logs-*"
    ],
    "Condition": {
      "StringEquals": {
        "s3:prefix": [
          "",
          "/"
        ]
      }
    }
  },
  {
    "Sid": "AllowCustomerCWLConsole",
    "Effect": "Allow",
    "Action": [
      "logs:DescribeLogStreams",
      "logs:DescribeLogGroups"
    ],
    "Resource": [
      "arn:aws:logs:*:*:log-group:*"
    ]
  },
  {
    "Sid": "AllowCustomerCWLAccessLogs",
    "Effect": "Allow",
    "Action": [
      "logs:FilterLogEvents",

```

```

    "logs:GetLogEvents"
  ],
  "Resource": [
    "arn:aws:logs:*:*:log-group:/aws/*",
    "arn:aws:logs:*:*:log-group:/infra/*",
    "arn:aws:logs:*:*:log-group:/app/*",
    "arn:aws:logs:*:*:log-group:RDSOSMetrics:*:*"
  ]
},
{
  "Sid": "AWSManagedServicesFullAccess",
  "Effect": "Allow",
  "Action": [
    "amscm:*",
    "amsskms:*"
  ],
  "Resource": [
    "*"
  ]
},
{
  "Sid": "ModifyAWSBillingPortal",
  "Effect": "Allow",
  "Action": [
    "aws-portal:Modify*"
  ],
  "Resource": [
    "*"
  ]
},
{
  "Sid": "DenyDeleteCWL",
  "Effect": "Deny",
  "Action": [
    "logs:DeleteLogGroup",
    "logs:DeleteLogStream"
  ],
  "Resource": [
    "arn:aws:logs:*:*:log-group:*"
  ]
},
{
  "Sid": "DenyMCCWL",
  "Effect": "Deny",

```

```

    "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:PutLogEvents"
    ],
    "Resource": [
        "arn:aws:logs:*:*:log-group:/mc/*"
    ]
},
{
    "Sid": "DenyS3MCNamespace",
    "Effect": "Deny",
    "Action": [
        "s3:*"
    ],
    "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/encrypted/mc/*",
        "arn:aws:s3:::mc-a*-logs-*/mc/*",
        "arn:aws:s3:::mc-a*-logs-*--audit/*",
        "arn:aws:s3:::mc-a*-internal-*/*",
        "arn:aws:s3:::mc-a*-internal-*"
    ]
},
{
    "Sid": "ExplicitDenyS3CfnBucket",
    "Effect": "Deny",
    "Action": [
        "s3:*"
    ],
    "Resource": [
        "arn:aws:s3:::cf-templates-*"
    ]
},
{
    "Sid": "DenyListBucketS3LogsMC",
    "Action": [
        "s3:ListBucket"
    ],
    "Effect": "Deny",
    "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
    ]
}

```

```

    ],
    "Condition": {
      "StringLike": {
        "s3:prefix": [
          "auditlog/*",
          "encrypted/mc/*",
          "mc/*"
        ]
      }
    }
  },
  {
    "Sid": "DenyS3LogsDelete",
    "Effect": "Deny",
    "Action": [
      "s3:Delete*",
      "s3:Put*"
    ],
    "Resource": [
      "arn:aws:s3:::mc-a*-logs-*/*"
    ]
  },
  {
    "Sid": "DenyAccessToKmsKeysStartingWithMC",
    "Effect": "Deny",
    "Action": [
      "kms:*"
    ],
    "Resource": [
      "arn:aws:kms::*:key/mc-*",
      "arn:aws:kms::*:alias/mc-*"
    ]
  },
  {
    "Sid": "DenyListingOfStacksStartingWithMC",
    "Effect": "Deny",
    "Action": [
      "cloudformation:*"
    ],
    "Resource": [
      "arn:aws:cloudformation::*:stack/mc-*"
    ]
  },
  {

```

```

    "Sid": "AllowCreateCWMetricsAndManageDashboards",
    "Effect": "Allow",
    "Action": [
        "cloudwatch:PutMetricData"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "AllowCreateandDeleteCWDashboards",
    "Effect": "Allow",
    "Action": [
        "cloudwatch:DeleteDashboards",
        "cloudwatch:PutDashboard"
    ],
    "Resource": [
        "*"
    ]
}
]
}

```

Politique partagée du Customer Secrets Manager

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSecretsManagerListSecrets",
      "Effect": "Allow",
      "Action": "secretsmanager:listSecrets",
      "Resource": "*"
    },
    {
      "Sid": "AllowCustomerAdminAccessToSharedNameSpaces",
      "Effect": "Allow",
      "Action": "secretsmanager:*",
      "Resource": [
        "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
        "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
      ]
    }
  ]
}

```



```

    ]
  },
  {
    "Sid": "DenyCustomerGetSecretCustomerNamespace",
    "Effect": "Deny",
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
  },
  {
    "Sid": "AllowCustomerReadOnlyAccessToAMSNameSpace",
    "Effect": "Deny",
    "NotAction": [
      "secretsmanager:Describe*",
      "secretsmanager:Get*",
      "secretsmanager:List*"
    ],
    "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
  }
]
}

```

Politique d'abonnement du Customer Marketplace

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowMarketPlaceSubscriptions",
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Subscribe"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}

```

Enregistrement et surveillance des événements de sécurité

AMS surveille en permanence l'environnement géré pour détecter les menaces de sécurité. Des événements de sécurité peuvent être détectés par AMS ou par vous-même. AMS met régulièrement à jour son processus d'automatisation, basé sur le guide de gestion des incidents de sécurité informatique du National Institute of Standards and Technology (NIST), afin de mieux détecter les menaces de sécurité.

Sécurité des terminaux (EPS)

Les ressources que vous fournissez dans votre environnement AMS Advanced incluent automatiquement l'installation d'un client de surveillance de la sécurité des terminaux (EPS). Ce processus garantit que les ressources gérées par AMS Advanced sont surveillées et prises en charge 24 heures sur 24, 7 jours sur 7. En outre, AMS Advanced surveille toutes les activités des agents et un incident est créé si un événement de sécurité est détecté.

Note

Les incidents de sécurité sont traités comme des incidents ; pour plus d'informations, consultez la section [Réponse aux incidents](#).

Endpoint Security fournit une protection contre les programmes malveillants. En particulier, les actions suivantes sont prises en charge :

- EC2 les instances s'enregistrent avec EPS
- EC2 les instances se désinscrivent d'EPS
- EC2 protection anti-malware en temps réel des instances
- Rythme cardiaque initié par l'agent EPS
- EPS restaure le fichier mis en quarantaine
- Notification d'événement EPS
- Rapports EPS

AMS Advanced utilise Trend Micro pour la sécurité des terminaux (EPS). Il s'agit des paramètres EPS par défaut. Pour en savoir plus sur Trend Micro, consultez le [centre d'aide de Trend Micro Deep Security](#) ; notez que les liens n'appartenant pas à Amazon peuvent être modifiés sans préavis.

Les paramètres par défaut de la zone d'atterrissage multi-comptes AMS (MALZ) sont décrits dans les sections suivantes ; pour les paramètres EPS de zone d'atterrissage multi-comptes autres que ceux par défaut d'AMS, [voir Paramètres EPS non par défaut de la zone d'atterrissage multi-comptes AMS Advanced](#).

 Note

Vous pouvez apporter votre propre EPS, voir [AMS apporter votre propre EPS](#).

Paramètres EPS généraux

Paramètres réseau généraux de sécurité des terminaux.

Valeurs par défaut d'EPS

Paramètre	Par défaut
Ports de pare-feu (groupe de sécurité des instances)	Les agents EPS Deep Security Manager (DSMs) doivent avoir le port 4120 ouvert Agent/Relay pour les communications avec le gestionnaire et le port 4119 pour la console du gestionnaire. Le port 4122 des relais EPS doit être ouvert pour permettre la communication avec Manager/Agent le relais. Aucun port spécifique ne doit être ouvert pour les communications entrantes entre les instances du client, car les agents sont à l'origine de toutes les demandes.
Direction de la communication	Initié par l'agent/l'appliance
Intervalle entre les battements cardiaques	Dix minutes
Nombre de battements cardiaques manqués avant une alerte	Deux
Dérive maximale autorisée (différence) entre les heures des serveurs	Illimité

Paramètre	Par défaut
Génère des erreurs hors ligne pour les machines virtuelles inactives (enregistrées, mais pas en ligne)	Non
Politique par défaut	Politique de base (décrite ci-dessous)
Activation de plusieurs ordinateurs avec le même nom d'hôte	Est autorisé
Des alertes pour les mises à jour en attente sont émises	Après sept jours
Calendrier de mise à jour	AMS cible un cycle de publication mensuel pour les mises à jour logicielles de Trend Micro Deep Security Manager (DSM) /Deep Security Agent (DSA). Cependant, AMS ne maintient pas de contrat de niveau de service pour les mises à jour. Les mises à jour sont effectuées à l'échelle de la flotte par les équipes de développement d'AMS lors d'un déploiement. Les mises à jour DSA/DSA sont enregistrées dans les événements du système Trend Micro DSM qu'AMS conserve localement par défaut pendant 13 semaines. Pour la documentation des fournisseurs, consultez la section Événements système dans le centre d'aide de Trend Micro Deep Security. Les journaux sont également exportés vers le groupe de journaux/ aws/ams/eps/var/log/DSM.log sur Amazon CloudWatch.
Source de mise à jour	Serveur de mise à jour Trend Micro (https://ipv6-iaus.trendmicro.com/iau_server.dll/)

Paramètre	Par défaut
Suppression des données d'événements ou de journaux	Les événements et les journaux sont supprimés de la base de données DSM au bout de sept jours.
Les versions du logiciel de l'agent sont conservées	Jusqu'à cinq
Les dernières mises à jour des règles ont lieu	Jusqu'à dix
Stockage des journaux	Par défaut, les fichiers journaux sont stockés de manière sécurisée dans Amazon S3, mais vous pouvez également les archiver sur Amazon Glacier pour répondre aux exigences d'audit et de conformité.

Politique de base

Paramètres par défaut de la politique de base de sécurité des terminaux.

Politique de base EPS

Paramètre	Par défaut
Modules activés	Antimalware
Modules désactivés	Réputation sur le Web
	Pare-feu
	Protection contre les intrusions
	Surveillance de l'intégrité
	Inspection du journal
	Contrôle des applications

Protection contre les programmes malveillants

Paramètres anti-malware de sécurité des terminaux.

Paramètres par défaut de l'anti-malware EPS

Paramètre	Par défaut	Remarques
Scan en temps réel	Scannez tout	Mettez en quarantaine tous les virus suspects. IntelliTrap Activation et spyware/grayware protection.
	Tous les Day/All jours (24 heures)	Les spywares et les graywares déclenchent l'anti-malware et entraînent la mise en quarantaine de l'élément.
Scan manuel	Scannez tout	Doit être demandé, puis suit la configuration de scan en temps réel par défaut.
Scan programmé	Scannez tout	Prévu le dernier dimanche de chaque mois, à 6 heures du matin.
Protection intelligente	Désactivées	N/A
Fichiers mis en quarantaine	Gestionnaire de sécurité Trend Micro Deep (DSM)	Environ 1 Go de disque réservé à la quarantaine.
Limitation de numérisation	Trend Micro DSM	Scannez des fichiers de toutes tailles.

Paramètre	Par défaut	Remarques
Spyware ou grayware autorisés	Aucune	N/A
Notification d'événement local	Oui	N/A

Processus d'atténuation des malwares

AMS utilise la plateforme Deep Security Platform (système anti-malware) de Trend Micro pour détecter les malwares sur vos instances gérées par AMS et y répondre. Par défaut, l'agent de détection Trend Micro s'exécute sur toutes les EC2 instances Amazon, y compris celles des services partagés et des sous-réseaux privés, pour les systèmes d'exploitation Windows et Linux. Le système anti-programme malveillant est connecté à la surveillance AMS afin qu'un événement soit généré chaque fois qu'un logiciel malveillant est détecté. S'il y a un impact sur le client, l'événement est transféré au processus de gestion des incidents (pour plus de détails, voir [Réponse aux incidents AMS](#)). Pendant qu'AMS évalue l'impact, vous êtes averti et des tentatives sont faites pour atténuer l'impact.

Les définitions anti-malware de Trend Micro sont mises à jour automatiquement lorsque Trend Micro publie des mises à jour.

Lors de l'intégration de l'application, vous indiquez l'action que vous souhaitez qu'AMS entreprenne lorsqu'un logiciel malveillant est détecté sur une instance :

- Assurez-vous que le fichier mis en quarantaine figure dans la liste des fichiers autorisés, retirez-le de la quarantaine et réintégrez-le dans le système de fichiers.
- Supprimez le fichier mis en quarantaine, en le retirant de l'instance.
- Suspendez l'instance et remplacez-la. Vous pouvez ensuite monter l'instance suspendue à des fins de recherche médico-légale.

Après l'intégration de l'application :

- Lorsque le système anti-programme malveillant découvre un logiciel malveillant sur une instance, AMS le met automatiquement en quarantaine. Cela déclenche un événement et une enquête de suivi.
- AMS vous informe de l'événement par le biais d'une notification de service et commence à suivre l'action d'atténuation par défaut que vous avez sélectionnée.

- Si vous n'avez pas choisi d'action par défaut, AMS vous demande quelle action effectuer. Après avoir reçu vos instructions, AMS exécute l'action sélectionnée et vous en informe. AMS vous avertit à nouveau une fois l'action terminée, y compris les informations nécessaires à l'analyse médico-légale, le cas échéant.

Activez l'IDS et l'IPS dans Trend Micro Deep Security

Vous pouvez demander à AMS d'activer le système de détection d'intrusion (IDS) et les systèmes de protection contre les intrusions (IPS) de Trend Micro, des fonctionnalités autres que celles par défaut, pour votre compte.

Pour ce faire, soumettez une demande de mise à jour (Gestion | Autre | Autre | Mise à jour) et incluez une liste d'adresses e-mail pour recevoir les notifications IDS et IPS. Ces adresses sont ajoutées à une rubrique SNS de votre compte, créée par AMS pour vous.

Note

AMS ne peut ajouter aucun service Trend Micro susceptible d'interférer avec notre capacité à fournir d'autres services AMS.

Analyses complètes des programmes malveillants du système

La norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) exige des analyses complètes des logiciels malveillants du système, qui sont activées par défaut sur votre VPC géré par AMS. Les analyses complètes du système sont programmées pour être effectuées à 2 heures du matin (selon le fuseau horaire défini sur le serveur) car elles utilisent beaucoup de processeur. Les analyses complètes du système s'ajoutent aux analyses régulières des logiciels malveillants qui n'utilisent pas beaucoup de processeur.

Il existe un nouveau type de modification de gestion (CT), Désactiver les analyses de programmes malveillants, qui vous permet de désactiver les analyses complètes des programmes malveillants du système. Vous pouvez trouver le CT dans Gestion | Sécurité de l'hôte | Analyse complète du système | Désactiver la classification, modifier l'ID ct-1pybwg08h8qsz. Pour réactiver les scans, utilisez le logiciel Management | Other | Other | Update CT. La désactivation des analyses complètes du système ne désactive pas les analyses régulières des programmes malveillants.

Sécurité d'Amazon Inspector

Le service Amazon Inspector surveille la sécurité de vos piles gérées par AMS. Amazon Inspector est un service d'évaluation automatique de la sécurité qui permet d'identifier les lacunes en matière de sécurité et de conformité de l'infrastructure déployée sur AWS. Les évaluations de sécurité d'Amazon Inspector vous permettent d'évaluer automatiquement les risques, les vulnérabilités et les écarts par rapport aux meilleures pratiques en vérifiant l'absence d'accessibilité involontaire au réseau et de vulnérabilités dans vos instances Amazon EC2 . Après avoir effectué une évaluation, Amazon Inspector produit une liste détaillée des résultats de sécurité classés par niveau de gravité. Les évaluations Amazon Inspector sont proposées sous forme de packages de règles prédéfinis correspondant aux meilleures pratiques et définitions de sécurité courantes. Ces règles sont régulièrement mises à jour par les chercheurs en AWS sécurité. Pour plus d'informations sur Amazon Inspector, rendez-vous sur [Amazon Inspector](#).

AMS Amazon Inspector FAQs

- Amazon Inspector est-il installé par défaut sur mes comptes AMS ?

Non Amazon Inspector ne fait pas partie de la génération d'AMI par défaut ni de l'ingestion de la charge de travail.

- Comment accéder à Amazon Inspector et l'installer ?

Soumettez une RFC (Management | Other | Other | Create) pour demander l'accès au compte et l'installation à Inspector. L'équipe des opérations AMS modifiera le ReadOnly rôle Customer_ _Role afin de fournir un accès à la console Amazon Inspector (sans accès SSM).

- L'agent Amazon Inspector doit-il être installé sur toutes les EC2 instances Amazon que je souhaite évaluer ?

Non, les évaluations Amazon Inspector avec le package de règles d'accessibilité au réseau peuvent être exécutées sans agent pour aucune instance Amazon EC2 . L'agent est requis pour les packages de règles d'évaluation de l'hôte. Pour plus d'informations sur l'installation des agents, consultez la section [Installation des agents Amazon Inspector](#).

- Y a-t-il un coût supplémentaire pour ce service ?

Oui. Les tarifs d'Amazon Inspector sont disponibles sur le site de [tarification d'Amazon Inspector](#).

- Quelles sont les conclusions d'Amazon Inspector ?

Les résultats sont des problèmes de sécurité potentiels découverts lors de l'évaluation par Amazon Inspector de la cible d'évaluation sélectionnée. Les résultats sont affichés dans la console Amazon Inspector ou dans l'API et contiennent à la fois une description détaillée des problèmes de sécurité et des recommandations pour les résoudre.

- Les rapports d'évaluation d'Amazon Inspector sont-ils disponibles ?

Oui. Un rapport d'évaluation est un document qui détaille les éléments testés lors de l'exécution d'évaluation, ainsi que les résultats de l'évaluation. Les résultats de votre évaluation se présentent sous la forme de rapports standard, qui sont générés afin que vous puissiez partager les résultats avec votre équipe et mettre en place les mesures correctives nécessaires, enrichir vos données d'audit de conformité, ou stocker ces informations pour référence ultérieure. Un rapport d'évaluation Amazon Inspector peut être généré pour une exécution d'évaluation une fois celle-ci terminée avec succès.

- Puis-je utiliser des balises pour identifier les piles sur lesquelles je souhaite générer des rapports Amazon Inspector ?

Oui.

- Les équipes d'AMS Operations auront-elles accès aux résultats de l'évaluation d'Amazon Inspector ?

Oui. Toute personne ayant accès à la console Amazon Inspector dans AWS peut consulter les résultats et les rapports d'évaluation.

- Les équipes opérationnelles d'AMS recommanderont-elles ou prendront-elles des mesures en fonction des conclusions des rapports Amazon Inspector ?

Non Si vous souhaitez que des modifications soient apportées sur la base des conclusions du rapport Amazon Inspector, vous devez demander des modifications par le biais d'une RFC (Management | Other | Other | Update).

- AMS sera-t-il averti lorsque je publie un rapport Amazon Inspector ?

Lorsque vous demandez l'accès à Amazon Inspector, l'opérateur AMS exécutant la RFC informe votre CSDM de la demande.

Pour plus d'informations, consultez [Amazon Inspector FAQs](#).

Réponse aux incidents AMS

AMS utilise les meilleures pratiques traditionnelles 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 plusieurs centres d'opérations dans le monde entier, avec des opérateurs dédiés qui surveillent activement les tableaux de bord et les files d'attente d'incidents.

Nos ingénieurs d'exploitation utilisent des outils internes de suivi des incidents pour identifier, enregistrer, classer, hiérarchiser, diagnostiquer, résoudre et clôturer les incidents et vous fournir des mises à jour sur toutes ces activités via la console AMS ou via l' Support API. Nos opérateurs, dont beaucoup ont travaillé pour AWS Premium Support dans différents profils technologiques et ont occupé différents rôles, tirent parti de divers Support outils internes pour les aider dans toutes ces activités. Ces opérateurs connaissent parfaitement les infrastructures prises en charge par AMS et possèdent des compétences techniques de niveau expert pour résoudre tous les problèmes de support identifiés. Dans les rares cas où nos opérateurs ont besoin d'assistance, les équipes de support et de AWS service Premium sont disponibles pour les aider en cas de besoin.

Dans les cas où des incidents hautement prioritaires ont un impact sur vos charges de travail critiques, AMS recommandera une restauration de l'infrastructure. Il faut souvent trouver un compromis entre le dépannage d'un problème ou la restauration à partir d'une sauvegarde dont le fonctionnement a été vérifié, les risques pour les clients et les impacts liés aux interruptions de service étant les facteurs décisifs. Si vous avez du temps à consacrer à la résolution des problèmes, AMS vous aidera, mais si l'urgence de la restauration est élevée, nous pouvons lancer une restauration immédiatement.

Note

Les données éphémères qui ne font pas partie du modèle de pile ou de la restauration des données sont perdues. AMS déploie des efforts raisonnables pour restaurer l'infrastructure lorsque les offres AWS de services ne sont pas disponibles. La restauration de l'infrastructure est terminée une fois que les offres de AWS services sont disponibles.

Si vous n'autorisez pas la restauration de l'infrastructure conformément aux recommandations d'AMS, vous ne serez pas éligible à un crédit de service correspondant à l'engagement de service AMS concernant le délai de résolution des incidents.

Validation de conformité

AMS déploie et gère une bibliothèque de AWS Config règles et d'actions correctives afin de vous protéger contre les erreurs de configuration susceptibles de réduire la sécurité et l'intégrité opérationnelle de vos comptes.

Par exemple, lorsqu'un compartiment Amazon S3 est créé, AWS Config vous pouvez évaluer le compartiment Amazon S3 par rapport à une règle qui oblige les compartiments Amazon S3 à refuser l'accès public en lecture. Si la politique de compartiment ou la liste de contrôle d'accès aux compartiments (ACL) d'Amazon S3 autorise l'accès public en lecture, AWS Config signale à la fois le compartiment et la règle comme non conformes. Ils AWS Config Rules marquent les ressources comme conformes, non conformes ou non applicables, en fonction du résultat de leur évaluation. Pour plus d'informations sur le AWS Config service, consultez le [guide du AWS Config développeur](#).

Vous pouvez utiliser la AWS Config console, la AWS CLI ou AWS Config l'API pour consulter les règles déployées dans votre compte et l'état de conformité de vos règles et ressources. Pour plus d'informations, consultez la AWS Config documentation : [Visualisation de la conformité des configurations](#).

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.

Zone d'atterrissage multi-comptes affichant l'état de conformité de votre AWS Config Rules

La zone de landing zone multi-comptes AMS utilise le service d' AWS Config agrégation pour créer une vue centralisée de la conformité de tous vos comptes. Cela signifie que vous pouvez consulter l'état de conformité de l' AWS Config Rules ensemble de votre environnement de zone d'atterrissage multi-comptes AMS sous l' AWS Config agrégateur de votre compte de sécurité.

Voici un exemple de l' AWS Config agrégateur présentant l'état de conformité central de AWS Config Rules tous les comptes.

Pour plus d'informations, consultez la documentation AWS relative à [Config Aggregator](#).

- Comment AMS utilise-t-il les règles AWS Config ?

AMS crée AWS Config Rules pour donner une visibilité sur la configuration de vos AWS ressources par rapport aux conditions spécifiées dans les règles. Si une règle n'est pas conforme, vous pouvez demander une modification et l'équipe AMS Ops travaillera avec vous pour prendre des mesures correctives.

- Dans ce cas, les modifications suivantes apparaissent dans vos comptes AMS :
 - AWS Config Rules sous AWS Config > Règles
 - Des règles de configuration personnalisées avec leurs fonctions Lambda existent dans votre compte
 - Agrégateur de configuration dans le compte de sécurité et autorisation de configuration dans tous les comptes (zone d'accueil multi-comptes uniquement)

Voici un exemple AWS Config Rules et les résultats de leur évaluation de conformité sont présentés ci-dessous :

Pour en savoir plus sur AWS Config, consultez :

- AWS Config : [qu'est-ce que Config ?](#)
- Règles AWS Config : [évaluation des ressources à l'aide de règles](#)
- Règles de configuration AWS : [vérification dynamique de la conformité : règles de configuration AWS — Vérification dynamique de la conformité pour les ressources du cloud](#)
- AWS Config Aggregator : agrégation de données [multicomptes et multirégions](#)

Restrictions relatives à la politique de contrôle du service de zone d'atterrissage multi-comptes AMS

Cette section a été supprimée car elle contient des informations sensibles relatives à la sécurité AMS. Ces informations sont disponibles dans la documentation de la console AMS. Pour accéder à AWS

Artifact, vous pouvez contacter votre CSDM pour obtenir des instructions ou consulter [Getting Started with AWS Artifact](#).

Résilience

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section [Infrastructure AWS globale](#).

Sécurité de l'infrastructure

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.

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-Support la 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.

Utilisation des groupes de sécurité

Un groupe de sécurité fonctionne comme un pare-feu virtuel contrôlant le trafic d'une ou de plusieurs instances. Les groupes de sécurité AMS vous permettent de définir des règles de trafic entrant et sortant au niveau de l'instance. Vous pouvez créer un groupe de sécurité et spécifier des ressources dans votre compte AMS, les EC2 instances Amazon, les instances de base de données Amazon RDS, les équilibreurs de charge, les instances de réplication Deep Security Manager (DSM), les cibles de montage EFS et les ElastiCache clusters, à associer au groupe de sécurité. Une fois associé, le trafic à destination ou en provenance de ces instances est limité par les règles définies dans le groupe de sécurité.

Pour mieux comprendre la sécurité générale d'AWS, consultez les [meilleures pratiques en matière de sécurité, d'identité et de conformité](#) et les [groupes EC2 de sécurité Amazon pour les instances Linux](#).

AMS dispose désormais d'un ensemble de types de modifications pour créer et gérer des groupes de sécurité :

- Déploiement | Composants de pile avancés | Groupe de sécurité | Créer (ct-10xx2g2d7hc90)
- Gestion | Composants de pile avancés | Groupe de sécurité | Supprimer (ct-3cp96z7r065e4)
- Gestion | Composants de pile avancés | Groupe de sécurité | Mise à jour (ct-3memthlcmvc1b)

Pour des exemples, consultez [la section Groupes de sécurité](#).

Groupes de sécurité

Dans AWS VPCs, les groupes de sécurité AWS agissent comme des pare-feux virtuels, contrôlant le trafic pour une ou plusieurs piles (une instance ou un ensemble d'instances). Lorsqu'une pile est

lancée, elle est associée à un ou plusieurs groupes de sécurité, qui déterminent le trafic autorisé à l'atteindre :

- Pour les piles de vos sous-réseaux publics, les groupes de sécurité par défaut acceptent le trafic HTTP (80) et HTTPS (443) en provenance de tous les emplacements (Internet). Les piles acceptent également le trafic SSH et RDP interne en provenance de votre réseau d'entreprise et des bastions AWS. Ces piles peuvent ensuite sortir via n'importe quel port vers Internet. Ils peuvent également accéder à vos sous-réseaux privés et à d'autres piles de votre sous-réseau public.
- Les piles de vos sous-réseaux privés peuvent être transférées vers n'importe quelle autre pile de votre sous-réseau privé, et les instances d'une pile peuvent communiquer pleinement entre elles via n'importe quel protocole.

Important

Le groupe de sécurité par défaut pour les piles sur les sous-réseaux privés permet à toutes les piles de votre sous-réseau privé de communiquer avec les autres piles de ce sous-réseau privé. Si vous souhaitez restreindre les communications entre les piles d'un sous-réseau privé, vous devez créer de nouveaux groupes de sécurité décrivant cette restriction. Par exemple, si vous souhaitez restreindre les communications avec un serveur de base de données afin que les piles de ce sous-réseau privé ne puissent communiquer qu'à partir d'un serveur d'applications spécifique via un port spécifique, demandez un groupe de sécurité spécial. La procédure à suivre est décrite dans cette section.

Groupes de sécurité par défaut

MALZ

Le tableau suivant décrit les paramètres par défaut du groupe de sécurité entrant (SG) pour vos piles. Le SG est nommé « SentinelDefaultSecurityGroupPrivateOnly -VPC-ID ». Il s'agit **ID** d'un identifiant VPC dans votre compte de zone d'atterrissage multi-comptes AMS. Tout le trafic sortant vers « mc-initial-garden - SentinelDefaultSecurityGroupPrivateOnly » est autorisé via ce groupe de sécurité (tout le trafic local au sein des sous-réseaux de pile est autorisé).

Tout le trafic sortant vers 0.0.0.0/0 est autorisé par un deuxième groupe de sécurité « ». SentinelDefaultSecurityGroupPrivateOnly

Tip

Si vous choisissez un groupe de sécurité pour un type de modification AMS, tel que EC2 create ou OpenSearch create domain, vous devez utiliser l'un des groupes de sécurité par défaut décrits ici, ou un groupe de sécurité que vous avez créé. Vous trouverez la liste des groupes de sécurité, par VPC, dans la EC2 console AWS ou dans la console VPC.

D'autres groupes de sécurité par défaut sont utilisés à des fins AMS internes.

Groupes de sécurité AMS par défaut (trafic entrant)

Type	Protocole	Plage de ports	Source
Tout le trafic	Tous	Tous	SentinelDefaultSecurityGroupPrivateOnly (limite le trafic sortant aux membres du même groupe de sécurité)
Tout le trafic	Tous	Tous	SentinelDefaultSecurityGroupPrivateOnlyEgressAll (ne limite pas le trafic sortant)
HTTP, HTTPS, SSH, RDP	TCP	80/ 443 (Source : 0,0,0,0/0) L'accès SSH et RDP est autorisé depuis les bastions	SentinelDefaultSecurityGroupPublic (ne limite pas le trafic sortant)
Bastions du MALZ :			
SSH	TCP	22	SharedServices VPC CIDR et DMZ VPC CIDR, ainsi que sur site fournis par le client CIDRs
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	
Bastions SALZ :			

Type	Protocole	Plage de ports	Source
SSH	TCP	22	mc-initial-garden- LinuxBastion SG
SSH	TCP	22	mc-initial-garden- LinuxBastion DMZG
RDP	TCP	3389	mc-initial-garden- WindowsBastion SG
RDP	TCP	3389	mc-initial-garden- WindowsBastion DMZG

SALZ

Le tableau suivant décrit les paramètres par défaut du groupe de sécurité entrant (SG) pour vos piles. Le SG est nommé « mc-initial-garden - SentinelDefaultSecurityGroupPrivateOnly - **ID** » où se **ID** trouve un identifiant unique. Tout le trafic sortant vers « mc-initial-garden - SentinelDefaultSecurityGroupPrivateOnly » est autorisé via ce groupe de sécurité (tout le trafic local au sein des sous-réseaux de pile est autorisé).

Tout le trafic sortant vers 0.0.0.0/0 est autorisé par un deuxième groupe de sécurité « - - »mc-initial-garden. SentinelDefaultSecurityGroupPrivateOnlyEgressAll **ID**

Tip

Si vous choisissez un groupe de sécurité pour un type de modification AMS, tel que EC2 create ou OpenSearch create domain, vous devez utiliser l'un des groupes de sécurité par défaut décrits ici, ou un groupe de sécurité que vous avez créé. Vous trouverez la liste des groupes de sécurité, par VPC, dans la EC2 console AWS ou dans la console VPC.

D'autres groupes de sécurité par défaut sont utilisés à des fins AMS internes.

Groupes de sécurité AMS par défaut (trafic entrant)

Type	Protocole	Plage de ports	Source
Tout le trafic	Tous	Tous	SentinelDefaultSecurityGroupPrivateOnly (limite le trafic sortant aux membres du même groupe de sécurité)

Type	Protocole	Plage de ports	Source
Tout le trafic	Tous	Tous	SentinelDefaultSecurityGroupPrivateOnlyEgressAll (ne limite pas le trafic sortant)
HTTP, HTTPS, SSH, RDP	TCP	80/ 443 (Source : 0,0,0,0/0) L'accès SSH et RDP est autorisé depuis les bastions	SentinelDefaultSecurityGroupPublic (ne limite pas le trafic sortant)
Bastions du MALZ :			
SSH	TCP	22	SharedServices VPC CIDR et DMZ VPC CIDR, ainsi que sur site fournis par le client CIDRs
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	
Bastions SALZ :			
SSH	TCP	22	mc-initial-garden- LinuxBastion SG
SSH	TCP	22	mc-initial-garden- LinuxBastion DMZG
RDP	TCP	3389	mc-initial-garden- WindowsBastion SG
RDP	TCP	3389	mc-initial-garden- WindowsBastion DMZG

Création, modification ou suppression de groupes de sécurité

Vous pouvez demander des groupes de sécurité personnalisés. Dans les cas où les groupes de sécurité par défaut ne répondent pas aux besoins de vos applications ou de votre organisation, vous pouvez modifier ou créer de nouveaux groupes de sécurité. Une telle demande serait considérée comme nécessitant une approbation et serait examinée par l'équipe des opérations de l'AMS.

Pour créer un groupe de sécurité en dehors des piles VPCs, soumettez une RFC en utilisant le type de Deployment | Advanced stack components | Security group | Create (review required) modification (ct-10xx2g2d7hc90).

Pour les modifications du groupe de sécurité Active Directory (AD), utilisez les types de modifications suivants :

- Pour ajouter un utilisateur : soumettez une RFC à l'aide de Management | Directory Service | Utilisateurs et groupes | Ajouter un utilisateur au groupe [ct-24pi85mjtza8k]
- Pour supprimer un utilisateur : soumettez une RFC à l'aide de Management | Directory Service | Utilisateurs et groupes | Supprimer un utilisateur du groupe [ct-2019s9y3nfm14]

Note

Lorsque vous utilisez « révision requise » CTs, AMS vous recommande d'utiliser l'option ASAP Scheduling (choisissez ASAP dans la console, laissez les heures de début et de fin vides dans l'API/CLI) car elles CTs nécessitent qu'un opérateur AMS examine la RFC et communique éventuellement avec vous avant qu'elle ne puisse être approuvée et exécutée. Si vous les planifiez RFCs, veillez à prévoir au moins 24 heures. Si l'approbation n'intervient pas avant l'heure de début prévue, le RFC est automatiquement rejeté.

Rechercher des groupes de sécurité

Pour rechercher les groupes de sécurité attachés à une pile ou à une instance, utilisez la EC2 console. Après avoir trouvé la pile ou l'instance, vous pouvez voir tous les groupes de sécurité qui y sont attachés.

Pour savoir comment rechercher des groupes de sécurité sur la ligne de commande et filtrer la sortie, consultez [describe-security-groups](#).

Bibliothèque de contrôles préventifs et de détection AMS

AWS Managed Services (AMS) vous fournit une sélection de politiques library/catalog de contrôle des services éprouvées (SCPs) ConfigRules qui peuvent être utilisées pour améliorer votre niveau de sécurité et atténuer les lacunes de conformité de vos comptes AMS.

Rubriques

- [Règles de curated SCPs et de configuration](#)
- [Notification personnalisée pour les règles de configuration](#)

Règles de curated SCPs et de configuration

Règles de configuration SCPs et de curation pour AMS Advanced.

- Politiques de contrôle des services (SCPs) : SCPs Les politiques fournies s'ajoutent aux politiques AMS par défaut.

Vous pouvez utiliser ces contrôles de bibliothèque en tandem avec ceux par défaut pour répondre à des exigences de sécurité spécifiques.

- Règles de configuration : comme mesure de base, AMS recommande d'appliquer des packs de conformité (voir [Packs de conformité](#) dans le AWS Config guide) en plus des règles de configuration AMS par défaut (voir AMS Artifacts pour les règles par défaut). Les packs de conformité couvrent la majorité des exigences de conformité et AWS les met régulièrement à jour.

Les règles répertoriées ici peuvent être utilisées pour combler les lacunes spécifiques à des cas d'utilisation qui ne sont pas couvertes par les packs de conformité

Note

Au fur et à mesure que les règles par défaut et les packs de conformité d'AMS sont mis à jour au fil du temps, vous pouvez voir des doublons de ces règles.

AMS recommande de nettoyer régulièrement les règles de configuration dupliquées en général.

Pour AMS Advanced, les règles de configuration ne doivent pas utiliser de corrections automatiques (voir Corriger [les ressources AWS non conformes par les règles de configuration AWS](#)) afin d'éviter les modifications. out-of-band

SCP-AMS-001 : Restreindre la création d'EBS

Empêchez la création de volumes EBS si le chiffrement n'est pas activé.

