Informations d'inscription au compte AMS Advanced

Guide d'intégration avancé d'AMS

Version February 11, 2026

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Guide d'intégration avancé d'AMS: Informations d'inscription au compte AMS Advanced

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques et la présentation commerciale d’Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n’est pas d’Amazon, d’une manière susceptible de créer une confusion parmi 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

Présentation de l'intégration à AWS Managed Services 1
En savoir plus sur AMS 1
Termes clés 2
Modes AMS 9
Modes AMS et applications ou charges de travail 9
Conseils prescriptifs de l'AMS après le compte 17
Ce que nous faisons, ce que nous ne faisons pas 18
Gestion du trafic de sortie AMS 19
Rôle d'utilisateur IAM 20
MALZ : Rôles utilisateur IAM par défaut 21
SALZ : rôle d'utilisateur IAM par défaut 34
Règles de pare-feu d'accès par défaut 42
Ports d'instance Linux Stack 42
Ports d'instance Windows Stack 42
Gestion des services 44
Gouvernance des comptes 44
Début du service 45
Gestion de la relation client (CRM) 45
Processus CRM 46
Réunions CRM 47
Arrangements de réunions CRM 48
Rapports mensuels du CRM 49
Optimisation des coûts 50
Cadre d'optimisation des coûts 50
Matrice de responsabilité pour l'optimisation des coûts 53
Heures de service 55
Obtenir de l'aide 56
Modes de gestion des modifications 57
Vue d'ensemble des modes 58
Types de modes et de comptes dans AMS 59
Modes AMS et applications ou charges de travail 62
Cas d'utilisation réels des modes AMS 70
Mode RFC 74
En savoir plus sur RFCs 75

Quels sont les types de modifications ? 117
Résolution des erreurs RFC 130
Mode de changement direct 141
Commencer à utiliser le mode Direct Change 142
Sécurité et conformité 144
Gestion du changement en mode Direct Change 150
Création de piles à l'aide du mode Direct Change 152
Cas d'utilisation du mode de changement direct 155
Mode développeur 156
Commencer à utiliser le mode développeur 157
Sécurité et conformité 159
Gestion des modifications 161
Provisionnement de l'infrastructure 167
Contrôles de détection 168
Journalisation, surveillance et gestion des événements 168
Gestion des incidents 168
Gestion des correctifs 169
Gestion de la continuité 169
Gestion de la sécurité et des accès 169
Mode de provisionnement en libre-service dans AMS 170
Commencer à utiliser le mode SSP dans AMS 171
Amazon API Gateway 171
Alexa for Business 172
WorkSpaces Applications Amazon 174
Amazon Athena 177
Amazon Bedrock 178
Amazon CloudSearch 179
Amazon CloudWatch Synthetics 181
Amazon Cognito 182
Amazon Comprehend 184
Amazon Connect 185
Amazon Data Firehose 187
Amazon DevOps Guru 188
Amazon DocumentDB (compatible avec MongoDB) 189
Amazon DynamoDB 190
Amazon Elastic Container Registry 192

EC2 Image Builder 193
Amazon ECS sur AWS Fargate 195
Amazon EKS sur AWS Fargate 197
Amazon EMR 201
Amazon EventBridge 204
Amazon Forecast 206
Amazon FSx 209
Amazon FSx pour OpenZFS 210
Amazon FSx pour NetApp ONTAP 212
Amazon Inspector Classic 214
Amazon Kendra 215
Amazon Kinesis Data Streams 216
Amazon Kinesis Video Streams 217
Amazon Lex 218
Amazon MQ 219
Service géré Amazon pour Apache Flink 220
Amazon Managed Streaming for Apache Kafka 221
Amazon Managed Service for Prometheus 222
Amazon Personalize 223
Amazon Quick 226
Amazon Rekognition 228
Amazon SageMaker AI 229
Amazon Simple Email Service 233
Amazon Simple Workflow Service 234
Amazon Textract 235
Amazon Transcribe 236
Amazon WorkSpaces 237
Services liés au code AMS 239
AWS Amplify 243
AWS AppSync 244
AWS App Mesh 245
AWS Audit Manager 246
AWS Batch 247
AWS Certificate Manager 248
AWS Autorité de certification privée 250
AWS CloudEndure 253

AWS CloudHSM 254
AWS CodeBuild 256
AWS CodeCommit 257
AWS CodeDeploy 259
AWS CodePipeline 260
Optimiseur de calcul AWS 262
AWS DataSync 263
AWS Device Farm 265
Reprise après sinistre AWS Elastic 266
AWS Elemental MediaConvert 267
AWS Elemental MediaLive 268
AWS Elemental MediaPackage 269
AWS Elemental MediaStore 270
AWS Elemental MediaTailor 271
AWS Global Accelerator 272
AWS Glue 273
AWS Lake Formation 275
AWS Lambda 276
AWS License Manager 278
AWS Migration Hub 279
AWS Outposts 280
AWS Resilience Hub 280
AWS Secrets Manager 282
AWS Security Hub CSPM 285
AWS Service Catalog AppRegistry 286
AWS Shield 287
AWS Snowball Edge 288
AWS Step Functions 290
AWS Systems Manager Magasin de paramètres 291
AWS Systems Manager Automatisation 292
AWS Transfer Family 296
AWS Transit Gateway 297
AWS WAF 298
AWS Well-Architected Tool 299
AWS X-Ray 300
VM Import/Export 302

Mode géré par le client 303
Commencer à utiliser le mode géré par le client 304
AMS et AWS Service Catalog 304
Commencer à utiliser Service Catalog 304
Service Catalog dans AMS avant de commencer 305
Intégration à la zone d'atterrissage multi-comptes (MALZ) d'AMS 309
Architecture réseau MALZ 309
À propos de l'architecture du réseau de zones d'atterrissage multi-comptes 309
Choisir un seul MALZ ou plusieurs MALZs 312
Comptes multi-comptes Landing Zone 317
MALZ : Intégration du compte principal 342
Créez un compte principal AWS multi-comptes pour la zone de landing zone 342
Créez un rôle IAM pour qu'AMS puisse accéder à votre compte 344
Sécurisez le nouveau compte avec l'authentification multifactorielle (MFA) pour l'utilisateur root 345
Abonnez-vous à AWS Marketplace for EPS 346
Configuration de la mise en réseau 347
Configuration de la gestion des accès 351
MALZ : Intégration du compte d'application 356
Demande d'un nouveau compte d'application 357
Configuration d'Active Directory pour fédérer l'accès aux rôles AMS IAM 358
Configuration de la mise en réseau avec le nouveau compte d'application 362
Configuration de fonctionnalités supplémentaires VPCs dans le compte de l'application 363
Annexe : liste des points à considérer pour l'intégration dans une zone d'atterrissage multicompte (MALZ) 363
Configuration du compte 364
Alertes de surveillance de la zone d'atterrissage multi-comptes AMS 365
Configuration réseau 365
Configuration d'Active Directory 367
Protection des terminaux Trend Micro (EPS) 367
Accès : Bastions, SSH et RDP 367
Fédération 369
Intégration à la zone d'atterrissage à compte unique (SALZ) AMS 370
Processus d'intégration d'AMS SALZ 370
Architecture du réseau SALZ 371
Services partagés de zone d'atterrissage à compte unique AMS 372

SALZ : Créez un nouveau AWS compte pour AMS 373
Créez un Compte AWS 373
Configurez la facturation consolidée : associez le nouveau compte au compte du payeur 376
Configurez votre accès Compte AWS pour AMS 377
Abonnez-vous à AWS Marketplace for EPS 379
S'abonner à AWS Marketplace pour CentOS 7.6 380
Sécurisez le nouveau compte avec l'authentification multifactorielle (MFA) pour l'utilisateur root 381
SALZ : Configuration de la mise en réseau 381
Allouez de l'espace IP à votre environnement AMS 381
Établissez une connectivité réseau privée avec AWS 382
Configurez votre pare-feu 384
Options d'AMS Bastion lors de la migration/de l'intégration des applications 384
SALZ : Configuration de la gestion des accès 385
Établir une relation de confiance Active Directory (AD) 386
Fédérez votre Active Directory avec les rôles AMS Gestion des identités et des accès AWS 392
SALZ : paramètres par défaut 399
Sécurité des terminaux (EPS) 399
Groupes de sécurité 404
EC2 Profil d'instance IAM 409
Valeurs par défaut des métriques surveillées 417
Valeurs par défaut de conservation et de rotation des journaux 435
Paramètres par défaut de gestion de la continuité 436
Paramètres par défaut des correctifs 437
Valider le service AMS (SALZ) 439
Rechercher les paramètres du compte 439
Recherche d'un ID d'instance ou d'une adresse IP 443
Noms de bastion compatibles avec le DNS 446
Trouver les adresses IP des bastions 447
Instances EC2 : création 448
Accès, demande 457
Autre | Autre RFC, création (CLI) 465
N'importe quelle pile : suppression, redémarrage, démarrage, arrêt 467
Exemples d'accès 479
Signaler un incident 490

Création d'une demande de service 493
Étapes postérieures à l'intégration 495
Didacticiels 496
Annexe : Questionnaire d'intégration de la SALZ 523
Récapitulatif du déploiement 524
Considérations relatives à l'architecture environnementale 524
Alertes de surveillance des zones d'atterrissage à compte unique 525
Fenêtre de maintenance 526
Étapes suivantes 526
Annexe : règle de réclamation des services de ActiveDirectory fédération (ADFS) et paramètres SAML 527
Configurations des règles de réclamation ADFS 527
console Web 528
Accès à l'API et à la CLI avec SAML 528
Configuration du script 528
Configuration de Windows 528
Configuration de Linux 531
Historique de la documentation 532
..... dxxxv

Présentation de l'intégration à AWS Managed Services

Bienvenue sur AWS Managed Services (AMS). AMS est un service d'entreprise qui assure la gestion continue de votre infrastructure AWS. Ce guide est conçu pour vous aider à commencer à utiliser AMS, notamment comment configurer un nouveau compte pour AMS, configurer le réseau et l'accès à AMS, et valider votre configuration d'intégration.