```
{  
  "Condition": {  
    "Bool": {
```

```
    "ec2:Encrypted": "false"
  },
  "Action": "ec2:CreateVolume",
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-002 : Restreindre le lancement EC2

Empêchez le lancement d'une EC2 instance si le volume EBS n'est pas chiffré. Cela inclut le refus d'un EC2 lancement en mode non chiffré, AMIs car ce SCP s'applique également aux volumes racines.

```
{
  "Condition": {
    "Bool": {
      "ec2:Encrypted": "false"
    }
  },
  "Action": "ec2:RunInstances",
  "Resource": "arn:aws:ec2:*:*:volume/*",
  "Effect": "Deny"
}
```

SCP-ADV-001 : Restreindre les soumissions de RFC

Empêchez les rôles AMS par défaut de soumettre des données automatisées spécifiques, RFCs telles que Create VPC ou Delete VPC. Cela est utile si vous souhaitez appliquer des autorisations plus détaillées à vos rôles fédérés.

Par exemple, vous souhaitez peut-être que la valeur par défaut `AWSTransferServiceChangeManagement` rôle soit en mesure de soumettre la plupart des informations disponibles, à l'exception de celles qui autorisent la création et la suppression d'un VPC, la création de sous-réseaux supplémentaires, le transfert d'un compte d'application, la mise à jour ou la suppression de fournisseurs d'identité SAML :

SCP-AMS-003 : Restreindre EC2 ou créer des RDS dans AMS

Empêchez la création d'instances Amazon EC2 et RDS qui ne possèdent pas de balises spécifiques, tout en autorisant le `AMS Backup IAM` rôle par défaut AMS à le faire. Cela est nécessaire pour la reprise après sinistre ou la DR.

```
{
  "Sid": "DenyRunInstanceWithNoOrganizationTag",
  "Effect": "Deny",
  "Action": [
    "ec2:RunInstances",
    "rds:CreateDBInstance"
  ],
  "Resource": [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:rds:*:*:db:*"
  ],
  "Condition": {
    "Null": {
      "aws:RequestTag/organization": "true"
    },
    "StringNotLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam::<Account_Number>:role/ams-backup-iam-role"
      ]
    }
  }
}
```

SCP-AMS-004 : Restreindre les téléchargements de S3

Empêchez le téléchargement d'objets S3 non chiffrés.

```
{
  "Sid": "DenyUnencryptedS3Uploads",
  "Effect": "Deny",
  "Action": "s3:PutObject",
  "Resource": "*",
  "Condition": {
    "StringNotLike": {
      "s3:x-amz-server-side-encryption": ["aws:kms", "AES256"]
    },
    "Null": {
      "s3:x-amz-server-side-encryption": "false"
    }
  }
}
```

```
}
```

SCP-AMS-005 : Restreindre l'accès à l'API et à la console

Empêchez l'accès à la console AWS et à l'API pour les demandes provenant d'adresses IP erronées connues en tant que client déterminé InfoSec.

SCP-AMS-006 : Empêcher l'entité IAM de supprimer le compte membre de l'organisation

Empêcher une AWS Identity and Access Management entité de supprimer des comptes de membres de l'organisation.

```
{
  "Effect": "Deny",
  "Action": ["organizations:LeaveOrganization"],
  "Resource": ["*"]
}
```

SCP-AMS-007 : Empêchez le partage de ressources avec des comptes extérieurs à votre organisation

Empêchez le partage de ressources avec des comptes externes extérieurs à votre AWS organisation

```
{
  "Effect": "Deny",
  "Action": [
    "ram:*"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "Bool": {
      "ram:AllowsExternalPrincipals": "true"
    }
  }
},
{
  "Effect": "Deny",
  "Action": [
    "ram:CreateResourceShare",
```



```

    "ram:UpdateResourceShare"
  ],
  "Resource": "*",
  "Condition": {
    "Bool": {
      "ram:RequestedAllowsExternalPrincipals": "true"
    }
  }
}

```

SCP-AMS-008 : Empêcher le partage avec des organisations ou des unités organisationnelles () OUs

Empêchez le partage de ressources avec and/or une unité d'organisation associée à un compte.

```

{
  "Effect": "Deny",
  "Action": [
    "ram:CreateResourceShare",
    "ram:AssociateResourceShare"
  ],
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringLike": {
      "ram:Principal": [
        "arn:aws:organizations:::account/o-${OrganizationId}/${AccountId}",
        "arn:aws:organizations:::ou/o-${OrganizationId}/ou-${OrganizationalUnitId}"
      ]
    }
  }
}

```

SCP-AMS-009 : Empêcher les utilisateurs d'accepter des invitations à partager des ressources

Empêchez les comptes membres d'accepter des invitations AWS RAM à rejoindre des partages de ressources. Cette API ne prend en charge aucune condition et empêche les partages uniquement à partir de comptes externes.

```

{
  "Effect": "Deny",
  "Action": ["ram:AcceptResourceShareInvitation"],
  "Resource": ["*"]
}

```

SCP-AMS-010 : Empêcher les actions d'activation et de désactivation de la région du compte

Empêchez d'activer ou de désactiver de nouvelles AWS régions pour vos AWS comptes.

```
{
  "Effect": "Deny",
  "Action": [
    "account:EnableRegion",
    "account:DisableRegion"
  ],
  "Resource": "*"
}
```

SCP-AMS-011 : Empêcher les actions de modification de facturation

Empêchez les modifications de la configuration de facturation et de paiement.

```
{
  "Effect": "Deny",
  "Action": [
    "aws-portal:ModifyBilling",
    "aws-portal:ModifyAccount",
    "aws-portal:ModifyPaymentMethods"
  ],
  "Resource": "*"
}
```

SCP-AMS-012 : Empêcher la suppression ou la modification de données spécifiques CloudTrails

Empêchez les modifications apportées à des AWS CloudTrail sentiers spécifiques.

```
{
  "Effect": "Deny",
  "Action": [
    "cloudtrail:DeleteEventDataStore",
    "cloudtrail:DeleteTrail",
    "cloudtrail:PutEventSelectors",
    "cloudtrail:PutInsightSelectors",
    "cloudtrail:UpdateEventDataStore",
    "cloudtrail:UpdateTrail",
    "cloudtrail:StopLogging"
  ],
}
```

```
"Resource": [  
  "arn:${Partition}:cloudtrail:${Region}:${Account}:trail/${TrailName}"  
]  
}
```

SCP-AMS-013 : Empêcher la désactivation du chiffrement EBS par défaut

Empêchez la désactivation du chiffrement Amazon EBS par défaut.

```
{  
  "Effect": "Deny",  
  "Action": [  
    "ec2:DisableEbsEncryptionByDefault"  
  ],  
  "Resource": "*"   
}
```

SCP-AMS-014 : Empêcher la création d'un VPC et d'un sous-réseau par défaut

Empêchez la création d'un Amazon VPC et de sous-réseaux par défaut.

```
{  
  "Effect": "Deny",  
  "Action": [  
    "ec2:CreateDefaultSubnet",  
    "ec2:CreateDefaultVpc"  
  ],  
  "Resource": "*"   
}
```

SCP-AMS-015 : Empêcher la désactivation et la modification GuardDuty

Empêchez GuardDuty la modification ou la désactivation d'Amazon.

```
{  
  "Effect": "Deny",  
  "Action": [  
    "guardduty:AcceptInvitation",  
    "guardduty:ArchiveFindings",  
    "guardduty:CreateDetector",  
    "guardduty:CreateFilter",  
  ]  
}
```

```

    "guardduty:CreateIPSet",
    "guardduty:CreateMembers",
    "guardduty:CreatePublishingDestination",
    "guardduty:CreateSampleFindings",
    "guardduty:CreateThreatIntelSet",
    "guardduty:DeclineInvitations",
    "guardduty>DeleteDetector",
    "guardduty>DeleteFilter",
    "guardduty>DeleteInvitations",
    "guardduty>DeleteIPSet",
    "guardduty>DeleteMembers",
    "guardduty>DeletePublishingDestination",
    "guardduty>DeleteThreatIntelSet",
    "guardduty:DisableOrganizationAdminAccount",
    "guardduty:DisassociateFromMasterAccount",
    "guardduty:DisassociateMembers",
    "guardduty:InviteMembers",
    "guardduty:StartMonitoringMembers",
    "guardduty:StopMonitoringMembers",
    "guardduty:TagResource",
    "guardduty:UnarchiveFindings",
    "guardduty:UntagResource",
    "guardduty:UpdateDetector",
    "guardduty:UpdateFilter",
    "guardduty:UpdateFindingsFeedback",
    "guardduty:UpdateIPSet",
    "guardduty:UpdateMalwareScanSettings",
    "guardduty:UpdateMemberDetectors",
    "guardduty:UpdateOrganizationConfiguration",
    "guardduty:UpdatePublishingDestination",
    "guardduty:UpdateThreatIntelSet"
  ],
  "Resource": "*"
}

```

SCP-AMS-016 : Empêche l'activité de l'utilisateur root

Empêchez l'utilisateur root d'effectuer une quelconque action.

```

{
  "Action": "*",
  "Resource": "*",
  "Effect": "Deny",
  "Condition": {

```

```
"StringLike": {
  "aws:PrincipalArn": [
    "arn:aws:iam::*:root"
  ]
}
}
```

SCP-AMS-017 : Empêcher la création de clés d'accès pour l'utilisateur root

Empêchez la création de clés d'accès pour l'utilisateur root.

```
{
  "Effect": "Deny",
  "Action": "iam:CreateAccessKey",
  "Resource": "arn:aws:iam::*:root"
}
```

SCP-AMS-018 : Empêcher la désactivation du blocage de l'accès public au compte S3

Empêchez la désactivation du blocage de l'accès public d'un compte Amazon S3. Cela empêche tout compartiment du compte de devenir public.

```
{
  "Effect": "Deny",
  "Action": "s3:PutAccountPublicAccessBlock",
  "Resource": "*"
}
```

SCP-AMS-019 : Empêcher la désactivation d'AWS Config ou la modification des règles de configuration

Empêchez la désactivation ou la modification des AWS Config règles.

```
{
  "Effect": "Deny",
  "Action": [
    "config:DeleteConfigRule",
    "config:DeleteConfigurationRecorder",
    "config:DeleteDeliveryChannel",
    "config:DeleteEvaluationResults",

```

```
"config:StopConfigurationRecorder"
],
"Resource": "*"
}
```

SCP-AMS-020 : Empêche toutes les actions de l'IAM

Empêchez toutes les actions IAM.

```
{
  "Effect": "Deny",
  "Action": [
    "iam:*"
  ],
  "Resource": "*"
}
```

SCP-AMS-021 : Empêche la suppression de journaux, de groupes et de flux CloudWatch

Empêchez la suppression de groupes et de flux Amazon CloudWatch Logs.

```
{
  "Effect": "Deny",
  "Action": [
    "logs:DeleteLogGroup",
    "logs:DeleteLogStream"
  ],
  "Resource": "*"
}
```

SCP-AMS-022 : Empêcher la suppression de Glacier

Empêchez la suppression d'Amazon Glacier.

```
{
  "Effect": "Deny",
  "Action": [
    "glacier:DeleteArchive",
    "glacier:DeleteVault"
  ],
  "Resource": "*"
}
```

```
}
```

SCP-AMS-023 : Empêcher la suppression d'IAM Access Analyzer

Empêchez la suppression d'IAM Access Analyzer.

```
{
  "Action": [
    "access-analyzer:DeleteAnalyzer"
  ],
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-024 : Empêcher les modifications apportées au Security Hub

Empêcher la suppression de AWS Security Hub.

```
{
  "Action": [
    "securityhub:DeleteInvitations",
    "securityhub:DisableSecurityHub",
    "securityhub:DisassociateFromMasterAccount",
    "securityhub:DeleteMembers",
    "securityhub:DisassociateMembers"
  ],
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-025 : Empêcher la suppression sous Directory Service

Empêcher la suppression de ressources sous AWS Directory Service.

```
{
  "Action": [
    "ds:DeleteDirectory",
    "ds:DeleteLogSubscription",
    "ds:DeleteSnapshot",
    "ds:DeleteTrust",
    "ds:DeregisterCertificate",
    "ds:DeregisterEventTopic",

```

```
"ds:DisableLDAPS",
"ds:DisableRadius",
"ds:DisableSso",
"ds:UnshareDirectory"
],
"Resource": "*",
"Effect": "Deny"
}
```

SCP-AMS-026 : Empêcher l'utilisation d'un service refusé

Empêchez l'utilisation de services refusés.

Note

Remplacez *service1* et *service2* par les noms de vos services. Exemple *access-analyzer* ou *IAM*.

```
{
  "Effect": "Deny",
  "Resource": "*",
  "Action": ["service1:", "service2:"]
}
```

SCP-AMS-027 : Empêchez l'utilisation de services refusés dans des régions spécifiques

Empêchez l'utilisation de services refusés dans des régions spécifiques AWS .

Note

Remplacez *service1* et *service2* par les noms de vos services. Exemple *access-analyzer* ou *IAM*.

Remplacez *region1* et *region2* par les noms de vos services. Exemple *us-west-2* ou *use-east-1*.

```
{
  "Effect": "Deny",
  "Resource": "*",
```



```

"Action": ["service1:", "service2:"],
"Condition": {
  "StringEquals": {
    "aws:RequestedRegion": [
      "region1",
      "region2"
    ]
  }
}
}

```

SCP-AMS-028 : Empêche la modification des tags sauf par des personnes autorisées

Empêchez les utilisateurs de modifier les balises, à l'exception des principaux autorisés. Utilisez des balises d'autorisation pour autoriser les principaux. Les balises d'autorisation doivent être associées aux ressources et aux principaux. A n' user/role est considéré comme autorisé que si les balises de la ressource et du principal correspondent. Pour plus d'informations, consultez les ressources suivantes :

- [Sécurisation des balises de ressources utilisées pour l'autorisation à l'aide d'une politique de contrôle des services dans AWS Organizations](#)
- [Empêcher la modification des balises, sauf par des personnes autorisées](#)

```

{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateTags",
    "ec2:DeleteTags"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "StringNotEquals": {
      "ec2:ResourceTag/access-project": "${aws:PrincipalTag/access-project}",
      "aws:PrincipalArn": "arn:aws:iam::ACCOUNT_ID:RESOURCE_TYPE/RESOURCE_NAME"
    },
    "Null": {
      "ec2:ResourceTag/access-project": false
    }
  }
}

```

```

},
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateTags",
    "ec2:DeleteTags"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "StringNotEquals": {
      "aws:RequestTag/access-project": "${aws:PrincipalTag/access-project}",
      "aws:PrincipalArn": "arn:aws:iam::{ACCOUNT_ID}:{RESOURCE_TYPE}/{RESOURCE_NAME}"
    },
    "ForAnyValue:StringEquals": {
      "aws:TagKeys": [
        "access-project"
      ]
    }
  }
},
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateTags",
    "ec2:DeleteTags"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "StringNotEquals": {
      "aws:PrincipalArn": "arn:aws:iam::{ACCOUNT_ID}:{RESOURCE_TYPE}/{RESOURCE_NAME}"
    },
    "Null": {
      "aws:PrincipalTag/access-project": true
    }
  }
}
}

```

SCP-AMS-029 : Empêcher les utilisateurs de supprimer les journaux de flux Amazon VPC

Empêchez la suppression des journaux de flux Amazon VPC.

```
{
  "Action": [
    "ec2:DeleteFlowLogs",
    "logs:DeleteLogGroup",
    "logs:DeleteLogStream",
    "s3:DeleteBucket",
    "s3:DeleteObject",
    "s3:DeleteObjectVersion",
    "s3:PutLifecycleConfiguration",
    "firehose:DeleteDeliveryStream"
  ],
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-030 : Empêcher le partage du sous-réseau VPC avec un compte autre qu'un compte réseau

Empêchez le partage de sous-réseaux Amazon VPC avec des comptes autres que le compte réseau.

 Note

NETWORK_ACCOUNT_ID Remplacez-le par votre identifiant de compte réseau.

```
{
  "Effect": "Deny",
  "Action": [
    "ram:AssociateResourceShare",
    "ram:CreateResourceShare"
  ],
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "ram:Principal": "NETWORK_ACCOUNT_ID"
    },
    "StringEquals": {
      "ram:RequestedResourceType": "ec2:Subnet"
    }
  }
}
```

SCP-AMS-031 : Empêcher le lancement d'instances avec des types d'instances interdits

Empêchez le lancement de types d' EC2 instances Amazon interdits.

Note

Remplacez *instance_type1* et *instance_type2* par les types d'instances que vous souhaitez restreindre, par exemple *t2.micro* ou par une chaîne générique telle que **.nano*.

```
{
  "Effect": "Deny",
  "Action": "ec2:RunInstances",
  "Resource": [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition": {
    "ForAnyValue:StringLike": {
      "ec2:InstanceType": [
        "instance_type1",
        "instance_type2"
      ]
    }
  }
}
```

SCP-AMS-032 : Empêcher le lancement d'instances sans IMDSv2

Empêchez EC2 les instances Amazon sans IMDSv2.

```
[
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringNotEquals": {
        "ec2:MetadataHttpTokens": "required"
      }
    }
  },
  {
```

```

    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "NumericGreaterThan": {
        "ec2:MetadataHttpPutResponseHopLimit": "3"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "NumericLessThan": {
        "ec2:RoleDelivery": "2.0"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:ModifyInstanceMetadataOptions",
    "Resource": "*"
  }
]

```

SCP-AMS-033 : Empêcher les modifications d'un rôle spécifique de l'IAM

Empêchez les modifications des rôles IAM spécifiés.

```

{
  "Action": [
    "iam:AttachRolePolicy",
    "iam>DeleteRole",
    "iam>DeleteRolePermissionsBoundary",
    "iam>DeleteRolePolicy",
    "iam:DetachRolePolicy",
    "iam:PutRolePermissionsBoundary",
    "iam:PutRolePolicy",
    "iam:TagRole",
    "iam:UntagRole",
    "iam:UpdateAssumeRolePolicy",
    "iam:UpdateRole",
    "iam:UpdateRoleDescription"
  ]
}

```

```

],
"Resource": [
  "arn:aws:iam::{ACCOUNT_ID}:role/{RESOURCE_NAME}"
],
"Effect": "Deny"
}

```

SCP-AMS-034 : Empêcher AssumeRolePolicy la modification de rôles IAM spécifiques

Empêchez les modifications apportées AssumeRolePolicy aux rôles IAM spécifiés.

```

{
  "Action": [
    "iam:UpdateAssumeRolePolicy"
  ],
  "Resource": [
    "arn:aws:iam::{ACCOUNT_ID}:role/{RESOURCE_NAME}"
  ],
  "Effect": "Deny"
}

```

ConfigRule: Tags obligatoires

Vérifiez si EC2 les instances disposent des balises personnalisées dont vous avez besoin. En outre InfoSec, cela est également utile pour votre gestion des coûts

```

ConfigRuleName: required-tags
Description: >-
  A Config rule that checks whether EC2 instances have the required tags.
Scope:
  ComplianceResourceTypes:
    - 'AWS::EC2::Instance'
InputParameters:
  tag1Key: COST_CENTER
  tag2Key: APP_ID
Source:
  Owner: AWS
  SourceIdentifier: REQUIRED_TAGS

```

ConfigRule: touche d'accès pivotée

Vérifiez que les clés d'accès sont pivotées dans le délai spécifié. Ce délai est généralement fixé à 90 jours conformément aux exigences de conformité habituelles.

```
ConfigRuleName: access-keys-rotated
Description: >-
  A config rule that checks whether the active access keys are rotated
  within the number of days specified in maxAccessKeyAge. The rule is
  NON_COMPLIANT if the access keys have not been rotated for more than
  maxAccessKeyAge number of days.
InputParameters:
  maxAccessKeyAge: '90'
Source:
  Owner: AWS
  SourceIdentifier: ACCESS_KEYS_ROTATED
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: clé d'accès root IAM dans AMS

Vérifiez qu'aucune clé d'accès root n'est présente sur un compte. Pour les comptes AMS Advanced, cela devrait être conforme out-of-the-box.

```
ConfigRuleName: iam-root-access-key-check
Description: >-
  A config rule that checks whether the root user access key is available. The
  rule is COMPLIANT if the user access key does not exist.
Source:
  Owner: AWS
  SourceIdentifier: IAM_ROOT_ACCESS_KEY_CHECK
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: géré par SSM EC2

Vérifiez que vous EC2s êtes géré par SSM Systems Manager.

```
ConfigRuleName: ec2-instance-managed-by-systems-manager
Description: >-
  A Config rule that checks whether the EC2 instances in the
  account are managed by AWS Systems Manager.
Scope:
  ComplianceResourceTypes:
    - 'AWS::EC2::Instance'
    - 'AWS::SSM::ManagedInstanceInventory'
Source:
  Owner: AWS
  SourceIdentifier: EC2_INSTANCE_MANAGED_BY_SSM
```

ConfigRule: utilisateur IAM non utilisé dans AMS

Vérifiez les informations d'identification de l'utilisateur IAM qui n'ont pas été utilisées pendant une durée spécifiée. Tout comme le contrôle de rotation des clés, ce délai est généralement de 90 jours par défaut, conformément aux exigences de conformité habituelles.

```
ConfigRuleName: iam-user-unused-credentials-check
Description: >-
  A config rule that checks whether IAM users have passwords
  or active access keys that have not been used within the
  specified number of days provided.
InputParameters:
  maxCredentialUsageAge: '90'
Source:
  Owner: AWS
SourceIdentifier: IAM_USER_UNUSED_CREDENTIALS_CHECK
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: journalisation du compartiment S3

Vérifiez que la journalisation a été activée pour les compartiments S3 du compte.

```
ConfigRuleName: s3-bucket-logging-enabled
Description: >-
  A Config rule that checks whether logging is enabled for S3 buckets.
Scope:
  ComplianceResourceTypes:
    - 'AWS::S3::Bucket'
Source:
  Owner: AWS
SourceIdentifier: S3_BUCKET_LOGGING_ENABLED
```

ConfigRule: gestion des versions du compartiment S3

Vérifiez que le contrôle de version et la suppression MFA (facultatif) sont activés sur tous les compartiments S3

```
ConfigRuleName: s3-bucket-versioning-enabled
Description: >-
  A Config rule that checks whether versioning is enabled for S3
  buckets. Optionally, the rule checks if MFA delete is enabled for S3 buckets.
Scope:
  ComplianceResourceTypes:
```



```
- 'AWS::S3::Bucket'
```

Source:

Owner: AWS

SourceIdentifier: S3_BUCKET_VERSIONING_ENABLED

ConfigRule: accès public S3

Vérifiez que les paramètres d'accès public (Public ACL, Public Policy, Public Buckets) sont restreints sur l'ensemble du compte

ConfigRuleName: s3-account-level-public-access-blocks

Description: >-

A Config rule that checks whether the required public access block settings are configured from account level. The rule is only NON_COMPLIANT when the fields set below do not match the corresponding fields in the configuration item.

Scope:

ComplianceResourceTypes:

```
- 'AWS::S3::AccountPublicAccessBlock'
```

InputParameters:

IgnorePublicAcls: 'True'

BlockPublicPolicy: 'True'

BlockPublicAcls: 'True'

RestrictPublicBuckets: 'True'

Source:

Owner: AWS

SourceIdentifier: S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS

ConfigRule: Résultats non archivés GuardDuty

Vérifiez si les GuardDuty résultats non archivés sont antérieurs à la durée spécifiée. La durée par défaut est de 30 jours pour les valeurs basses, 7 jours pour les valeurs moyennes et 1 jour pour les valeurs élevées.

ConfigRuleName: guardduty-non-archived-findings

Description: >-

A Config rule that checks whether the Amazon GuardDuty has findings that are non archived. The rule is NON_COMPLIANT if GuardDuty has non archived low/medium/high severity findings older than the specified number.

InputParameters:

daysLowSev: '30'

daysMediumSev: '7'

daysHighSev: '1'

```
Source:
  Owner: AWS
  SourceIdentifier: GUARDDUTY_NON_ARCHIVED_FINDINGS
  MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: suppression de la clé CMK

Vérifiez les clés principales AWS Key Management Service personnalisées (CMKs) dont la suppression est planifiée (c'est-à-dire en attente). Ceci est crucial car l'ignorance de la suppression des CMK peut rendre les données irrécupérables.

```
ConfigRuleName: kms-cmk-not-scheduled-for-deletion
Description: >-
  A config rule that checks whether customer master keys (CMKs) are not
  scheduled for deletion in AWS Key Management Service (AWS KMS). The rule is
  NON_COMPLIANT if CMKs are scheduled for deletion.
Source:
  Owner: AWS
SourceIdentifier: KMS_CMK_NOT_SCHEDULED_FOR_DELETION
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: rotation de la CMK

Vérifiez que la rotation automatique est activée pour chaque CMK du compte

```
ConfigRuleName: cmk-backing-key-rotation-enabled
Description: >-
  A config rule that checks that key rotation is enabled for each customer
  master key (CMK). The rule is COMPLIANT, if the key rotation is enabled
  for specific key object. The rule is not applicable to CMKs that have
  imported key material.
Source:
  Owner: AWS
SourceIdentifier: CMK_BACKING_KEY_ROTATION_ENABLED
MaximumExecutionFrequency: TwentyFour_Hours
```

Notification personnalisée pour les règles de configuration

Il peut arriver que des règles de configuration critiques non conformes nécessitent une sensibilisation accrue directement auprès de votre équipe InfoSec et de votre équipe de direction. Pour de tels scénarios, AMS vous recommande de configurer une notification personnalisée basée sur un événement de non-conformité.

Exemples :

```

ConfigRuleName: required-tags
  Description: >-
    A Config rule that checks whether EC2 instances have the mandated tags.
  Scope:
    ComplianceResourceTypes:
      - 'AWS::EC2::Instance'
  InputParameters:
    tag1Key: COST_CENTER
    tag2Key: APP_ID
  Source:
    Owner: AWS
SourceIdentifier: REQUIRED_TAGS
NotificationEventRule:
  Type: 'AWS::Events::Rule'
  Properties:
    Name: CWEventForrequired-tags
    Description: >-
      SNS Notification for Non-Compliant Events of Config Rule:
      required-tags
    State: ENABLED
    EventPattern:
      detail-type:
        - Config Rules Compliance Change
      source:
        - aws.config
      detail:
        newEvaluationResult:
          complianceType:
            - NON_COMPLIANT
        configRuleARN:
          - 'Fn::GetAtt':
            - RequiredEC2Tags
            - Arn
    Targets:
      - Id: RemediationNotification
        Arn:
          Ref: SnsTopic
        InputTransformer:
          InputTemplate: >-
            "EC2 Instance <Instance_ID> is non-compliant. Please add required tags:
            COST_CENTER, APP_ID, Name, and Backup."
          InputPathsMap:

```

```
        instance_id: $.detail.resourceId
SnsTopic:
  Type: 'AWS::SNS::Topic'
  Properties:
    Subscription:
      - Endpoint: Cloud_Ops_Leaders@customer.com
        Protocol: email
    TopicName: noncompliant-instance-notification
SnsTopicPolicy:
  Type: 'AWS::SNS::TopicPolicy'
  Properties:
    PolicyDocument:
      Statement:
        - Sid: __default_statement_ID
          Effect: Allow
          Principal:
            AWS: '*'
          Action:
            - 'SNS:GetTopicAttributes'
            - 'SNS:SetTopicAttributes'
            - 'SNS:AddPermission'
            - 'SNS:RemovePermission'
            - 'SNS:DeleteTopic'
            - 'SNS:Subscribe'
            - 'SNS:ListSubscriptionsByTopic'
            - 'SNS:Publish'
            - 'SNS:Receive'
          Resource:
            Ref: SnsTopic
          Condition:
            StringEquals:
              'AWS:SourceOwner':
                Ref: 'AWS::AccountId'
        - Sid: TrustCWEToPublishEventsToMyTopic
          Effect: Allow
          Principal:
            Service: events.amazonaws.com
          Action: 'sns:Publish'
          Resource:
            Ref: SnsTopic
  Topics:
    - Ref: SnsTopic
```

Rôle lié au service Amazon EventBridge Rule pour AMS Advanced

AMS Advanced utilise le rôle lié au service (SLR) nommé `AWSServiceRoleForManagedServices_Events`— Ce rôle fait confiance à l'un des principaux 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. Cette règle est l'infrastructure requise dans votre AWS compte pour transmettre à AWS Managed Services les informations relatives au changement d'état des alarmes depuis votre compte.

Autorisations pour EventBridge SLR pour AMS Advanced

Le rôle lié à un service `AWSServiceRoleForManagedServices_Events` approuve les services suivants pour endosser le rôle :

- `events.managedservices.amazonaws.com`

La politique `AWSManagedServices_EventsServiceRolePolicy` AWS gérée est associée à ce rôle (voir [Politique gérée par AWS : `AWSManagedServices\_EventsServiceRolePolicy`](#)). Le service utilise ce rôle pour transmettre à AWS Managed Services les informations relatives au changement d'état des alarmes 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 la section [Autorisations relatives aux rôles liés aux services](#) dans le guide de l'utilisateur d'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 Advanced

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous intégrez AMS via la console AWS de gestion AWS CLI, l'API ou l'AWS API, AMS Advanced 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 Advanced 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 Advanced crée à nouveau le rôle lié au service pour vous.

Modification d'un EventBridge reflex pour AMS Advanced

AMS Advanced 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 EventBridge photo reflex pour AMS Advanced

Vous n'avez pas besoin de supprimer manuellement le rôle AWSServiceRoleForManagedServices_Events . Lorsque vous quittez AMS via la console de AWS gestion, AWS CLI ou l' AWS API, AMS Advanced 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 Advanced 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 Advanced utilisées par le rôle lié au AWSServiceRoleForManagedServices_Events 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.

Bonnes pratiques de sécurité

Cette section a été supprimée car elle contient des informations sensibles relatives à la sécurité AMS. Ces informations sont disponibles dans la documentation de la console AMS. Pour accéder à AWS Artifact, vous pouvez contacter votre CSDM pour obtenir des instructions ou consulter Getting [Started with AWS](#) Artifact.

Zone d'atterrissage multi-comptes AMS (paramètres EPS autres que ceux par défaut)

Cette section a été supprimée car elle contient des informations sensibles relatives à la sécurité AMS. Ces informations sont disponibles dans la documentation de la console AMS. Pour accéder à AWS Artifact, vous pouvez contacter votre CSDM pour obtenir des instructions ou consulter Getting [Started with AWS](#) Artifact.

Rambardes AMS

Un garde-fou est une règle de haut niveau qui fournit une gouvernance continue de l'ensemble de votre environnement AMS.

Cette section a été supprimée car elle contient des informations sensibles relatives à la sécurité AMS. Ces informations sont disponibles dans la documentation de la console AMS. Pour accéder à AWS Artifact, vous pouvez contacter votre CSDM pour obtenir des instructions ou consulter Getting [Started with AWS](#) Artifact.

Politiques de contrôle des services MALZ

Cette section a été supprimée car elle contient des informations sensibles relatives à la sécurité AMS. Ces informations sont disponibles dans la documentation de la console AMS. Pour accéder à AWS Artifact, vous pouvez contacter votre CSDM pour obtenir des instructions ou consulter Getting [Started with AWS](#) Artifact.

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 étiquetez-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 (IAM, EC2, 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, Endpoint Protection GuardDuty, Network Traffic et les flux internes de Threat Intelligence d'Amazon.

Les clients AMS dotés du modèle d'exploitation AMS Advanced installent automatiquement le client de surveillance de la sécurité des terminaux (EPS) sur les ressources provisionnées. Cela garantit que les ressources sont surveillées et prises en charge 24 heures sur 24, 7 jours sur 7, y compris la création d'un incident de sécurité lorsqu'un événement est détecté.

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 grâce à une solution GuardDuty de surveillance de la sécurité des terminaux. 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.

Examens de sécurité des demandes de modification dans AMS Advanced

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 Advanced](#) définissent 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 de gestion avancée des risques liés à la sécurité des clients (CSRM) d'AMS 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 Advanced

Les catégories de normes techniques AMS Advanced sont les suivantes :

ID	Catégorie
AMS-STD-001	Configuration du balisage
AMS-STD-002	AWS Identity and Access Management
AMS-STD-003	Sécurité du réseau
AMS-STD-004	Tests de pénétration
AMS-STD-005	Amazon GuardDuty
AMS-STD-006	Sécurité de l'hôte
AMS-STD-007	Journalisation
AMS-STD-008	JE SUIS FOU
AMS-STD-009	Divers

Commandes standard dans AMS Advanced

Les commandes standard d'AMS sont les suivantes :

AMS-STD-001 - Configuration du balisage

Voici le contrôle standard pour 001 - Configuration du balisage.