Il est destiné aux administrateurs informatiques chargés de préparer et d'exécuter les tâches requises pour intégrer le service AMS à un nouveau compte AWS. L'intégration du service AMS nécessite des privilèges spéciaux pour configurer les approbations Active Directory et effectuer d'autres tâches au niveau du réseau. Pour obtenir de l'aide pour décider d'utiliser des comptes de zone d'atterrissage à comptes multiples ou des comptes de zone d'atterrissage à compte unique, consultez l'article Choisir un seul MALZ ou plusieurs. MALZs

> **Important**
>
> Ce guide est divisé en deux parties après cette introduction : l'une pour les comptes de zone d'atterrissage multi-comptes et l'autre pour les comptes de zone d'atterrissage à compte unique. L'intégration est très différente pour les deux, veuillez vous référer à la section du guide qui s'applique à votre situation.

Rubriques

- En savoir plus sur AMS
- Termes clés d'AMS
- Modes AMS
- Conseils prescriptifs de l'AMS après le compte
- Ce que nous faisons, ce que nous ne faisons pas
- Gestion du trafic de sortie AMS
- Rôle d'utilisateur IAM dans AMS
- Règles de pare-feu d'accès par défaut

En savoir plus sur AMS

Pour mieux comprendre AMS, reportez-vous aux sections du guide de l'utilisateur AMS suivantes :

- What Is AWS Managed Services présente le service AMS et décrit les principales fonctionnalités, opérations et interfaces, ainsi qu'une architecture réseau typique gérée par AMS. Ce chapitre fournit également des informations sur la gestion des accès, notamment sur la manière d'accéder à vos ressources gérées par AMS et d'utiliser des bastions.
- Key Terms fournit des définitions et des explications pour la terminologie AMS.
- Understanding AMS Defaults fournit les valeurs par défaut utilisées par AMS, y compris les valeurs par défaut pour les composants de base de l'environnement, IAM et les proxys EC2, les métriques surveillées, la journalisation, la sécurité des terminaux (EPS), les sauvegardes et les correctifs.
- La gestion des modifications fournit des détails sur le fonctionnement des demandes de modification (RFCs) et des types de modification (CTs) et inclut des exemples d'utilisation d'AMS RFCs.
- Plusieurs chapitres supplémentaires traitent de l'accès à la console AWS, de l'interface de ligne de commande AMS, de l'AMS SKMS, de la sécurité, des demandes de service, des incidents, de la surveillance, des journaux, de l'EPS, des sauvegardes et de la gestion des correctifs.

Pour en savoir plus sur l'architecture de zone d'atterrissage multi-comptes AMS, voir Architecture réseau de zones d'atterrissage multicomptes

Pour en savoir plus sur l'architecture de la zone d'atterrissage à compte unique AMS, voir Architecture du réseau de la zone d'atterrissage à compte unique

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 Gestion des identités et des accès AWS 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.

Modes AMS

Utilisez-le 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 migrate/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 supposent que vous avez déjà pris la décision de tirer parti d'AMS pour accélérer votre transition vers le cloud. Consultez ce paper à deux étapes de votre parcours de migration vers le cloud : tout d'abord, pendant la phase initiale de configuration de la plateforme gérée par AMS. Ensuite, 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, vous vous concentrez sur la gouvernance et les opérations des applications.

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 minimes 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 Servic	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	

Problèmes de décision	Mode CM standard/ OOD *	AWS Servic	Mode de changement direct	Provisionnement en libre-service	Mode développeur	Géré par le client
					système AMS CM	
Gestion de l'accès au niveau de l'instance	Géré par AMS via AD Trust unidirectionnel avec domaine sur site. Nécessite une infrastructure gérée pour rejoindre le domaine AMS			Non applicable	Client responsable des 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 Servic	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 Servic	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 Servic	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 Servic	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.

Conseils prescriptifs de l'AMS après le compte

À mesure que les entreprises adoptent des opérations et DevOps des pratiques distribuées, il existe un ensemble de fonctionnalités opérationnelles de base qui doivent être appliquées à chaque compte avant le déploiement des charges de travail afin de répondre aux piliers de Well Architected.

Ce lien télécharge un fichier ZIP contenant un document Word et un fichier ZIP contenant des scripts et des exemples. La configuration automatique de compte est un ensemble de scripts permettant d'automatiser, ou de démarrer, la configuration d'un nouveau compte d'application.

Une fois qu'un nouveau compte est vendu, et avant le déploiement de toute charge de travail, afin de préparer le compte du point de vue des opérations, de la sécurité et de la gestion, vous configurez des plans de sauvegarde, des fenêtres de correctifs et le chiffrement par défaut (et plus encore). Pour améliorer l'agilité, la cohérence et la réactivité lors de la configuration des comptes d'applications, l'exemple de « Comment faire » suivant est fourni à titre de référence.

Configuration automatique du compte.

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.

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.

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'instances Amazon EC2 pendant une longue période, vous pouvez les appeler. APIs Pour en savoir plus, consultez Instances réservées Amazon EC2.

> **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 utilisateur IAM existant ou en ajouter un nouveau, soumettez une RFC IAM : Update Entity ou IAM : Create Entity, respectivement.

Si vous ne connaissez pas les rôles Amazon IAM, 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

Role	Politique ou politiques
AWSManagedServicesReadOnlyRole	ReadOnlyAccess(Politique publique gérée par AWS).
AWSManagedServicesCaseRole	ReadOnlyAccess

Role	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

Role	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

Role	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

Role	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

Role	Politique ou politiques
	d'informations, consultez Getting Started with AWS Support.
AWSManagedServicesSecurityOpsRole	ReadOnlyAccess
	AWSSupportExemple 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

Role	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/hashes 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/hashes 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/*"
  }
```

```
 ]
}
```

AMSChangeManagementPolicy

`AMSChangeManagementPolicy`

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 réservées Amazon EC2 ; pour obtenir des informations sur les tarifs, consultez Instances réservées Amazon EC2.

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 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 pour s'abonner, se désabonner et 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 aux hôtes EC2 ou aux hôtes de base de données.

Si vous avez une politique active Compte AWS, vous pouvez utiliser ce lien ReadOnlyAccesspour 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 Gestion des identités et des accès AWS 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": [
        "*"
      ]
    }
  ]
}
```

Règles de pare-feu d'accès par défaut

Il s'agit des règles de pare-feu par défaut requises pour accéder à vos instances.

> **Note**
>
> Pour plus d'informations sur les règles de pare-feu et les ports requis pour établir une confiance unidirectionnelle AD, consultez le guide de sécurité AMS en accédant à la console AWS Artifact -> onglet Reports et en recherchant AWS Managed Services.

Ports d'instance Linux Stack

Ces règles sont requises pour votre authentification dans les stacks AMS Linux.

Règles de port des instances Linux DEPUIS : instance Linux Stack VERS : contrôleur de domaine CORP

Port	Protocole	Service	Direction
389	TCP	LDAP	Ingress
389	UDP	LDAP	Ingress
88	TCP	Kerberos	Ingress
88	UDP	Kerberos	Ingress

Ports d'instance Windows Stack

Ces règles sont requises pour votre authentification dans AMS Windows Stacks.

DEPUIS : instance Windows Stack VERS : contrôleur de domaine CORP

Port	Protocole	Service	Direction
88	TCP | UDP	Kerberos	Entrée et sortie
135	TCP | UDP	Service de localisation DCE/RPC	Entrée et sortie

Port	Protocole	Service	Direction
389	TCP | UDP	LDAP	Entrée et sortie
3268	TCP | UDP	msft-gc, Microsoft Global Catalog (service LDAP contenant des données provenant de forêts Active Directory)	Entrée et sortie
445	TCP	Microsoft-DS Active Directory, partages Windows	Entrée et sortie
49152 - 65535	TCP	Ports dynamiques ou privés qui ne peuvent pas être enregistrés auprès de l'IANA. Cette gamme est utilisée pour des services privés, personnal isés ou à des fins temporaires et pour l'attribution automatique de ports éphémères.	Entrée et sortie

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'opérate

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'orienta tion 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 : représent ant de l'opérate ur de l'applica tion, représent ant 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
Compilation des recommandations de réduction des coûts et préparation du rapport	I	R
Présentation d'un rapport sur les économies de coûts	C	R
Planification des changements associés à la réduction des coûts	R	C
Évaluation de l'impact du	R	C

Activité	Client	AMS
changement et des risques		
Récolter RFCs des fonds pour mettre en œuvre les changements	R	C
Révision RFCs et mise en œuvre des modifications	C	R
Tester l'application et valider la mise en œuvre des modifications	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.

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 migrate/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 résultantes	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 AMSet 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 chacune de ces unités d'organisation est soumise au mode AMS spécifique proposé par ces unités d'organisation fondamentales. 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, et d'EC2, 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 minimes 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 Servic	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.			Non applicable	Client responsable des	

Problèmes de décision	Mode CM standard/ OOD *	AWS Servic	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 Servic	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 Servic	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 Servic	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 Servic	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 CICD dans AMS : un client cherche à configurer un pipeline CICD 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 CICD 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 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'`CreateRfc`API. 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 CreateRfcsection 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'`CreateRfc`API, 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, voirCréation d'une RFC.