1. Toutes les AWS ressources requises par l'équipe AMS à des fins opérationnelles et de gestion doivent avoir la paire clé-valeur suivante.
 - AppId= AMSInfrastructure
 - Environnement= AMSInfrastructure
 - AppName = AMSInfrastructure
 - AMSResource=Vrai
2. Toutes les balises requises par l'équipe AMS autres que celles répertoriées précédemment doivent avoir des préfixes tels que mentionnés dans la liste des préfixes AMS (voir Remarque).

3. Les valeurs de balise requises par l'équipe AMS (AppId, Environment et AppName) peuvent être modifiées sur toutes les ressources que vous avez créées en fonction de vos demandes de modification.
4. Aucune balise sur les piles requise par AMS ne doit être supprimée en fonction de vos demandes de modification.
5. Vous ne pouvez pas utiliser la convention de dénomination des balises AMS pour votre infrastructure, comme indiqué au point 2.
6. Vous pouvez créer des balises personnalisées dans les ressources requises par AMS (généralement pour les cas d'utilisation liés à la facturation et aux rapports de coûts). Les balises personnalisées sont conservées si les ressources sont mises à jour par stack update et non par mise à jour du modèle.

 Note

Liste des préfixes AMS

1. suis-*
2. AWSManagedServices*
3. /suis/ *
4. suis*
5. SUIS*
6. Amnis*
7. mc*
8. MC*
9. Mc*
- 10sentinelle*
- 11Sentinelle*
- 12Services_gérés*
- 13Nouvelles AMS*
- 14AWS_*
- 15frais*
- 16.VPC_*
- 17.CloudTrail*

- 18.Cloud Trail*
- 19/aws_réservé/
- 20INGÉRER*
- 21EPSDB*
- 22MM*
- 23.TemplateId*
- 24.StackSet-suis*
- 25.StackSet-Zone d'atterrissage AWS
- 26.IAMPolicy*
- 27.client-mc-*
- 28.Racine*
- 29.LandingZone*
- 30.StateMachine*
- 31.codedeploy_service_role
- 32hôte de gestion
- 33.sentinel.int.
- 34.eps
- 35.UnhealthyInServiceBastion
- 36.ms-

AMS-STD-002 - (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.
1.2	Le temps d'accès à la pile par défaut est de 12 heures.

Commandes standard dans AMS Advanced

Version October 3, 2025 835

ID	Norme technique
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	Pour les comptes de zone d'atterrissage à compte unique (SALZ) et les comptes de gestion de zone d'atterrissage multicomptes (MALZ) (anciennement connus sous le nom de Master/Billing compte), l'authentification MFA virtuelle doit être activée sur le compte utilisateur root et le jeton logiciel MFA est supprimé lors de l'intégration du compte, de sorte que ni AMS ni les clients ne peuvent se connecter en tant que root. Le processus standard de perte du mot de passe AWS root doit être suivi conjointement avec votre AMS Cloud Service Delivery Manager (CSDM). Cette configuration doit être maintenue pendant le cycle de vie des comptes gérés par AMS.
2.3	Vous ne devez pas créer de clés d'accès pour le compte root.
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.

ID	Norme technique
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.
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'infrastructure (écriture et gestion des autorisations) dans le compte client ne doivent pas être créés sans acceptation des risques. Des exceptions 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	Les utilisateurs IAM ayant un accès programmatique, nommés <code>customer_serviceno_w_user</code> et <code>customer_serviceno_w_logging_user</code> requis pour ServiceNow l'intégration dans le compte d'application SALZ ou MALZ et les *comptes principaux* peuvent être créés sans aucune politique de limitation dans le temps.

ID	Norme technique
3.4	Les utilisateurs IAM disposant d'un accès programmatique, utilisant <code>customer_cloud_endure_policy</code> et <code>customer_cloud_endure_deny_policy</code> (avec accès en lecture seule) requis pour CloudEndure l'intégration dans les comptes SALZ et MALZ peuvent être créés, mais ils ont besoin d'une politique limitée dans le temps pour la période de migration prévue. Le délai peut être d'une durée maximale de 180 jours sans polyarthrite rhumatoïde. Le SCP est également autorisé à modifier les comptes MALZ afin de permettre à ces politiques de fonctionner pendant la période requise. Vous définissez les fenêtres de migration adaptées à vos besoins et vous les ajustez selon les besoins.
4,0	Politiques, actions et APIs
4.1	Tous vos utilisateurs et rôles IAM dans les comptes SALZ doivent être soumis à la politique de refus du client (CDP) par défaut afin de protéger l'infrastructure AMS contre tout dommage accidentel ou intentionnel.
4.2	AMS SCPs doit être activé dans tous les comptes gérés par AMS dans MALZ.
4.3	Les identités capables d'effectuer des actions administratives sur des clés KMS, telles que <code>PutKeyPolicy</code> , et <code>ScheduleKeyDeletion</code> , doivent être limitées aux opérateurs AMS et aux principaux d'automatisation uniquement.

ID	Norme technique
4,4	Une politique ne doit pas fournir un accès administrateur avec une déclaration équivalente à « Effet » : « Autoriser » avec « Action » : « * » au-dessus de « Ressource » : « * » sans acceptation du risque.
4,5	La politique IAM ne doit inclure aucune action incluant l'action Allow S3 :*** sur un compartiment sans acceptation de 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.
4,7	Les actions qui contournent le processus de gestion des modifications (RFC) ne doivent pas être autorisées, telles que le démarrage ou l'arrêt de l'instance, la création d'un compartiment S3 ou d'une instance RDS, etc.
4.8	Les actions qui modifient les enregistrements DNS de l'infrastructure AMS dans Amazon Route 53 ne doivent pas être autorisées.
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.

ID	Norme technique
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 spécifique AWS Secrets Manager au sein du même compte.
4,11	Les autorisations AWS Managed Services Change Management (AMSCM) ou AWS Managed Services Service Knowledge Management System (AMSSKMS) peuvent être ajoutées à n'importe quel rôle (possibilité d'ouvrir des autorisations). SR/Incident/RFC
4,12	La politique IAM ne doit inclure aucune action incluant l'action Autoriser les journaux : DeleteLogGroup et les journaux : DeleteLogStream 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	Pour donner accès au compartiment S3 ARNs qui n'est pas encore créé dans vos comptes, utilisez la clé de condition S3 spécifique au service <code>s3:ResourceAccount</code> pour spécifier le numéro de compte.
4,15	Vous pouvez consulter, créer, répertorier et supprimer l'accès à votre tableau de bord personnalisé, mais uniquement sur les CloudWatch tableaux de bord Amazon.
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 rôles/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 un Service AWS 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	Les politiques IAM ne doivent pas autoriser un accès en lecture illimité aux objets du compartiment Amazon S3 (par exemple, Amazon S3 :GetObject) dans tous les compartiments d'un compte : • Dans les comptes en mode développeur : les violations entraînent une notification de risque • Dans les comptes en mode non-développeur : les violations nécessitent une acceptation des risques
4,21	Toutes les autorisations IAM pour le type de ressource « savingsplan » peuvent être accordées aux clients.

ID	Norme technique
4,22	Les ingénieurs d'AMS ne sont pas autorisés à copier ou à déplacer les données clients (fichiers, objets S3, bases de données) 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.
4,23	La politique SCP ne doit pas être modifiée pour autoriser un accès supplémentaire à l'un des comptes gérés par AMS.
4,24	Toute modification de la politique SCP susceptible de perturber l'infrastructure ou les capacités de gestion d'AMS ne doit pas être autorisée. (Remarque : les ressources AMS possèdent le tag AppId= AMSInfrastructure et suivent l'espace de noms protégé AMS).
4,25	La fonctionnalité AMS Automated IAM Provisioning doit être activée dans vos comptes en tant que fonctionnalité opt-in.
4,26	Les rôles ou utilisateurs assumés par l'homme d'AMS ne doivent pas avoir accès au contenu client dans S3, RDS, DynamoDB, Redshift, Elasticache, EFS et FSx. En outre, tout accès à une nouvelle API publiée par un tiers Services AWS qui accorde l'accès au contenu du client doit être explicitement refusé dans les rôles d'opérateur.
5,0	Fédération

ID	Norme technique
5.1	L'authentification doit être configurée à l'aide de la fédération dans le compte géré AMS.
5.2	Il ne doit y avoir qu'une confiance sortante unidirectionnelle entre AMS AD et votre Active Directory (AMS AD fait confiance à AD sur site).
5.3	Vos magasins d'identités utilisés pour vous authentifier auprès d'AMS ne doivent pas exister dans les comptes d'applications gérés par AMS.
6.0	Politiques relatives aux comptes multiples
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.

ID	Norme technique
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.
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.

ID	Norme technique
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.
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 d'AMS sur un compte non-AMS (ou d'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 au nom de AWS Organizations l'entreprise du client).
6,10	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 tiers à partir d'un compte AMS avec accès en lecture seule peuvent être configurés.

ID	Norme technique
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 configurés.
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
8.1	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	Vos ressources doivent être configurées avec des politiques basées sur le moindre privilège , sauf si vous spécifiez explicitement une politique différente.
9,0	Services fournis en libre-service (SSPS)

ID	Norme technique
9.1	Le rôle ou la politique IAM par défaut d'AMS (y compris le profil d'instance, le SSPS, le modèle) ne doit pas être modifié avec ou sans acceptation des risques. Des exceptions sont autorisées (sans acceptation du risque) pour les politiques de confiance. Le balisage du rôle, de la politique ou des modifications apportées par l'utilisateur est également autorisé dans les rôles SSP par défaut.
9.3	La politique SSPS pour le rôle de console Systems Manager Automation ne peut être attachée à aucun rôle personnalisé autre que le rôle par défaut. Les autres politiques SSPS ne doivent être associées à des rôles IAM personnalisés qu'après avoir vérifié que l'attachement de la politique à un rôle personnalisé ne fournit pas d'autorisations supplémentaires en dehors de la conception prévue pour le service SSPS par défaut.

AMS-STD-003 - Sécurité réseau

Voici le contrôle standard pour 003 - Network Security :

ID	Norme technique
	Réseaux
1.0	Toutes les EC2 instances doivent être accessibles via SSH ou RDP uniquement via les hôtes Bastion, la plage d'adresses CIDR VPC des hôtes bastion ou depuis la même plage d'adresses CIDR VPC d'instance.

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.
4.0	Tout le trafic sortant doit passer par le compte IGW ou TGW.
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/137-139 ne doit pas être autorisé depuis l'extérieur 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 équilibres de charge, mais pas directement aux ressources 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 fait référence aux normes chaque fois qu'il est demandé d'associer un groupe de sécurité à une instance.
13,0	L'accès au bastion du client sur les ports 3389 et 22 doit être autorisé uniquement à partir de plages d'adresses IP privées acheminées vers le VPC via DX, VPC-Peer ou VPN.
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.

ID	Norme technique
15,0	Les connexions de peering VPC entre des comptes appartenant au même client peuvent être autorisées.
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 correspondre 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 acceptation 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	La connexion Transit Gateway à un compte tiers (n'appartenant pas au client) ne doit pas être autorisée.
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.

ID	Norme technique
23,0	Le partage des règles du résolveur avec celles Compte AWS appartenant au même client est autorisé moyennant une notification des risques
19,0	ICMP
19,1	Les demandes ICMP entrantes adressées EC2 à Amazon par le client infra nécessiteront une notification des risques.
19,2	Les demandes entrantes provenant du public IPs acheminées vers Amazon VPC via DX, VPC-Peer ou VPN via un groupe de sécurité sont autorisées.
19,3	Les demandes entrantes émanant du public qui ne sont pas acheminées vers Amazon VPC via DX, VPC-Peer ou VPN via un groupe de sécurité nécessiteraient une acceptation des risques.
19,4	Les demandes ICMP sortantes d'Amazon EC2 vers n'importe quelle destination sont autorisées.
20,0	Partage de groupes de sécurité
20.1	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.

ID	Norme technique
20,2	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-004 - Test de pénétration

Voici le contrôle standard pour 004 - Tests 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-005 - GuardDuty

Ce qui suit est le contrôle standard pour 005 - GuardDuty

1. GuardDuty doit être activé dans tous les comptes clients à tout moment.
2. GuardDuty Les résultats du compte d'application géré par le client (CMA) dans MALZ n'entraîneront pas d'alarmes pour l'équipe opérationnelle.
3. GuardDuty les alertes doivent être stockées dans le même compte ou dans tout autre compte géré par la même organisation.

4. 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.
5. GuardDuty la délégation d'administrateur ne doit pas être activée dans MALZ car l'administrateur délégué serait en mesure d'effectuer des actions à privilèges élevés, comme la désactiver GuardDuty dans les autres comptes, sans accepter de risque.
6. GuardDuty Les filtres d'archivage automatique doivent utiliser l'étendue minimale pour obtenir un rendement maximal. Par exemple, si AMS détecte plusieurs éléments imprévisibles IPs dans différents blocs CIDR et qu'il existe un ASN d'entreprise approprié, utilisez l'ASN. Toutefois, si vous pouvez vous limiter à des plages spécifiques ou à des adresses /32, vous pouvez vous y étendre.

AMS-STD-006 - Sécurité de l'hôte

Voici le contrôle standard pour 006 - Host Security

- Un agent antivirus doit être exécuté sur toutes les EC2 instances à tout moment. (par exemple, Trend Micro DSM).
- Le module anti-malware doit être activé.
- L'agent EPS doit inclure tous les répertoires et fichiers à analyser.
- Les fichiers mis en quarantaine par la solution antivirus peuvent être partagés avec vous à la demande.
- Aucune solution de sécurité des terminaux tierce ne doit être installée.
- La fréquence de mise à jour des signatures antivirus doit être définie sur au moins une fois par jour.
- La fréquence de numérisation planifiée doit être réglée sur au moins une fois par mois.
- Le scan en temps réel (à l'accès) doit être activé et exécuté à tout moment.
- AMS ne doit exécuter aucun script personnalisé qui n'est pas détenu ou créé par AMS sur vos instances. (Remarque : vous pouvez le faire en utilisant l'accès Stack Admin via le Stack Admin access CT ou en utilisant [AWS Systems Manager Automation \(AMS SSPS\)](#)).
- L'authentification au niveau du réseau (NLA) ne doit pas être désactivée sur l'hôte Windows.
- Le système d'exploitation hôte doit être à jour avec les derniers correctifs de sécurité conformément au cycle de correctifs configuré.
- Un compte géré par AMS ne doit pas comporter d'instance non gérée dans le compte.
- La création de comptes d'administrateurs locaux sur votre instance par AMS ne doit pas être autorisée.

- La paire de clés EC2 activée ne doit pas être créée.
- Vous ne devez pas utiliser de systèmes d'exploitation déclarés en fin de vie (EOL) et aucun autre support de sécurité n'est fourni par le fournisseur ou un tiers.

AMS-STD-007 - Journalisation

Voici le contrôle standard pour 007 - 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 utilisations 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.
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

ID	Norme technique
	charge dans toutes les régions et transmettre les fichiers d'instantanés de configuration aux compartiments S3 au moins une fois par jour.
1.6	Journaux du système EPS (Endpoint Protection System) : la journalisation de la solution EPS doit être activée et configurée pour transmettre les CloudWatch journaux à un groupe de journaux.
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.
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

ID	Norme technique
2.1	Vous ne devez pas disposer d'un accès en écriture ou en suppression dans les compartiments S3 requis par AMS pour stocker les CloudWatch journaux et les groupes de journaux.
2.2	Vous devez disposer d'un accès en lecture seule à tous les journaux de vos comptes.
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 de votre contact de sécurité autorisé.
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. La « validation du fichier journal » doit être configurée dans les AWS CloudTrail parcours requis 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.
6.3	Les journaux d'un compte client ne doivent pas être transférés vers un compte tiers (qui n'appartient pas au client).

AMS-STD-008 - AMS-MAD

Voici la commande standard pour 008 - AMS-MAD

ID	Norme technique
1.0	Gestion des accès

ID	Norme technique
1.1	Seuls les utilisateurs privilégiés AMS disposant de connexions interactives et de tâches d'automatisation doivent être autorisés à se connecter à l'hôte de gestion pour administrer l'AD géré dans les comptes clients.
1.2	Les administrateurs AD doivent uniquement disposer de privilèges d'administrateur délégués (groupe d'administrateurs délégués AMS).
1.3	Les ingénieurs qui se connectent aux environnements AD des clients (hôte de gestion ou instances) doivent disposer d'un accès limité dans le temps.
1.4	Les clients ont un accès en lecture seule aux objets AD à l'aide des outils d'administration de serveur distant dans une EC2 instance.
1.5	Les droits d'administration relatifs à l'utilisateur ou au groupe Active Directory ne doivent pas être autorisés.
1.6	AWS Le partage d'annuaires avec le Compte AWS propriétaire du même client est autorisé moyennant une notification des risques.
2.0	Comptes de service
2.1	Les comptes de services gérés de groupe (GMSA) doivent être utilisés partout où ils sont pris en charge par des applications au lieu d'un compte de service standard.

ID	Norme technique
2.2	Tous les autres comptes de service doivent être créés après le processus d'acceptation des risques.
2.3	Les groupes de sécurité AD ne doivent pas être réutilisés sauf demande explicite du client. De nouveaux groupes AD doivent être créés. Les objets informatiques demandant l'accès au compte de service doivent être ajoutés au nouveau groupe de sécurité.
2,4	Tout compte de service GMSA doit être ajouté dans l'unité organisationnelle (OU) « Compte de service géré ».
2,5	Tout compte de service n'appartenant pas à la GMSA doit être ajouté dans l'unité d'organisation « Utilisateurs→Comptes de service ».
3,0	Objets de stratégie de groupe (GPO)
3.1	Aucun paramètre de l'objet GPO « Paramètres Windows > Paramètres de sécurité » ne doit être modifié s'il réduit de quelque manière que ce soit le niveau de sécurité du compte par rapport à son état actuel.
3.2	Dans MALZ, RFCs soumis depuis un compte d'application demandant la création d'un GPO, le GPO doit être lié à l'unité d'organisation correspondant au compte de l'application. Tout GPOs ce qui concerne tous les comptes doit provenir du compte Shared Service.

ID	Norme technique
3.3	Le délai d'expiration de la session d'inactivité RDP par défaut doit être défini à 15 minutes pour tous les serveurs du domaine Active Directory.
4,0	Confiance dans Active Directory
4.1	La confiance sortante unidirectionnelle (annuaire hébergé par AMS vers répertoire client) est autorisée si les IPs redirecteurs conditionnels sont routés vers un VPC via DX, VPC-Peer ou VPN.
5,0	Autres
5.1	Le mécanisme d'intégrité du fichier journal doit être activé. La « validation du fichier journal » doit être configurée dans les AWS CloudTrail parcours requis par les équipes AMS.
6.0	Transfert de journaux
6.1	Les utilisateurs, groupes, objets informatiques, unités d'organisation ou autres entités du client ne doivent pas utiliser la convention de dénomination AMS conformément à la convention de dénomination AMS.
6.2	Tous OUs doivent être gérés par AMS.

AMS-STD-009 - Divers

Voici le contrôle standard pour 009 - Divers

- Si le chiffrement est activé dans une ressource, un objet, une base de données ou un système de fichiers, il ne doit pas être désactivé.

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
- High_Risk-IAM-010 : Provisionnement IAM automatisé avec autorisations read/write

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 (L'approbation du responsable du site Ops est requise)
- High_Risk-Log-002 : Désactive les journaux de flux VPC. (L'approbation du responsable du site Ops est requise)
- High_Risk-log-003 : transfert du journal par 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 non-AMS pour CloudTrail

Sécurité de l'hôte

- High_Risk-Host-001 : Désactivez la sécurité des points de terminaison dans le compte pour quelque raison que ce soit. (L'approbation du responsable du site Ops est requise)
- High_Risk-Host-002 : Désactive l'application de correctifs dans une ressource ou au niveau du compte.
- High_Risk-Host-003 : Déploiement d'une instance non EC2 gérée dans le compte.
- High_Risk-Host-004 : Exécution d'un script personnalisé fourni par le client.
- High_Risk-Host-005 : Création de comptes d'administrateur local sur les instances.
- High_Risk-Host-006 : Exclusions d'analyse des types de fichiers/extensions de Trend Micro EPS ou désactivation de la protection contre les programmes malveillants sur les terminaux.

Note

L'acceptation des risques n'est pas requise pour les exclusions ou les règles de GuardDuty suppression des programmes malveillants EPS liées aux tests d'intrusion ou aux analyses de vulnérabilité ou pour les problèmes de events/known performance ayant un impact sur

le service justifiant des actions proactives. Une notification des risques est suffisante dans ces situations.

- High_Risk-Host-007 : Créer pour KeyPair EC2
- High_Risk-Host-008 : Désactiver la sécurité des points de terminaison dans EC2
- High_Risk-Host-009 : Comptes utilisant le système d'exploitation de fin de vie (EOL)

Miscellaneous

- High_Risk-enc-001 : Désactive le chiffrement dans n'importe quelle ressource s'il est activé

Active Directory géré

- High_Risk-AD-001 : Fournir des droits d'administrateur à un utilisateur ou à un groupe directeur actif
- High_RISK-AD-002 : Politiques GPO capables de réduire le niveau de sécurité du compte

Gestion de la continuité dans AMS Advanced

Dans le cadre de la gestion de la continuité, AWS Managed Services (AMS) fournit un accès automatique à AWS Backup un service natif avec AWS. Cela facilite l'accès à un service compatible avec Amazon EBS, Amazon EC2, Amazon RDS, Amazon EFS, etc.

Pour en savoir plus, voir [AWS Backup: Comment ça marche](#).

Rubriques

- [Qu'est-ce que la gestion de la continuité ?](#)
- [Comment fonctionne la gestion de la continuité](#)
- [Réponse à la reprise après sinistre](#)
- [Planification de la reprise après sinistre](#)

Qu'est-ce que la gestion de la continuité ?

La gestion de la continuité est le processus utilisé par AMS pour fournir des sauvegardes et des instantanés pour votre compte.

AMS fournit un accès AWS Backup via des types de modifications que vous utilisez pour créer et gérer des tâches et des plans de sauvegarde.

Comment fonctionne la gestion de la continuité

AMS les utilise [AWS Backup](#) pour la gestion de la continuité.

Lorsque vous commencez à travailler avec AWS Backup dans AMS :

1. Exécuter une sauvegarde à la demande
2. Créez un plan de sauvegarde (facultatif, AMS fournit des plans de sauvegarde par défaut)
3. Utiliser les coffres-forts de sauvegarde AMS par défaut (facultatif)
4. Gérez (exécutez, affinez, supprimez, etc.) vos plans de sauvegarde et vos points de restauration

Plans de sauvegarde AMS

Un plan de sauvegarde est une expression de politique qui définit quand et comment vous souhaitez sauvegarder les ressources AWS prises en charge, telles que les bases de données RDS, les volumes EBS, les tables DynamoDB et les systèmes de fichiers EFS. Les politiques de planification et de rétention sont gérées via des plans de sauvegarde personnalisés, que vous pouvez créer à l'aide d'un type de modification (CT) avec AMS Advanced ou AWS Backup avec AMS Accelerate. Attribuez des ressources à vos plans de sauvegarde à l'aide de balises, puis sauvegardez et conservez AWS Backup automatiquement les sauvegardes des ressources attribuées conformément au plan de sauvegarde défini. Vous pouvez créer plusieurs plans de sauvegarde si vous avez des charges de travail avec des exigences de sauvegarde différentes.

Un plan de sauvegarde peut comporter jusqu'à six règles de sauvegarde qui définissent un calendrier et une période de conservation, entre autres détails. Le calendrier de sauvegarde détermine à quel AWS Backup moment une tâche de sauvegarde est lancée et à quelle fréquence une sauvegarde est créée. Vous pouvez choisir une fréquence horaire, quotidienne, hebdomadaire ou mensuelle. Le paramètre des jours de suppression détermine le nombre de jours pendant lesquels l'instantané est stocké avant d'être automatiquement supprimé.

Note

AMS Advanced : Si vous migrez depuis l'ancien système de sauvegarde AMS, AMS crée un plan de sauvegarde par défaut à des fins de rétrocompatibilité. La paire clé:valeur dans ce scénario est Backup:True. Pour garantir la rétrocompatibilité, la valeur ici ne distingue pas les majuscules et minuscules. Backup:True ou Backup:True sont donc toutes des balises valides. Toutes les autres paires clé:valeur distinguent les majuscules et minuscules.

AWS Backup peut fonctionner au niveau du volume EBS ou au niveau de l' EC2 instance Amazon, mais ne faites pas les deux en même temps, car cela peut créer une situation de course où les sauvegardes risquent de se heurter.

Plans de sauvegarde par défaut, zone de landing zone multi-comptes

Lors de la nouvelle RFC de création de compte, AMS s'assure qu'il existe un plan de sauvegarde par défaut global au niveau du compte afin de protéger vos charges de travail. Les valeurs des champs obligatoires sont définies par défaut, comme indiqué dans la section suivante :

Plan de sauvegarde AMS par défaut

default-backup-plan

Clé TAG : Backup

Valeur TAG : True

```
RuleForDailyBackups schedule expression: cron(30 23 ? * *) (a daily backup for 23:30 UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForWeeklyBackups schedule expression: cron(30 23 ? * 7 *) (a weekly backup for 23:30 UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
RuleForMonthlyBackups schedule expression: cron(30 23 * ? *) (a monthly backup for 23:30 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(30 23 1 1 ? *) (a yearly backup for 23:30 UTC time on day 1 of the month, only in January)
RuleForYearlyBackups delete after years: 2 years
```

Plan de sauvegarde AMS par défaut	Start Time	Retention
sauvegarde horaire	N/A	N/A
sauvegarde quotidienne	tous les jours à 23 h 30 UTC	7 jours
sauvegarde hebdomadaire	chaque semaine à 23 h 30 UTC, uniquement le samedi	4 semaines
sauvegarde mensuelle	tous les mois à 23 h 30 UTC, le premier jour du mois	26 semaines
sauvegarde annuelle	23 h 30 UTC, le premier jour du mois	2 ans

Plan de sauvegarde AMS par défaut amélioré

Ce plan est un modèle de bonnes AWS Backup pratiques de protection contre les attaques de ransomware. Il met en œuvre une stratégie de sauvegarde quotidienne, hebdomadaire, mensuelle

et annuelle. AWS Backup la [sauvegarde continue](#) est activée avec une rétention maximale (31 jours) sur les [ressources prises en charge](#).

ams-enhanced-default-backup-planifier

Clé TAG : backup-orchestrator-enhanced

Valeur TAG : true

```
RuleForDailyBackups schedule expression: cron(0 0 4 ? * * ) (a daily backup for 04:00 UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForDailyBackups continuous backup: true
RuleForWeeklyBackups schedule expression: cron(0 0 2 ? * 7) (a weekly backup for 02:00 UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
RuleForMonthlyBackups schedule expression: cron(0 2 1 * ? *) (a monthly backup for 02:00 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(0 2 1 1 ? *) (a yearly backup for 02:00 UTC time on day 1 of the month, only in January)
RuleForYearlyBackups delete after years: 2 years
```

Plan de sauvegarde AMS amélioré	Start Time	Retention
sauvegarde horaire	N/A	N/A
sauvegarde quotidienne	tous les jours à 4:00 UTC	31 jours
sauvegarde hebdomadaire	Samedi, 2:00 UTC	6 semaines
sauvegarde mensuelle	1er du mois, 2h00 UTC	26 semaines
sauvegarde annuelle	1er janvier, 14h00 UTC	2 ans

Plan de sauvegarde AMS sensible aux données

Ce plan définit les meilleures pratiques d'AWS Backup afin de protéger les applications sensibles contre les attaques de ransomware. Il met en œuvre une stratégie de sauvegarde horaire,

quotidienne, hebdomadaire, mensuelle et annuelle. La sauvegarde [continue d'AWS Backup](#) est activée avec une rétention maximale (31 jours) sur les [ressources prises en charge](#).

ams-data-sensitive-backup-planifier

Clé TAG : backup-orchestrator-data-sensitive

Valeur TAG : true

```
RuleForHourlyBackups schedule expression: cron(0 * ? * * *) (an hourly backup at the
hour mark)
RuleForHourlyBackups delete after days: 7 days
RuleForDailyBackups schedule expression: cron(0 0 4 ? * * ) (a daily backup for 04:00
UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForWeeklyBackups schedule expression: cron(0 0 2 ? * 7) (a weekly backup for 02:00
UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
RuleForMonthlyBackups schedule expression: cron(0 2 1 * ? *) (a monthly backup for
02:00 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(0 2 1 1 ? *) (a yearly backup for 02:00
UTC time on day 1 of the month, only in January)
RuleForYearlyBackups delete after years: 2 years
```

Plan de sauvegarde AMS sensible aux données	Start Time	Retention
sauvegarde horaire	à l'heure	7 jours
sauvegarde quotidienne	tous les jours à 4:00 UTC	31 jours
sauvegarde hebdomadaire	Samedi, 2:00 UTC	6 semaines
sauvegarde mensuelle	1er du mois, 2h00 UTC	26 semaines
sauvegarde annuelle	1er janvier, 14h00 UTC	2 ans

coffres-forts de sauvegarde AMS

AWS Backup organise les instantanés dans des unités de stockage logiques appelées coffres-forts.

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	Description
ams-automated-backups	Ce coffre-fort reçoit tous les points de restauration utilisés par le AWS Backup plan par défaut AMS Advanced default-backup-plan.
ams-automated-enhanced-backups	Ce coffre-fort reçoit tous les points de restauration pris par le AWS Backup plan ams-enhanced-default-backup par défaut amélioré d'AMS Advanced.
ams-automated-data-sensitive-sauvegardes	Ce coffre-fort reçoit tous les points de restauration pris par AMS Advanced AWS Backup plan ams-data-sensitive-backup-plan.
ams-manual-backups	Il s'agit de l'emplacement par défaut pour toutes les sauvegardes issues des plans de sauvegarde Start Backup Job RFC (ct-2hhud2lx01tq7), si aucun nom de coffre n'est défini.
ams-custom-backups	Il s'agit de l'emplacement par défaut pour les instantanés réalisés par AMS avant d'appliquer des correctifs à une instance à l'aide de Patch Orchestrator ou des activités de patch mensuelles. Ils sont automatiquement supprimés conformément à la politique par

Nom du coffre-fort AMS	Description
	défaut de 60 jours du cycle de vie des correctifs AMS.

Types de modifications de sauvegarde AMS

AMS en fournit plusieurs CTs pour vous permettre de créer et d'utiliser des plans de sauvegarde.

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.

- [Plan de sauvegarde : créer](#)
- [Backup Job : Démarrer](#)
- [Backup Job : Arrêter](#)
- [Point de récupération : Supprimer](#)
- [DynamoDB | Création à partir d'une sauvegarde](#)
- [Volume EBS : créer à partir d'une sauvegarde](#)
- [Amazon Elastic File System \(EFS\) : création à partir d'une sauvegarde](#)

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 [de sauvegarde quotidien](#).

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.

Réponse à la reprise après sinistre

Outre les options décrites dans les sections suivantes, il est utile que vous sachiez quelles mesures prendre pour lancer une reprise après sinistre (DR) avec AMS.

En cas de sinistre et que vous devez lancer une restauration, suivez les instructions générales suivantes :

1. Ouvrez un incident hautement prioritaire avec la catégorie Disponibilité. AMS ouvrira une passerelle de conférence et invitera votre équipe à la rejoindre.
2. Connaissiez la liste des ressources que vous devez récupérer.
3. Connaissiez la zone d'atterrissage cible (LZ) vers laquelle vous devez récupérer (par exemple, le même compte, une autre AZ ou un autre compte et une région différente).
4. Soumettez des demandes de restauration pour chaque ressource de la zone d'atterrissage cible. Suivez votre plan de reprise après sinistre existant ou consultez les options de la section suivante (par exemple [Protection contre les sinistres EC2 avec des instantanés EBS sur AMS](#), ou [Protection contre les sinistres EC2 avec Elastic Disaster Recovery sur AMS](#)).
5. Restaurez les fonctionnalités de l'application et utilisez l'assistance AMS pour résoudre les problèmes liés à l'infrastructure.

AMS peut vous aider à préparer cet événement et à créer un plan de reprise après sinistre pour votre organisation afin de répondre à ces questions. Pour plus de détails, contactez votre responsable de prestation de services cloud (CSDM) ou votre architecte cloud (CA).

Planification de la reprise après sinistre

La reprise après sinistre (DR) est un service essentiel pour la continuité des activités et la conformité des entreprises. AMS s'associe à vous pour vous aider à planifier, mettre en œuvre et maintenir votre stratégie de reprise après sinistre sur AMS.

La zone d'atterrissage AMS (LZ), multicompte et compte unique, fournit une haute disponibilité native, multi-AZ et une haute disponibilité pour les composants de l'infrastructure AMS qui répondent à la plupart des scénarios de protection contre les catastrophes. Toutefois, selon la couverture géographique de votre entreprise, vous pourriez avoir besoin d'une protection régionale. Pour la disponibilité interrégionale et la reprise après sinistre, un autre compte AMS est requis dans une région différente (c'est le cas à la fois pour la zone d'atterrissage multi-comptes et pour la zone d'atterrissage monocompte).

AMS s'aligne sur les directives AWS DR décrites dans ce blog, [Rapidly restore mission-critical systems in a disaster](#), et prend en charge les quatre options suivantes :

- Multisite (ou haute disponibilité)
- Veille chaude
- Lampe pilote
- Sauvegarde et restauration

Ces options et leur prise en charge par AMS sont décrites dans les sections suivantes.

Multisite ou haute disponibilité (HA)

La solution HA est généralement fournie par les fonctionnalités intégrées de l'application, telles que le clustering ou la réplication synchrone. Les utilisateurs sont dirigés à la fois vers Prod et vers les HA/DR nœuds. Le DNS pointe vers les nœuds directement ou via un équilibreur de charge élastique (ELB).

Votre architecte cloud (CA) AMS travaillera avec vous dans le cadre de votre planification Well-Architected-Review et de la reprise après sinistre.

HA DR utilise des applications et des services et fonctionnalités AWS natifs, comme illustré dans le graphique suivant :

Le site DR peut être identique ou différent Région AWS.

 Note

Une région différente (inter-régions) aura un environnement Active Directory différent.

Étapes DR (failover) : basculement automatique, aucune étape manuelle n'est requise. En cas de défaillance de la LZ principale, les utilisateurs seront automatiquement redirigés vers le nœud. DR/HA Ceci est réalisé à la fois par le DNS et par la configuration de l'application.