Rubriques

- Qu'est-ce que c'est 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

Qu'est-ce que c'est 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.

RFCs passer par deux étapes clés : la validation et l'exécution.

1. Au cours de la phase de validation, AMS vérifie l'exhaustivité et l'exactitude de la demande RFC. AMS évalue également la demande de sécurité conformément à nos normes techniques de sécurité. AMS vérifie que la modification demandée est valide et exécutable.
2. Au cours de la phase d'exécution, AMS tente d'apporter les modifications demandées à votre compte.

AMS gère les deux étapes par le biais d'un processus automatisé, d'un processus manuel ou d'une combinaison des deux. Le processus manuel est géré par l'équipe des opérations AMS. Pour de plus amples informations, veuillez consulter Automatisé et manuel CTs.

AMS propose trois modes d'exécution pour le traitement des demandes :

- Mode d'exécution (recommandé par AMS) : Automatisé. Ils CTs utilisent l'automatisation pour les validations et les exécutions des RFC, ce qui constitue le moyen le plus rapide d'atteindre vos objectifs commerciaux.
- (Suggéré par AMS) Mode d'exécution : manuel et désignation : automatisation gérée. Ils CTs utilisent une combinaison de processus automatisés et manuels pour les validations et les exécutions des RFC. Si l'automatisation ne peut pas exécuter la modification demandée, le RFC est transféré (par routage automatique ou par la création d'un RFC de remplacement) à l'équipe des opérations AMS pour un traitement manuel. Leur soumission CTs permet une prise en charge plus structurée de votre demande, complétée par l'automatisation AMS afin d'améliorer le délai de traitement et d'exécution des résultats.
- Mode d'exécution : manuel et désignation : révision requise. Modifications demandées via ct-1e1xtak34nx76 Management | Autre | Autre | Mise à jour (révision requise) ou ct-0xdawir96cy7k Management | Autre | Autre | Créer (révision requise). Celles-ci CTs reposent sur une manipulation

manuelle pour les validations et les exécutions. Elles CTs dépendent de l'interprétation manuelle de la demande de modification.

AMS vous avertit lorsque la modification s'est terminée avec succès (réussite) ou non (échec).

> **Note**
>
> Pour plus d'informations sur le dépannage des défaillances RFC, consultezRésolution 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 AssumeRoleWithWebIdentityAWS 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 profil `set AWS_DEFAULT_PROFILE=saml` (pour Windows ; pour Linux, ce serait le cas`export 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 ActionStateest automatiquement définie sur. AwsActionPending
- Lorsqu'une RFC est créée, elle ActionStateest automatiquement définie sur. NoActionPending
- Lorsqu'un RFC est soumis, le ActionStateest automatiquement défini sur. AwsActionPending
- Lorsqu'un RFC est rejeté, annulé ou terminé avec un statut de réussite ou d'échec, ActionStateil 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'exécuti on, 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 égalementMettre 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 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 correction de la dérive 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 « automatisation gérée », l'autre est mode d'exécution = automatisé.

Ressources prises en charge pour la correction de la dérive (ct-3kinq0u4l33zf)

Il s'agit des ressources prises en charge par le type de modification de correction de la dérive (ct-3kinq0u4l33zf). Pour corriger n'importe quelle ressource, utilisez plutôt le type de modification « automatisation gérée » (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 correction de la dérive

Questions et réponses sur l'utilisation des types de modifications de correction de dérive AMS.

Pour obtenir la liste des ressources prises en charge pour la fonctionnalité de correction de la dérive, consultezRessources prises en charge pour la correction de la dérive (ct-3kinq0u4l33zf).

> **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 (ct-3kinq0u4l33zf), sans automatisation gérée, ne prend en charge que 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 vous recommandons d'utiliser la tomodensitométrie automatisée sans automatisation gérée (ct-3kinq0u4l33zf) 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 l'automatisation gérée, le manuel ou le CT à la place.

Nous recommandons d'utiliser l'automatisation gérée, la tomographie manuelle (ct-34sxfo53yuzah) uniquement lorsque les types de ressources dérivées ne sont pas pris en charge par la correction de la dérive, aucune automatisation gérée, automatisée, la tomographie automatique (ct-3kinq0u4l33zf), ou lorsque la correction de la dérive (aucune automatisation gérée, automatisée, tomodensitométrie) 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 pendant 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 Gestion | Autres | Autres requêtes.

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 si la correction échoue ?

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 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 DryRunoption 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 d'automatisation gérés, il est nécessaire que vous demandiez 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 « automatisations gérées » ASAP RFCs sont automatiquement rejetées 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. Dans le cas d'un changement de type « automatisation gérée », 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 a`RequestedStartTime`, le RFC est considéré comme planifié et `RequestedEndTime` est renseigné à l'aide de la `ExecutionDurationInMinutes` valeur.
- seulement un`RequestedEndTime`, 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'autre`RequestedEndTime`, 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 le mode manuel 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 : ApproveRfcmarque 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 : RejectRfcmarque 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 UpdateRestrictedExecutionTimesAPI 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 ListRestrictedExecutionTimesAPI. Exemple :

```
aws amscm  --profile saml list-restricted-execution-times
```

Si vous souhaitez soumettre une RFC pendant une durée d'exécution limitée spécifiée, ajoutez le RestrictedExecutionTimesOverrideIdavec 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 :

Fonctionnement :

1. Accédez à la page Créer une RFC : Dans le volet de navigation de gauche de la console AMS, cliquez RFCspour 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

Fonctionnement :

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 (évitez 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-0ltm873rsebx9 |
+-----------+--------------------------+--------------------------+
```

2. Trouvez la version la plus récente du CT :

   `ChangeTypeId`et `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 CT à longue durée UserData : Create EC2 et 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-sdhopv00000000000",
"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, cela s'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). UserData 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, piles 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 par`Canceled`) :

   ```
   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 AwsOperatorAssignedle fait qu'un opérateur examine actuellement la RFC, AwsActionPendingce qui signifie qu'un opérateur AMS doit effectuer quelque chose avant que l'exécution de la RFC ne puisse se poursuivre, ou CustomerActionPendingle 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).
   - État : Planifié, annulé, en cours, réussi, rejeté, modifié ou échec.
   - 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 ListRfcSummariesfonctionnement 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 et`Values`.

Filtrage RFC

Attribut	Valeurs valides	Conditions valides	État par défaut	Remarques
ActualEndTime	Toute chaîne représentant une ISO8601 date et une heure (par exemple, « 20170101T 000000Z »)	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 ISO8601 date/heure (par exemple, « 20170101T 000000Z »)	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
AutomationStatusId	Manuel, automatisé	Égal à	Égal à	Il n'y a que deux statuts d'automatisation

Attribut	Valeurs valides	Conditions valides	État par défaut	Remarques
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 ISO8601 date/heure (par exemple, « 20170101T 000000Z »)	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 ISO8601 date/heure (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 ISO8601 date/heure (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 ISO8601 date/heure (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 ISO8601 date/heure (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
Titre	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-123h45t6uz7jl|
|Management| Monitoring & Notification  |SQS    |Update |ct-123h45t6uz7jl|
+----------+---------------------------------+-------+-------+----------------+
```

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 requête au format 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 RFCsliste 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, consultez 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'`query`argument 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 spécifiiez 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'`--region`option 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'`--region`option.

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 vous 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'`AutomationStatusId`attribut 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.

> **Note**
>
> Lorsque vous utilisez le mode manuel 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, voirAutomatisé 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.

Si la condition d'approbation du CT est	Il nécessite l'approbation de	And
`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'ApproveRfcopération.
`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.
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 souhaiterez 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-sft6rv00000000000",
      "type": "string",
      "enum": ["stm-sft6rv00000000000"]
    },
    "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.",
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "Key": {
            "type": "string",
            "minLength": 1,
```

La première partie du schéma fournit des informations à AMS sur le type de modification demandé.

```
            "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.",
          "type": "string",
          "minLength": 1,
          "maxLength": 100,
          "pattern": "^[a-zA-Z0-9._+=,@-]{1,100}$"
        }
```

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 quels paramètres sont obligatoires et lesquels sont facultati fs.

```
      },
      "additionalProperties": false,
      "required": [
        "CodeDeployApplicationName"
      ]
    }
  },
  "additionalProperties": false,
  "required": [
    "Description",
    "VpcId",
    "StackTemplateId",
    "Name",
    "TimeoutInMinutes",
    "Parameters"
  ]
}
```

> **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'`--query`option.

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-abc123 xyz7890)	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 une pile liée à EC2. 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.

AMS a pour objectif de répondre à un scanner manuel dans les huit heures et répondra 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 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 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 débloquer 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 l'absence 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, consultezComprendre 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 CloudFormation des modèles. En tant que client, vous avez un accès en lecture seule à tous les services AWS. Vous pouvez notamment CloudFormation identifier rapidement la CloudFormation pile qui représente votre pile en fonction de la description de la pile à l'aide de la CloudFormation console. La pile défaillante sera probablement dans l'état DELETE_COMPLETE. Une fois que vous avez identifié la 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 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)
- Création d'une pile EC2 : 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 s'exécutant en tant que serveur virtuel dans le cloud. Les AMI sont très utiles et nécessaires pour créer des instances EC2 ou des groupes Auto Scaling ; vous devez toutefois 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 défaillance d'EC2 ou d'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 Créer. 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 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. Pour plus d'informations, consultez Correspondance et pièce jointe RFC (console).