Métriques HA DR :

- Objectif du point de récupération (RPO) : <5 min
- Objectif de temps de récupération et (RTO) : <5 min
- Maintenance : élevée (des modifications synchrones sont requises dans les deux environnements, telles que la configuration des applications, les correctifs, les SG ou ALB, les certificats, etc.).
- Coût : élevé

Secours semi-automatique

Le terme « veille chaude » est utilisé pour décrire un scénario de reprise après sinistre (DR) dans lequel une version réduite de l'environnement s'exécute dans le cloud.

La réplication des données est gérée par la couche application, généralement de manière asynchrone, vers une instance en ligne, tandis que les autres instances (par exemple, au niveau Application et au niveau Web) peuvent être désactivées pour réduire les coûts. Les utilisateurs sont uniquement dirigés vers le site de production. D'autres AWS ressources, comme Elastic Load Balancer (ELB), peuvent également être préprovisionnées sur le site de reprise après sinistre.

Votre AMS Cloud Architect (CA) travaillera avec vous dans le cadre de votre planification Well-Architected-Review et de la reprise après sinistre.

Warm Standby DR utilise des applications et des services et fonctionnalités AWS natifs, comme illustré dans le graphique suivant :

Le site DR peut être identique ou différent Région AWS.

 Note

Une région différente (inter-régions) aura un environnement Active Directory différent.

Étapes DR (failover) :

1. Freiner la réplication des données et faire de l'instance de données du site DR le maître
2. Mettez à jour la configuration de l'application selon les besoins (nouvelle adresse IP, nom du serveur, etc.)
3. Rediriger le DNS vers le site DR (ELB)
4. Dépendances AD si nécessaire (comptes de service SPNs GPOs,,, etc.)

Métriques HA DR :

- Objectif du point de reprise (RPO) : <1 heure
- Objectif de temps de restauration et (RTO) : <1 heure (dépend du nombre d'instances et de l'orchestration)
- Maintenance : élevée (des modifications synchrones sont requises dans les deux environnements, telles que la configuration des applications, les correctifs, les groupes de sécurité (SG) ou l'équilibreur de charge des applications (ALB), les certificats, etc.).
- Coût : moyen

Veilleuse

Dans cette approche de reprise après sinistre (DR), vous répliquez une partie de votre environnement Prod pour un ensemble limité de services de base. Une petite partie de votre infrastructure fonctionne en permanence, synchronisant simultanément les données modifiables (telles que les bases de données ou les documents), tandis que d'autres parties de votre infrastructure sont désactivées et utilisées uniquement pendant les tests. Contrairement à une approche de sauvegarde et de restauration, vous devez vous assurer que les éléments essentiels les plus critiques sont déjà configurés et fonctionnent dans la zone d'atterrissage de la DR (la veilleuse).

Votre architecte du cloud AMS travaillera avec vous dans le cadre de votre planification Well-Architected-Review et de celle de la reprise après sinistre.

Pilot Light DR utilise des applications et des services et fonctionnalités AWS natifs, comme illustré dans le graphique suivant :

Le site DR peut être identique ou différent Région AWS.

 Note

Une région différente (inter-régions) aura un environnement Active Directory différent.

Étapes DR (failover) :

1. Freiner la réplication des données et faire de l'instance de données du site DR le maître
2. Démarrez les instances et l'infrastructure désactivées
3. Mettez à jour la configuration de l'application selon les besoins (nouvelle adresse IP, nom du serveur, etc.)
4. Ajoutez les instances à l'ELB selon les besoins
5. Rediriger le DNS vers le site DR (ELB)
6. Dépendances AD, si nécessaire (comptes de service SPNs GPOs,,, etc.)

Indicateurs de Pilot Light DR :

- Objectif du point de reprise (RPO) : <1 heure
- Objectif de temps de restauration et (RTO) : environ 1 heure (dépend du nombre d'instances et de l'orchestration)
- Entretien : moyen
- Coût : moyen

Sauvegarde et restauration

Cette approche de reprise après sinistre (DR) simple et peu coûteuse sauvegarde vos données et applications depuis n'importe où vers la zone d'atterrissage de la reprise après sinistre pour les utiliser lors de la reprise après sinistre.

Votre AMS Cloud Architect travaille avec vous dans le cadre de votre planification de Backup et de DR.

Backup and Restore DR utilise les outils et processus automatisés AMS, comme illustré dans le graphique suivant :

Deux méthodes de sauvegarde et de réplication peuvent être utilisées :

- Instantané EBS (Recovery Point Objective (RPO) > 1 heure), connu sous le nom d' « EBS »
- AWS Elastic Disaster Recovery (Objectif de point de récupération (RPO) ~ 0,25 heure), connu sous le nom de « DRS »

Le site DR peut être identique ou différent Région AWS.

 Note

Une région différente (inter-régions) possède un environnement Active Directory différent.

Étapes DR (failover) :

1. Restaurez les instances à partir de snapshots (processus en deux étapes avec d'abord une instance de remplacement)
2. Mettre à jour la configuration de l'application (nouvelle adresse IP, nom du serveur, etc.)
3. Configurez d'autres infrastructures selon les besoins (SG, ELB, etc.)
4. Rediriger le DNS vers le site DR (ELB)
5. Mettez à jour ou restaurez les dépendances AD si nécessaire (comptes de service, noms principaux de service (SPNs), objets de stratégie de groupe (GPOs), etc.)

Mesures de sauvegarde et de restauration après sinistre :

- Objectif du point de reprise (RPO) : > 1 heure ou environ 0,25 heure (dépend de la solution sélectionnée - EBS ou DRE)
- Objectif de temps de restauration et (RTO) : environ 1 heure (dépend du nombre d'instances et de l'orchestration)

- Maintenance : des modifications importantes (synchrones) sont nécessaires dans les deux environnements, telles que la configuration des applications, les correctifs, les groupes de sécurité ou les équilibres de charge des applications, les certificats, etc.
- Coût : moyen

Protection contre les sinistres EC2 avec des instantanés EBS sur AMS

Prérequis :

- Zone d'atterrissage d'AMS Prod (source)
- Zone d'atterrissage AMS DR (cible DR)
- Les instantanés EBS sont activés pour les EC2 instances (AWS Backup)

Solution de réplication de snapshots :

- Cross AZ : Non applicable - Les instantanés EBS sont hautement disponibles dans la région dès leur conception
- Interrégional : AWS Backup

Le schéma suivant représente le processus de EC2 restauration à partir de snapshots EBS sur AMS :

EC2 Étapes DR sur AMS :

1. Déclenchez une RFC pour partager les instantanés EBS avec le compte cible (obligatoire pour la DR interrégionale).

: Gestion, composants de pile avancés, EBS Snapshot, partage
2. Créez une pile EC2 AMS fictive dans le sous-réseau de destination (sous-réseau du site DR). Il est recommandé d'utiliser l'ingestion de CFN pour créer la pile, car le client peut combiner les étapes d'attribution de groupes de sécurité et d'autres étapes (comme l'ajout de l'instance à un ELB) dans la même pile.

Type de modification : déploiement, ingestion, empilage à partir d' CloudFormation un modèle, création

3. Déclenchez une RFC pour effectuer la restauration du volume de EC2 pile.

Type de modification : gestion, composants de pile avancés, pile d' EC2 instances, volumes de restauration.

Le CT restaure les volumes à partir des instantanés partagés à l'étape 1 et les attache à l'instance d'espace réservé créée à l'étape 2.

Fonctionnalité Volume Restore CT :

- Arrêtez l'instance d'espace réservé
- Restaurer des volumes à partir des instantanés
- Échangez les volumes
- Démarrez l'instance
- Quitter l'ancien domaine
- Modifier le nom d'hôte
- Redémarrer. Les scripts d'amorçage AMS relient l'instance au domaine cible (DR) au démarrage

Entrée CT de restauration du volume :

- InstanceId (identifiant d'instance substituable)
- RootDeviceSnapshotId, le snapshot EBS du volume racine restauré
- KMSKeyId, l'identifiant de clé KMS, ou ARN, pour chiffrer tous les volumes restaurés sur l'instance EC2
- DeviceNames, jusqu'à 25 (facultatif)
- SnapshotIds, jusqu'à 25 (facultatif). Liste des instantanés des volumes à restaurer

Protection contre les sinistres EC2 avec Elastic Disaster Recovery sur AMS

Prérequis :

- Zone d'atterrissage d'AMS Prod (source)
- Zone d'atterrissage AMS DR (cible DR)
- Vous devez d'abord initialiser le service Elastic Disaster Recovery pour toutes les Régions AWS applications dans lesquelles vous comptez l'utiliser.

Créez un rôle IAM dans votre zone de landing zone de reprise après sinistre (LZ) pour accéder à la console Elastic Disaster Recovery.

- Important : un document SSM est créé en tant qu'action post-lancement dans DRS. Cette action doit être activée sur tous vos serveurs dans les PostLaunch paramètres.
- l'instance de destination (espace réservé) doit avoir une clé de balise : "AWSDRS«, une valeur : "AllowLaunchingIntoThisInstance ». L'instance Placeholder doit être à l'état arrêté. Sinon, AMS ne pourra pas sélectionner l'instance d'espace réservé dans les paramètres de lancement et Elastic Disaster Recovery ne pourra pas effectuer de restauration au-dessus de l'instance d'espace réservé.

Pour un schéma du processus de configuration et de restauration d'Elastic Disaster Recovery EC2 sur AMS, reportez-vous à la section [Architecture générale AWS Elastic Disaster Recovery \(AWS DRS\)](#).

EC2 Étapes de reprise après sinistre avec Elastic Disaster Recovery sur AMS :

1. Créez une pile EC2 AMS d'espace réservé dans le sous-réseau de destination (sous-réseau du site DR) avec les balises appropriées. Pour plus d'informations, consultez la section précédente. Nous vous recommandons d'utiliser l'ingestion CFN pour créer la pile, car vous pouvez combiner les étapes consistant à attribuer des groupes de sécurité et à étiqueter l'instance, le volume EBS et d'autres (comme l'ajout de l'instance à un ELB) dans la même pile.

Type de modification : déploiement, ingestion, empilage à partir d' CloudFormation un modèle, création

2. Arrêtez l'instance d'espace réservé.

Type de modification : Gestion, composants de pile avancés, EC2 instance, arrêt

3. Si ce n'est pas le cas à l'étape 1, balisez l'instance d'espace réservé et son volume EBS avec key : "AWSDRS«, value : " »AllowLaunchingIntoThisInstance.

Type de modification : gestion, composants de pile avancés, étiquette, mise à jour.

4. Utilisez l'instance fictive de l'étape 1 comme cible sous Launch into instance ID, DRS Launch Settings pour le serveur source. Lancez un exercice de restauration d'instance depuis la console Elastic Disaster Recovery pour le serveur source.

 Note

Les volumes d'instance réservés sont conservés dans le compte. Pour supprimer ces volumes, soumettez un type de modification Management | Advanced stack components | EBS Volume | Delete (ct-3e3h8u0sp5z80) à la fin de l'opération de reprise après sinistre.

Workflow de restauration d'Elastic Disaster Recovery :

- L'instance cible (espace réservé) doit être à l'état arrêté
- Échangez les volumes et supprimez le volume racine source (espace réservé)
- Démarrez l'instance
- Exécutez les actions après le lancement pour terminer les tâches suivantes :
 - Activez l'agent SSM.
 - Échangez les volumes et supprimez le volume racine source (espace réservé).
 - Démarrez l'instance
 - Exécutez le document PostLaunchScript SSM. Ce document effectue les opérations suivantes :
 1. Quitte l'ancien domaine.
 2. Modifie le nom d'hôte.
 3. Redémarrer. Les scripts d'amorçage AMS relient l'instance au domaine cible (DR) lors du démarrage.

Gestion des correctifs dans AMS

Rubriques

- [AMS Patch Orchestrator : un modèle de patching basé sur des balises](#)
- [Utilisation de Patch Orchestrator](#)
- [Correctifs à la demande](#)
- [Correctif standard AMS](#)
- [Engagements relatifs aux services de correction](#)

Dans AMS, la gestion des correctifs est un service qui vous aide à maintenir les mises à jour des fournisseurs de systèmes d'exploitation sur vos instances Amazon Elastic Compute Cloud (Amazon EC2). Vous êtes libre de personnaliser la fréquence et le processus d'application des correctifs à vos EC2 instances Amazon.

Vous configurez la gestion des correctifs lors de l'intégration et vous pouvez la mettre à jour à l'aide du processus RFC. Les piles créées à l'aide du système de gestion des modifications et d'un modèle compatible avec les correctifs (pour Amazon, le groupe EC2 Auto Scaling, la pile HA à un ou deux niveaux) sont automatiquement souscrites à la gestion des correctifs.

AMS fournit une fonctionnalité, Patch Orchestrator, qui consiste à appliquer des correctifs à partir de balises, pour configurer les correctifs.

Pour les définitions des termes relatifs à l'application de correctifs, voir [Termes clés d'AMS](#).

Important

- Il n'est pas possible pour les piles ou les instances constituant une pile de refuser la gestion des correctifs si le modèle AMS à partir duquel la pile est créée est compatible avec la gestion des correctifs. Actuellement, l'application de correctifs est compatible avec les modèles de pile suivants :
 - Amazon EC2 Stack | Create et Amazon EC2 Stack | Create (avec volumes supplémentaires)
 - EC2 Instance Amazon lancée avec AWS CloudFormation ingest
 - Auto Scaling group | Create (les EC2 instances Amazon du groupe sont corrigées)

- Pile à un niveau à haute disponibilité | Création et pile à deux niveaux à haute disponibilité | Créer
- Si un incident en cours affecte une pile, les opérateurs AMS peuvent replanifier ou annuler les correctifs programmés.
- Par défaut, toutes les instances d'une pile compatible avec les correctifs sont corrigées sur place. Pour patcher des groupes Auto Scaling en remplaçant une Amazon Machine Image (AMI) à l'aide de l'AMI latest/patched AMS, soumettez une demande de service. AMIs Les mises à jour sont partagées sur les comptes chaque mois.

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
- Utiliser par défaut les référentiels des fournisseurs de systèmes d'exploitation standard lorsque cela est possible
- Auditez régulièrement les configurations de référentiels personnalisées

Tip

AMS vous recommande d'activer les sauvegardes pour les instances contenant des applications ou des services utiles. Pour plus d'informations sur l'activation des sauvegardes, consultez [Gestion de la continuité dans AMS Advanced](#).

AMS Patch Orchestrator : un modèle de patching basé sur des balises

Si vous avez été intégré au nouveau modèle de correction basé sur des balises AMS Patch Orchestrator, vous pouvez utiliser des balises pour appliquer votre configuration de correctif à un ensemble précis de ressources, appelé groupe de correctifs, allant d'une instance à toutes vos instances. Pour plus d'informations sur les balises AMS, consultez la section [Utilisation des balises](#). Les instructions relatives à la configuration des balises Patch Orchestrator sont fournies dans la section suivante.

Les correctifs sont installés pendant les fenêtres de correctifs que vous définissez avec la [fenêtre de correctifs SSM | Créer](#). Chaque fenêtre de correctifs est une fenêtre de maintenance d'AWS Systems Manager qui s'exécute selon le calendrier de votre choix, a une durée configurée et s'applique à un groupe de correctifs. Les instances qui ne font pas partie d'une fenêtre de correctifs explicite sont corrigées pendant la fenêtre de maintenance par défaut que vous définissez lors de l'intégration de Patch Orchestrator.

Important

Si plusieurs fenêtres de maintenance des correctifs sont planifiées pour s'exécuter simultanément, moins de 1 001 instances doivent être traitées à la fois. Il s'agit d'une limitation d'AWS Systems Manager. AMS recommande au moins une heure toutes les cinquante instances.

Par défaut, tous les correctifs de système d'exploitation (OS) fournis par le fournisseur sont installés pendant une période de maintenance ou un correctif à la demande. C'est ce qu'on appelle la ligne de base de correctif par défaut. Si vous souhaitez limiter les correctifs installés, vous pouvez définir une ligne de base de correctifs personnalisée avec l'une des lignes de base de correctifs créées CTs (par OSes), voir la [sous-catégorie Patching](#). Par exemple, vous pouvez utiliser une ligne de base de correctifs personnalisée afin que seules les mises à jour de sécurité critiques et importantes soient installées pour un ou plusieurs groupes de correctifs.

Une fois les correctifs installés sur une instance, celle-ci est redémarrée. Les notifications relatives aux correctifs sont envoyées avant et après l'application des correctifs, et un rappel supplémentaire est envoyé dans les 96 heures précédant le début prévu. En outre, AMS applique des mises à

jour aux outils de gestion de l'infrastructure (tels que l'agent AWS SSM) pendant la période de maintenance sélectionnée.

Important

AMS déconseille les rapports mensuels de conformité des correctifs pour les instances présentant des correctifs manquants et n'enverra pas de rapports mensuels. Cette modification a été apportée compte tenu des rapports opérationnels en libre-service récemment publiés qui sont actualisés toutes les 24 heures, sont disponibles sur demande et fournissent les données les plus récentes et détaillées. Pour en savoir plus sur les rapports, consultez la section Rapports en libre-service. Pour en savoir plus sur les rapports, voir [Rapports en libre-service](#).

Pour plus d'informations sur les notifications, consultez [Notifications de correctifs](#).

Utilisation de Patch Orchestrator

Activez AMS Patch Orchestrator pour votre compte en soumettant une demande de service incluant les informations suivantes :

- Catégorie : Autres
- Objet : Intégration à Patch Orchestrator
- E-mails CC : les adresses e-mail CC reçoivent des notifications lorsque le statut de cette RFC d'intégration change
- Détails : collez les informations suivantes dans l'e-mail et indiquez vos valeurs. Notez que ThirdTagKey c'est facultatif. Pour des recommandations et des exemples, consultez le tableau suivant.

```
Default maintenance window Schedule:  
Default Maintenance Window Schedule TimeZone:  
Default Maintenance Window Duration:  
Default Maintenance Window Cutoff:  
Default Patch Backup Retention In Days:  
Default Maintenance Window Notification Emails:  
First Tag Key:  
Second Tag Key:  
Third Tag Key:
```

Le tableau suivant décrit le format et les recommandations pour les valeurs que vous avez fournies.

Configurations de correctifs basées sur des balises Patch Orchestrator

Nom du paramètre	Informations	Recommandation ou exemple
Calendrier de la fenêtre de maintenance par défaut	Le calendrier de la fenêtre de maintenance par défaut sous la forme d'une expression cron ou rate. Exemples : <code>cron(0 3 ? * 6L *)</code>: 03h00 le dernier vendredi de chaque mois <code>rate(7 days)</code>: Tous les sept jours Pour plus d'informations sur la création d'expressions cron et des liens vers des ressources d'expressions cron et rate, voir Expressions cron et rate pour les fenêtres de maintenance.	Nous recommandons de faire fonctionner la fenêtre au moins une fois par mois, un jour de semaine régulier.
Fuseau horaire de planification de la fenêtre de maintenance par défaut	Le fuseau horaire sur lequel s'exécute la fenêtre de maintenance par défaut est basé sur le format IANA (Internet Assigned Numbers Authority).	Exemples : <code>America/Los_Angeles</code> <code>Etc/UTC</code>
Durée de la fenêtre de maintenance par défaut	Durée de la fenêtre de maintenance par défaut en heures.	Au moins 1 heure toutes les 50 instances, plus 2 heures pour la coupure.
Coupure de la fenêtre de maintenance par défaut	Nombre d'heures avant la fin de la fenêtre de maintenance par défaut pendant laquelle	Au moins 2 heures.

Nom du paramètre	Informations	Recommandation ou exemple
	aucune nouvelle commande d'application de correctifs n'est lancée. Cet intervalle existe pour laisser suffisamment de temps pour que l'application des correctifs soit terminée avant la fin de la fenêtre.	
Conservation des correctifs de sauvegarde par défaut en jours (facultatif)	Durée par défaut, en jours, pour conserver les points de restauration EBS créés avant d'appliquer des correctifs aux instances.	Nous vous recommandons de conserver la valeur par défaut, qui est 60.
E-mails de notification de la fenêtre de maintenance par défaut	Une à cinq adresses e-mail ou listes de distribution pour recevoir des notifications concernant l'état d'application des correctifs par défaut dans les fenêtres de maintenance.	Nous vous recommandons d'utiliser des listes de distribution de groupe plutôt que des e-mails individuels.
Clé du premier tag	La première clé de balise à utiliser pour créer les valeurs des balises de votre groupe de patches.	Par exemple, Appld. Spécifiez null si vous avez déjà défini vos propres groupes de correctifs avec une balise Patch Group.
Deuxième clé de tag	Deuxième clé de balise à utiliser pour créer les valeurs des balises de votre groupe de patches.	Par exemple, Environnement. Spécifiez null si vous avez déjà défini vos propres groupes de correctifs avec une balise Patch Group.

Nom du paramètre	Informations	Recommandation ou exemple
Troisième clé de tag (facultatif)	Troisième clé de balise facultative à utiliser pour créer les valeurs des balises de votre groupe de patches.	Par exemple, Group.

Une fois que vous êtes intégré au nouveau modèle de service de correctifs Patch Orchestrator, toutes les instances correctement étiquetées de votre compte appartiennent à un groupe de correctifs doté d'une balise Patch Group. Patch Orchestrator utilise soit votre balise de groupe de patches existante, soit une balise créée par AMS composée des deux ou trois valeurs de balise concaténées que vous avez spécifiées lors de l'intégration de Patch Orchestrator. Par exemple, `{Tag Value 1} - {Tag Value 2} - {Tag Value 3}`. AMS met à jour ces balises de groupe de correctifs appliquées par AMS toutes les 12 heures. Si nécessaire, vous pouvez mettre à jour les valeurs des balises de votre groupe de correctifs avec les types de modification [Tag | Mettre à jour \(révision requise\)](#) ou [Tag | Mettre à jour \(révision requise\)](#).

Par exemple, si votre EC2 instance Amazon possède les paires clé:valeur de balise suivantes :

- AppId:MyApplication
- Environment:Production
- Group:1

Lors de l'intégration, vous avez spécifié les clés de balise suivantes :

- First Tag Key = AppId
- Second Tag Key = Environment
- Third Tag Key = Group

AMS crée la balise Patch Group suivante et l'applique à vos instances :Patch Group:MyApplication-Production-1.

 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.

Conditions préalables requises pour Patch Orchestrator

Le flux de travail Patch Orchestrator cible EC2 les instances Amazon auxquelles des correctifs sont appliqués par la dernière version de System Manager Automation Document : `AWSManagedServices-PatchInstanceFromMaintenanceWindow`

Dans le cadre du flux de travail documentaire, le document de commande d'exécution « AWS-RunPatchBaseline » est exécuté sur chacune des EC2 instances Amazon des membres du groupe de correctifs. Pour en savoir plus, consultez la section [À propos du document SSM AWS-RunPatchBaseline](#).

Prérequis:

- EC2 Instance Amazon déployée à partir d'Amazon Machine Image (AMI) fournie par AMS, ou sur une AMI via le CT « Stack from migration partner migrated instance » (ct-257p9zjk14ija).
- Connexion Internet de sortie activée. Pour les firewall/proxy solutions, l'exigence est d'autoriser les points de terminaison du référentiel and/or Linux Windows Update à mettre en miroir les points de terminaison, les paramètres de proxy d'AWS System Manager et la configuration du proxy de métadonnées. Pour plus d'informations, voir [Configuration de l'agent SSM pour utiliser un proxy](#) et [Utilisation d'un proxy HTTP](#)
- Rôle IAM correspondant à un accès permissif minimum pour le service SSM ou le rôle IAM. `customer-mc-ec2-instance-profile`
- Nous recommandons 10 Go d'espace de partition racine disponible. Pour le système d'exploitation Linux, au moins 2 Go sont disponibles dans la `/var` partition.
- Autorité de certification fonctionnelle et valide pour les téléchargements de mises à jour.
- Windows Server Update Services (WSUS) - Registre comprenant, mais sans s'y limiter : `DisableWindowsUpdateAccess`, `NoWindowsUpdate` ; Les mises à jour automatiques ne doivent pas entraver le fonctionnement du processus Windows Update.

Validation :

- Pour les instances du système d'exploitation Linux utilisant le gestionnaire de packages yum, vous pouvez valider la disponibilité des mises à jour en exécutant `#yum check-update`
- Pour les systèmes d'exploitation Linux RedHat 5.7 et versions ultérieures, 6.1 et versions ultérieures, et 7.0 et versions ultérieures ; les EC2 instances Amazon ont migré vers votre compte AMS via le CT « Stack from migration partner migrated instance » (ct-257p9zjk14ija), vous devez valider le statut du gestionnaire d'abonnements pour connaître les performances des mises à jour.
- Sur le système d'exploitation Windows, activez Windows Server Update Services (WSUS). Aucune politique locale ne devrait empêcher WSUS de scanner ou d'installer des mises à jour. Une fois connecté en tant qu'administrateur, vous pouvez le valider en analysant les mises à jour disponibles depuis la console Windows Update Service. Les versions du système d'exploitation Windows Server, y compris 2012R2, 2016 et 2019, comportent des paramètres Windows Update par défaut pour le téléchargement et l'installation. Vous pouvez configurer les paramètres souhaités avant de procéder à la numérisation. Dans les versions ultérieures du système d'exploitation, cette opération peut déclencher l'installation ; configurez au préalable le comportement souhaité.
- Demandez une validation à l'équipe des opérations AMS en soumettant une demande de service : « Document AWSManagedServices-CheckPatchingPrerequisites d'automatisation à exécuter sur une EC2 instance Amazon pour évaluer l'état de préparation des correctifs ».

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.

Fenêtres de correctifs

Les instances d'un groupe de correctifs spécifique sont corrigées pendant une ou plusieurs fenêtres de correctifs. Les fenêtres de correctifs s'exécutent selon un calendrier défini sous la forme d'une expression cron ou rate, et ont une durée configurable destinée à maintenir les interruptions liées aux correctifs dans un intervalle de temps choisi. AMS recommande de créer plusieurs fenêtres de correctifs qui couvrent collectivement toutes vos instances, afin de correspondre aux routines d'application de correctifs spécifiques de votre organisation et d'utiliser la fenêtre de maintenance par défaut comme solution de secours. Les fenêtres de correctifs sont créées avec le type de modification RFC Deployment | Patching | Window de patch SSM | Create (ct-0e12j07llrxs7). Toutes

les instances qui ne font pas partie d'une fenêtre de correctifs sont corrigées pendant la fenêtre de maintenance par défaut créée lors de l'intégration.

Normalement, il n'est pas nécessaire de mettre à jour une fenêtre de correctif pour inclure de nouvelles instances. Cela se fait généralement en modifiant les balises d'instance. Par exemple, considérez la séquence d'événements suivante :

1. Deux instances sont étiquetées

`avecAppId:MyApplication,Environment:Production,Group:1.`

Cela produit une balise sur ces instances, en supposant que la première clé de balise = AppId, la deuxième clé de balise = environnement, la troisième clé de balise = groupe et qu'une fenêtre de correctifs pour le groupe de correctifs MyApplication -Production-1 est créée.

2. Trois autres instances sont créées et étiquetées

`avecAppId:MyApplication,Environment:Production,Group:1.`

Cela produit une balise pour Patch Group : MyApplication -Production-1.

Aucune modification de la fenêtre de correctif n'est nécessaire car elle récupère les cinq instances lors de la prochaine exécution planifiée.

Pour une discussion plus détaillée et une présentation détaillée de l'utilisation de ce type de modification, voir [SSM Patch Window | Create](#).

Notifications de correctifs

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.

Les adresses e-mail abonnées (jusqu'à cinq) reçoivent un e-mail similaire au suivant juste avant le début de la fenêtre de maintenance des correctifs :

Dear Customer,
The AMS Patch Maintenance Window *THE_MAINTENANCE_WINDOW_NAME* was started at:
2020-02-21T12:02:18.196Z.
Details:
Maintenance Window AccountId: *YOUR_ACCOUNT_ID*

```

Maintenance Window Region:    YOUR_ACCOUNT_REGION
Maintenance Window Id:        THE_MAINTENANCE_WINDOW_ID
Maintenance Window Name:      THE_MAINTENANCE_WINDOW_NAME
Maintenance Window Description: MaintenanceWindow for patching patch
Group PATCH_GROUP_NAME
Maintenance Window Patch Group: PATCH_GROUP_NAME
Maintenance Window ExecutionId: THE_EXECUTION_ID

Targets:
InstanceId      InstanceName      StackId
-----
THE_INSTANCE_ID  THE_INSTANCE_NAME  THE_STACK_NAME

```

A follow-up message with a detailed report is sent as soon as the maintenance window is over.

Please raise a service request if you have any inquires about AMS Patch Orchestrator by following this URL:

<https://console.aws.amazon.com/managedservices/servicerequest/new>

Kind Regards,

Amazon Web Services
Amazon Managed Services
Patch Team

À la fin de l'activité du correctif, les adresses e-mail abonnées reçoivent un e-mail similaire au suivant :

```

Dear Customer,
The AMS Patch Maintenance Window THE_MAINTENANCE_WINDOW_NAME ended at:
2020-02-21T12:03:20.058Z, with status: SUCCESS.
Details:
Maintenance Window AccountId:  YOUR_ACCOUNT_ID
Maintenance Window Region:     YOUR_ACCOUNT_REGION
Maintenance Window Id:         THE_MAINTENANCE_WINDOW_ID
Maintenance Window Name:       THE_MAINTENANCE_WINDOW_NAME
Maintenance Window Description: MaintenanceWindow for patching patch
Group PATCH_GROUP_NAME
Maintenance Window Patch Group: PATCH_GROUP_NAME
Maintenance Window ExecutionId: THE_EXECUTION_ID

Targets:
RfcId      InstanceId      InstanceName      StackId
-----
Status

```

THE_RFC_ID THE_INSTANCE_ID THE_INSTANCE_NAME THE_STACK_NAME
STATUS

You can view the current Patch Compliance of your Amazon EC2 Instances by following this URL:

https://console.aws.amazon.com/systems-manager/compliance?region=YOUR_ACCOUNT_REGION

Please raise an Incident if an issue is impacting one of your production applications by following this URL:

<https://console.aws.amazon.com/managedservices/incident/new>

Kind Regards,

Amazon Web Services
 Amazon Managed Services
 Patch Team

Toutes les 96 heures, le système de correctifs AMS identifie toutes les fenêtres de maintenance gérées par les correctifs à venir au cours de ces 96 heures et envoie une notification de rappel à toutes les adresses e-mail abonnées comprises dans cette fenêtre de 96 heures. Cela peut se faire à peine une heure avant la fenêtre ou pendant les 96 heures complètes. Exemples :

Dear Customer,

The AMS Patch Maintenance Window *THE_MAINTENANCE_WINDOW_NAME* will start at:
 2020-05-06T16:35:36.523Z.

Details:

Maintenance Window AccountId: *YOUR_ACCOUNT_ID*
 Maintenance Window Region: *YOUR_ACCOUNT_REGION*
 Maintenance Window Id: *THE_MAINTENANCE_WINDOW_ID*
 Maintenance Window Name: *THE_MAINTENANCE_WINDOW_NAME*
 Maintenance Window Description: MaintenanceWindow for patching patch

Group *PATCH_GROUP_NAME*

Maintenance Window Patch Group: *PATCH_GROUP_NAME*
 Maintenance Window Next Start Time: 2020-05-06T16:35:36.523Z
 Maintenance Window Schedule: rate(24 hours)
 Maintenance Window Timezone: *THE_TIMEZONE*

At this time, these are the instances in the "*PATCH_GROUP_NAME*" Patch Group:

InstanceId	InstanceName	StackId	InstanceState

<code>THE_INSTANCE_ID</code>	<code>THE_INSTANCE_NAME</code>	<code>THE_STACK_NAME</code>	running/stopped
<code>THE_INSTANCE_ID</code>	<code>THE_INSTANCE_NAME</code>	<code>THE_STACK_NAME</code>	running/stopped
<code>THE_INSTANCE_ID</code>	<code>THE_INSTANCE_NAME</code>	<code>THE_STACK_NAME</code>	running/stopped

A notification message is sent as soon as the maintenance window starts.

You can view the current Patch Compliance of your Amazon EC2 Instances by following this URL:

https://console.aws.amazon.com/systems-manager/compliance?region=YOUR_ACCOUNT_REGION

If you would like to disable this maintenance window or you have inquires about the AMS Patch Orchestrator click on the following URL:

<https://console.aws.amazon.com/managedservices/servicerequest/new>

If you would like to delete this maintenance window, you can run the CT with id "ct-0q0bic0ywqk6c" against the stack id "stack-rctyznutkyj4tkkzq".

Kind Regards,

Amazon Web Services
Amazon Managed Services
Patch Team

Références de correctifs

Par défaut, tous les correctifs fournis par le fournisseur du système d'exploitation (OS) sont installés à l'aide de la ligne de base de correctifs par défaut d'AMS. Si vous souhaitez limiter les correctifs installés, vous pouvez éventuellement créer une ligne de base de correctifs à l'aide du type de modification RFC Deployment | Patching | Baseline de patch SSM | Create **OS** (l'ID CT varie en fonction du système d'exploitation).

Pour plus d'informations sur l'utilisation de ces types de modifications, consultez la [sous-catégorie Patching](#).

Balises réservées à Patch Orchestrator

Patch Orchestrator génère également les balises suivantes qui ne peuvent pas être modifiées :

- **AMSPatchGroup** — Cette balise est utilisée pour générer la valeur des balises Patch Group. Vous ne devez pas modifier le AMSPatch groupe. Vous pouvez modifier la balise « Patch Group » si vous souhaitez utiliser une valeur personnalisée « Patch Group ». Patch Orchestrator continue de générer une valeur pour AMSPatch Group en fonction des clés de balise fournies lors de

l'intégration, mais ne modifiera pas la valeur de balise « Patch Group » si vous l'avez définie sur une valeur personnalisée. Pour arrêter d'utiliser une valeur personnalisée de « groupe de correctifs », vous pouvez définir la valeur de « groupe de correctifs » pour qu'elle corresponde à la valeur de la balise de AMSPatch groupe.

- AMSDefaultPatchGroup— Cette balise indique si une instance fait partie de la fenêtre de maintenance par défaut, avec une valeur True ou False. Si le groupe de correctifs d'une instance n'est pas affecté à une fenêtre de maintenance, cette valeur est définie sur True.

Correctifs à la demande

AMS propose un type de modification qui fonctionne avec votre ligne de base de correctifs, afin de vous permettre d'exécuter un correctif sur des instances à la demande. Il peut s'agir de la ligne de base par défaut que vous avez définie lors de l'intégration ou de la ligne de base de correctifs de Patch Orchestrator Systems Manager que vous avez définie avec le type de modification de la ligne de base de correctifs (l'ID CT varie en fonction du système d'exploitation).

Vous pouvez utiliser le type de modification des correctifs à la demande avec ou sans Patch Orchestrator.

Pour plus d'informations sur l'utilisation de ce type de modification, voir Application [de correctifs à la demande](#) | [Exécuter](#).

Note

Vous ne pouvez pas utiliser d'instances faisant partie d'un groupe Auto Scaling dans un type de modification par application de correctifs à la demande.

Correctif standard AMS

AMS prend en charge les clients existants en utilisant le modèle de correctif standard AMS, mais ce modèle n'est pas disponible pour les nouveaux clients et est en train d'être retiré au profit d'AMS Patch Orchestrator.

Le contenu typique des correctifs pour les correctifs standard AMS inclut les mises à jour du fournisseur pour les systèmes d'exploitation pris en charge et les logiciels préinstallés avec les systèmes d'exploitation pris en charge (par exemple, IIS et Apache Server).

Lors de l'intégration d'AMS, vous spécifiez les exigences en matière de correctifs, la politique, la fréquence et les fenêtres de correctifs préférées. Grâce à ces configurations, vous pouvez éviter de mettre les applications hors ligne en une seule fois pour appliquer des correctifs à l'infrastructure. Vous pouvez ainsi contrôler quelle infrastructure doit être corrigée et à quel moment.

Note

Le processus d'application de correctifs décrit dans cette rubrique s'applique uniquement à vos piles. L'infrastructure AMS est corrigée au cours d'un processus distinct. La fenêtre de maintenance (ou fenêtre de maintenance) AWS Managed Services (ou fenêtre de maintenance) exécute les activités de maintenance d'AWS Managed Services (AMS) et a lieu le deuxième jeudi de chaque mois de 15 h 00 à 16 h 00, heure du Pacifique. AMS peut modifier le créneau de maintenance avec un préavis de 48 heures. Vous configurez la fenêtre de correctifs AMS lors de l'intégration, ou vous approuvez ou rejetez la notification mensuelle du service de correctifs.

AMS analyse régulièrement les EC2 instances Amazon gérées pour détecter les mises à jour disponibles via la fonctionnalité de mise à jour du système d'exploitation. Nous fournissons également des mises à jour régulières de la base AMS Amazon Machine Images (AMIs) prise en charge dans notre environnement.

Une fois validées, les versions de l'AMI AMS sont partagées avec tous les comptes AMS. Vous pouvez consulter les versions AWS AMI disponibles en utilisant l'appel [DescribeImages](#) d'EC2 API Amazon ou en utilisant la EC2 console Amazon. Pour trouver les AMS disponibles AMIs, voir [Trouvez AMI IDs, AMS](#).

AMS exécute des programmes d'application de correctifs ad hoc uniquement lorsque vous le demandez. Auparavant, AMS envoyait une notification ; actuellement, aucune notification n'est envoyée.

Note

Par défaut, AMS utilise Systems Manager pour appliquer des correctifs en demandant au gestionnaire de packages (Linux) ou au service System Update (Windows) d'interroger son référentiel par défaut pour voir quels nouveaux packages sont disponibles. Si, au cours de vos day-to-day opérations, vous avez installé un package sur un hôte Linux à l'aide du gestionnaire de packages par défaut, ce dernier récupère également les nouveaux packages

pour ce logiciel lorsqu'ils sont disponibles. Dans ce cas, vous souhaitez peut-être effectuer une action de correction (décrite dans cette section) pour vous désinscrire de cette instance.

Systèmes d'exploitation pris en charge

Systèmes d'exploitation pris en charge (x86-64)

- 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 pris en charge (ARM64)

- Amazon Linux 2023
- Amazon Linux 2 (date de fin de support AMS prévue le 30 juin 2026)

Patches pris en charge

AWS Managed Services prend en charge l'application de correctifs principalement au niveau du système d'exploitation. Les correctifs installés peuvent varier en fonction du système d'exploitation.

Important

Toutes les mises à jour sont téléchargées depuis les référentiels distants du service de base de correctifs de Systems Manager configurés sur l'instance et décrits plus loin dans cette rubrique. L'instance doit être en mesure de se connecter aux référentiels pour que le correctif puisse être effectué.

Pour désactiver le service de base de correctifs pour les référentiels qui fournissent des packages que vous souhaitez gérer vous-même, exécutez la commande suivante pour désactiver le référentiel :

```
yum-config-manager DASHDASHdisable REPOSITORY_NAME
```

Récupérez la liste des référentiels actuellement configurés à l'aide de la commande suivante :

```
yum repolist
```

- Référentiels préconfigurés Amazon Linux (généralement quatre) :

ID du référentiel	Nom du référentiel
amzn-main/latest	Base principale AMZN
mises à jour/dernières mises à jour d'amzn-	Base de mises à jour AMZN
épel/x86_64	Packages supplémentaires pour Enterprise Linux 6 - x86_64
pbis	Mises à jour des packages PBIS

- Référentiels préconfigurés Red Hat Enterprise Linux (cinq pour Red Hat Enterprise Linux 7 et cinq pour Red Hat Enterprise Linux 6) :

ID du référentiel	Nom du référentiel
Région RHUI- -7/x86_64 client-config-server	Ensemble de configuration du client Red Hat Update Infrastructure 2.0
Région RHUI- /7Server/x86_64 rhel-server-releases	Serveur Red Hat Enterprise Linux 7
Région RHUI- /7Server/x86_64 rhel-server-releases	Red Hat Enterprise Linux Server 7 RH Common (RPMs)
épel/x86_64	Packages supplémentaires pour Enterprise Linux 7 - x86_64

ID du référentiel	Nom du référentiel
pbis	Mises à jour des packages PBIS
ID du référentiel	Nom du référentiel
Région de Rhui--6 client-config-server	Red Hat Update Infrastructure 2.0
Région du Rhui- rhel-server-releases	Serveur Red Hat Enterprise Linux (6RPMs)
Région du Rhui- rhel-server-rh-common	Red Hat Enterprise Linux Server 6 RH Common (RPMs)
peler	Packages supplémentaires pour Enterprise Linux 6 - x86_64
pbis	Mises à jour des packages PBIS

- Référentiels préconfigurés CentOS 7 (généralement cinq) :

ID du référentiel	Nom du référentiel
base/7/x86_64	CentOS-7 - Base
mises à jour/7/x86_64	CentOS-7 - Mises à jour
extras/7/x86_64	CentOS-7 - Suppléments
épel/x86_64	Packages supplémentaires pour Enterprise Linux 7 - x86_64
pbis	Mises à jour des packages PBIS

- Pour Microsoft Windows Server, toutes les mises à jour sont détectées et installées à l'aide de l'agent Windows Update, qui est configuré pour utiliser le catalogue Windows Update (cela n'inclut pas les mises à jour de Microsoft Update).

Sur les systèmes d'exploitation Microsoft Windows, Patch Manager utilise le fichier CAB wsusscn2.cab de Microsoft comme source des mises à jour de sécurité du système d'exploitation

disponibles. Ce fichier contient des informations sur les mises à jour liées à la sécurité que Microsoft publie. Patch Manager télécharge régulièrement ce fichier auprès de Microsoft et l'utilise pour mettre à jour l'ensemble des correctifs disponibles pour les instances Windows. Le fichier contient uniquement des informations que Microsoft identifie comme liées à la sécurité. À mesure que les informations du fichier sont traitées, le Gestionnaire de correctifs supprime également les mises à jour ayant été remplacées par des mises à jour ultérieures. Par conséquent, seule la mise à jour la plus récente est affichée et disponible pour être installée. Par exemple, si KB4 012214 remplace 012214 KB3135456, seul KB4 012214 est disponible sous forme de mise à jour dans le Gestionnaire de correctifs.

Pour en savoir plus sur le fichier wsusscn2.cab, consultez l'article de Microsoft [utilisant WUA pour rechercher des mises à jour hors ligne](#).

Conception des correctifs et de l'infrastructure

AMS utilise différentes méthodes de correction en fonction de la conception de votre infrastructure : mutables ou immuables (pour des définitions détaillées, voir). [Termes clés d'AMS](#)

Dans le cas des infrastructures mutables, les correctifs sont effectués selon une méthodologie traditionnelle sur place qui consiste à installer les mises à jour directement sur les EC2 instances Amazon, individuellement, par les ingénieurs d'exploitation d'AMS. Cette méthode d'application de correctifs est utilisée pour les piles qui ne sont pas des groupes Auto Scaling et qui contiennent une ou plusieurs EC2 instances Amazon. Dans ce scénario, le remplacement de l'AMI sur laquelle l'instance ou la pile était basée détruirait toutes les modifications apportées à ce système depuis son déploiement initial. Cela n'est donc pas fait. Les mises à jour sont appliquées au système en cours d'exécution, et il est possible que le système soit indisponible (selon la configuration de la pile) en raison du redémarrage de l'application ou du système. Cela peut être atténué par une stratégie de Blue/Green mise à jour. Pour plus d'informations, voir Présentation des [AWS CodeDeploy Blue/Green déploiements](#).

Dans le cas d'infrastructures immuables, la méthode d'application de correctifs consiste à remplacer les AMI. Les instances immuables sont mises à jour de manière uniforme à l'aide d'une AMI mise à jour qui remplace l'AMI spécifiée dans la configuration du groupe Auto Scaling. AMS publie des mises à jour (c'est-à-dire corrigées) AMIs tous les mois, généralement la semaine du Patch Tuesday. La section suivante décrit comment cela fonctionne.

Comment fonctionne l'application de correctifs standard AMS

AMS utilise le service Systems Manager Run Command pour l'application régulière de correctifs mensuels et selon les besoins, avec deux méthodes principales d'application des correctifs, sur place et en remplacement des AMI, en fonction de la stratégie de déploiement de votre infrastructure (mutable ou immuable). Cette section décrit le service de correctifs AMS, ses types, ses méthodes et ses processus.

AMS définit deux types de correctifs, qui sont planifiés différemment :

- **Correctifs critiques** : les mises à jour sont appliquées le plus rapidement possible, après acceptation de l'avis.
- **Correctifs standard** : mises à jour régulières du fournisseur du système d'exploitation et appliquées tous les mois.

Les correctifs sont appliqués soit par application de correctifs sur place, soit par remplacement de l'AMI (sur demande).

Mettre à jour le scan

AMS utilise le [service Amazon EC2 Run Command](#) pour contacter vos Amazon EC2 Stacks et déployer les scripts de numérisation et de correction requis. AMS utilise le composant natif de gestion des packages déjà installé sur le système d'exploitation pris en charge pour effectuer tous les comportements d'analyse et de correction requis sur la EC2 pile Amazon. Pour Red Hat et Amazon Linux, le service utilise yum. Pour Windows, le service utilise l'agent Windows Update.

Les scans sont effectués quotidiennement à l'aide de [SSM Maintenance Windows](#) et du RunPatchBaseline document AWS par défaut d'AMS. Chaque EC2 pile Amazon accessible est analysée à l'aide des référentiels de mise à jour pour Linux et Windows. Le processus de correction AMS détecte toutes les EC2 piles Amazon accessibles, puis effectue les analyses par lots afin que la pile reste toujours saine, même en cas de défaillance lors de l'exécution du scan. Les résultats du scan sont ensuite enregistrés pour chaque EC2 pile Amazon.

Pour consulter les résultats de l'analyse d'une pile ou d'une instance, soumettez une demande de service avec l'ID de pile ou d'instance.

Le processus d'application des correctifs AMS par défaut consiste à installer tous les correctifs disponibles, indépendamment de leur classification ou de leur gravité (par exemple, critique ou

standard). Les correctifs que vous avez explicitement exclus de la pile font exception à cette règle (les correctifs définis comme obligatoires par AMS ne doivent pas être exclus).

Vous recevez une notification de service d'application de correctifs 14 jours avant la période de maintenance proposée. Cela vous laisse le temps de tester les correctifs proposés et de les accepter ou de les rejeter. Si vous ne répondez pas à la notification du service d'application de correctifs, vos instances ne sont pas corrigées. Au moment d'installer les correctifs, AMS crée une demande de modification (RFC) pour chaque pile, et cette RFC apparaît dans la liste des RFC de votre compte.

Fenêtre et avis de maintenance configurés par AMS

Avec les correctifs configurés par AMS, chaque compte dispose d'une fenêtre de maintenance mensuelle, que vous définissez lors de l'intégration de votre compte. La fenêtre de maintenance (ou fenêtre de maintenance) AWS Managed Services (ou fenêtre de maintenance) exécute les activités de maintenance d'AWS Managed Services (AMS) et a lieu le deuxième jeudi de chaque mois de 15 h 00 à 16 h 00, heure du Pacifique. AMS peut modifier le créneau de maintenance avec un préavis de 48 heures.

La fenêtre d'application des correctifs est différente. La demande de service sortante d'application de correctifs (également appelée notification de service) inclut une fenêtre de correctifs suggérée.

Note

Pour plus d'informations sur la réponse à la notification du service d'application de correctifs, consultez [Actions que vous pouvez effectuer dans le cadre de l'application de correctifs standard AMS](#)

La notification du service de correctifs est envoyée par e-mail à l'adresse e-mail de contact enregistrée pour votre compte. La notification inclut un lien vers la console AWS Support où vous pouvez y répondre. Vous pouvez également répondre à la notification via la page de demande de service AMS. La notification de service inclut :

- Une liste des mises à jour IDs (CSUs, IUs, et OUs) qui s'appliquent à la pile, ainsi que les mises à jour que vous avez demandées à exclure de l'application de correctifs (le cas échéant).
- IDs des instances qui seront affectées.
- Une fenêtre de correction proposée dans laquelle les mises à jour seront appliquées. Vous pouvez demander une autre fenêtre d'application des correctifs.

- Une demande demandant que vous acceptiez le correctif proposé ou que vous demandiez des informations supplémentaires. AMS vous donne le temps de tester l'impact des mises à jour et d'approuver ou de rejeter les correctifs, ou de demander que des mises à jour spécifiques soient exclues. Si vous avez besoin de plus de temps pour effectuer les tests et que vous souhaitez que les mises à jour soient appliquées après les tests, répondez à la notification de service et décrivez ce que vous souhaitez, ou soumettez une demande de service pour un nouveau correctif RFC en vous basant sur les détails de la RFC précédente. Si vous ne répondez pas du tout à la notification de service, aucune action corrective n'est entreprise et le RFC est annulé.

Si vous approuvez la notification de service, AMS exécute le correctif RFC et applique les mises à jour dans le délai convenu, conformément à l'engagement de service.

Lorsque l'application des correctifs est terminée, AMS vous envoie une correspondance dans la demande de service, avec un résumé du résultat de l'activité d'application des correctifs (réussite ou échec).

Correctifs sur place

L'application de correctifs sur place fait référence à une méthode par laquelle AMS se connecte à chaque instance de pile et applique des correctifs.

Les correctifs sur place sont appliqués sur des infrastructures mutables à l'aide d' EC2 instances Amazon exécutant un système d'exploitation compatible. L'application de correctifs s'applique à toutes les mises à jour non exclues disponibles jusqu'à présent. Lorsque des correctifs critiques sont publiés, un processus de correction critique supplémentaire est mis en œuvre.

Correctif standard : sur place

Les correctifs standard sont exécutés selon le calendrier de correctifs convenu suggéré dans la notification du service de correctifs, et incluent des mises à jour régulières des correctifs qui ne sont pas considérées comme critiques.

Avant la fenêtre de correction proposée, et avec votre réponse affirmative à la notification, une RFC de correctifs est créée et apparaît dans votre tableau de bord RFC.

Correctifs critiques : sur place

Lorsqu'un fournisseur de système d'exploitation publie une mise à jour de sécurité critique, AMS vous informe du correctif RFC en vous envoyant une notification de service (à l'adresse e-mail de

contact associée à votre compte) pour chaque pile, conformément à l'engagement de service AMS. La notification de service inclut les informations suivantes pour chaque mise à jour :

- Mettre à jour la date de sortie
- Criticité des mises à jour
- Détails de la mise à jour (référence KB, etc.)
- IDs des piles touchées

Vous pouvez tester les mises à jour répertoriées dans la notification et approuver ou rejeter les correctifs en répondant à la notification de service. Si vous approuvez la notification, vous devez fournir une fenêtre de correctif spécifique par pile pour l'installation des mises à jour.

 Note

Les fenêtres de correctifs qui se situent dans les 24 heures suivant la réponse à la notification de service peuvent être reprogrammées en fonction de la capacité disponible.

Si vous ne répondez pas dans les 10 jours ou si vous rejetez le correctif proposé, le correctif est annulé.

Si vous souhaitez appliquer les mises à jour après la période autorisée (indiquée dans la notification), soumettez une demande de service pour un nouveau calendrier de correctifs basé sur les détails de la notification précédente.

Si vous approuvez la notification de service, AMS applique les mises à jour dans la fenêtre de correctif que vous avez spécifiée, conformément à l'engagement de service.

Dans le cas de mises à jour multiples, vous pouvez exclure des mises à jour spécifiques des correctifs en spécifiant les mises à jour à exclure dans votre réponse à la notification de service.

AMS vous envoie une notification de service pour chaque pile, indiquant le résultat de chaque mise à jour (réussite ou échec).

AMI met à jour les correctifs (en utilisant des correctifs AMIs pour les groupes Auto Scaling)

Les correctifs de remplacement des AMI sont effectués sur des infrastructures immuables en mettant à jour l'ID d'AMI configuré pour déployer de nouvelles EC2 instances Amazon dans un groupe Auto Scaling.

Amazon Machine Images (AMIs) est publié régulièrement pour les systèmes d'exploitation pris en charge. Les fournisseurs de systèmes d'exploitation publient régulièrement de nouveaux correctifs. AMS utilise l'AMI fournie par Amazon, la met à jour avec les derniers correctifs, puis ajoute les composants appropriés pour lui permettre de fonctionner dans l'environnement AMS. Ensuite, il met la nouvelle AMI AMS à la disposition de tous les clients AMS en partageant l'AMI avec les comptes. Les piles de votre groupe Auto Scaling peuvent être actualisées tous les mois grâce à ces nouveaux AMS. AMIs Le graphique suivant illustre comment AMIs sont utilisés dans AMS vos environnements.

Les groupes Auto Scaling créent leurs instances en fonction de l'AMI configurée pour le groupe Auto Scaling. Lorsque les partages AMS sont mis à jour AMIs, vous disposez des options suivantes en fonction de la façon dont vous gérez les mises à jour des AMI :

- Si vous utilisez un outil de déploiement d'applications (par exemple UserData, CodeDeploy, etc.) qui personnalise automatiquement vos instances après leur création, vous pouvez effectuer les opérations suivantes :
 - Répondez à la notification du service d'application de correctifs ou soumettez une demande de service pour obtenir la dernière AMI AMS afin de remplacer l'AMI de configuration de votre groupe Auto Scaling actuel. Après le remplacement de l'ID d'AMI dans la configuration de vos groupes Auto Scaling, AMS lance les mises à jour continues de vos instances et les configurations de vos instances de groupe Auto Scaling (par exemple, l'installation d'applications, de scripts de démarrage, etc.) sont automatiquement appliquées aux nouvelles instances créées avec la nouvelle AMI AMS.
- Si vous utilisez une custom/golden AMI dans la configuration de vos groupes Auto Scaling, vous pouvez :
 - Créez une instance avec la nouvelle AMI AMS, personnalisez-la et créez une nouvelle AMI dorée. Partagez la nouvelle AMI dorée avec AMS à l'aide de la EC2 console Amazon et soumettez une demande de service à AMS pour mettre à jour la configuration de vos groupes Auto Scaling afin d'utiliser votre nouvelle AMI personnalisée.

- Partagez votre AMI dorée existante avec AMS à l'aide de la EC2 console Amazon et soumettez une demande de service pour qu'AMS mette à jour votre AMI dorée. Pour ce faire, AMS crée une instance à partir de votre AMI dorée, applique les correctifs à cette instance, crée une nouvelle AMI dorée pour vous, puis met à jour la configuration de vos groupes Auto Scaling pour utiliser la nouvelle AMI. L'inconvénient est qu'AMS ne peut pas vérifier que votre nouvelle AMI personnalisée fonctionne comme vous le souhaitez. Vous devez plutôt tester l'instance créée avec la nouvelle AMI et vérifier que tout fonctionne correctement avant de créer une nouvelle AMI dorée, de la partager et de demander à AMS de mettre à jour vos groupes Auto Scaling. AMS ne recommande pas cette option.

Correctifs standard : mises à jour de l'AMI

Chaque mois, AMS publie de nouvelles Amazon Machine Images (AMIs) avec des améliorations de service et de nouveaux correctifs qui s'appliquent aux AMIs.

Note

Les nouveaux AMS AMIs sont générés après le Patch Tuesday à partir de la mise à jour d'AWS AMIs. AMS les teste ensuite avant de les mettre à disposition. Après le nouveau test de AMIs réussite, AMS partage des comptes gérés mis AMIs à jour.

Correctifs critiques : mises à jour de l'AMI

En cas de besoin, AMS fournit des AMIs mises à jour avec des correctifs de sécurité critiques publiés depuis la dernière version mensuelle de l'AMI.

Le processus des mises à jour de sécurité critiques pour les infrastructures immuables est identique au processus mensuel des AMI pour les infrastructures immuables, sauf qu'une nouvelle AMI AMS est créée en dehors du calendrier normal (Patch Tuesday), sur la base de la publication de nouvelles mises à jour critiques. AMS met à disposition une nouvelle AMI contenant les correctifs de sécurité critiques conformément aux accords de niveau de service (SLAs) définis pour votre compte. Mises à jour AMS des groupes Auto Scaling uniquement sur demande. Utilisez une demande de service pour soumettre des demandes de remplacement d'AMI.

Défaillances des correctifs standard AMS

En cas d'échec des mises à jour, AMS effectue une analyse pour comprendre la cause de l'échec et vous communique le résultat de l'analyse. Si la panne est imputable à AMS, nous réessayons les

mises à jour pendant la période de maintenance. Dans le cas contraire, AMS crée des notifications de service pour l'échec de la mise à jour de l'instance et attend vos instructions.

En cas de panne imputable à votre système, vous pouvez soumettre une demande de service avec un nouveau correctif RFC pour mettre à jour les instances.

Actions que vous pouvez effectuer dans le cadre de l'application de correctifs standard AMS

Outre le fait d'en tester de nouvelles AMIs, vous pouvez prendre plusieurs mesures pour gérer l'application de correctifs à votre infrastructure :

- Si le test des mises à jour a pris plus de temps que le délai autorisé par la fenêtre de correctif, vous pouvez demander à AMS d'appliquer les mises à jour annulées lorsque vous êtes prêt en soumettant une demande de service (utilisez les informations figurant dans la notification de service d'origine comme base).
- Vous pouvez demander qu'une mise à jour importante (UI) ou une autre mise à jour (UO) soit appliquée avant la prochaine fenêtre de mise à jour automatique en soumettant une demande de service fournissant une liste des mises à jour, les instances applicables et d'autres informations, le cas échéant. Comme cette tomographie n'est pas automatisée, sa planification et son exécution prennent plus de temps. Vérifiez les objectifs de niveau de service (SLOs) au moment opportun. Pour de plus amples informations, veuillez consulter [Objectifs de niveau de service AMS \(SLOs\)](#).

En outre, vous pouvez utiliser un AMS existant, patché, AMIs pour créer des messages personnalisés AMIs. Pour plus d'informations, voir [AMI | Create](#).

Note

Vous ne pouvez pas demander une nouvelle AMI AMS sur la base d'une mise à jour importante ou d'une autre mise à jour avant la prochaine fenêtre de maintenance, car le processus de publication de l'AMI AMS suit une cadence uniforme au profit de tous les clients AMS.

Changer ce qui patched/opting en sort

Avec les correctifs configurés par AMS, dans votre réponse à la notification du service d'application de correctifs ou dans le cadre d'une demande de service, vous pouvez modifier les ressources auxquelles des correctifs sont appliqués. Vous pouvez effectuer les actions suivantes :

- Définissez une liste de correctifs à exclure de la correction, par pile et par système d'exploitation.
- Définissez une liste de ressources qui doivent être exclues de certains correctifs ou de tous les correctifs.
- Définissez une liste de ressources qui doivent toujours être exclues de tous les correctifs.
- Définissez une liste de ressources qui doivent être corrigées à un jour et à une heure donnés (utile si vous n'avez pas défini de fenêtre de maintenance).

Pour exclure un ou plusieurs correctifs, soumettez une demande de service ou répondez à la notification du service d'application de correctifs à l'aide du modèle fourni ci-dessous. Ne soumettez pas de RFC. Incluez dans la demande le ou les noms du correctif que vous souhaitez exclure et pourquoi. Incluez ces informations dans une demande de service comme suit :

- Nom : nom du correctif. Pour les correctifs Windows, il s'agit du nom de la base de connaissances, par exemple KB3145384. Pour les correctifs Linux, il s'agit du nom du package, par exemple openssh-6.6.1p1-25.61.amzn1.x86_64.
- Motif : commentaire indiquant pourquoi le correctif est exclu.
- Date d'expiration : date/time date d'expiration de l'exclusion.

Si un correctif exclu est déjà installé, il est supprimé.

La demande est examinée par un opérateur qui en discutera avec vous si l'exclusion de ces correctifs présente un risque de sécurité important. La date d'expiration des patchs exclus est également négociée. Après la date d'expiration convenue, l'exclusion expire et le correctif est installé lors de tout correctif ultérieur.

Les correctifs figurant sur la liste d'exclusion sont toujours renvoyés dans les résultats de l'analyse, le cas échéant.

Note

Contrairement à Windows, les correctifs Linux sont spécifiques à chaque version. Cette distinction est importante car les nouvelles versions d'un correctif exclu ne sont pas automatiquement exclues. Il est de votre responsabilité de demander à AMS d'exclure les nouvelles versions d'un correctif Linux si c'est ce que vous souhaitez faire.

Modèles de réponse aux notifications du service de correctifs

Vous devez répondre aux notifications du service d'application de correctifs, en utilisant le format spécifié, pour que les correctifs soient appliqués à vos instances. Vous devez le faire si vous n'avez pas encore défini de fenêtre de maintenance avec AMS.

Lorsque vous répondez à une notification de service, utilisez le format indiqué.

Si aucune fenêtre de maintenance n'est définie, indiquez-nous quand appliquer les correctifs, comme indiqué ci-dessous :

UTC	StartTime	StackId	InstanceId (Optional)
2019-04-01	15:00	stack-123456789012	i-1234566789
2019-04-01	15:00	stack-123456789013	i-1234566784
2019-04-01	15:00	stack-123456789014	i-1234566783
2019-04-01	15:00	stack-123456789015	i-1234566782

Si vous avez défini une période de maintenance et que vous souhaitez que certaines ressources soient exclues de certains correctifs, utilisez le format suivant :

StackId	InstanceId (Optional)	Exclude Patches
stack-123456789012	i-1234566789	<i>PATCH</i>
stack-123456789013	i-1234566784	<i>PATCH</i>
stack-123456789014	i-1234566783	<i>PATCH</i>
stack-123456789015	i-1234566782	<i>PATCH</i>

Si vous disposez d'une fenêtre de maintenance définie et que vous souhaitez que certaines ressources soient toujours exclues de tous les correctifs, utilisez le format suivant :

StackId	InstanceId (Optional)	Exclude Patches
stack-123456789012	i-1234566789	ALL

stack-123456789015

i-1234566782

ALL

Préparation à l'application des correctifs

Pour préparer votre environnement à l'application automatique de correctifs, nous vous recommandons ce qui suit :

- Assurez-vous de disposer d'un inventaire complet de toutes les instances à appliquer.
- Assurez-vous que vos ressources sont régulièrement sauvegardées dans le cadre de votre stratégie de continuité des activités. Des sauvegardes supplémentaires sont créées dans le cadre de la séquence de correctifs, et elles sont automatiquement supprimées conformément à la politique de rétention de Patch Orchestrator que vous avez configurée (la valeur par défaut est de 60 jours).
- Assurez-vous que toutes les licences pertinentes sont à jour.
- Modifiez vos fenêtres de maintenance des piles pour échelonner les correctifs afin que les piles de test soient corrigées avant les piles de production. Ainsi, toute erreur liée aux correctifs est détectée dans les piles de test et peut être identifiée avant que les piles de production ne soient corrigées.

Affichage des paramètres du correctif

Pour connaître la configuration actuelle de vos correctifs, vous pouvez effectuer les opérations suivantes :

- Soumettez une demande de service à AMS avec la requête.
- Attendez une notification du service de correctifs. L'avis d'application de correctifs vous indique tous les correctifs à appliquer et les instances à appliquer, et suggère également une fenêtre de correctifs.

Vous pouvez soumettre une demande de service pour modifier les éléments suivants :

- Intervalle d'analyse : délai, en minutes, entre les analyses de conformité effectuées sur les instances de cette pile.

La valeur par défaut est 240 (4 heures).

- NotificationWindow: combien de temps à l'avance (en minutes) d'une modification planifiée (correctif) la notification doit vous être envoyée. La valeur par défaut est 10080 (7 jours).

Correctif standard AMS FAQs

Cette section fournit des réponses à certaines questions fréquemment posées.

- Q : Comment puis-je désactiver l'application de correctifs à l'échelle mondiale ?

R : Pour désactiver globalement l'application de correctifs, déposez une demande de service. Notez que vous ne pouvez pas désactiver les correctifs obligatoires d'AMS. Toutes les piles continueront d'être analysées afin que nous puissions signaler les vulnérabilités.

- Q : Comment exclure des piles spécifiques de l'application de correctifs ?

R : Pour exclure définitivement des piles spécifiques de l'application de correctifs, soumettez une demande de service. Pour exclure certaines piles d'un cycle de correctifs donné, répondez à l'avis d'application des correctifs à venir en indiquant la liste des piles à exclure. Pour plus d'informations, consultez [Changer ce qui patched/opting en sort](#). Notez que vous ne pouvez pas désactiver les correctifs obligatoires.

- Q : Que se passe-t-il si je n'approuve pas une notification du service d'application de correctifs ?

R : Vous disposez de 14 jours pour approuver une demande de service de correctifs standard et de 10 jours pour approuver un avis de correction critique. Si vous n'approuvez pas la demande de service dans le délai imparti, l'engagement de service est annulé et aucun correctif n'est appliqué. Dans le cas de correctifs obligatoires, les correctifs sont appliqués quelle que soit la réponse à la demande de service.

- Q : Comment puis-je exclure l'installation de correctifs et de packages spécifiques ?

R : Pour exclure définitivement des correctifs ou des packages spécifiques, soumettez une demande de service. Pour exclure certains correctifs ou packages d'un cycle de correctifs particulier, répondez à l'avis d'application des correctifs à venir en indiquant la liste des correctifs ou packages à exclure. Pour en savoir plus, consultez [Changer ce qui patched/opting en sort](#). Notez que vous ne pouvez pas désactiver les correctifs obligatoires.

- Q : Que se passe-t-il si un système tombe en panne à la suite d'un correctif ?

R : AMS surveille chaque système. AMS vous envoie une notification de service indiquant le résultat de chaque mise à jour (réussite ou échec) par pile et par instance. Si une défaillance est détectée, AMS enquête, travaille à la restauration de l'instance, puis un ingénieur des opérations AMS tente de le corriger manuellement. Pour plus d'informations, consultez [Défaillances des correctifs standard AMS](#).

- Q : Quelles sont les mises à jour gérées par AMS ?

R : AMS gère les mises à jour au niveau du système d'exploitation dont AMS est informé par le fournisseur. Pour de plus amples informations, veuillez consulter [Patches pris en charge](#).

- Q : Quelles sont les mises à jour qui ne sont pas gérées par AMS ?

R : Les mises à jour au niveau de l'application ne sont pas gérées par AMS.

- Q : Comment les groupes Auto Scaling sont-ils mis à jour ?

R : Les groupes Auto Scaling sont mis à jour avec un remplacement d'AMI dans la configuration du groupe Auto Scaling et effectuent une mise à jour continue. Une mise à jour continue respecte le HealthyHostThreshold réglage de votre configuration d'application des correctifs, qui détermine le nombre d' EC2 instances Amazon d'une pile qui doivent rester actives pendant l'application des correctifs. Pour de plus amples informations, veuillez consulter [AMI met à jour les correctifs \(en utilisant des correctifs AMIs pour les groupes Auto Scaling\)](#).

- Q : Comment installer les mises à jour en dehors du cycle normal ?

R : Pour les mises à jour au niveau du système d'exploitation que vous souhaitez installer en dehors du calendrier normal d'application des correctifs, soumettez une demande de service en utilisant la notification d'application de correctifs que vous avez reçue. Cela peut se produire si le test d'un correctif proposé a duré plus de 21 jours (pour un correctif standard) ou 14 jours (pour un correctif critique). Out-of-bands correctifs peuvent être effectués sur place pour les instances Amazon EC2 autonomes.

- Q : Comment les stacks ou instances nouvellement déployés sont-ils corrigés ?

R : Lorsque vous créez une nouvelle instance Amazon EC2 Stack ou un nouveau groupe Auto Scaling, vous devez toujours spécifier l'AMI AMS la plus récente, sur laquelle figureront déjà les derniers correctifs. Pour les infrastructures mutables, l'application de correctifs en ligne doit être effectuée dès le déploiement de la pile.

Engagements relatifs aux services de correction

En fonction de votre type de déploiement d'infrastructure et de l'importance de la mise à jour, nous fournissons des engagements de service pour les mises à jour de sécurité critiques pour les infrastructures mutables et immuables, ainsi que pour les mises à jour importantes pour les infrastructures mutables et immuables.

Correctifs standard

Il s'agit des engagements de service AMS pour les correctifs standard.

Correctifs standard, infrastructure mutable (correctifs sur place)

Événement/Action	Mesure de l'engagement de service
Des mises à jour importantes sont publiées dans un mois.	L'horloge démarre
Quatorze jours après la création de la notification de correctif standard, AMS vous informe des prochains correctifs prévus par le biais d'une notification de service et par e-mail pour chaque pile. La notification de service inclut : • Une liste des mises à jour IDs (CSUs et IUs) applicables (nécessaires et non appliquées) à la pile, et des mises à jour exclues des correctifs • IDs des piles touchées	L'horloge s'arrête après l'envoi de la notification de service.