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 instances EC2 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'instance EC2 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 instance EC2 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 le`customer-mc-ec2-instance-profile`, vous pouvez vérifier cela dans la console EC2 :

Erreurs d'arrêt de la pile d'instances EC2

- Vérifiez si l'instance est déjà arrêtée ou terminée.
- Si l'instance EC2 est en ligne et que le `InternalError` message d'erreur s'affiche, envoyez 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-3mvvt2zkyveqj pour arrêter une instance de groupe Auto Scaling (ASG). Si vous devez arrêter une instance ASG, soumettez une demande de service.

La pile d'instances EC2 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.

Erreurs de restauration du volume d'instance EC2

AMS crée une RFC de dépannage interne lorsque la restauration du volume d'instance EC2 échoue. Cela est dû au fait que la restauration du volume d'instance EC2 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.

- Si vous avez besoin d'assistance pour une RFC ouverte ou une RFC terminée mais incorrecte, contactez AMS via une correspondance bidirectionnelle RFC. Pour plus d'informations, consultez Correspondance et pièce jointe RFC (console).
- 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, consultez la section 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`, ou`AWSServicePrincipals`. 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-accès [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 queCreate/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 (voirRôles 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 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	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. La norme indiquée dans le tableau AMS-STD-003 ci-dessous indique que vous pouvez modifier l'environnement et AppId AppName, mais pas pour les ressources appartenant à AMS. Non réalisable par le biais des autorisations IAM.	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.
Aucune balise figurant sur les piles appartenant à AMS ne doit être	Oui CloudFormation ne prend pas en charge la `aws:TagsKey` condition de		

Normes	Est-ce que ça se casse	Risques	Recommandations
supprimée en fonction de vos demandes de modification.	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 EC2 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	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	L'utilisateur IAM doit être limité dans le temps et bénéficier d'autorisations basées sur le moindre privilège et. need-to-know

Normes	Est-ce que ça se casse	Risques	Recommandations
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.		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.	

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 formel d'acceptation des risques ou d'un cas d'utilisation valide par les équipes internes.	Oui. Les actions en libre-service vous permettent d'associer et de dissocier des adresses IP élastiques (EIP).	L'ajout d'une adresse IP élastique à une instance l'expose à Internet. Cela augmente le risque de divulgation d'informations et d'activités non autorisées.	Bloquez tout trafic inutile vers cette instance par le biais de groupes de sécurité et vérifiez 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.

Normes	Est-ce que ça se casse	Risques	Recommandations
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.
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.	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.	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. Nous pouvons vérifier cela de plusieurs manières, consultez votre responsable de prestation de services cloud (CSDM).
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 Organizations compte ou en faisant correspondre le domaine de messagerie au nom de l'entreprise du client et au compte lié à PAYER) à l'aide d'outils internes.			

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	Créer
Gestion des identités et des accès AWS (JE SUIS)	N’importe lequel
Site-to-Site VPN	N’importe lequel
Planificateur de ressources AMS	
AWS Backup	Création d'un plan de sauvegarde
Ingestion de la charge de travail AMS (WIGs)	N’importe lequel
Modifications du compte AMS Advanced MALZ	
Amazon GuardDuty	
Accès avancé à AMS Stack	N’importe lequel
Volume Amazon Elastic Block Store (EBS)	Suppression
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 de sécurité Amazon EC2	N’importe lequel
AMS (SSPS avancé)	
AWS Microsoft AD géré	

Service	Action
Mode développeur AMS Advanced	
Amazon Simple Storage Service (Amazon S3)	Création de politiques relatives aux compartiments S3
AWS Systems Manager	Créer

Création de piles à l'aide du mode Direct Change

Pour que la pile soit gérée par AMS`AWSManagedServicesCloudFormationAdminRole`, 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 CloudFormation (CFN) de créer ou de mettre à jour la pile. Pour ce faire, vous devez transmettre le dans 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. APIs
> 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'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'`Transform`instruction 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 CloudFormation

- Intégrez l' CloudFormationoutillage 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 `AWSManagedServicesDevelopmentRole` prédéfini Gestion des identités et des accès AWS (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 Gestion des identités et des accès AWS (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 : `AWSManagedServicesDevelopmentRole`
- 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 dansPrérequis 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 (automatisation gérée). Pour un exemple d'utilisation de ce CT, voir Mode développeur | Activer (automatisation gérée).

   Une fois le CT traité, le rôle IAM prédéfini (`AWSManagedServicesDevelopmentRole`pour MALZ, `customer_developer_role` pour SALZ) est configuré dans le compte demandé.
3. Attribuez le rôle approprié aux utilisateurs qui ont besoin d'un accès 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.

Service	Remarques
	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 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` • `ds:GetAuthorizedApplication Details` • `ds:ListAuthorizedApplications` • `ds:UnauthorizeApplication` 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.

Service	Remarques
Amazon Elastic Compute Cloud	Impossible d'accéder à Amazon EC2 APIs contenant la chaîne : `DhcpOptio ns Gateway`,`Subnet`,`VPC`, et`VPN`. Impossible d'accéder aux EC2 ressources Amazon dont le préfixe de balise est`AMS`,, `mcManagementHostASG` , and/or `sentinel` 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
Gestion des identités et des accès AWS (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 (`AWSManagedServices DevelopmentRole` 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 :`AWSManagedServices DevelopmentRolePermissionsBoundary` , 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 par`AMS`.
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
Groupes de ressources AWS	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 Directeur (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 : • `lakeformation:DescribeResource` • `lakeformation:GetDataLakeSettings` • `lakeformation:DeregisterResource` • `lakeformation:RegisterResource` • `lakeformation:UpdateResource` • `lakeformation:PutDataLakeSettings`
Amazon Elastic Inference	Vous pouvez uniquement appeler l'action Elastic Inference API. `elastic-inference:Connect` Cette autorisation est incluse dans `customer_sagemaker_admin_policy` le document joint `aucustomer_sagemaker_admin_role` . 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 Gestion des identités et des accès AWS 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 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 en a 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 Lambdan'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.
- `CREATE`les 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 approvisionner 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-approvisionné | Ajouter (automatisation gérée) (ct-3qe6io8t6jtny). Cette RFC attribue le rôle IAM suivant à votre compte :. `customer_alexa_console_role` Un `customer_alexa_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 fonctionne 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_alexa_gateway_installer_user` et `customer_alexa_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 Deployment | Advanced stack components | Identity and Access Management (IAM) | Create entity or policy (automatisation gérée) de type (automatisation gérée) (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 Autorité de certification privée 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 WorkSpaces Applications sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'Amazon WorkSpaces Applications (WorkSpaces Applications) directement depuis votre compte géré AMS. WorkSpaces Les applications vous permettent de déplacer vos applications de bureau vers AWS, sans les réécrire. Vous pouvez installer vos applications sur WorkSpaces Applications, définir des configurations de lancement et mettre vos applications à la disposition des utilisateurs. WorkSpaces Applications 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. WorkSpaces Les applications vous permettent de lancer des applications sur votre propre réseau, ce qui signifie que vos applications peuvent interagir avec vos AWS ressources existantes.

Amazon WorkSpaces Applications 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 WorkSpaces Applications.

WorkSpaces FAQ sur les applications dans AWS Managed Services

Q : Comment puis-je demander l'accès aux WorkSpaces applications depuis mon compte AMS ?

Demandez l'accès aux WorkSpaces applications 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 WorkSpaces des applications sur 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 de points de terminaison VPC d'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.
  - Joindre WorkSpaces des flottes d'applications et des générateurs d'images aux domaines Microsoft Active Directory.
  - Création de rapports d'utilisation personnalisés pour les WorkSpaces applications.
  - L'image de marque personnalisée n'est actuellement pas prise en charge.

Q : Quels sont les prérequis ou les dépendances pour utiliser WorkSpaces les applications dans mon compte AMS ?

Lorsque vous soumettez la RFC aux WorkSpaces applications intégrées, incluez le nom du compartiment Amazon S3 à utiliser pour le rapport d'utilisation WorkSpaces des applications. Le nom du bucket est ajouté au `customer-appstream-usagereports-policy` bucket créé lors de l' WorkSpaces intégration des applications.

Q : Quelles fonctionnalités WorkSpaces des applications doivent être séparées RFCs ?

- Afin de choisir un point de terminaison VPC d'interface pour les WorkSpaces applications, soumettez une RFC de type Management | Other | Other | Update pour créer un point de terminaison VPC dans votre compte. Pour savoir comment créer des points de terminaison personnalisés pour les WorkSpaces applications, consultez la section Création et diffusion à partir de points de terminaison VPC d'interface dans WorkSpaces le guide de l'utilisateur des applications.
- 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 aux WorkSpaces applications les autorisations dont elles ont besoin 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 WorkSpaces le guide de l'utilisateur des applications.
- Pour créer et 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 (automatisation gérée) (ct-3dpd8mdd9jn1r) demandant le rôle IAM avec la politique requise. Le nom du rôle IAM doit toujours commencer par le préfixe « customer_appstream ».
- WorkSpaces Les flottes et les générateurs d'images Amazon Applications peuvent être joints à des domaines dans Microsoft Active Directory en soumettant une RFC de type de modification de type 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 WorkSpaces des applications, à la section Octroi d'autorisations pour créer et gérer des objets informatiques Active Directory.
- Afin de créer des rapports d'utilisation WorkSpaces des applications 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`
  - L'ARN du compartiment Amazon S3 pour les WorkSpaces applications, les rapports d'utilisation et les journaux.