Événement/Action	Mesure de l'engagement de service
La fenêtre de maintenance au cours de laquelle les mises à jour seront appliquées Vous testez l'impact des mises à jour et vous approuvez ou rejetez la RFC. Si vous ne répondez pas dans les 14 jours ou si vous refusez le correctif dans votre réponse à la notification de service, aucune action n'est entreprise. Si le test prend plus de 14 jours et que vous souhaitez que les mises à jour soient appliquées après la période de 14 jours, soumettez une demande de service pour un nouveau correctif RFC en vous basant sur les détails du RFC précédent.	Si vous n'approuvez pas ou ne répondez pas dans les 14 jours, la modification en attente est annulée et l'engagement de service pour les mises à jour n'est pas applicable.
Si vous approuvez la notification de service dans les 14 jours, AMS applique les mises à jour. Vous pouvez choisir d'exclure des mises à jour spécifiques d'une RFC en spécifiant les mises à jour à exclure dans votre réponse à la notification de service.	Le compte à rebours démarre si vous approuvez la notification de service dans les 14 jours suivant sa réception. L'horloge s'arrête après la tentative d'installation de la mise à jour.

Événement/Action	Mesure de l'engagement de service
AMS vous envoie une notification de service indiquant le résultat de chaque tentative de mise à jour. La notification de service inclut les informations suivantes : • ID d' EC2 instance Amazon • Succès ou échec de la mise à jour 1 : ARN a1, ARN a2... • Succès ou échec de la mise à jour 2 : ARN b1, ARN b2... • Succès ou échec de la mise à jour N : ARN c1, ARN c2...	Non applicable.
En cas d'échec des mises à jour, AMS effectue une analyse pour comprendre la cause de l'échec et vous communique le résultat de l'analyse. Si la panne est imputable à AMS, AMS réessaie les mises à jour si la fenêtre de maintenance est en cours. Dans le cas contraire, AMS crée des notifications de service pour l'échec de la combinaison instance-mise à jour et attend vos instructions pendant la fenêtre de maintenance.	Non applicable.
Pour les défaillances qui vous sont imputables, soumettez une demande de service pour un nouveau correctif RFC afin de mettre à jour les instances.	Non applicable.

Correctifs critiques

Il s'agit des engagements de service d'AMS pour les mises à jour de sécurité critiques.

Mises à jour de sécurité critiques, infrastructure mutable

Événement/Action	Mesure de l'engagement de service
Le CSU est publié.	L'horloge démarre
AMS vous informe de la RFC du correctif par le biais d'une notification de service (qui envoie également un e-mail) pour chaque pile. La notification de service inclut : • Date de sortie des mises à jour • Criticité des mises à jour • Détails de la mise à jour : référence KB, etc. • IDs des piles touchées	L'horloge s'arrête après l'envoi de la notification de service.
Vous testez les mises à jour répertoriées dans le RFC et vous approuvez ou rejetez le RFC dans les 10 jours en répondant à la notification de service. Vous fournissez une fenêtre de maintenance spécifique (par pile) pour l'installation des mises à jour. Les fenêtres de maintenance spécifiées qui se situent dans les 24 heures suivant la réponse à la notification de service peuvent être reprogrammées en fonction de la capacité disponible. Si vous ne répondez pas dans les 10 jours ou si vous rejetez le correctif RFC, l'action en attente est annulée. Si vous souhaitez appliquer les mises à jour après la période de 14 jours, soumettez une demande de service pour un nouveau correctif RFC basé sur les détails du RFC précédent.	Si vous n'approuvez pas ou ne répondez pas dans les 14 jours, la modification en attente est annulée et l'engagement de service relatif à la mise à jour n'est pas applicable.

Événement/Action	Mesure de l'engagement de service
Si vous approuvez la notification de service, AMS applique les mises à jour. Pour les mises à jour multiples, vous pouvez choisir d'exclure des mises à jour spécifiques de la modification en spécifiant les mises à jour à exclure dans votre réponse à la notification de service.	Si la fenêtre de maintenance souhaitée n'est pas comprise dans le délai d'engagement de service, l'engagement de service pour la mise à jour n'est manqué que si la RFC n'est pas exécutée pendant la période de maintenance souhaitée.
AMS vous envoie une notification de service indiquant le résultat de chaque mise à jour appliquée. La notification de service inclut les informations suivantes : • ID d' EC2 instance Amazon • Mise à jour réussie : ARN a1, ARN a2... • Echec de la mise à jour : ARN c1, ARN c2...	Non applicable.
En cas d'échec des mises à jour, AMS effectue une analyse pour comprendre la cause de l'échec et vous communique le résultat de l'analyse. Si la panne est imputable à AMS, AMS réessaie les mises à jour si la fenêtre de maintenance est en cours. Dans le cas contraire, AMS crée des notifications de service pour l'échec de la combinaison instance-mise à jour et attend vos instructions lors d'une nouvelle fenêtre de maintenance.	Non applicable.
Pour les défaillances qui vous sont imputables, soumettez une demande de service pour un nouveau correctif RFC afin de mettre à jour les instances.	Non applicable.

Mises à jour de sécurité critiques, infrastructure immuable

Événement/Action	Mesure de l'engagement de service
Le CSU est publié.	L'horloge démarre
AMS vous informe de ce qui suit par le biais d'une notification de service : • Mettre à jour la date de sortie • Criticité des mises à jour • Détails de la mise à jour (référence KB, etc.) • AMS Amazon Machine Images (AMI) concerné • Date et heure de publication prévues pour la nouvelle mise à jour AMIs	L'horloge continue de tourner.
Les versions d'AMS ont été mises AMIs à jour dans le compte géré.	L'horloge s'arrête.
Si vous approuvez la notification de service, AMS applique les mises à jour. AMS vous informe des informations AMIs partagées sur votre compte, par le biais d'une notification de service et par e-mail.	Non applicable.
Si le test de la nouvelle application AMIs prend plus de temps que prévu (une semaine), vous pouvez envoyer une demande de service à AMS pour mettre à jour vos groupes Auto Scaling avec la nouvelle AMI AMS (telle quelle). Si vous souhaitez modifier la nouvelle AMI AMS avec vos configurations, utilisez une RFC avec le CT Management Other Other Update (ct-0xdawir96cy7k) pour demander que nous mettions à jour vos groupes Auto Scaling.	Non applicable.

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 patch AMS](#)
- [Rapports AMS Backup](#)
- [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 patch AMS

Rapports disponibles

- [Rapport récapitulatif des détails de l'instance de correctif](#)
- [Rapport sur les détails des correctifs](#)
- [Rapport sur les instances pour lesquelles des correctifs ont été omis](#)
- [Rapport sur la couverture des correctifs SSM](#)

Rapport récapitulatif des détails de l'instance de correctif

Le rapport récapitulatif des détails des instances de patch fournit des informations détaillées sur les instances collectées pour les instances intégrées aux rapports. Il s'agit d'un rapport informatif qui permet d'identifier toutes les instances intégrées, le statut 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 rapport fournit les informations suivantes :

1. Données relatives aux instances de production et de non-production d'un compte. Remarque : Les étapes de production et de non-production sont dérivées du nom du compte et non des balises d'instance.
2. Données sur la distribution des instances par type de plateforme. Remarque : le type de plateforme « N/A » correspond à l' AWS Systems Manager impossibilité de récupérer les informations de la plate-forme.
3. Données sur la distribution de l'état des instances et le nombre d'instances en cours d'exécution, arrêtées ou résiliées.

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

Nom du champ	Définition
Nom du compte	Nom du compte AWS
Compte de production	Identifiant des comptes AMS prod, non-prod, selon que le nom du compte inclut ou non les valeurs « PROD » ou « NONPROD ». Exemple : PROD, NONPROD, non disponible
État du compte	État du compte AMS. Par exemple : ACTIF, INACTIF
Engagement en matière de service de compte AMS	PRIME, PLUS
Zone d'atterrissage	Drapeau correspondant au type de zone de landing zone du compte. Par exemple : MALZ, NON-MALZ
Restrictions d'accès	Régions auxquelles l'accès est restreint. Par exemple : US SOIL
ID d'instance	ID de l' EC2 instance
Nom de l'instance	Nom de l' EC2 instance
Type de plate-forme d'instance	Type de système d'exploitation (OS). Par exemple : Windows, Linux, etc.
Nom de la plate-forme d'instance	Nom du système d'exploitation (OS). Par exemple : MicrosoftWindowsServer 2012R2Standard, RedHatEnterpriseLinuxServer
Nom de la pile	Nom de la pile contenant l'instance
Type de pile	Stack AMS (infrastructure AMS intégrée au compte client) ou stack client (infrastructure gérée AMS qui prend en charge les applications des clients). Exemples : AMS, CLIENT

Nom du champ	Définition
Nom du groupe Auto Scaling	Nom du groupe Auto Scaling (ASG) qui contient l'instance
Groupe de correctifs d'instance	Nom du groupe de correctifs utilisé pour regrouper les instances et appliquer la même fenêtre de maintenance. Si le groupe de correctifs n'est pas attribué, la valeur sera « Non attribué »
Type de groupe de correctifs d'instance	Type de groupe de correctifs. PAR DÉFAUT : groupe de correctifs par défaut avec la fenêtre de maintenance par défaut, déterminée par le <code>AMSDefaultPatchGroup:True</code> tag de l'instance. CLIENT : groupe de correctifs créé par le client. NOT_ASSIGNED : aucun groupe de correctifs n'est attribué
État de l'instance	État au sein du cycle de vie de l' EC2 instance. Exemples : TERMINÉ, EN COURS D'EXÉCUTION, ARRÊT, ARRÊTÉ, ARRÊT, ARRÊT, EN ATTENTE. Pour plus d'informations, consultez la section Cycle de vie des instances.
Couverture des fenêtres de maintenance	S'il existe une future fenêtre de maintenance sur cette instance. Exemples : COVERED ou NOT_COVERED
Date/heure d'exécution de la fenêtre de maintenance	La prochaine fois, la fenêtre de maintenance devrait s'exécuter. Si la valeur est NULL, exécution dans une fenêtre unique, c'est-à-dire non récurrente

Rapport sur les détails des correctifs

Le rapport sur les détails des correctifs d'AWS Managed Services (AMS) fournit des informations détaillées sur les correctifs et couvre la période de maintenance de différentes instances, notamment :

1. Données sur les groupes de correctifs et leurs types.
2. 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.
3. Données relatives à tous les systèmes d'exploitation associés au compte et nombre d'instances où ce système d'exploitation est installé.

Nom du champ	Définition
Date/heure du rapport	Date et heure de génération du rapport.
ID de compte	ID de compte AWS auquel appartient l'ID d'instance
Nom du compte	Nom du compte AWS
ID d'instance	ID de l' EC2 instance
Compte de production	Identifiant des comptes AMS prod, non-prod, selon que le nom du compte inclut ou non les valeurs « PROD » ou « NONPROD ». Si les données ne sont pas disponibles, la valeur sera « Non disponible »
État du compte	État du compte AMS. Par exemple : ACTIF, INACTIF
Type de plate-forme d'instance	Type de système d'exploitation (OS). Par exemple : Windows, Linux
Nom de la plate-forme d'instance	Nom du système d'exploitation (OS). Par exemple : MicrosoftWindowsServer 2012R2Standard, RedHatEnterpriseLinuxServer

Nom du champ	Définition
Type de pile	Stack AMS (infrastructure AMS au sein d'un compte client) ou stack client (infrastructure gérée par AMS qui prend en charge les applications des clients). Par exemple : AMS, CLIENT
Groupe de correctifs d'instance	Nom du groupe de correctifs utilisé pour regrouper les instances et appliquer la même fenêtre de maintenance. Si le groupe de correctifs n'est pas attribué, la valeur sera « Non attribué »
Type de groupe de correctifs d'instance	Type de groupe de correctifs. PAR DÉFAUT : groupe de correctifs par défaut avec fenêtre de maintenance par défaut, déterminé par le <code>AMSDefaultPatchGroup:True</code> tag de l'instance CLIENT : groupe de correctifs créé par le client NON ATTRIBUÉ : aucun groupe de correctifs n'est attribué
État de l'instance	État au sein du cycle de vie de l' EC2 instance. Par exemple : TERMINATED, RUNNING, STOPPING, STOPPED, SHUTTING-DOWN, PENDING Pour plus d'informations, consultez la section Cycle de vie des instances.
ID de fenêtre de maintenance	Identifiant de fenêtre de maintenance
État de la fenêtre de maintenance	Les valeurs possibles sont ACTIVÉES ou DÉSACTIVÉES.

Nom du champ	Définition
Type de fenêtre de maintenance	Type de fenêtre de maintenance
Date et heure de la prochaine exécution de la fenêtre de maintenance	La prochaine fois, la fenêtre de maintenance devrait s'exécuter. Si la valeur est NULL, exécution dans une fenêtre unique, c'est-à-dire non récurrente
Fenêtre de maintenance de la dernière exécution	Dernière exécution de la fenêtre de maintenance
Durée de la fenêtre de maintenance (heures)	Durée de la fenêtre de maintenance en heures
Couverture des fenêtres de maintenance	La couverture de la fenêtre de maintenance
ID de référence du correctif	Ligne de base de correctifs actuellement attachée à l'instance
État du correctif	État général de conformité des correctifs. Par exemple : COMPLIANT, NON_COMPLIANT. S'il manque au moins un correctif, l'instance est considérée comme non conforme, sinon conforme.
Conforme - Total	Nombre de correctifs conformes (tous niveaux de gravité confondus)
Non conforme - Total	Nombre de correctifs non conformes (tous niveaux de gravité confondus)
Conforme - Critique	Nombre de correctifs conformes présentant un niveau de gravité « critique »
Conforme - Élevé	Nombre de correctifs conformes présentant un niveau de gravité « élevé »
Conforme - Moyen	Nombre de correctifs conformes de gravité « moyenne »

Nom du champ	Définition
Conforme - Faible	Nombre de correctifs conformes dont le niveau de gravité est « faible »
Conforme - Informatif	Nombre de correctifs conformes dont le niveau de gravité est « informatif »
Conforme - Non spécifié	Nombre de correctifs conformes dont le niveau de gravité est « non spécifié »
Non conforme - Critique	Nombre de correctifs non conformes présentant une gravité « critique »
Non conforme - Élevé	Nombre de correctifs non conformes présentant un niveau de gravité « élevé »
Non conforme - Moyen	Nombre de correctifs non conformes de gravité « moyenne »
Non conforme - Faible	Nombre de correctifs non conformes dont le niveau de gravité est « faible »
Non conforme - Informatif	Nombre de correctifs non conformes dont le niveau de gravité est « informatif »
Non conforme - Non spécifié	Nombre de correctifs non conformes dont la gravité est « non spécifiée »

Rapport sur les instances pour lesquelles des correctifs ont été omis

Le rapport Instances That Missed Patches d'AWS Managed Services (AMS) fournit des informations détaillées sur les instances pour lesquelles des correctifs ont été manqués lors de la dernière exécution de la fenêtre de maintenance, notamment :

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

Nom du champ	Définition
Date/heure du rapport	Date et heure de génération du rapport.
ID de compte	ID de compte AWS auquel appartient l'ID d'instance
Nom du compte	Nom du compte AWS
Compte de production	Identifiant des comptes AMS prod, non-prod, selon que le nom du compte inclut ou non la valeur « PROD », « NONPROD ».
État du compte	État du compte AMS. Par exemple : ACTIF ou INACTIF
Niveau de service du compte AMS	PREMIUM ou PLUS
ID d'instance	ID de l' EC2 instance
Type de plate-forme d'instance	Type de système d'exploitation (OS). Par exemple : Windows
État de l'instance	État du cycle de vie de l' EC2 instance. Par exemple : TERMINATED, RUNNING, STOPPING, STOPPED, SHUTTING-DOWN, PENDING Pour plus d'informations, voir Cycle de vie de l' instance .
ID du correctif	ID du correctif publié. Exemples : KB3172729
Gravité des correctifs	Gravité du correctif par éditeur. Par exemple : CRITIQUE, IMPORTANT, MODÉRÉ, FAIBLE, NON SPÉCIFIÉ
Classification des correctifs	Classification des correctifs par éditeur. Par exemple : CRITICALUPDATES, SECURITYUPDATES, UPDATEROLLUPS, UPDATES, FEATUREPACKS

Nom du champ	Définition
Date de publication du correctif (UTC)	Date de sortie du correctif par éditeur
État d'installation du correctif	État d'installation du correctif sur une instance par SSM. Par exemple : INSTALLÉ, MANQUANT, NON APPLICABLE
Jours non corrigés	Nombre de jours pendant lesquels l'instance n'a pas reçu de correctif depuis le dernier scan SSM
Nombre de jours non patchés	Nombre de jours non corrigés. Par exemple : <30 JOURS, 30 À 60 JOURS, 60 À 90 JOURS, PLUS DE 90 JOURS

Rapport sur la couverture des correctifs SSM

Le rapport AMS Patching SSM Coverage 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

Nom du champ	Définition
Taille de sauvegarde	Taille de la sauvegarde en Go
Point de récupération (ARN)	L'ARN de la sauvegarde créée
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.

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'automatisation exécutée
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
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
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 ; $\text{adjust\_aws\_charges} * \text{uplift\_percent}$
Instances : EC2 dépenses RDS	Dépenses consacrées EC2 aux instances RDS
Frais AMS	Total des frais AMS pour le produit ; $\text{uplifted\_aws\_charges} + \text{instance\_ec2\_rds\_spend} + \text{uplifted\_ris} + \text{uplifted\_sp}$
Frais minimaux calculés au prorata	Le montant que nous facturons pour respecter le minimum contractuel
Frais minimaux	Frais minimaux d'AMS (le cas échéant)

Nom du champ	Définition
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

Nom du champ	Définition
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.
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

Nom du champ	Définition
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
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.

Nom du champ	Définition
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.

Important

Pour accéder à cette fonctionnalité, vous devez avoir l'un des rôles suivants :

- Zone d'atterrissage multi-comptes : `AWSMangedServicesReadOnlyRole`
- Zone d'accueil à compte unique : `ReadOnlyCustomer_ _Role`

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 demandé `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

-
- [Détails du patch](#)
- [Instances n'ayant pas reçu de correctifs](#)

Il s'agit d'un rapport informatif qui permet d'identifier toutes les instances intégrées à Patch Orchestrator (PO), 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

Nom du champ de console	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	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'instance	instance_patch_group	Nom du groupe de correctifs 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 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

Nom du champ de console	Nom du champ du jeu de données	Définition
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 de la pile	nom_stack_instance	Nom de la pile contenant l'instance

Nom du champ de console	Nom du champ du jeu de données	Définition
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
État du compte	état_du compte	État du compte AMS

Nom du champ	Nom du champ du jeu de données	Définition
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 correctifs 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'instance 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 (infrastructure gérée par AMS qui prend en charge les applications 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_HHMM	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	region_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 récupération
Identifiant du point de récupération	identifiant_point de récupération	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_key_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'incident. « 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'augmentation (sous forme décimale V.WXYZ) basé sur pricing_plan, SLA et service AWS
AWS Charges ajustées	utilisation_aws_ajustable	AWS utilisation ajustée pour AMS
Charges augmentées AWS	factures_majorées_facturations	Pourcentage de AWS frais à facturer pour AMS ; $\text{adjust\_aws\_charges} * \text{uplift\_percent}$
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 ; $\text{ris\_charges} * \text{uplift\_percent}$
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 ; $\text{sp\_charges} * \text{uplift\_percent}$
Frais AMS	ams_charges	Total des frais d'armes pour le produit ; $\text{uplifted\_aws\_charges} + \text{instance\_ec2\_rds\_spend} + \text{uplifted\_ris} + \text{uplifted\_sp}$

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 ressources (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 appartient 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 prédéfinie ou créée sur mesure.
drapeau d'exception	Drapeau d'exception	L'indicateur d'exception de ressource indique l'acceptation 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 effectuées 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 conservation des données
Résumé des détails de l'instance (Patch Orchestrator)	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.

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

Rubriques

- [Gestion des incidents](#)
- [Gestion des demandes de service](#)
- [Questions relatives à la facturation](#)

Avec AWS Managed Services (AMS), vous pouvez demander de l'aide pour des problèmes opérationnels et des demandes à tout moment via la console AMS. Les ingénieurs opérationnels d'AMS sont disponibles pour répondre à vos incidents et demandes de service 24 heures sur 24, 7 jours sur 7, avec des accords de niveau de service (SLAs) et des objectifs de niveau de service (SLOs) en fonction du niveau de service que vous avez sélectionné pour votre compte (Plus, Premium). Les ingénieurs opérationnels d'AMS vous informent de manière proactive des alertes et des questions importantes en utilisant les mêmes mécanismes.

Gestion des incidents

Rubriques

- [Qu'est-ce que la gestion des incidents ?](#)
- [Engagements relatifs aux services de gestion des incidents](#)
- [Exemples de gestion des incidents](#)

Les incidents sont des problèmes de Service AWS performance qui ont un impact sur votre environnement géré, tel que déterminé par AWS Managed Services (AMS) ou par vous-même. Les incidents identifiés par l'équipe AMS sont d'abord reçus sous la forme d'« événements » : un changement d'état du système capté par le monitoring. Si un seuil configuré est dépassé, l'événement déclenche une alarme, également appelée alerte. L'équipe des opérations AMS 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 résolus).

L'équipe AMS reçoit également les incidents que vous avez identifiés par le biais du Support centre ou par programmation à l'aide de l'[API AWS Support](#) avec le code de service. `sentinel-report-incident`

Une fois que l'équipe des opérations d'AMS a reçu votre incident, il est examiné afin de s'assurer qu'il n'est pas préférable de le classer comme une demande de service. Si elle doit être classée comme une demande de service, elle est immédiatement reclassée et l'équipe de demande de service AMS prend le relais et vous en êtes informé. Si l'incident peut être résolu par l'opérateur récepteur, des mesures sont prises pour le résoudre immédiatement. Les opérateurs AMS 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. Pour être tenu informé à chaque étape du processus de résolution des incidents, assurez-vous de remplir l'option CC Emails et, si vous souhaitez vous connecter par fédération, connectez-vous avant de suivre le lien contenu dans l'e-mail envoyé par AMS. Une fois le problème résolu, l'équipe des opérations AMS documente l'incident et sa résolution pour une utilisation future.

Si la résolution d'un incident nécessite des modifications de l'infrastructure, un examen de sécurité peut être nécessaire. Les modifications de l'infrastructure susceptibles de nécessiter un examen de sécurité incluent celles liées à l'IAM, à la politique basée sur les ressources ou aux approbations de risques. Ces types d'incidents nécessitent qu'un ingénieur des opérations AMS crée une RFC avant d'apporter la modification, et votre approbation pour cette RFC est requise. Par exemple, si la résolution d'un incident nécessite la mise à jour d'une politique IAM, il y aura un examen de sécurité AMS, puis un ingénieur des opérations AMS créera une RFC avec le type Management | Advanced stack components | Identity and Access Management (IAM) | Update entité ou changement de politique (ct-27tuth19k52b4) et attendra que vous approuviez la RFC avant de continuer.

 Note

AMS permet désormais de résoudre les incidents qui nécessitent des modifications de l'infrastructure sans passer par l'étape supplémentaire d'approbation de la RFC. Si les modifications nécessaires pour résoudre l'incident ne nécessitent PAS de révision de sécurité (la modification n'est pas liée à l'IAM, à la politique basée sur les ressources ou aux approbations de risques), AMS peut apporter les modifications en fonction de l'approbation que vous avez reçue lors de l'incident, sans avoir besoin d'une approbation séparée dans un RFC.

Pour les définitions des termes relatifs à la gestion des incidents, consultez les [termes clés d'AMS](#).

Pour comprendre la trajectoire d'escalade des incidents, consultez la section [Obtenir de l'aide](#).

Pour une description de la réponse d'AMS aux incidents, voir [Réponse aux incidents d'AMS](#).

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. Réservez 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.

Problème ou incident

Lorsqu'AMS estime qu'un incident révèle un défaut plus important ou une mauvaise configuration et qu'il est susceptible de se reproduire, il est considéré comme un problème plutôt que comme un simple incident. Dans de tels cas, AMS analyse le problème et propose des suggestions pour le résoudre.

Engagements relatifs aux services de gestion des incidents

Engagements relatifs aux services de gestion des incidents

Événement ou action	Mesure de l'engagement de service
Cas 1 : Un événement dont l'impact est connu est généré. AMS ouvre un incident et vous en informe. Cas 2 : AMS vous contacte pour confirmer l'impact de l'événement. Vous confirmez qu'il s'agit d'un incident. Cas 3 : Vous remarquez un problème et soumettez un rapport d'incident.	Le délai de réponse aux incidents et de résolution des incidents commence lorsque : Cas 1 : AMS crée un incident. Cas 2 : Vous confirmez que l'alerte est un incident. Cas 3 : Vous soumettez un incident. Les engagements de service dépendent de la priorité de l'incident créé.
Si vous soumettez l'incident, AMS envoie une réponse pour en accuser réception. Si AMS crée l'incident en votre nom, aucune réponse à l'incident distincte n'est envoyée.	Le temps nécessaire à la résolution des incidents continue de tourner. Le temps de réponse à l'incident s'arrête lorsque AMS envoie l'accusé de réception de l'incident.  Note Le temps passé à attendre vos informations est exclu du calcul du temps de résolution des incidents. Pour les incidents créés par AMS, le délai de réponse initial est le moment de la

Événement ou action	Mesure de l'engagement de service
	création de la notification d'incident initiale qui vous est adressée.
Pour les ressources/services en question, AMS vérifie l'état de santé pour vérifier si : • L'événement détecté par AMS ou l'incident soumis par le client est considéré comme un incident, et • l'incident est correctement priorisé, et Si un incident que vous soumettez n'est pas correctement priorisé, AMS le redéfinit. Si AMS modifie la priorité d'un incident, une notification vous est envoyée avec les raisons du changement de priorité. Dans certains cas, un problème que vous avez soumis peut ne pas être considéré comme un incident, selon la cause. Dans ces cas, AMS clôt l'incident et vous envoie une notification expliquant pourquoi. Quelle que soit la catégorisation de l'événement, AMS travaille avec vous pour vous aider en cas de besoin. Pour comprendre les règles de catégorisation des incidents, voir Priorité de l'incident.	En cas de modification de la priorité de l'incident, l'engagement de service correspondant à la nouvelle priorité s'applique ; le compte à rebours continue. Dans les cas où un incident est clos parce qu'il ne répond pas à la définition d'un incident, les engagements de service ne sont pas applicables ; le temps s'arrête.

Événement ou action	Mesure de l'engagement de service
AMS travaille sur l'incident pour le résoudre dans le respect de son engagement de service. Dans certains cas, si AMS détermine que les piles ou ressources indisponibles ne peuvent pas être résolues en temps opportun, AMS proposera la restauration de l'infrastructure comme option de résolution. La restauration de l'infrastructure implique le redéploiement des piles existantes, sur la base des modèles des piles concernées, et le lancement d'une restauration des données en fonction du dernier point de restauration connu (instantané EBS/RDS), sauf indication contraire de votre part. Les données éphémères relatives à des EC2 instances individuelles seront perdues. Si vous n'autorisez pas une restauration de l'infrastructure conformément aux recommandations d'AWS, vous ne pourrez pas prétendre à un crédit de service correspondant au délai de résolution des incidents associé.	L'horloge s'arrête lorsque : - AMS a rétabli l'état disponible de tous les services ou ressources non disponibles relatifs à cet incident, ou - une restauration de l'infrastructure est lancée.
AMS a parfois besoin d'éclaircissements de votre part ou d'une activité de votre part pour poursuivre les efforts de résolution des incidents, sauf si vous disposez d'une action approuvée et prédéfinie. Par conséquent, il existe une communication entre AMS et vous afin de résoudre les incidents	L'horloge s'arrête lorsque : AMS attend une réponse ou une action de votre part. L'horloge redémarre lorsque : AMS reçoit la réponse de votre part ou lorsque l'action qu'AMS vous demande est terminée.

 Note

Pour obtenir la liste complète des engagements de service, téléchargez le [contrat de niveau de service AMS](#).

Exemples de gestion des incidents

Exemples de gestion des incidents.

Rubriques

- [Tests d'incidents](#)
- [Signalement des incidents](#)
- [Surveillance et mise à jour des incidents](#)
- [Gestion des incidents avec l'API AWS Support](#)
- [Réagir aux incidents générés par l'AMS](#)

Les exemples suivants décrivent l'utilisation de la console AMS pour soumettre un incident. Une fois soumis, l'équipe AMS travaille avec vous pour résoudre l'incident conformément à votre accord de niveau de service (SLA).

Tests d'incidents

Lorsque vous testez les soumissions d'incidents AMS, nous vous demandons d'inclure dans le texte du sujet ce drapeau : `AMSTestNoOpsActionRequired`. Ce drapeau indique à AMS que l'incident est soumis uniquement à des fins de test. Lorsque les ingénieurs des opérations d'AMS voient ce drapeau, ils ne répondent en aucune façon à la soumission de l'incident.

Signalement des incidents

Utilisez la console AMS pour signaler un incident. Il est important de créer un nouvel incident pour chaque nouveau problème ou question. Lorsque vous ouvrez des dossiers liés à d'anciennes demandes, il est utile d'inclure le numéro de dossier correspondant afin que nous puissions nous référer à la correspondance précédente.

Note

Si la correspondance s'écarte du problème initial, un opérateur AMS peut vous demander de signaler un nouvel incident.

Pour signaler un incident à l'aide de la console AMS :

1. Dans le menu de navigation de gauche, choisissez Incidents

La liste des incidents s'ouvre :

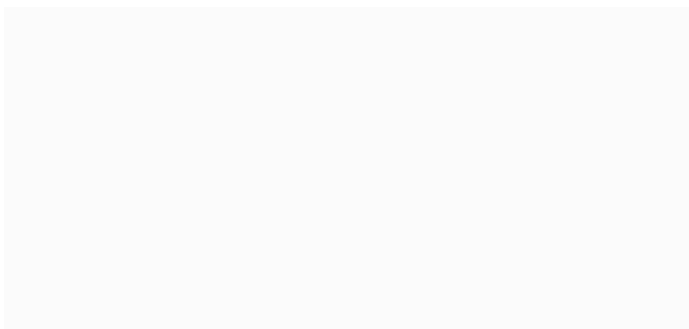
Si votre liste d'incidents est vide, l'option Effacer le filtre réinitialise le filtre sur N'importe quel statut.

Si vous souhaitez utiliser le téléphone ou le chat, cliquez sur Créer un incident dans le Centre de support pour ouvrir la page de création d'un incident dans la console du Centre de support, renseignée automatiquement avec le type de service AMS.

Important

- Les appels téléphoniques initiés avec Support sont enregistrés afin de mieux répondre. Si l'appel est interrompu, vous devez le rappeler via le dossier du Support Center, AWS qui ne dispose d'aucun mécanisme pour vous rappeler.
- L'assistance par téléphone et par chat est conçue pour résoudre les cas d'assistance, les incidents et les demandes de service, et non pour les problèmes de RFC ou de sécurité.
- Pour les problèmes RFC, utilisez l'option de correspondance sur la page de détails RFC correspondante pour contacter un ingénieur AMS.
- Pour les problèmes de sécurité, créez un dossier d'assistance prioritaire (P1 ou P2). La fonction de chat en direct n'est pas destinée aux événements de sécurité.

2. Si vous souhaitez rechercher un incident existant, sélectionnez un filtre de statut d'incident dans la liste déroulante.

	• Tous les incidents qui ne sont pas encore résolus. • Un nouvel incident qui n'est pas encore attribué. • Un incident qui a été attribué. • Un incident que vous avez ouvert.

- Un incident complexe et assigné.
- Incidents qui nécessitent votre feedback avant l'étape suivante.
- Incidents pour lesquels vous avez récemment soumis des informations.
- Un incident qui a pris fin.
- Tous les incidents du compte.

3. Choisissez Créer.

La page Créer un incident s'ouvre :

4. Sélectionnez une priorité :

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

5. Sélectionnez une catégorie.

 Note

Si vous souhaitez tester la fonctionnalité d'incident, ajoutez le drapeau de non-action (AMSTestNoOpsActionRequired) au titre de votre incident.

6. Entrez les informations pour :

- Objet : titre descriptif du rapport d'incident.
- E-mails CC : liste des adresses e-mail des personnes que vous souhaitez informer du signalement et de la résolution de l'incident.
- Détails : Description complète de l'incident, des systèmes concernés et du résultat attendu de la résolution. Répondez aux questions prédéfinies ou supprimez-les et saisissez les informations pertinentes.

Pour ajouter une pièce jointe, choisissez Ajouter une pièce jointe, recherchez la pièce jointe souhaitée, puis cliquez sur Ouvrir. Pour supprimer la pièce jointe, cliquez sur l'icône Supprimer :

7. Sélectionnez Envoyer.

Une page de détails s'ouvre avec des informations sur l'incident, telles que le type, le sujet, la création, l'ID et le statut, ainsi qu'une zone de correspondance qui inclut la description de la demande que vous avez créée.

Cliquez sur Répondre pour ouvrir une zone de correspondance et fournir des informations supplémentaires ou des mises à jour du statut.

Cliquez sur Fermer le dossier lorsque l'incident a été résolu.

Cliquez sur Charger plus s'il y a plus de correspondance que ce que peut contenir une page.

N'oubliez pas d'évaluer la communication !

Votre incident s'affiche sur la page de liste des incidents.

YouTube Vidéo : [Comment signaler un incident depuis la console AWS Managed Services ?](#)

Surveillance et mise à jour des incidents

Vous pouvez mettre à jour, surveiller et examiner les rapports d'incidents et les demandes de service, appelés cas, à l'aide de la console AMS ou par programmation à l'aide de l' Support API. Pour plus d'informations sur l'utilisation de l' Support API, consultez la section [DescribeCases](#) Fonctionnement.

Pour surveiller un dossier, un incident ou une demande de service à l'aide de la console AMS, procédez comme suit.

1. Dans le tableau de bord des rapports d'incidents ou des demandes de service de la console AMS, accédez à un dossier et choisissez le sujet pour ouvrir une page de détails avec le statut actuel et les correspondances.

Lorsqu'un incident signalé ou une demande de service est mis à jour par l'équipe des opérations AMS, vous recevez un e-mail et un lien vers l'incident dans la console AMS afin que vous puissiez y répondre. Vous ne pouvez pas répondre à la correspondance liée à un incident en répondant à l'e-mail.

 Important

Vous devez avoir saisi une adresse e-mail pour recevoir des notifications de changement d'état dans le cadre d'une demande de service ou d'un cas d'incident. 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 fonctionnera que si vous utilisez un serveur de messagerie sur votre réseau fédéré AMS. Vous pouvez toutefois répondre à la correspondance en accédant à votre console AMS et en utilisant la page des détails du dossier.