Une fois le rôle configuré, intégrez-le à votre solution de fédération et connectez-vous, puis accédez à Athena pour générer AWS GlueAWS Glue des rapports personnalisés à l'aide du rôle de rapport d'utilisation. Pour plus de détails sur l'utilisation WorkSpaces des rapports d'utilisation des applications, voir Création de rapports personnalisés et analyse WorkSpaces des données d'utilisation des applications dans la documentation WorkSpaces des applications.

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, AWS Glue les autorisations 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 (automatisation gérée) (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 (`AWSManagedServicesAdminRole`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-caseun 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 (automatisation gérée) (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 à la prise en charge 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 créé pour ce 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 (automatisation gérée) (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 (automatisation gérée) (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 (automatisation gérée) (ct-3qe6io8t6jtny). Cette RFC attribue le rôle IAM

suivant à votre 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 EC2) 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 d'entité ou de politique de mise à jour (automatisation gérée) Management | Advanced stack components | Identity and Access Management (IAM) | Update (automatisation gérée) (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 Gestion des identités et des accès AWS (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 dans votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités d'EC2 Image Builder directement dans votre compte géré AMS. EC2 Image Builder est un service entièrement AWS géré qui facilite l'automatisation de la création, de la gestion et du déploiement d'images de serveur personnalisées, sécurisées up-to-date et « 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 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.

FAQ sur EC2 Image Builder dans AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès à EC2 Image Builder depuis mon compte AMS ?

Demandez l'accès en soumettant un type de modification Gestion | AWS service | Service auto-approvisionné | Ajouter (automatisation gérée) (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 relatives 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 ?

- Rôle lié à un service EC2 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}/*`). Par exemple :

  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 Conteneurs sur AWS) sans avoir à gérer des serveurs ou des clusters d'instances Amazon EC2. 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_rolecustomer_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 Activation du 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-approvisionnement :
  - 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 (automatisation gérée) (ct-1oxx2g2d7hc90). 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 (automatisation gérée) (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 groupes de nœuds EC2 gérés ou autogérés n'est pas prise en charge dans AMS. Si vous devez utiliser des nœuds de travail EC2, 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.

- EKSCTL 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 plus d'informations, veuillez consulter la rubrique
    - Activation des rôles IAM pour les comptes de service de votre cluster
    - Présentation de rôles IAM précis pour les comptes de service
- Nous recommandons que les règles Config soient configurées et surveillées pour
  - Points de terminaison de clusters publics
  - Journalisation de l'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 de l'équilibreur de charge d'application (ALB) 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 des enveloppes, consultez Amazon EKS ajoute le chiffrement des enveloppes 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 (automatisation gérée) (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 cluster EC2 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
  - Profil d'instance EC2 : customer_emr_cluster_instance_profile
  - Rôle Auto Scaling : customer_emr_cluster_autoscaling_role
- Groupes de sécurité EC2 :
  - 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 | Add (automatisation gérée) (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 changement d'entité ou de politique (automatisation gérée) Deployment | Advanced stack components | Identity and Access Management (IAM) | Create entity or policy (automatisation gérée) (ct-3dpd8mdd9jn1r) avant de l'utiliser pour déclencher EventBridge d'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 auditiez 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 (automatisation gérée) 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 Gestion des identités et des accès AWS (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 Gestion des identités et des accès AWS, 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-36cn2avfrrj9v), 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-approvisionné | Ajouter (automatisation gérée) (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 (automatisation gérée) (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 (automatisation gérée) (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 (automatisation gérée) (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 (Managed automation) :

  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 Quick sur votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux fonctionnalités Quick directement dans votre compte géré AMS. Quick est un service de business intelligence rapide et basé sur le cloud qui fournit des informations à tous les membres de votre organisation. En tant que service entièrement géré, Quick vous permet de créer et de publier facilement des tableaux de bord interactifs qui incluent des informations sur l'apprentissage automatique (ML). Pour en savoir plus, consultez Amazon Quick.

FAQ sur Quick in AWS Managed Services

Questions et réponses courantes :

Q : Comment puis-je demander l'accès à Quick dans 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 relatives à l'utilisation de Quick sur mon compte AMS ?

- AWS les paramètres des ressources sur Quick 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.
- Quick 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 permettant d'intégrer Quick à Active Directory (AD). Quick on AMS ne prend pas en charge l'intégration avec AD en raison d'incompatibilités entre la structure du compte AMS et les exigences de Quick Trust.

Q : Quels sont les prérequis ou les dépendances pour utiliser Quick dans mon compte AMS ?

- Lorsque AMS reçoit cette RFC pour ajouter Quick, vous recevez une demande de service pour obtenir des informations supplémentaires ; fournissez-leur les informations suivantes :
  - Nom rapide du compte (par exemple, *`CustomerName`*`-quicksight`
  - Édition rapide (Standard ou Enterprise)
  - AWS Région dans laquelle activer le service rapide (par défaut, c'est votre AWS région AMS).
  - Une adresse e-mail de notification pour le compte Quick.
  - (Facultatif) Le compartiment S3 dans lequel se trouvent les fichiers de données à analyser.

- Le VPC et le sous-réseau IDs qui se connectent à Quick prennent en charge une fonctionnalité permettant d'ajouter une connexion VPC, qui permet une connectivité privée entre Quick et les ressources du compte.

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-approvisionné | Ajouter (automatisation gérée) (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). {région} .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 : Passing `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 (automatisation gérée) (ct-27tuth19k52b4) pour augmenter les autorisations de mise à l'échelle automatique temporairement ou définitivement, car l'autoscaling 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 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 (automatisation gérée) (ct-3qe6io8t6jtny). Cette RFC fournit les rôles IAM suivants à votre compte :`customer_textract_console_role`,`customer_textract_human_review_execution_ro`

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 (automatisation gérée) (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 postes de travail 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 (automatisation gérée) (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 l'utiliser WorkSpaces dans 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 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 un compte de services partagés géré par AMS, soumettez une autre RFC de type 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, consultezUtilisez 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, consultezUtilisez 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, consultezUtilisez 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, consultezUtilisez 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 (automatisation gérée) (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_rolecustomer_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'informationsUtilisez AMS SSP pour approvisionner AWS CodeBuild votre compte AMS, voirUtilisez AMS SSP pour approvisionner AWS CodeDeploy votre compte AMS, etUtilisez 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 CodeCommit est limitée ; les utilisateurs doivent s'authentifier avec Credential Helper. Certaines commandes KMS sont également restreintes : kms: Chiffrer, kms: Déchiffrer, kms:ReEncrypt, kms: GenereteDataKey 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 Amazon EC2/ sur site 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
  - Étape Invoke : 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 approvisionner 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-approvisionné | Ajouter (automatisation gérée) (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 approvisionner 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 | Self-provisioned Service | Add (automatisation gérée) (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 AWS Audit Manager sont fournies pour.

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 Autorité de certification privée, vous payez mensuellement pour le fonctionnement du 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 des certificats existants, car ces actions nécessitent un accès administrateur complet (utilisez le type de modification Management | Advanced stack components | ACM | Delete certificate certificate (ct-1q8q56cmwqj9m)). 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 Autorité de certification privée votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS Autorité de certification privée 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 instances EC2, 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-0fpjlxa808sh2 (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 (automatisation gérée) (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 utiliser CloudEndure 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 approvisionner 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 à l' CodePipeline aide d'une seule RFC, soumettez le type de changement Management | AWS Service | Self-provisioned Service | Add (automatisation gérée) (ct-3qe6io8t6jtny) et demandez les trois services :, et. CodeBuild CodeDeploy CodePipeline Ensuite, les trois rôles, `customer_codebuild_service_rolecustomer_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 utiliser CodeBuild mon compte AMS ?

Si des autorisations IAM supplémentaires sont requises pour le rôle de AWS CodeBuild service défini, demandez-les via 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 à l' CodePipeline aide d'une seule RFC, soumettez le type de changement Management | AWS Service | Self-provisioned Service | Add (automatisation gérée) (ct-3qe6io8t6jtny) et demandez les trois services :, et. CodeBuild CodeDeploy CodePipeline Ensuite, les trois rôles, `customer_codebuild_service_rolecustomer_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:Encryptkms:Decrypt`,`kms:ReEncrypt`,`kms:GenereteDataKey`,`kms:GenerateDataKeyWithou` `etkms:DescribeKey`.

Q : Quels sont les prérequis ou les dépendances pour pouvoir l'utiliser AWS CodeCommit dans mon compte AMS ?

Si les compartiments S3 sont chiffrés à l'aide de clés KMS, S3 et KMS doivent être utilisés AWS CodeCommit.

Utilisez AMS SSP pour approvisionner 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 et vos AWS Fargate serveurs AWS Lambda 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 à l' CodePipeline aide d'une seule RFC, soumettez le type de changement Management | AWS Service | Self-provisioned Service | Add (automatisation gérée) (ct-3qe6io8t6jtny) et demandez les trois services :, et. CodeBuild CodeDeploy CodePipeline Ensuite, les trois rôles, `customer_codebuild_service_rolecustomer_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 prenons uniquement en charge les plateformes de calcul telles qu'Amazon EC2/ 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 approvisionner 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 à l' CodePipeline aide d'une seule RFC, soumettez le type de changement Management | AWS Service | Self-provisioned Service | Add (automatisation gérée) (ct-3qe6io8t6jtny) et demandez les trois services :, et. CodeBuild CodeDeploy CodePipeline Ensuite, les trois rôles, `customer_codebuild_service_rolecustomer_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 nommécustomer_code_pipeline_lambda_execution_role, qui sera une copie decustomer_lambda_basic_execution_role. customer_code_pipeline_lambda_policy

Q : Quels sont les prérequis ou les dépendances pour pouvoir l'utiliser CodePipeline dans 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 Optimiseur de calcul AWS votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux Optimiseur de calcul AWS fonctionnalités directement dans votre compte géré AMS. Optimiseur de calcul AWS 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 ASG) 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'instances Amazon EC2 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 Optimiseur de calcul AWS.