2. Si la liste contient de nombreux cas, vous pouvez utiliser l'option Filtrer :

- Tout est ouvert (par défaut) : utilisez ce filtre pour voir tous les cas non résolus.
- Non attribué : à utiliser si vous venez de soumettre le dossier et que vous n'avez reçu aucune notification indiquant que l'état du dossier a changé. Notez que les incidents et les demandes de service sont traités avec une rapidité différente en fonction de la priorité soumise (incidents) ou de votre accord de niveau de service (demandes de service).
- Ouvert : à utiliser si vous avez reçu une notification indiquant que le dossier est « En attente d'Amazon » ; cela signifie que le dossier a été attribué mais que le travail n'a pas encore commencé.
- Réouverture : à utiliser si vous avez reçu un avis indiquant que le dossier a été rouvert après avoir été résolu.
- Travail en cours : à utiliser si vous avez été informé qu'un opérateur a commencé à travailler sur le boîtier.
- En attente d'une action du client : à utiliser si vous avez reçu une demande d'action de votre part de l'opérateur.
- Action du client terminée : à utiliser si vous avez reçu une notification indiquant que votre action concernant le dossier a été traitée.
- Résolu : à utiliser pour afficher les cas dont vous savez qu'ils ont été résolus. Les cas résolus sont conservés dans l'historique pendant douze mois.

- N'importe quel statut : utilisez ce filtre pour voir tous les cas, quel que soit leur statut.
3. Pour vérifier le dernier statut, 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 incidents avec l'API AWS Support

L'[API AWS Support](#) vous permet de créer des incidents et d'y ajouter de la correspondance tout au long des enquêtes sur vos problèmes et des interactions avec le personnel de support AWS. L'API AWS Support modélise une grande partie du comportement du [centre de support AWS](#). Pour plus de détails sur la manière dont vous pouvez utiliser ce service de support AWS, consultez [Programmation d'un dossier de support AWS](#).

Note

Lorsque vous utilisez l'API AWS Support, ou SAPI, pour les incidents AMS Advanced, utilisez ce code de service : `sentinel-report-incident`.

Réagir aux incidents générés par l'AMS

AMS surveille vos ressources de manière proactive ; pour plus d'informations, consultez la section [Surveillance et gestion des événements](#). AMS identifie et crée parfois un cas d'incident, le plus souvent pour vous informer d'un incident. Si une action de votre part est requise pour résoudre un incident, AMS envoie une notification aux coordonnées que vous avez fournies pour le compte. Vous réagissez à cet incident de la même manière que vous le feriez pour tout autre incident. Vous répondez généralement aux incidents via la console AMS ; dans certains cas, un contact par e-mail ou par téléphone est nécessaire.

 Note

AMS envoie les communications à votre adresse e-mail principale associée à votre compte AWS ; nous vous recommandons d'ajouter un autre alias d'e-mail de contact des opérations afin de faciliter le processus de gestion des incidents. Cela est abordé lors du processus d'intégration d'AMS et de la documentation d'intégration associée. Si vous avez fourni à AMS des contacts non liés aux ressources (dont vous avez informé votre CSDM) lors de l'intégration, ces contacts sont utilisés. Par exemple, vous pouvez fournir une liste de contacts nommée « SecurityContacts » à utiliser CSDMs/CAs pour les incidents ou les notifications liés à la sécurité. Les balises de contact qui se trouvent sur vos instances/ressources sont utilisées pour les incidents générés par AMS, si vous avez donné votre accord à CSDM pour l'utilisation des informations des balises.

Pour en savoir plus sur ce service de notification, consultez la section [Notifications](#).

Gestion des demandes de service

Rubriques

- [Quand utiliser une demande de service](#)
- [Comment fonctionne la gestion des demandes de service](#)
- [Test d'une demande de service dans AMS](#)
- [Création d'une demande de service dans AMS](#)
- [Surveillance et mise à jour des demandes de service dans AMS](#)
- [Répondre à une demande de service générée par AMS](#)

Les demandes de service sont des communications que vous avez créées à AMS pour demander des informations ou des conseils. Un bon exemple de demande de service standard est de demander des conseils ou de l'aide pour configurer un service AMS, comme Alarm Manager, Patch Orchestrator, etc. Vous pouvez également recevoir des demandes de service de la part d'AMS ; il s'agit de demandes de service sortantes ou de notifications de service. Pour consulter la liste de vos demandes de service et des demandes de service sortantes (notifications de service) qui vous ont été envoyées par AMS, consultez la page des demandes de service de la console AMS.

Pour en savoir plus sur les demandes de service sortantes, consultez [Répondre à une demande de service générée par AMS](#).

Vous créez une demande de service AWS Managed Services (AMS) à l'aide de la console AMS ou, par programmation, à l'aide de l' Support API. Pour plus de détails sur l'utilisation de l'API, consultez la section [Support API](#). Pour AMS, choisissez le code `sentinel-service-request` de service.

Une fois que votre demande de service est reçue par l'équipe des opérations AMS, elle est priorisée conformément à votre accord de niveau de service. Pour être tenu informé à chaque étape du processus de résolution des demandes de service, assurez-vous de remplir l'option CC Emails et, si vous souhaitez vous connecter par fédération, connectez-vous avant de suivre le lien contenu dans l'e-mail envoyé par AMS.

Utilisez la page Créer une demande de service de la console AMS pour effectuer les tâches suivantes :

- Création et mise à jour d'une demande de service
- Obtenez une liste et des informations détaillées sur toutes vos demandes de service en cours
- Affinez votre recherche pour les demandes de service par date et identifiant d'incident, y compris les demandes résolues
- Ajoutez des communications et des pièces jointes à vos demandes, et ajoutez des destinataires par e-mail pour la correspondance des dossiers
- Résoudre les demandes de service
- Communications relatives aux demandes de services tarifaires

Quand utiliser une demande de service

Les exemples suivants décrivent une demande de service :

- 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

- Défaillance du RFC ou RFC entraînant une interruption d'activité (utiliser l'incident pour une interruption d'activité)
- Questions RFC, saisie supplémentaire ou modification de la portée de la RFC (Utiliser la correspondance bidirectionnelle RFC)

Comment fonctionne la gestion des demandes de service

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

Une fois que votre demande de service est reçue par l'équipe des opérations AMS, elle est examinée pour s'assurer qu'elle n'est pas correctement classée comme un incident. S'il doit être classé comme un incident, il est immédiatement reclassé, l'équipe de gestion des incidents AMS prend le relais et vous en êtes informé.

Si la demande de service peut être résolue par la soumission d'un RFC, l'opérateur de révision vous envoie un e-mail vous demandant de soumettre le RFC approprié (les détails sont fournis).

Si l'opérateur AMS peut 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, l'opérateur envoie la demande à votre responsable de prestation de services cloud afin qu'il puisse communiquer avec vous, ou à l'équipe AWS opérationnelle 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 pour faciliter les communications.

Test d'une demande de service dans AMS

Lorsque vous testez des demandes de service AMS, nous vous demandons d'inclure dans le texte du sujet cet indicateur : `AMSTestNoOpsActionRequired` pour indiquer à AMS que la demande de service est uniquement destinée à des tests. Lorsque les ingénieurs opérationnels d'AMS voient ce drapeau, ils ne répondent pas à la demande de service.

Création d'une demande de service dans AMS

Pour créer une demande de service à l'aide de la console AWS Managed Services (AMS) :

1. Dans le menu de navigation de gauche, sélectionnez Demandes de service.

La liste des demandes de service s'ouvre.

Si votre liste de demandes de service est vide, l'option Effacer le filtre réinitialise le filtre sur N'importe quel statut.

Si vous souhaitez utiliser le téléphone ou le chat, cliquez sur Créer une demande de service dans le Centre de support pour ouvrir la page de création de demande de service dans la console du Centre de support, renseignée automatiquement avec le type de service AMS.

Note

Les appels téléphoniques initiés avec le Support centre sont enregistrés afin de mieux répondre. Si l'appel est interrompu, vous devez le rappeler via le dossier du Support Center, AWS qui ne dispose d'aucun mécanisme pour vous rappeler.

Important

L'assistance par téléphone et par chat est conçue pour répondre aux cas d'assistance, aux incidents et aux demandes de service. Pour les problèmes RFC, utilisez l'option de correspondance sur la page de détails RFC correspondante pour contacter un ingénieur AMS.

2. Si vous souhaitez rechercher une demande de service existante, sélectionnez un filtre de statut de demande de service dans la liste déroulante.

- Toutes les demandes de service qui ne sont pas encore résolues.
- Une nouvelle demande de service qui n'est pas encore attribuée.
- Une demande de service qui a été attribuée.
- Une demande de service que vous avez rouverte.
- Une demande de service complexe et assignée.
- Demandes de service nécessitant vos commentaires avant l'étape suivante.
- Demandes de service auxquelles vous avez récemment soumis des informations.
- Une demande de service terminée.
- Toutes les demandes de service sont enregistrées dans le compte.

3. Choisissez Créer.

La page Créer une demande de service s'ouvre.

4. Sélectionnez une catégorie.

 Note

Si vous souhaitez tester la fonctionnalité de demande de service, ajoutez l'indicateur de non-action, `AMSTestNoOpsActionRequired`, au titre de votre demande de service.

5. Entrez les informations pour :

- Objet : Cela crée un lien vers les détails de la demande de service sur la page de liste.

- E-mails CC : Ces e-mails reçoivent de la correspondance en plus de vos contacts e-mail par défaut.
- Détails : Fournissez ici autant d'informations que possible.

Pour ajouter une pièce jointe, choisissez Ajouter une pièce jointe, recherchez la pièce jointe souhaitée, puis cliquez sur Ouvrir. Pour supprimer la pièce jointe, cliquez sur l'icône Supprimer :

6. Sélectionnez Envoyer.

Une page de détails s'ouvre avec des informations sur la demande de service, telles que le type, l'objet, la création, l'ID et le statut, ainsi qu'une zone de correspondance contenant la description de la demande que vous avez créée.

En outre, votre demande de service s'affiche sur la page de liste des demandes de service. Utilisez-le lorsque vous avez reçu une alerte mais que vous n'avez pas encore reçu de nouvelles d'AMS.

Cliquez sur Répondre pour ouvrir une zone de correspondance et fournir des informations supplémentaires ou des mises à jour de statut.

Cliquez sur Résoudre le dossier lorsque la demande de service a été résolue.

Cliquez sur Charger plus pour afficher les correspondances supplémentaires qui ne rentrent pas dans la page initiale.

N'oubliez pas d'évaluer la communication !

Pour les requêtes liées à la facturation, créez un dossier de demande de service depuis la console du Centre de support.

YouTube Vidéo : [Comment et quand envoyer des demandes de service depuis la console AWS et quels sont ses objectifs de niveau de service ?](#)

Surveillance et mise à jour des demandes de service dans AMS

Vous pouvez mettre à jour, surveiller et examiner les rapports d'incidents et les demandes de service, appelés cas, à l'aide de la console AMS ou par programmation à l'aide de l' Support API. Pour plus d'informations sur l'utilisation de l' Support API, consultez la section [DescribeCases](#) Fonctionnement.

Pour surveiller un dossier, un incident ou une demande de service à l'aide de la console AMS, procédez comme suit.

1. Dans le tableau de bord des rapports d'incidents ou des demandes de service de la console AMS, accédez à un dossier et choisissez le sujet pour ouvrir une page de détails avec le statut actuel et les correspondances.

Lorsqu'un incident signalé ou une demande de service est mis à jour par l'équipe des opérations AMS, vous recevez un e-mail et un lien vers l'incident dans la console AMS afin que vous puissiez y répondre. Vous ne pouvez pas répondre à la correspondance liée à un incident en répondant à l'e-mail.

Important

Vous devez avoir saisi une adresse e-mail pour recevoir des notifications de changement d'état dans le cadre d'une demande de service ou d'un cas d'incident. 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 fonctionnera que si vous utilisez un serveur de messagerie sur votre réseau fédéré AMS. Vous pouvez toutefois répondre à la correspondance en accédant à votre console AMS et en utilisant la page des détails du dossier.

2. Si la liste contient de nombreux cas, vous pouvez utiliser l'option Filtrer :
 - Tout est ouvert (par défaut) : utilisez ce filtre pour voir tous les cas qui n'ont pas été résolus.
 - Non attribué : à utiliser si vous venez de soumettre le dossier et que vous n'avez reçu aucune notification indiquant que l'état du dossier a changé. Notez que les incidents et les demandes de service sont traités avec une rapidité différente en fonction de la priorité soumise (incidents) ou de votre accord de niveau de service (demandes de service).

- Ouvert : à utiliser si vous avez reçu une notification indiquant que le dossier est « En attente d'Amazon » ; cela signifie que le dossier a été attribué mais que le travail n'a pas encore commencé.
 - Réouverture : à utiliser si vous avez reçu un avis indiquant que le dossier a été rouvert après avoir été résolu.
 - Travail en cours : à utiliser si vous avez été informé qu'un opérateur a commencé à travailler sur le boîtier.
 - En attente d'une action du client : à utiliser si vous avez reçu une demande d'action de votre part de l'opérateur.
 - Action du client terminée : à utiliser si vous avez reçu une notification indiquant que votre action concernant le dossier a été traitée.
 - Résolu : à utiliser pour afficher les cas dont vous savez qu'ils ont été résolus. Les cas résolus sont conservés dans l'historique pendant douze mois.
 - N'importe quel statut : utilisez ce filtre pour voir tous les cas, quel que soit leur statut.
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 !

Répondre à une demande de service générée par AMS

La gestion des correctifs AMS vous envoie des demandes de service (c'est-à-dire des notifications de service) avant l'heure de la fenêtre de maintenance que vous avez définie ; pour plus d'informations, consultez la section [Fenêtre de maintenance AMS](#). AMS vous envoie également des notifications de service lorsqu'il est possible que votre infrastructure soit affectée par un AWS service ou lorsqu'une EC2 instance de votre compte doit être redémarrée ; pour plus d'informations, consultez la section Notifications de [service](#).

 Note

AMS envoie les communications à l'adresse e-mail principale de votre AWS compte que vous avez indiquée ; nous vous recommandons d'ajouter un autre alias d'e-mail de contact des opérations afin de faciliter le processus de gestion des demandes de service ou des notifications de service. L'ajout de ces e-mails est abordé lors du processus d'intégration d'AMS et de la documentation d'intégration associée.

Questions relatives à la facturation

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

1. Ouvrez le [AWS Support centre](https://console.aws.amazon.com/support/) 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.

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 AWS](#) où 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 modifications à l'aide de runbooks et surveillent les builds d'AMI à l'aide de Monitoring. CloudWatch 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 interagissant avec EC2 Image Builder.	Le niveau de sécurité des clients s'est amélioré et le temps passé par les clients à construire 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 entreprise 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 meilleures 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 définition, à la création et à l'exécution de demandes de modification personnalisées. Les modifications peuvent être manuelles ou automatisées (CloudFormationSSM). Comprend une consultation Support pour obtenir des conseils de configuration si nécessaire. Non destiné aux modifications du code de l'application, à l'installation/au déploiement d'applications, à la migration des données ou aux modifications de configuration du système d'exploitation.

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 opérations continues du pare-feu. Pour ce faire, nos ingénieurs tirent parti de nos meilleures pratiques opérationnelles 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 modifications 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 rapidement les modifications involontaires du pare-feu réseau, ce qui a permis d'améliorer la résolution des incidents et de réduire le temps d'analyse des causes profondes des problèmes attendus et inattendus.
AMS Accelerate	AWS Control Tower opérations	Exploitation et gestion continues de votre zone AWS Control Tower d'atterrissage, y compris AWS Transit Gateway, et AWS Organizations 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-fous CT), de la gestion des politiques 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 configurer et de gérer un AWS environnement 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 opérationnelles 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 sauvegarde 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.

Historique du document

Le tableau suivant décrit les modifications importantes apportées à chaque version du guide de l'utilisateur avancé d'AMS. Pour recevoir les notifications de mise à jour de cette documentation, abonnez-vous à un flux RSS.

- Version de l'API : 2019-05-21
- Nouveau ou mis à jour CTs et procédures pas à pas : historique du [document de référence AMS Advanced Change Type](#).
- Nouvel AMS AMIs : [Images de machines AMS Amazon \(AMIs\)](#).

Modification	Description	Date
Tableau mis à jour pour AWS Identity and Access Management (IAM) dans les contrôles standard de la section AMS Advanced	Informations mises à jour dans le tableau concernant les politiques IAM et l'accès aux compartiments Amazon S3.	25 septembre 2025
Étape mise à jour pour les requêtes relatives à la facturation	Étape mise à jour pour créer des demandes de service pour les requêtes liées à la facturation dans la section Création d'une demande de service dans AMS.	25 septembre 2025
Informations mises à jour pour les notifications par e-mail pour les types de modifications	Informations mises à jour et exemple d'ajout de notifications par e-mail pour les types de modification dans la section Configurer les notifications par e-mail RFC (console).	25 septembre 2025
Type de modification mis à jour	Section de balisage automatique de l'infrastructure AMS mise à jour avec type de	25 septembre 2025

modification pour le balisage des ressources créées par AMS.

[FAQ sur la machine virtuelle mise Import/Export à jour dans AWS Managed Services](#)

Mise à jour de la RFC utilisée pour demander un profil d'instance afin de permettre aux outils d'exécuter des commandes depuis l'instance.

24 septembre 2025

[Demande de modification \(RFC\) mise à jour pour le lancement d'une instance SUSE Linux Enterprise Server pour SAP Applications 15 SP6](#)

Étape 2 mise à jour de la procédure de lancement d'une nouvelle SP6 instance de SUSE Linux Enterprise Server pour SAP Applications 15 avec le RFC approprié.

22 septembre 2025

[Demande de modification mise à jour \(RFC\)](#)

Mise à jour AWS Elastic Disaster Recovery dans la section FAQ d'AWS Managed Services avec la RFC appropriée pour créer les rôles IAM nécessaires au sein de votre compte.

22 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 :

22 septembre 2025

- 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

[Note mise à jour pour les zones de disponibilité \(AZs\)](#)

Informations mises à jour concernant les groupes de sécurité dans AMS.

5 septembre 2025

[Type de modification mis à jour](#)

Mise à jour de la section FAQ d'Amazon FSx dans AWS Managed Services avec le type de modification permettant de partager le Managed AD avec le compte de l'application.

5 septembre 2025

[Type de modification mis à jour](#)

Amazon DocumentDB a été mis à jour dans la section FAQ d'AWS Managed Services avec le type de modification à supprimer. APIs

5 septembre 2025

[Type de modification mis à jour](#)

Mise à jour de la section FAQ d'Alexa for Business dans AWS Managed Services avec changement de type pour deux utilisateurs IAM à accès limité pour l'installation et le fonctionnement de votre passerelle Alexa for Business.

5 septembre 2025

[Type de modification mis à jour](#)

Mise à jour AppStream 2.0 dans la section FAQ d'AWS Managed Services avec le type de modification permettant de créer et de choisir un rôle IAM qui sera disponible sur toutes les instances de streaming de flotte

5 septembre 2025

[Type de modification mis à jour](#)

Mise à jour EventBridge dans la section FAQ d'AWS Managed Services avec le type de modification permettant de demander un rôle de EventBridge service avant de l'utiliser EventBridge pour déclencher d'autres AWS ressources.

5 septembre 2025

Mise à jour Trusted Advisor du support des contrôles de sécurité 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
Mise à jour Trusted Advisor du support des contrôles de sécurité par Trusted Remediator	Contrôle Trusted Advisor de sécurité mis à jour pour ajouter la version 2 de Hs4Ma3G184 - La journalisation des équilibres de charge d'application et des équilibres 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 de la section Contrôles d'excellence Trusted Advisor opérationnelle pris en charge par Trusted Remediator pour ajouter le nouveau contrôle pris en charge c1fd6b96l4 activé pour les journaux d'accès Amazon S3.	28 août 2025
Type de modification mis à jour	Modifiez le type pour le rôle IAM personnalisé.	25 août 2025
Mise à jour à CloudWatch l'aide d'Application Insights pour .Net et SQL Server dans la section AMS	Type de modification révisé pour utiliser CloudWatch Application Insights.	25 août 2025
Demande de modification mise à jour (RFC)	Demande de modification (RFC) pour ajouter des balises supplémentaires au compartiment Amazon S3.	25 août 2025

Demande de modification mise à jour (RFC)	Demande de modification (RFC) pour étiqueter toutes les ressources créées par AMS à des fins de gestion.	25 août 2025
Lambda mis à jour dans la section FAQ d'AWS Managed Services	Type de modification révisé pour l'accès à d'autres AWS services afin de créer des sources d'événements.	25 août 2025
Lambda mis à jour dans la section FAQ d'AWS Managed Services	Type de modification révisé pour provisionner les fonctions Lambda.	25 août 2025
Section Créer, modifier ou supprimer des groupes de sécurité mise à jour	Type de modification révisé pour créer un groupe de sécurité en dehors des piles et VPCs.	25 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

[Recommandation précise sur le type de changement](#)

Pour intégrer votre métrique client à votre système de surveillance des applications, demandez à AMS de créer une rubrique Amazon SNS pour la métrique en soumettant une RFC avec le formulaire Deployment | Monitoring and notification | SNS | Create CT (ct-3dfnglm4ombbs).

8 août 2025

[Recommandation précise sur le type de changement](#)

Pour supprimer des volumes d'instance réservés, soumettez un type de modification Management | Advanced stack components | EBS Volume | Delete (ct-3e3h8u0sp5z80).

8 août 2025

[Nouvelles alertes de surveillance SecureChannelFailure et canal sécurisé défaillant](#)

[Alertes issues de la surveillance de base dans AMS](#) [AMS, correction automatique des alertes.](#)

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
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
Obsolète du service de provisionnement en libre-service	Le CloudEndure service de provisionnement en libre-service est déconseillé au profit de. AWS Application Migration Service	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

Tableau des commandes mis à jour	Suppression de certains contrôles dupliqués dans la section du tableau AMS-STD-002 - AWS Identity and Access Management (IAM).	26 juin 2025
Conditions requises pour le service AWS Transfer Family SSP mises à jour	Informations ajoutées à la section des prérequis.	26 juin 2025
Exemple de politique IAM mise à jour	Exemple de politique IAM mis à jour avec davantage de restrictions, comme recommandé.	26 juin 2025
AMI mise à jour prise en charge OSES	Ajout d'Ubuntu Linux 24.04 sous Ubuntu Linux 22.04 et modification de toutes les références à SP5 . SP6	26 juin 2025
Service de provisionnement en libre-service, obsolète MediaStore	Ajout d'une note de dépréciation pour. AWS Elemental MediaStore	26 juin 2025
Service de provisionnement en libre-service, Amazon Inspector Classic est obsolète	Ajout d'une note de dépréciation pour Amazon Inspector Classic.	26 juin 2025
Service de mise en service en libre-service, Amazon Connect est obsolète	Ajout d'une note de dépréciation pour Amazon Connect.	26 juin 2025
Section mise à jour pour les configurations prises en charge dans AMS	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 AMS.	25 juin 2025

Service de provisionnement en libre-service, obsolète WorkDocs	Page supprimée et référencés à la version obsolète WorkDocs.	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.	10 juin 2025
Mises à jour des systèmes d'exploitation compatibles	Les systèmes d'exploitation pris en charge par AMS Advanced sont mis à jour, certains ajoutés, d'autres supprimés.	22 mai 2025
Uniquement en interne APIs	Uniquement internes APIs qui apparaissent dans certains CloudWatch journaux.	22 mai 2025
mises à jour d'AMS Trusted Remediator	Comment utiliser un nouveau paramètre pour personnaliser <code>preconfigured-parameters</code> les Trusted Advisor contrôles dans Trusted Remediator.	22 mai 2025
Mises à jour du SSP Amazon Elastic Container Registry	D'autres rôles sont automatiquement attribués lorsque vous intégrez le service Amazon ECR.	8 mai 2025

FAQ et mises à jour d'AMS Advanced 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 Advanced Standard.	Ajout de contrôles « Partage de groupes de sécurité ».	8 mai 2025
Espaces de noms protégés AMS Advanced.	Espaces de noms protégés par AMS EPSMarket placeSubscriptionRole et EPS ajoutés.	24 avril 2025
Emplacements des journaux AMS Advanced.	Des emplacements de journal supplémentaires ont été ajoutés.	24 avril 2025
Mise à jour des prérequis du mode AMS Advanced Self-Service Provisioning pour la AppStream version 2.0.	Une condition préalable à la AppStream version 2.0 a été ajoutée : vous devez inclure un nom de compartiment Amazon S3 lorsque vous soumettez la RFC de provisionnement pour le service.	24 avril 2025

<u>Nouvelle alerte de correction automatique d'Amazon RDS d'AMS Advanced.</u>	ID d'alerte : - 0224, se déclenche lorsque le stockage alloué demandé atteint ou dépasse le seuil de stockage maximal configuré.	27 mars 2025
<u>AMS Advanced AWS a fermé l'accès des nouveaux clients à Amazon CloudSearch à compter du 25 juillet 2024.</u>	Les clients existants peuvent toujours utiliser le service, mais il n'y aura pas de nouvelles fonctionnalités.	27 mars 2025
<u>AMS Advanced AWS a fermé l'accès des nouveaux clients à AWS CodeCommit, à compter du 25 juillet 2024.</u>	Les clients existants peuvent toujours utiliser le service, mais il n'y aura pas de nouvelles fonctionnalités.	27 mars 2025
<u>Trusted Remediator est désormais disponible.</u>	Trusted Remediator, une solution AWS Managed Services qui automatise la correction des AWS Trusted Advisor contrôles, est désormais disponible.	19 mars 2025
<u>Nouvelle alerte RDS d'auto-rémediation d'AMS Advanced.</u>	RDS-EVENT-0224 ajouté.	17 mars 2025
<u>Nouvelle fonctionnalité AMS Advanced : notifications d'incidents.</u>	Vous pouvez l'utiliser AppRegistry pour créer des applications et personnaliser les notifications d'incident pour ces applications.	13 mars 2025
<u>Mise à jour AMS du seuil de surveillance des alarmes RDS.</u>	Le seuil d'alarme d'utilisation moyenne du processeur RDS a été modifié de 75 % à 90 %.	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 :

28 janvier 2025

- Rapport de patch (quotidien)
- Rapport de sauvegarde (quotidien)
- Rapport d'incident (hebdomadaire)

[Mise à jour du AWS Batch SSP](#)

Vous pouvez utiliser la RFC suivante pour effectuer le provisionnement AWS Batch dans votre compte AMS : Management | Service AWS | Service auto-provisionné | Ajouter (ct-1w8z66n899dct).

28 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

<u>Mise à jour de la section Forecast SSP</u>	Remarque ajoutée : AWS a fermé l'accès des nouveaux clients à Amazon Forecast, à compter du 29 juillet 2024. Les clients existants d'Amazon Forecast peuvent continuer à utiliser le service normalement.	10 janvier 2025
<u>Mise à jour de la section sur les espaces de noms protégés par AMS</u>	Ajout d'un espace de noms protégé manquant (*mc, *MC et *Mc) à la liste des espaces de noms protégés par AMS.	9 janvier 2025
<u>Mise à jour de la section Fonctionnement de la surveillance</u>	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
<u>Mise à jour : contenu de mise à jour basé sur des balises</u>	Correction d'une faute de frappe dans le nom de clé et correction d'un mauvais chemin de fichier de configuration.	6 janvier 2025
<u>Mise à jour : AMS AMI Notes</u>	Le fichier zip contient des notes sur les dernières images de machines AMS Amazon (AMIs) et un fichier CSV contenant les dernières AMIs.	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 :

11 novembre 2024

- Microsoft Windows 2016 à Microsoft Windows 2022 et versions ultérieures

[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 :

1er novembre 2024

- 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

[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

[Images de machines AMS Amazon mises à jour \(AMIs\)](#)

Mise à jour basée sur Windows AMIs pour supprimer Windows 2012 et 2012 R2.
Mise à jour basée sur Linux AMIs pour supprimer plusieurs AMI qui ne sont plus prises en charge et pour ajouter les éléments suivants :

- Amazon Linux (2ARM64)
- RHEL 9
- Serveur SUSE Linux Enterprise 15 SP5

24 octobre 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

[Ajout de la section consacrée aux révisions de sécurité des demandes de modification.](#)

Une nouvelle section a été ajoutée qui fournit des détails sur le processus de vérification de la sécurité des demandes de modification.

17 septembre 2024

[Nouvelle section ajoutée.](#)

Une nouvelle section décrivant la manière dont les examens de sécurité des demandes de modification sont effectués dans AMS Advanced est désormais disponible.

12 septembre 2024

[Nouveau service pris en charge par AMS Advanced.](#)

AWS Resilience Hub est désormais pris en charge par AMS Advanced.

30 août 2024

[Nouveaux services pris en charge par AMS Advanced.](#)

Cinq nouveaux services sont désormais pris en charge par AMS Advanced :

21 août 2024

- Amazon Bedrock
- Amazon Kendra
- Amazon Quantum Ledger Database (Amazon QLDB)
- AWS Service Catalog AppRegistry
- Amazon Managed Service for Prometheus

[Un nouveau paramètre par défaut du réseau de sécurité des terminaux est désormais disponible.](#)

La source de mise à jour est désormais incluse dans les paramètres réseau par défaut d'EPS.

21 août 2024

[Mise à jour : AMS AMI Notes](#)

Le fichier zip contient des notes sur les dernières images de machines AMS Amazon (AMIs) et un fichier CSV contenant les dernières AMIs.

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

[AWS DataSync Mise à jour SSPS](#)

AWS DataSync le préfixe « datasync- » n'est plus nécessaire sur les noms de compartiment Amazon S3.

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 prend désormais en charge Oracle Linux 8.9, RHEL 8.10 et RHEL 9.4.	AMS prend désormais en charge Oracle Linux 8.9, RHEL 8.10 et RHEL 9.4.	5 juillet 2024
Amazon Bedrock est désormais disponible en mode d'approvisionnement en libre-service	Vous pouvez désormais demander Amazon Bedrock en mode AMS SSP.	27 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
Ajout d'informations supplémentaires sur la façon d'activer la fonctionnalité AMS bring your own EPS (BYOEPS).	Ajout d'informations supplémentaires sur la façon d'activer la fonctionnalité AMS bring your own EPS (BYOEPS).	5 juin 2024
Mise à jour : AMS AMI Notes	Le fichier zip contient des notes sur les dernières images de machines AMS Amazon (AMIs) et un fichier CSV contenant les dernières AMIs.	23 mai 2024
Informations ajoutées sur l'utilisation d'un rôle personnalisé AWS Amplify en mode de provisionnement en libre-service (environnements MALZ uniquement).	Des instructions ont été ajoutées sur la façon dont les environnements MALZ peuvent utiliser un rôle personnalisé en mode de provisionnement AWS Amplify en libre-service.	23 mai 2024
Amazon Kendra est désormais disponible en mode Self-Service Provisioning.	Amazon Kendra est désormais disponible en mode Self-Service Provisioning.	23 mai 2024

<u>AMS Advanced prend en charge d'autres systèmes d'exploitation.</u>	AMS Advanced prend en charge Red Hat Enterprise Linux (RHEL) 9.x et Ubuntu 20.04 et 22.04.	25 avril 2024
<u>AMS Advanced prend en charge ARM64 l'architecture d'Amazon Linux 2.</u>	AMS Advanced prend en charge ARM64 l'architecture d'Amazon Linux 2.	25 avril 2024
<u>Mise à jour de la section Offboard à partir des comptes de zone d'atterrissage multi-comptes (MALZ).</u>	Ajout d'informations détaillées sur la façon de déconnecter les comptes Application et Core de la zone de landing zone multi-comptes.	11 avril 2024
<u>Mise à jour : description de la gestion des demandes de service.</u>	Description de la gestion des demandes de service mise à jour dans la rubrique Description du service.	21 mars 2024
<u>Mise à jour : section sur les engagements relatifs aux services de gestion des incidents.</u>	Ajout d'un lien vers le contrat de niveau de service AMS.	21 mars 2024
<u>Mise à jour : section Fonctionnement de la gestion des demandes de service.</u>	Ajout de précisions sur la manière dont AMS gère les demandes de service contenant une demande de fonctionnalité ou un bogue.	21 mars 2024
<u>Mise à jour : section Obtenir de l'aide.</u>	Mise à jour de la section Obtenir de l'aide pour inclure une nouvelle section consacrée aux questions de facturation.	21 mars 2024

[Mise à jour : Approvisionnement IAM automatisé AMS](#)

Mise à jour du provisionnement IAM automatisé AMS avec des informations de liste de refus personnalisées

21 mars 2024

Mises à jour antérieures

Le tableau suivant décrit les modifications importantes apportées à la documentation du guide AMS Advanced avant mars 2024.

Modification	Description	Lien
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 .
Ajout d'une note aux alertes issues de la surveillance de base dans AMS.	Ajout d'une note indiquant que l'alarme pour l'utilisation du volume EC2 non root est désactivée par défaut.	Consultez Alertes issues de la surveillance de base dans AMS .
Ajout d'une nouvelle section AMS Event Router à la surveillance et à la gestion des événements.	Ajout d'une nouvelle section traitant de l'AMS Advanced Event Router.	Consultez Utilisation des règles EventBridge gérées par Amazon dans AMS .
Mise à jour : AMS AMI Notes	Le fichier zip contient des notes sur les dernières images de machines AMS Amazon (AMIs) et un fichier CSV contenant les dernières AMIs.	Voir AMIs. csv-and-notes2.02.2024
février 2024		

Modification	Description	Lien
Ajout d'une nouvelle section pour le rôle lié au service Amazon EventBridge Rule pour AMS Advanced	Ajout d'une nouvelle section pour le rôle lié au service Amazon EventBridge Rule pour AMS Advanced dans la section Sécurité de l'infrastructure.	Voir le rôle lié au service Amazon EventBridge Rule pour AMS Advanced
Section du mode de fourniture en libre-service mise à jour	Ajout d'une nouvelle section pour le nouvel Amazon Inspector en mode Self Servicing Provision.	Voir Amazon Inspector Classic (AMS SSPS)
janvier 2024		
Section de gestion des événements planifiés (PEM) mise à jour	Ajout de détails supplémentaires et d'une FAQ à la gestion des événements planifiés (PEM).	Consultez Gestion des événements planifiés dans AWS Managed Services .
Ajout d'une nouvelle section pour l'installation automatique de l'agent SSM	Ajout d'une nouvelle section pour l'installation automatique de l'agent SSM dans Configuration automatique des EC2 instances.	Consultez Installation automatique de l'agent SSM .
Ajouté AWS Resilience Hub (AMS SSPS)	Ajout d'un nouveau service SSPS.	Consultez Utilisez AMS SSP pour approvisionner AWS Resilience Hub votre compte AMS .
Mise à jour : AMS AMI Notes	Le fichier zip contient des notes sur les dernières images de machines AMS Amazon (AMIs) et un fichier CSV contenant les dernières AMIs.	Voir AMIs. csv-and-notes.01.2024

Modification	Description	Lien
décembre 2023		
Mode Direct Change mis à jour dans AMS	Ajout d'une nouvelle sous-section, Cas d'utilisation du mode de changement direct, au mode de changement direct dans AMS.	Consultez Mode de changement direct dans AMS .
Mis à jour AWS Amplify (AMS SSPS)	FAQ mise à jour pour préciser qu'une acceptation des risques est requise pour demander Amplify.	Consultez Utilisez AMS SSP pour approvisionner AWS Amplify votre compte AMS .
Nouveau AWS Elastic Disaster Recovery (AMS SSPS)	Ajout d'un nouveau service SSPS	Consultez Utilisez AMS SSP pour approvisionner AWS Elastic Disaster Recovery votre compte AMS .
Nouveau service géré Amazon pour Prometheus (AMS SSPS)	Ajout d'un nouveau service SSPS	Consultez Utilisez AMS SSP pour provisionner Amazon Managed Service for Prometheus sur votre compte AMS .
Mise à jour de la section Comment fonctionne la gestion de la continuité.	Ajout d'une nouvelle sous-section intitulée Surveillance et génération de rapports sur les sauvegardes AMS.	Consultez Comment fonctionne la gestion de la continuité .
Nouveau Amazon DevOps Guru (AMS SSPS)	Ajout d'un nouveau service SSPS	Consultez Utilisez AMS SSP pour approvisionner Amazon DocumentDB (compatible avec MongoDB) sur votre compte AMS .