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 (automatisation gérée) (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 Optimiseur de calcul AWS 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 reflex est étiqueté « AWSService RoleForComputeOptimizer ». Pour plus d'informations, voir Utilisation de rôles liés à un service pour Optimiseur de calcul AWS
- CloudWatch les métriques doivent être activées pour les métriques suivantes :
  - Utilisation du processeur : pourcentage d'unités de calcul Amazon EC2 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 (automatisation gérée) (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 utiliser DataSync 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'ID de l'AMI AWS DataSync Amazon EC2, le type d'instance, le sous-réseau, le groupe de sécurité ; et faites référence à une paire de clés Amazon EC2 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'AMI AWS DataSync Amazon EC2.

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 (automatisation gérée) (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 utiliser AWS Device Farm mon compte AMS ?

Aucune.

Utilisez AMS SSP pour approvisionner Reprise après sinistre AWS Elastic votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux Reprise après sinistre AWS Elastic fonctionnalités directement dans votre compte géré AMS. Reprise après sinistre AWS Elastic 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 Reprise après sinistre AWS Elastic 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 Reprise après sinistre AWS Elastic.

Reprise après sinistre AWS Elastic dans la FAQ AWS Managed Services

Q : Comment puis-je demander l'accès Reprise après sinistre AWS Elastic à mon compte AMS ?

Demandez l'accès en soumettant un type de modification Gestion | AWS service | Service auto-approvisionné | Ajouter (automatisation gérée) (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 Reprise après sinistre AWS Elastic sur mon compte AMS ?

Il n'y a aucune restriction d'utilisation Reprise après sinistre AWS Elastic dans votre compte AMS.

Q : Quels sont les prérequis ou les dépendances pour pouvoir l'utiliser Reprise après sinistre AWS Elastic dans 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 (automatisation gérée) 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 . 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 (automatisation gérée) (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 utiliser MediaConvert 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 (automatisation gérée) (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 (automatisation gérée) (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 four`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 l'utiliser MediaPackage dans 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 Il 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 (automatisation gérée) (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 un type de modification Management | AWS service | Self-provisioned Service | Add (automatisation gérée) (ct-3qe6io8t6jtny) et ajouter explicitement 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-approvisionné | Ajouter (automatisation gérée) (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 (automatisation gérée) (ct-3qe6io8t6jtny).

Q : Quels sont les prérequis ou les dépendances pour pouvoir l'utiliser AWS Lambda dans 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 (automatisation gérée) (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`Il 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 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,`AWSManagedServicesChangeManagementRole`.
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 Suivant.
5. Entrez le nom et la description du secret, le nom commence toujours par customer-shared/. Par exemple customer-shared/mykey2022. Cliquez sur 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`AMSSecretsManagerSharedPolicy`, est attaché au `AWSManagedServicesChangeManagementRole` 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 CSPM votre compte AMS

Utilisez le mode AMS Self-Service Provisioning (SSP) pour accéder aux AWS Security Hub CSPM fonctionnalités directement dans votre compte géré AMS. AWS Security Hub CSPM 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 CSPM centralise et hiérarchise les résultats de sécurité et de conformité provenant de AWS comptes, de services et de 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 CSPM.

FAQ sur le Security Hub CSPM dans AWS Managed Services

Q : Comment puis-je demander l'accès AWS Security Hub CSPM à mon compte AMS ?

Demandez l'accès au Security Hub CSPM 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 CSPM 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 l'utiliser AWS Security Hub CSPM dans mon compte AMS ?

Il n'y a aucun prérequis ni aucune dépendance à utiliser AWS Security Hub CSPM 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 | Add (automatisation gérée) (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 le`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 DDo. Cela est recommandé par AMS pour remédier le plus rapidement possible aux attaques DDo S, 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 vélocité 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 : assertAwsResource 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 condition nelles	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'automat isation —	Exécuter une autre automatis ation	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- RunShellS cript et AWS- RunPowerS hellScript
aws:sleep —	Retarder une automatisation	Aucune limitation
lois : waitForAws ResourceP roperty —	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-approvisionnement,
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'examens 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/Exportcapabilities 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-useinstances. 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-117rmp64d5mvb : 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.

Intégration à la zone d'atterrissage multi-comptes (MALZ) d'AMS

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 organisationnelles
- 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 organisationnelles

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 comme une seule unité)
- Les applications OU
- 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 (automatisation gérée). 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 pour 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 (automatisation gérée).

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 réutiliseriez 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.
Frais de configuration initiale (dans le respect des project/	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.

Entité	Zone d'atterrissage AMS unique	Plusieurs zones d'atterrissage (deux ou plus)
migration délais)		
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.
Evolutivité	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 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.

Entité	Zone d'atterrissage AMS unique	Plusieurs zones d'atterrissage (deux ou plus)
Risque opérationnel	(Cela dépend) Faible. Intégration opérationnelle et disponibilité opération nelle une seule fois. Moins de risques de dérives du processus.	(Cela dépend) Faible. Multiples activités d'intégration et opération nelles. 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.
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 modificat ions 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'outboun d (sortie) ne peuvent avoir d'impact que sur les charges de travail dans cette zone de landing multi-comptes spécifique.

Entité	Zone d'atterrissage AMS unique	Plusieurs zones d'atterrissage (deux ou plus)
Contrôles des données et des accès	(Cela dépend) Peu de contrôle si vous souhaitez vous connecter à différent s 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 différent s réseaux sur site et sur site pour les charges de travail Prod ADs et Non-Prod. Utilisez des zones d'atterri ssage séparées pour des exigences de conformité strictes.
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'atterri ssage 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 équilibreurs 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 effectuer les actions suivantes :

- 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.

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). Un aperçu général des ressources contenues dans le compte Shared Services est présenté dans le graphique suivant.

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 de 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 instances EC2, des instances EC2 relais et un agent présent dans tous les plans de données et les instances EC2 du client.

  Vous devez utiliser le `EPSMarketplaceSubscriptionRole` 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/VPNà 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 il peut 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, consultezModes 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 CustomerDefaultAssumeRolerôle.
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 `AWSManagedServicesMigrationRole` 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-dateinformations 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 `AWSManagedServicesMigrationRole` 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 : `AWSManagedServicesMigrationRole`
   - 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 (automatisation gérée).

   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 (automatisation gérée) (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 console EC2.

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.

MALZ : Intégration du compte principal

Les tâches principales que vous devrez accomplir lors de l'intégration à un AWS compte principal de zone de landing zone multi-comptes sont les suivantes :.

Rubriques

- Créez un AWS compte principal de zone de landing zone multi-comptes dans AMS
- Créez un rôle IAM pour qu'AMS puisse accéder à votre compte
- Sécurisez le nouveau compte avec l'authentification multifactorielle (MFA) pour l'utilisateur root dans AMS
- Abonnez-vous à AWS Marketplace for Trend Micro Endpoint Protection (EPS)
- Configuration de la mise en réseau
- Configuration de la gestion des accès

Pour toute question relative à l'intégration, contactez votre architecte cloud.

Créez un AWS compte principal de zone de landing zone multi-comptes dans AMS

La zone de destination multi-comptes AMS nécessite la mise en service d'un nouveau compte Amazon Web Services (AWS) qui servira de compte de gestion dans l'environnement de zone d'atterrissage multi-comptes AMS. Pour créer un Compte AWS, suivez ces step-by-step instructions : Comment créer et activer un nouveau compte Amazon Web Services ?

Les étapes simples sont les suivantes : accédez à Créer un compte, cliquez sur S'inscrire maintenant et, sur la page qui s'ouvre, cliquez sur Créer un nouveau Compte AWS. Suivez les instructions affichées à l'écran, notamment la réception d'un appel téléphonique et la saisie d'un code PIN à l'aide du clavier de votre téléphone. Vous devrez également saisir une carte de crédit. AMS utilise

ce compte comme compte de gestion, ou compte payeur, pour votre nouvelle zone de landing zone multi-comptes.

> **Note**
>
> Une fois que vous serez intégré, demandez à votre responsable de prestation de services cloud (CSDM) de transférer la facturation de votre carte de crédit vers un système de facturation. Les informations suivantes seront requises :
>
> - Nom de la société de facturation
> - Nom du contact de facturation
> - Numéro de téléphone du contact de facturation
> - Adresse e-mail du contact de facturation
> - Adresse de facturation
>
> Votre CSDM vous aidera à effectuer cette mise à jour. Une fois terminé, et pour modifier le mode de paiement, consultez la section Gestion de vos modes AWS de paiement.

> **Note**
>
> N'associez pas votre nouveau compte à un compte de gestion ou à un compte payeur existant.
> Assurez-vous que votre compte ne fait pas partie d'un compte existant AWS Organizations ; pour plus d'informations, voir Qu'est-ce que c'est AWS Organizations ?

> **Important**
>
> Il est très important de vous assurer qu'une adresse e-mail (une liste de distribution, pas l'adresse e-mail d'un individu) et un numéro de téléphone sont associés au compte afin de recevoir des réponses aux incidents de sécurité potentiels. Le numéro de téléphone et l'adresse e-mail du compte ne peuvent pas être modifiés sans réinitialiser le mot de passe du compte, ce qui est une tâche importante pour un compte root AMS. Pour garantir la stabilité de ces valeurs, il est essentiel de sélectionner des informations de contact non associées à des personnes, qui peuvent changer. Choisissez un alias d'e-mail qui peut pointer vers un

groupe. Suivez la même procédure pour sélectionner un numéro de téléphone : choisissez un numéro qui peut pointer vers un groupe ou vers un numéro appartenant à l'entreprise et non à un individu.

Pour plus de détails sur les questions qui vous seront demandées pour intégrer votre compte Core à la zone d'atterrissage multi-comptes AMS, consultezAnnexe : liste des points à considérer pour l'intégration dans une zone d'atterrissage multicompte (MALZ).

Créez un rôle IAM pour qu'AMS puisse accéder à votre compte

Maintenant que vous avez créé votre nouveau compte avec succès Compte AWS, l'étape suivante du processus consiste à autoriser AMS à accéder au nouveau compte afin de créer et de configurer votre environnement AMS, et de répondre aux demandes de modification et de provisionnement en cours. Pour plus de détails, consultez la section Accès délégué entre AWS comptes à l'aide de rôles IAM.

Gestion des identités et des accès AWS (IAM) est un service Web qui vous permet de contrôler en toute sécurité l'accès aux AWS ressources pour vos utilisateurs. Vous utilisez IAM pour contrôler qui peut utiliser vos AWS ressources (authentification), quelles ressources ils peuvent utiliser et de quelle manière (autorisation).

Activer l'accès IAM à la console AWS

1. Connectez-vous à la console de AWS gestion à l'aide des informations d'identification de votre compte root (e-mail et mot de passe que vous avez utilisés pour créer votre compte Compte AWS). Ne vous connectez pas avec d'autres informations d'identification IAM. La page d'accueil AWS de la console de gestion s'ouvre.
2. Dans la barre de navigation supérieure, ouvrez le menu déroulant correspondant au nom de votre compte, puis choisissez Compte. La page d'accueil de facturation s'ouvre.
3. Faites défiler la page jusqu'à l'accès des utilisateurs et des rôles IAM aux informations de facturation, puis choisissez Modifier. Une zone d'accès Activate IAM s'ouvre.
4. Cochez la case, puis choisissez Mettre à jour. Vous pouvez désormais utiliser des politiques IAM pour contrôler les pages auxquelles un utilisateur peut accéder.

Création d'un rôle IAM à utiliser par AMS

1. Procurez-vous un fichier JSON ou YAML qui définit un rôle IAM à utiliser par AMS pour créer votre infrastructure. Deux options s'offrent à vous :
   - Votre architecte cloud AMS (CA) vous fournit un fichier JSON ou YAML.
   - Vous pouvez télécharger le fichier onboarding_iam_roles.zip et choisir l'une des options suivantes :
     - onboarding_role_admin.json (plus court, accorde un accès administrateur complet)
     - onboarding_role_minimal.json (plus long, accorde le moins de privilèges)
2. Connectez-vous à la CloudFormation console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudformation.
3. Sélectionnez Créer une pile. La page suivante s'affiche.
4. Choisissez Télécharger un fichier modèle, chargez le fichier JSON ou YAML du rôle IAM, puis choisissez Next. La page suivante s'affiche.
5. Entrez **`ams-onboarding-role`** dans la section Nom de la pile et continuez à faire défiler la page vers le bas et à sélectionner Suivant jusqu'à ce que vous atteigniez cette page.
6. Assurez-vous que la case est cochée, puis sélectionnez Create Stack.
7. Assurez-vous que la pile a été créée avec succès.

Sécurisez le nouveau compte avec l'authentification multifactorielle (MFA) pour l'utilisateur root dans 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.

Abonnez-vous à AWS Marketplace for Trend Micro Endpoint Protection (EPS)

Trend Micro Endpoint Protection (EPS) est le principal composant d'AMS pour la sécurité du système d'exploitation. Pour configurer EPS une fois que la création de la zone de landing zone AMS est lancée, vous devez vous connecter au compte principal des services partagés et vous abonner à l'AMI Trend Micro Deep Security sur AWS Marketplace. Votre CSDM ou CA vous conseillera.

1. Connectez-vous à la AWS console en utilisant le rôle ou l'utilisateur que vous avez spécifié dans le questionnaire d'intégration pour `CustomerEPSSubscriptionIAMRoleOrUser`
2. Accédez à l'écran Switch Role.

   - Compte : fourni par AMS
   - Rôle : `EPSMarketplaceSubscriptionRole`
   - Nom d'affichage : Session d'abonnement EPS

   Pour vous abonner à Trend Micro Deep Security dans le AWS Marketplace, procédez comme suit après avoir changé de rôle dans la console :

   1. Accédez à l'AWS Marketplace.
   2. Sous Trouvez les AWS Marketplace produits qui répondent à vos besoins, sélectionnez les options suivantes :
      a. Fournisseurs : Trend Micro
      b. Plan tarifaire : apportez votre propre licence si vous en avez une ou selon la facturation des hôtes
      c. Modes de livraison : Amazon Machine Image
   3. Cliquez sur Continuer pour vous abonner dans le panneau de droite.
   4. Consultez les conditions générales, puis cliquez sur Accepter les conditions dans le coin supérieur droit.
   5. Déconnectez-vous du compte et confirmez auprès de votre architecte cloud que la procédure est terminée.

À ce stade, AMS déploie l'infrastructure dans votre environnement AMS et l'environnement est prêt à être utilisé une fois que vous avez connecté votre réseau et configuré votre accès.

Configuration de la mise en réseau

La mise en réseau dans l'environnement AMS est principalement gérée dans le compte réseau principal.

Plusieurs processus doivent être effectués pour configurer le réseau pour AWS Managed Services (AMS) :

- Allocation d'espace IP pour votre environnement AMS
- Établissement d'une connectivité réseau privée pour AWS
- Configuration de votre pare-feu pour autoriser les opérations AMS

Allocation d'espace IP pour votre environnement AMS

Vous devriez déjà avoir travaillé avec votre architecte cloud pour définir l'espace IP de votre environnement AMS en remplissant le questionnaire d'intégration.

Établissement d'une connectivité réseau privée vers AWS AMS

AWS offre une connectivité privée en utilisant la connectivité VPN et des lignes dédiées via AWS Direct Connect. La connectivité privée peut être configurée de deux manières :

- Connectivité Edge centralisée à l'aide de Transit Gateway
- Connexion du and/or VPN Direct Connect au compte VPCs

Connectivité périphérique centralisée à l'aide de Transit Gateway

AWS Transit Gateway est un service qui vous permet de connecter vos Amazon Virtual Private Clouds (VPCs) et vos réseaux locaux à une passerelle unique. Transit Gateway peut être utilisé pour consolider votre connectivité périphérique existante et l'acheminer via un ingress/egress point unique. Pour plus de détails, consultez AWS Transit Gateway.

Connexion de Direct Connect à Transit Gateway

Vous pouvez utiliser votre connexion Direct Connect existante ou créer une nouvelle connexion Direct Connect dans l'un de vos AWS comptes existants. La connexion Direct Connect doit être une connexion dédiée ou hébergée fonctionnant à 1 Gbit/s ou plus.

> **Note**
>
> Pour plus d'informations sur l'utilisation de Direct Connect avec AWS les services, consultez la section Mise en route sur un site AWS Direct Connect.

Pour utiliser une connexion dédiée Direct Connect existante, la connexion ne doit pas comporter plus de 3 interfaces virtuelles de transit créées dessus. Cela est dû Direct Connect au fait que les connexions dédiées ont une limite de 4 interfaces virtuelles de transit par connexion.

Pour plus d'informations sur les limites de Direct Connect, consultez la section Limites de AWS Direct Connect.

Une fois que la connexion Direct Connect est disponible, les événements suivants se produisent :

1. AMS crée une passerelle Direct Connect dans le compte réseau. Vous devez fournir un numéro de système autonome (ASN) pour la passerelle Direct Connect et les préfixes qui doivent être annoncés depuis la passerelle Direct Connect. Cet ASN est utilisé en tant qu'ASN Amazon.
2. Vous créez un nouveau Transit VIF et définissez le propriétaire de l'interface virtuelle comme compte réseau.
3. AMS se connecte au compte réseau et accepte la proposition de connexion.
4. AMS associe la passerelle de transit à la passerelle Direct Connect.
5. AMS associe la pièce jointe à la table de routage Transit Gateway sur site.

> **Note**
>
> L'ASN fourni pour la passerelle Direct Connect et le Transit Gateway doivent être différents.

Pour augmenter la résilience de votre connectivité, il est recommandé d'associer au moins deux interfaces virtuelles de transport, provenant de différents sites AWS Direct Connect, à la passerelle Direct Connect. Pour plus d'informations, consultez les recommandations en Direct Connect matière de résilience.

Connexion d'un VPN à Transit Gateway

Pour attacher une connexion VPN à votre passerelle de transit, vous devez indiquez la passerelle client. Pour plus d'informations sur les exigences relatives à une passerelle client, consultez la section Exigences relatives à votre passerelle client dans le guide de l'administrateur réseau Amazon VPC.

Vous devez fournir le numéro ASN BGP, l'adresse IP publique statique et l'option de routage (statique ou dynamique). Une fois ces informations fournies, AMS créera la pièce jointe VPN et associera la pièce jointe à la table de routage Transit Gateway sur site.

Pour plus de détails sur les pièces jointes Transit Gateway, consultez la section Pièces jointes du VPN Transit Gateway.

Connexion du and/or VPN Direct Connect au compte VPCs

Vous pouvez également vous connecter directement VPCs 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.