Modification	Description	Lien
Mise à jour : AMS AMI Notes	Le fichier zip contient des notes sur les dernières images de machines AMS Amazon (AMIs) et un fichier CSV contenant les dernières AMIs.	Voir AMIs. csv-and-notes1.12.2023
novembre 2023		
Amazon CloudWatch Synthetics (AMS SSPS) mis à jour	Mis FAQs à jour pour utiliser les noms de rôle corrects.	Consultez Utilisez AMS SSP pour approvisionner Amazon CloudWatch Synthetics sur votre compte AMS.
Mode de provisionnement en libre-service Amazon API Gateway mis à jour	Ajout d'un rôle supplémentaire dans la section API Gateway. <code>customer_apigateway_cloudwatch_role</code>	Consultez Utilisez AMS SSP pour configurer Amazon API Gateway sur votre compte AMS.
Ajout d'un nouveau service au mode de provisionnement en libre-service	Ajouté AWS Service Catalog AppRegistry à la section Mode de provisionnement en libre-service	Consultez Utilisez AMS SSP pour approvisionner AWS Service Catalog AppRegistry votre compte AMS.
Mise à jour : AMS AMI Notes	Le fichier zip contient des notes sur les dernières images de machines AMS Amazon (AMIs) et un fichier CSV contenant les dernières AMIs.	Voir AMIs. csv-and-notes1.11.2023
septembre 2023		

Modification	Description	Lien
Ajout d'une note à propos de l'utilisation de Patch Orchestrator	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 maintenance »	Consultez Gestion des correctifs dans AMS .
Chiffrement des données mis à jour avec des services supplémentaires	Ajout de services au chiffrement des données dans AMS.	Consultez Protection des données dans AMS .
Ajout d'un nouveau paragraphe aux messages d'erreur RFC.	Ajout d'un nouveau paragraphe pour ajouter Créer un lien de demande de service.	Consultez Résolution des erreurs RFC dans AMS .
Noms de rôles IAM corrigés.	Le nom de rôle IAM customer_emr_cluster_autoscaling_role a été corrigé.	Consultez Mode de provisionnement en libre-service dans AMS .
Informations de surveillance de base mises à jour	Suppression de la référence à deux alarmes RDSRead LatencyAlarm obsolètes et. RDSWrite LatencyAlarm	Consultez Alertes issues de la surveillance de base dans AMS .
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 .
juillet 2023		

Modification	Description	Lien
Ajouté : Provisionnement IAM automatisé	Ajout de documentation sur l'utilisation du provisionnement IAM automatisé.	Consultez Provisionnement IAM automatisé (AMS) .
Mise à jour : tableau des rôles d'accès	Ajout de rôles manquants pour AMS Access.	Consultez Accès au compte client AMS Rôles IAM .
juin 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.	Consultez Alertes issues de la surveillance de base dans AMS .
Mise à jour : tableau des rôles d'accès	Nouveaux rôles pour AMS Security.	Consultez Accès au compte client AMS Rôles IAM .
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.	Consultez Termes clés d'AMS .
avril 2023		

Modification	Description	Lien
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) .
Mise à jour : suppression du contenu « Patching standard »	AMS utilise Patch Orchestra.	Gestion des correctifs dans AMS
Mise à jour : Qu'est-ce que l'AMS ?	Certains sujets ont déjà été déplacés sous Qu'est-ce qu'AMS ? pour faire partie de la description du service AMS.	Service description (Description du service)
Mise à jour : zone d'atterrissage multi-comptes Offboarding	A apporté diverses clarifications.	Déconnectez-vous des comptes de zone d'atterrissage multi-comptes AMS
Mise à jour : AWS Transfer Family (AMS SSPS)	Ajout d'un lien vers le didacticiel de configuration du transfert.	Utilisez AMS SSP pour approvisionner AWS Transfer Family votre compte AMS
Contenu mis à jour : approvisionnement en libre-service	Remplacé « CodeSuite » par « Services de code » conformément à la législation d'AWS.	Utilisez AMS SSP pour fournir des services AMS Code sur votre compte AMS
Contenu mis à jour : CloudWatch métriques et alarmes	Ajout d'un lien vers Exemple : compter les occurrences d'un terme .	Création de CloudWatch métriques et d'alarmes personnalisées dans AMS

Modification	Description	Lien
Mise à jour : AMS AMI Notes	Le fichier zip contient des notes sur les dernières images de machines AMS Amazon (AMIs) et un fichier CSV contenant les dernières AMIs.	AMIs. csv-and-notes04/04/2023
mars 2023		
Contenu mis à jour : désencombrement d'AMS	Clarification des ressources supprimées lorsque vous déconnectez des comptes de zone d'atterrissage multi-comptes	Déconnectez-vous des comptes de zone d'atterrissage multi-comptes AMS
Mise à jour : AMS AMIs	Ajout d'un lien vers le fichier ZIP AMI pour chaque mois dans la section Historique des documents.	Historique du document
Mise à jour : correction automatique	Suppression du support LVM pour l'automatisation des EC2 volumes.	Correction automatique des alertes par AMS
Mise à jour : Patch RACI	Plusieurs mises à jour et clarifications du RACI pour les correctifs.	Matrice de responsabilité AMS (RACI)
Contenu mis à jour : approvisionnement en libre-service	Ajout d'une bullet FAQ. Pour lancer un nouvel agent AWS Datasync, l'ingestion de WIGS n'est pas requise.	Mode de provisionnement en libre-service dans AMS
Contenu mis à jour : approvisionnement en libre-service	Ajout d'une bullet FAQ. Pour lancer un nouvel agent AWS Datasync, l'ingestion de WIGS n'est pas requise.	Mode de provisionnement en libre-service dans AMS

Modification	Description	Lien
Mise à jour : AMS AMI Notes	Le fichier zip contient des notes sur les dernières images de machines AMS Amazon (AMIs) et un fichier CSV contenant les dernières AMIs.	AMIs. csv-and-notes03/03/2023
février 2023		
Contenu mis à jour : désencombrement d'AMS	Clarification de la manière de déconnecter les environnements de zone d'atterrissage multi-comptes et VPCs les comptes d'applications	Comptes AMS externes
Contenu mis à jour : recherche ARNs	Ajout de la CLI describe-table DynamoDB pour rechercher l'ARN d'une table DynamoDB	Trouvez les noms de ressources Amazon (ARNs) dans AMS

Modification	Description	Lien
Contenu mis à jour : approvisionnement en libre-service	Suppression de l'option AMS CodeSuite « » car il ne s'agit pas d'un SSPS réel. Vous pouvez toujours utiliser le type Management AWS service Self-provisioned Service Add (révision requise) (ct-3qe6io8t6jtny) et demander les trois services :, et. CodeBuild CodeDeploy CodePipeline AMS fournira ensuite les rôles IAM suivants à votre compte :customer_codebuild_service_role ,customer_codedeploy_service_role ,etaws_codepipeline_service_role . Une fois le rôle configuré dans votre compte, vous devez intégrer le rôle dans votre solution de fédération.	Mode de provisionnement en libre-service dans AMS
Contenu mis à jour : mise à jour de Secrets Manager	Rôles corrigés nécessaires pour la zone d'atterrissage multi-comptes (MALZ) par rapport à la zone d'atterrissage monocompte (SALZ).	FAQ sur le partage de clés à l'aide de Secrets Manager
Contenu mis à jour : correction automatique des alertes par AMS	Ajout de la prise en charge des volumes Logical Volume Manager (LVM).	EC2 automatisation de la correction de l'utilisation des volumes

Modification	Description	Lien
Contenu mis à jour : AMS Amazon Machine Images (AMIs)	Ajout de la section Offboarding AMS AMIs avec un exemple de code à supprimer AMIs de votre compte.	Images de machines AMS Amazon (AMIs)
Contenu mis à jour : rôle d'utilisateur IAM	Mise à jour de la politique IAM : AMSBilling Politique.	Rôle d'utilisateur IAM dans AMS
Nouveau contenu : non pris en charge OSes	Ajout d'informations sur les services fournis par AMS pour les systèmes d'exploitation non pris en charge (OSes).	Fonctionnalités pour les systèmes d'exploitation non pris en charge dans AMS
Contenu mis à jour : rapports à la demande	Certains rapports à la demande ne sont pas disponibles dans AMS Advanced et ont été affichés par erreur comme étant disponibles.	Rapports sur demande
Contenu mis à jour : désintégration des comptes AMS	Instructions clarifiées pour la désinscription des comptes de l'application MALZ.	Comptes d'application AMS externes
Contenu mis à jour : Secrets Manager	Correction des noms des rôles IAM requis pour utiliser Secrets Manager.	FAQ sur le gestionnaire des Secrets Manager dans AWS Managed Services
Mise à jour : AMS AMI Notes	Le fichier zip contient des notes sur les dernières images de machines AMS Amazon (AMIs) et un fichier CSV contenant les dernières AMIs.	AMIs. csv-and-notes2.02.2023

janvier 2023

Modification	Description	Lien
Nouveau contenu : AWS Device Farm (AMS SSPS)	Ajout d'un nouveau service SSPS : AWS Device Farm.	Utilisez AMS SSP pour approvisionner AWS Device Farm votre compte AMS
Mise à jour : versions Windows prises en charge	Ajout du support pour Windows Server 2022.	Images de machines AMS Amazon (AMIs), Configurations prises en charge et Notifications AMI AMS avec SNS
Mise à jour : gestion de la continuité	Les règles du plan de sauvegarde AMS par défaut ont été mises à jour.	Plans de sauvegarde par défaut, zone de landing zone multi-comptes
Mise à jour : AMS AMI Notes	Le fichier zip contient des notes sur les dernières images de machines AMS Amazon (AMIs) et un fichier CSV contenant les dernières AMIs.	AMIs. csv-and-notes01/01/2023
décembre 2022		
Mise à jour : utilisation de bastions	Correction d'un mauvais lien.	Accès aux instances à l'aide de bastions
Mise à jour : planificateur de ressources	Plusieurs améliorations ont été apportées et des liens vers AWS Instance Scheduler ont été ajoutés pour plus de contexte.	Planificateur de ressources AWS Managed Services

Modification	Description	Lien
Mise à jour : Windows AMIs et configurations prises en charge (pour les nouvelles versions de Windows AMIs)	Le contenu de l'AMI AMS a été mis à jour depuis EC2 Launch (Windows Server 2016 et versions ultérieures) vers EC2 Launch (Windows Server 2016 et Windows Server 2019) et ajout de EC2 LaunchV2 (Windows Server 2022 et versions ultérieures). Mise à jour basée sur Windows AMIs depuis Microsoft Windows Server (2012, 2012 R2, 2016 et 2019) vers Microsoft Windows Server (2012, 2012 R2, 2016, 2019 et 2022).	Images de machines AMS Amazon (AMIs) and Service description (Description du service)
Mise à jour : section Resourced Scheduler	Méthodes améliorées pour déployer et personnaliser le planificateur de ressources AMS.	Planificateur de ressources AWS Managed Services
Mise à jour : Configuration d'AMS : DNS privé et public	Le schéma de l'architecture DNS a été mis à jour.	Configuration de DNS privés et publics
Mise à jour : architecture réseau MALZ	Le diagramme a été mis à jour et des instructions ont été ajoutées pour les comptes de l'application Accelerate.	Architecture réseau MALZ

Modification	Description	Lien
Mise à jour : Configuration : utilisation de balises	Nouvelle remarque : le balisage personnalisé n'est pris en charge que pour les comptes d'applications MALZ, et non pour les comptes principaux.	Marquage automatique de l'infrastructure AMS
Mise à jour : Gestion des accès : utilisation de bastions	Introduction mise à jour pour inclure les bastions RDP.	Réduction des coûts sur les bastions de la zone d'atterrissage à compte unique (SALZ)
Mise à jour : paramètres par défaut d'AMS : alertes	EC2 Instance ajoutée : utilisation du volume non root dans le tableau des alertes.	Alertes issues de la surveillance de base dans AMS
Mise à jour : gestion de la continuité	Ajout de conseils sur les sauvegardes continues.	Comment fonctionne la gestion de la continuité
Mise à jour : Configuration automatique des EC2 instances	Ajout du support pour PowerBroker Identity Service (PBIS) et On Instance Code (OIC).	Mettre à jour automatiquement le PBIS sur les instances Linux and Mettre à jour automatiquement le code sur les instances Linux
Mise à jour : provisionnement en libre-service pour Secrets Manager	Mise à jour du CT pour ajouter Secrets Manager à votre compte (ci-dessous FAQs).	Utilisez AMS SSP pour approvisionner AWS Secrets Manager votre compte AMS
Mise à jour : gestion des journaux	Mise à jour de la liste des journaux EC2 au niveau du système.	Amazon Elastic Compute Cloud (Amazon EC2) : journaux au niveau du système

Modification	Description	Lien
Mise à jour : AMS AMI Notes	Le fichier zip contient des notes sur les dernières images de machines AMS Amazon (AMIs) et un fichier CSV contenant les dernières AMIs.	AMIs. csv-and-notes1.12.2022
novembre 2022		
Mise à jour : AMS Amazon Machine Images (AMIs)	Mise à jour des versions de SUSE Linux prises en charge.	Images de machines AMS Amazon (AMIs)
Mise à jour : comptes MALZ	Ajout de conseils pour supprimer un compte d'application géré par le client.	Comptes d'applications gérés par le client
Mise à jour : Configuration d'AMS	Ajouté customer-ams-amazon2-security-enhanced .	Notifications AMI AMS avec SNS
Mise à jour : Fonctionnement de la surveillance	Explication mise à jour des notifications de service et des rapports d'incidents.	Fonctionnement de la surveillance
Mise à jour : types de comptes de l'application MALZ	Amélioration de l'explication des types de comptes.	Types de comptes d'applications
Mise à jour : mode développeur	Ajout d'un avertissement concernant le mode développeur.	Avant de commencer avec le mode développeur AMS
Mise à jour : gestion des événements planifiés	Ajout de la section : Types de PEM	Gestion des événements planifiés dans AWS Managed Services
Mise à jour : Amazon Machine Images (AMIs)	Versions de SUSE Linux prises en charge mises à jour	Images de machines AMS Amazon (AMIs)

Modification	Description	Lien
Mise à jour : AMS AMI Notes	Le fichier zip contient des notes sur les dernières images de machines AMS Amazon (AMIs) et un fichier CSV contenant les dernières AMIs.	AMIs. csv-and-notes1.11.2022
octobre 2022		
Nouveau : Configuration automatique des instances	Une nouvelle section décrit le processus de configuration automatique des instances.	Configuration d'instance automatisée dans AMS Advanced
Nouveau : Seule la tomographie manuelle est acceptable pour certains SSPS	Mise à jour de plus de 50 services d'approvisionnement en libre-service FAQs pour utiliser le CT manuel et non le CT automatisé pour ajouter le SSPS.	Mode de provisionnement en libre-service dans AMS
Mise à jour : Configuration d'AMS	Ajout de deux politiques aux profils d'instance Amazon EC2 IAM pour MALZ.	EC2 Profil d'instance IAM
Nouveau : bibliothèque de règles de détection et de prévention personnalisées.	Ajout d'un ensemble d'exemples de politiques de contrôle des services (SCPs) et de contrôles préventifs des règles de configuration basés sur les enseignements de plusieurs clients.	Règles de curated SCPs et de configuration

Modification	Description	Lien
Mise à jour : AWS Backup avertissement	Ajout d'un avertissement : « Ne modifiez pas les plans de sauvegarde AMS car vos modifications risquent d'être perdues. Créez plutôt de nouveaux plans de sauvegarde à l'aide de ct-2hyozb pa0sx0m pour vos configurations personnalisées. »	Comment fonctionne la gestion de la continuité
Mise à jour : AWS Backup prudence	Ajout d'une remarque concernant l'ajout de nouveaux rôles IAM à votre fédération.	Déploiement de ressources IAM dans AMS Advanced
Mise à jour : gestion de la surveillance	Les alertes génèrent des rapports d'incidents, et non des demandes de service.	Fonctionnement de la surveillance
Mise à jour : apportez votre propre EPS	S'applique aussi bien au SALZ qu'au MALZ.	AMS : apportez votre propre EPS
Mise à jour : compte Accelerate Application	Il a été précisé que votre compte Accelerate est un compte d'application.	Types de comptes d'applications
Mise à jour : AMS AMI Notes	Le fichier zip contient des notes sur les dernières images de machines AMS Amazon (AMIs) et un fichier CSV contenant les dernières AMIs.	AMIs. csv-and-notes10.10.2022
septembre 2022		

Modification	Description	Lien
Mise à jour : exemples de commandes CLI pour trouver des ressources	Ajout d'un nouvel exemple et indiquant que l' --region option peut être nécessaire.	Trouver les données dont vous avez besoin (SKMS), AMS
Mise à jour : provisionnement des rôles IAM	Les rôles IAM peuvent désormais être créés et gérés à l'aide du AWS Management Services CloudFormation AdminRole .	Création de piles à l'aide du mode Direct Change
Mise à jour : normes techniques AMS	Journalisation AMS-STD-007 : (#20) Exigences de transfert clarifiées.	Sécurité et conformité
Mise à jour : Comment fonctionne la gestion de la continuité	Le libellé de Start Backup Job a été révisé en « à la demande » au lieu de « existant ».	Comment fonctionne la gestion de la continuité
Mise à jour : sécurité et conformité	Description et directives mises à jour pour la norme AMS-STD-007 numéro 20 : transfert de journaux entre comptes.	Sécurité et conformité
Mise à jour : cas d'utilisation de la gestion du changement	Suppression d'un lien rompu vers l'ancien guide de l'utilisateur de gestion des modifications.	Cas d'utilisation de la gestion du changement
Mise à jour : AMS AMI Notes	Le fichier zip contient des notes sur les dernières images de machines AMS Amazon (AMIs) et un fichier CSV contenant les dernières AMIs.	AMIs. csv-and-notes09/09/2022

Modification	Description	Lien
11 août 2022		

Modification	Description	Lien
Mise à jour : pour des raisons de cohérence et de lisibilité, les titres des chapitres ont été déplacés vers des sections plus appropriées	« Architecture réseau MALZ » et « architecture réseau SALZ » sont désormais toutes deux des sous-sections de la section de haut niveau « Architecture réseau », anciennement la section « Architecture réseau AMS » « Modes de gestion du changement » est le nouveau titre de « Gestion du changement » « Paramètres par défaut » est désormais une sous-section de « Configuration d'AMS » « Règle de réclamation AD FS et paramètres SAML » (anciennement « Règle de réclamation des services de ActiveDirectory fédération (ADFS) et paramètres SAML ») est désormais une sous-section de la section « Configuration d'AMS » « Gestion des accès » est le nouveau titre « Accès dans AMS » et est déplacé vers le haut dans la table des matières	Qu'est-ce qu'AWS Managed Services ?

Modification	Description	Lien
	« Trouver les données dont vous avez besoin » est la nouvelle rubrique « Gestion des connaissances relatives aux services » « Rapports et options » est le nouveau titre de « AMS Reporting » et se trouve plus bas dans la table des matières « Les opérations à la demande » est désormais le dernier sujet de la table des matières	
Mise à jour : recherche et ARN, nouveau : recherche d'une ressource avec un ARN	Les deux procédures ont été complètement réécrites pour des raisons d'utilité.	Trouvez les noms de ressources Amazon (ARNs) dans AMS et Trouver des ressources par ARN dans AMS .
Mise à jour : Connecter votre CMA à Transit Gateway	L'automatisation ne prend pas en charge l'ajout de routes aux domaines de route principaux, et la procédure devait être mise à jour.	Connecter votre CMA à Transit Gateway
Mise à jour : tarification des composants de base MALZ	Tous les prix sont en dollars américains, formatés avec le signe du dollar.	Composants de base de l'environnement AMS

Modification	Description	Lien
Mise à jour : AMS AMI Notes	Le fichier zip contient des notes sur les dernières images de machines AMS Amazon (AMIs) et un fichier CSV contenant les dernières AMIs.	AMIs. csv-and-notes08/08/2022
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.	Rapports en libre-service
Mise à jour : surveillance de base AMS	Alerte DeleteRecoveryPoint de sauvegarde ajoutée.	Alertes issues de la surveillance de base dans AMS
Mise à jour : Systèmes d'exploitation pris en charge	Date de fin de Support ajoutée pour Amazon Linux 2.	Configurations prises en charge
Mise à jour : approvisionnement en libre-service	Ajout d'un prérequis pour le AWS transfert SSPS.	Utilisez AMS SSP pour approvisionner AWS Transfer Family votre compte AMS
Mise à jour : AMS Reporting	Ajout d'une note concernant les régions optionnelles.	Rapports et options
Mise à jour : correspondance RFC et pièce jointe	Clarification des types de fichiers texte autorisés ; en particulier, les fichiers YAML doivent se terminer par .yaml (et non par .yml).	Ajouter de la correspondance RFC et des pièces jointes (console)
21 juin 2022		

Modification	Description	Lien
Contenu mis à jour	Le mode AMS, auparavant appelé « mode de gestion des modifications » ou « mode CM standard », est désormais connu sous le nom de « mode RFC ». La section des modes a été étendue.	Vue d'ensemble des modes.
Nouvelle alarme	Une AWS Backup alarme a été ajoutée.	Alertes issues de la surveillance de base dans AMS
16 juin 2022		
Nouveau contenu	Gestion des incidents Les incidents ne présentant aucun risque de sécurité peuvent désormais être résolus par AMS avec votre approbation dans le rapport d'incident et ne nécessitent pas de RFC ni d'approbation distinctes.	Gestion des incidents
Contenu mis à jour	MALZ : schéma d'architecture réseau mis à jour. Mises à jour : L'appairage du VPC du compte principal vers le VPC de services partagés doit être supprimé car il n'existe pas.	Architecture des comptes réseau
	Service provisionné en libre-service (SSPS) de Sagemaker . Mise à jour avec l'ajout d'un nouveau rôle IAM lors de l'intégration pour Sagemaker.	Utilisez AMS SSP pour configurer Amazon SageMaker AI sur votre compte AMS

Modification	Description	Lien
	À la liste des notifications AMIs prises en charge pour les notifications SNS : customer-ams-sles 12, customer-ams-sles 15, customer-ams-amazon 1 renforcées, customer-ams-rhel 8, 8, 8, customer-ams-rhel 8, customer-ams-ubuntu 18, 2012, 2019 et 2019 améliorées. customer-ams-windows customer-ams-windows customer-ams-windows Suppression de customer-ams-rhel 6 et customer-ams-rhel 6 améliorations de sécurité AMIs.	Notifications AMI AMS avec SNS
	Suppression des e-mails d'escalade.	Obtenir de l'aide sur AWS Managed Services
	La liste des sujets a été déplacée en dessous des paragraphes d'ouverture.	Qu'est-ce qu'AWS Managed Services ?
	Journaux de service mis à jour avec de meilleurs liens pour les journaux d'équilibrage de charge, également reformatés.	Journaux de service agrégés AMS

Modification	Description	Lien
Service de provisionnement en libre-service (SSPS) EKS. Ajout d'informations sur l'activation du chiffrement des enveloppes secrètes dans votre cluster.	Utilisez AMS SSP pour activer Amazon EKS sur AWS Fargate votre compte AMS	
9 juin 2022		
Contenu mis à jour, Obtenir de l'aide	Suppression des e-mails relatifs au chemin d'escalade. AMS fournit des méthodes de communication par le biais de rapports d'incidents, de demandes de service et RFCs.	Obtenir de l'aide sur AWS Managed Services
12 mai 2022		
Nouveau contenu, modèle d'abonnement Operations on Demand (OOD)	AMS a modifié l'intégration des opérations à la demande, passant du modèle actuel d'inscription et de renouvellement à un modèle d'allocation d'abonnement et d'option par défaut. Lorsque vous créez un compte AMS, vous êtes désormais automatiquement inscrit à Operations on Demand.	Opérations à la demande
14 avril 2022		
Nouveau contenu, optimisation des coûts	AMS fournit des recommandations pour l'optimisation des coûts.	Optimisation des coûts dans AWS Managed Services

Modification	Description	Lien
Contenu mis à jour, compte Accelerate dans MALZ	Un nom de rôle incorrect (CustomerDefaultAdminRole) a été mis à jour avec le nom de rôle correct (AccelerateDefaultAdminRole).	Comptes AMS Accelerate Section « Accès à votre compte Accelerate ».
Contenu mis à jour, accès AMS aux rôles IAM	Ajout d'autres rôles AMS IAM utilisés pour accéder à vos comptes.	Pourquoi et quand AMS accède à votre compte Section « Rôles IAM d'accès au compte client AMS ».
Contenu mis à jour, plans de sauvegarde AMS	Ajout de plans de sauvegarde gérés par AMS.	Plans de sauvegarde AMS and coffres-forts de sauvegarde AMS
Contenu mis à jour, AWS Secrets Manager	Mise à jour de la FAQ.	Utilisez AMS SSP pour approvisionner AWS Secrets Manager votre compte AMS
Contenu mis à jour, intégration du mode de changement direct (DCM)	AMS ne prend pas en charge l'intégration des clients Service Catalog dans DCM.	Commencer à utiliser le mode Direct Change
Contenu mis à jour, description du service	Clarification de la section Services pris en charge : • Amazon EKS sur AWS Fargate -> Amazon Elastic Kubernetes Service sur Fargate • Amazon ECS pour Fargate -> Amazon Elastic Container Service sur Fargate AWS • Amazon Kinesis -> Amazon Kinesis Data Streams	AWS Services pris en charge

Modification	Description	Lien
Contenu mis à jour, désintégration des comptes MALZ	Mis à jour pour faire référence aux nouveaux types de modifications pour les comptes d'applications de désinscription.	Comptes d'application AMS externes
Contenu mis à jour, gestion des incidents en mode développeur	Description du SLA de l'incident mise à jour en : Le SLA AMS ne s'applique pas aux ressources créées ou mises à jour en dehors de la gestion des modifications d'AMS (mode développeur inclus). Par conséquent, les ressources mises à jour ou créées en mode développeur sont automatiquement dégradées au rang de P3 et le support est le meilleur effort.	Gestion des incidents en mode AMS Developer
Contenu mis à jour, intégration de DCM	Le modèle RFC pour le nouveau DCM inclut désormais un champ pour l'ARN de votre fournisseur SAML.	Commencer à utiliser le mode Direct Change
Contenu mis à jour, DCM pour AWS CloudFormation	Les instructions de création et de mise à jour AWS CloudFormation des piles incluent désormais des exemples YAML.	Transformation AMS

Modification	Description	Lien
Contenu mis à jour, compte MALZ Tools	Il existe un nouveau rôle IAM pour les migrations : <code>AWSManagedServicesMigrationRole</code> .	AWS Service de migration d'applications (AWS MGN) and Activer l'accès au nouveau compte AMS Tools
Nouveau contenu, comptes de zone de landing zone multi-comptes	Vous pouvez créer un compte Accelerate dans votre compte AMS Management pour zone d'atterrissage multi-comptes.	Comptes AMS Accelerate
Contenu mis à jour, API/CLI installation du SDK	Les instructions d'installation indiquaient un nom de fichier incorrect pour Mac/Linux les installations et une commande incorrecte. Cela a été corrigé.	Utilisation de l'API et de la CLI AMS
Contenu mis à jour, compte Accelerate dans MALZ	Le nom de règle était incorrect (<code>CustomerDefaultAdminRole</code>), il a été mis à jour avec le nom correct (<code>AccelerateDefaultAdminRole</code>).	Comptes AMS Accelerate , section « Accès à votre compte Accelerate »
Contenu mis à jour, surveillance	La surveillance de l'utilisation des racines a été révisée de 85 % à 95 %.	Alertes issues de la surveillance de base dans AMS
Contenu mis à jour, notifications AMI	Vous pouvez créer de nombreux types de notifications SNS pour les nouveaux AMS AMIs. Nous avons ajouté des informations sur la création de différents types.	Notifications AMI AMS avec SNS
Contenu mis à jour, paramètres par défaut d'AMS	Les références à Macie Classic ont été supprimées, remplacées par Macie.	Alertes issues de la surveillance de base dans AMS

Modification	Description	Lien
Contenu mis à jour, préfixes réservés AMS	Liste alphabétique des préfixes réservés.	Préfixes réservés AMS
Contenu mis à jour, description du service	Les sections relatives aux fonctionnalités relatives à la gestion des modifications et au provisionnement en libre-service ont été mises à jour avec de plus amples informations sur les modes AMS.	Fonctionnalités du plan d'exploitation avancé d'AWS Managed Services (AMS) AMS
Contenu mis à jour, AWS Secrets Manager	Partage de clés à l'aide de Secrets Manager	10 février 2022
Nouveau contenu, approvisionnement en libre-service, Amazon Connect	Ajout d'une FAQ expliquant comment demander l'ajout d'une liste de pays pour les appels sortants ou entrants.	10 février 2022
Nouveau contenu, mise en service en libre-service, Amazon EKS on Fargate	Ajout d'une restriction de FAQ selon laquelle le déploiement de clusters EKS via le kit de développement AWS cloud (CDK) ou CloudFormation Ingest n'est pas pris en charge dans AMS.	10 février 2022
Contenu modifié, mode développeur	Correction, vous n'utilisez pas de RFC ou de demande de service pour attribuer des utilisateurs à votre solution de fédération, vous le faites vous-même en fonction de votre solution.	10 février 2022

Modification	Description	Lien
Contenu modifié, mode de changement direct (DCM)	Notez que l'IAM n'est pas pris en charge dans DCM.	10 février 2022
	DCM, notez les validations que nous effectuons.	10 février 2022
	DCM, clarifiez les restrictions des différents rôles.	10 février 2022
Contenu modifié, surveillance des alertes de base	Les alertes relatives aux ressources du cluster Redshift ont été modifiées.	10 février 2022
Contenu modifié, rapports en libre-service	Le nom exact du compartiment s3 (ams-reporting-data-a<Account_ID>) a été ajouté pour que les clients puissent l'utiliser pour récupérer les rapports.	10 février 2022

Modification	Description	Lien
Contenu modifié, contenu mis à jour pour faire référence à des types de modifications automatisés au lieu d'une gestion manuelle Autre Autre (MOO)	Le contenu du compte d'application de zone d'atterrissage multi-comptes (MALZ) a été mis à jour pour faire référence aux types de modifications automatisées (trois, « Association de la pièce jointe TGW à une table de routage », « Créez des itinéraires dans les tables de routage TGW pour vous connecter à ce VPC » et « Configuration de vos tables de routage VPC pour qu'elles pointent vers la passerelle de transit de la zone d'atterrissage multi-comptes AMS »). Réception d'alertes générées par AMS Notifications d'alerte basées sur des balises	10 février 2022
Contenu modifié : AMS AMIs.	Ajout de nouvelles informations sur la sécurité améliorée AMIs. Voir Configurations prises en charge Images de machines AMS Amazon (AMIs), et. Sécurité améliorée AMIs	27 janvier 2022

Modification	Description	Lien
Nouveau contenu : approvisionnement en libre-service.	Ajout d'Amazon Fax pour OpenZFS. Consultez Utilisez AMS SSP pour provisionner Amazon FSx pour OpenZFS sur votre compte AMS.	27 janvier 2022
Contenu modifié : service de provisionnement en libre-service (SSPS) Code-Deploy.	Nom de rôle supplémentaire et note de restriction supplémentaire. Voir Utilisez AMS SSP pour approvisionner AWS CodeDeploy votre compte AMS.	27 janvier 2022
Contenu modifié : liens mis à jour.	Liens brisés corrigés : AMS-AMIs, Recherche de vos paramètres, Recherche d'un identifiant de pile, Recherche d'un identifiant VPC, ListVpcSummaries ListStackSummaries, et. GetStack APIs Pour obtenir un exemple, consultez Trouver une pile IDs dans AMS.	13 janvier 2022
Contenu modifié : Support EKS pour Fargate	Limitation ajoutée à FAQs : La création ou la gestion de EC2 groupes de nœuds avec EKS ne sont pas prises en charge. Consultez Utilisez AMS SSP pour activer Amazon EKS sur AWS Fargate votre compte AMS.	13 janvier 2022

Modification	Description	Lien
Contenu modifié : CloudFormation, Mode de changement direct (DCM)	Ajout d'instructions pour créer ou mettre à jour des piles CF à l'aide AmsStackTransform de. Consultez Création de piles à l'aide du mode Direct Change .	13 janvier 2022
Contenu modifié : uniformité des noms de AWS service	Les références AMS doivent correspondre Services AWS exactement aux AWS titres officiels ou aux métadonnées. Auparavant, il existait des variations mineures qui compliquaient la correspondance des modèles. Pour obtenir un exemple, consultez Utilisez AMS SSP pour approvisionner Alexa for Business sur votre compte AMS .	13 janvier 2022
Contenu modifié : mise en service en libre-service d'Elastic Container Registry (ECR)	Ajout d'un élément de FAQ pour l'utilisation de l'ECR pour gérer les autorisations des utilisateurs. Consultez Utilisez AMS SSP pour approvisionner Amazon Elastic Container Registry sur votre compte 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.