> **Note**
>
> Le VPC de services partagés et le compte d'application VPCs doivent être connectés à une connexion Direct Connect ou VPN pour établir une connectivité privée.

Direct Connect configuration dans AMS

Configurez un Direct Connect pour communiquer entre votre VPC géré par AMS et votre réseau interne.

> **Note**
>
> Pour plus d'informations sur l'utilisation de Direct Connect avec AWS les services, voir Getting Started at an Direct Connect Location.

Pour configurer une connexion Direct Connect, procédez comme suit :

1. S'inscrire à Amazon Web Services (AWS)
2. Soumettez une demande de Direct Connect connexion.
3. Terminez le Cross Connect.
4. (Facultatif) Configurez les connexions redondantes avec Direct Connect.
5. Réalisé par AMS : créez une interface virtuelle.
6. Effectué par AMS : Téléchargez la configuration du routeur.
7. Vérifiez votre interface virtuelle.

Configuration du VPN

Les étapes de base suivies par AMS pour configurer un VPN afin de communiquer entre votre VPC géré par AMS et votre réseau interne.

> **Note**
>
> Pour mieux comprendre l'utilisation d'un VPN avec AWS des services, consultez Qu'est-ce qu'un AWS Site-to-Site VPN et votre passerelle client (votre appliance VPN).

Nous suivons les sections du Guide de l'utilisateur du AWS VPN Getting Started et Testing the Site-to-Site VPN Connection pour effectuer les étapes suivantes :

1. Dans votre AWS VPC, créez une passerelle client.
2. Dans votre AWS VPC, créez une passerelle privée virtuelle.
3. Dans votre AWS VPC, activez la propagation de routes dans votre table de routage.
4. Dans votre AWS VPC, mettez à jour votre groupe de sécurité pour activer l'accès SSH, RDP et ICMP entrant.
5. Dans votre réseau interne, créez une connexion VPN et configurez la passerelle client.
6. Testez la connectivité VPN entre le VPC et votre réseau interne.

Configuration de la gestion des accès

L'utilisation d'un réseau géré par AWS Managed Services (AMS) signifie donner à AMS un accès pour gérer votre infrastructure cloud. Vous devez configurer un moyen de connexion sécurisée entre votre réseau privé et AMS. Cela commence par quelques décisions :

- AMS API/CLI et accès à la console : vous devez installer l'AMS CLI (les instructions sont fournies dans ce document). Vous utilisez l'API de gestion des modifications AMS pour envoyer des demandes de modification à AMS et l'API AMS SKMS pour en savoir plus sur vos ressources gérées par AMS. À l'aide d'Active Directory Federation Services (AD FS), vous pouvez accéder à la console AMS.
- Accès utilisateur : la connectivité doit être établie entre AD du côté AMS (via les services d'annuaire) et l'annuaire que vous utilisez pour gérer les utilisateurs.
- Accès à l'instance : l'accès au niveau de l'instance s'effectue via une configuration de confiance unidirectionnelle. Les services d'annuaire font confiance aux informations d'identification de votre CORP AD, ce qui permet aux piles situées du côté AMS de permettre la connexion avec les informations d'identification CORP.

> **Note**
>
> L'Active Directory (AD) sur lequel AMS configure la confiance doit être l'annuaire contenant les comptes des utilisateurs que vous avez autorisés à accéder à vos ressources AWS.

Établir une relation de confiance Active Directory

Pour configurer un trust, AMS a besoin de votre contrôleur de domaine : politiques locales -> options de sécurité -> accès au réseau : canaux nommés accessibles de manière anonyme, dont les canaux Netlogon et lsarpc sont répertoriés. Ces canaux sont répertoriés par défaut, mais sont parfois supprimés pour des raisons de sécurité. Une fois la confiance établie, ils peuvent à nouveau être retirés de la liste.

Configuration du redirecteur conditionnel

1. Dans le gestionnaire DNS AD -> Créer un nouveau redirecteur conditionnel, sous Domaine DNS : utilisez le nom de domaine AMS qui vous a été fourni ; par exemple,

A523434123.amazonaws.com (remplacez-le par le nom de domaine sélectionné dans le questionnaire d'intégration).

2. Sous Adresses IP des serveurs principaux : ajoutez les adresses IP fournies par AMS. Assurez-vous qu'il n'y a aucun problème de connexion en validant les deux adresses.
3. Sélectionnez Stocker ce redirecteur conditionnel dans Active Directory et répliquez comme suit : Tous les serveurs DNS de ce domaine, puis appuyez sur OK.

Configuration de l'AD Trust

Suivez cet article de Microsoft AD sur la création d'une confiance forestière unidirectionnelle entrante pour un côté de la confiance, en utilisant les paramètres et les choix décrits dans cette section.

1. Ouvrez la boîte de dialogue Démarrer -> Outils d'administration -> Domaines et approbations Active Directory. Cliquez avec le bouton droit sur le nœud de domaine du domaine avec lequel vous souhaitez établir une approbation, puis cliquez sur Propriétés -> Approbations -> Nouvelle approbation pour ouvrir l'assistant de nouvelle approbation. Entrez le nom de domaine qui vous a été fourni par AMS pour le nom de confiance et appuyez sur Suivant.
2. Sous Type de confiance, sélectionnez le niveau de confiance approprié (par exemple Forest Trust). Appuyez sur Suivant.
3. Sous Direction de la confiance, sélectionnez Unidirectionnel : entrant. Appuyez sur Next (Suivant).
4. Sous Sides of Trust, sélectionnez Ce domaine uniquement. Appuyez sur Next (Suivant).
5. Sous Trust Password, saisissez le mot de passe de votre choix. Appuyez sur Next (Suivant).
6. Pour que les sélections de confiance soient terminées et que la création de la confiance soit terminée, appuyez simplement sur Suivant.
7. Sous Confirmer la confiance entrante, sélectionnez Non, ne pas confirmer la confiance entrante. Appuyez sur Next (Suivant).
8. Sous Terminer le nouvel assistant de confiance, sélectionnez Terminer, puis OK pour fermer.
9. Fournissez le mot de passe de confiance (contactez-nous via le numéro de téléphone de votre CSDM pour des raisons de sécurité). AMS achèvera la configuration de confiance.

Sites et services Active Directory

Pour réduire la latence de connexion, ajoutez la plage d'adresses CIDR VPC à vos sites et services Active Directory (Démarrer -> Outils d'administration -> Sites et services Active Directory). Ajoutez la

plage d'adresses CIDR VPC à un site Active Directory contenant les contrôleurs de domaine les plus proches d'AWS.

Indiquez le nom du site AD que vous avez dédié à AMS à votre CSDM. AMS renommera le site par défaut du côté AMS d'AD pour qu'il corresponde au nom fourni.

Routage des suffixes de noms Active Directory

Une fois la confiance forestière unidirectionnelle établie, effectuez les étapes suivantes pour valider le routage des suffixes :

1. Sous Démarrer > Tous les programmes > Outils d'administration, cliquez sur Domaines et approbations Active Directory.

   La console Active Directory Domains and Trusts s'ouvre.
2. Cliquez avec le bouton droit sur votre domaine d'entreprise, puis cliquez sur Propriétés

   La boîte de dialogue Propriétés de ce domaine s'ouvre.
3. Cliquez sur l'onglet Trusts.

   La page Trusts s'ouvre.
4. Cliquez sur le nom de domaine Amazon, puis sur Propriétés.

   La page Propriétés du domaine Amazon Trust s'ouvre.
5. Cliquez sur Name Suffix Routing, puis sur Actualiser.

   Assurez-vous qu'il n'y a aucun conflit afin de garantir que les noms principaux du service (SPNs) puissent être résolus en cas de confiance.

Fédérez votre Active Directory avec les rôles AMS IAM

L'objectif de la fédération de votre annuaire avec les rôles AMS IAM est de permettre aux utilisateurs professionnels d'utiliser leurs informations d'identification d'entreprise pour interagir avec la console AWS et AWS APIs, et donc avec la console AMS et. APIs

Exemple de processus de fédération

Cet exemple utilise les services de fédération Active Directory (AD FS) ; toutefois, toutes les technologies compatibles avec AWS IAM Federation sont prises en charge. Pour plus d'informations sur la fédération IAM prise en charge par AWS, consultez la section Partenaires IAM et fournisseurs

d'identité et fédération. Votre CSDM vous aidera tout au long de ce processus, qui implique un effort conjoint avec votre équipe AD et AMS.

Pour obtenir des informations détaillées sur l'intégration de SAML pour l'accès aux API, consultez ce blog AWS intitulé Comment implémenter un accès fédéré aux API et aux CLI à l'aide de SAML 2.0 et d'AD FS.

Pour un exemple d'installation de l'interface de ligne de commande AMS et du protocole SAML, consultez l'annexe : règle de réclamation AD FS et paramètres SAML.

Configuration de la fédération sur la console AMS (MALZ)

Les rôles IAM et le fournisseur d'identité SAML (entité de confiance) détaillés dans le tableau suivant ont été fournis dans le cadre de l'infrastructure AMS. Ces rôles vous permettent d'auditer et de consulter les comptes principaux d'AMS.

Rôle	Autorisations
AWSManagedServicesReadOnlyRole	Vous permet de visualiser l'infrastructure AMS dans les comptes principaux.
AWSManagedServicesCaseRole	Vous permet de consulter les ressources de votre nouveau compte d'application et de classer les incidents AMS et les demandes de service.
AWSManagedServicesChangeManagementRole	Vous permet de consulter l'infrastructure AMS dans les comptes principaux, de déposer des tickets AWS Support et d'en demander RFCs.

Pour la liste complète des rôles disponibles sous différents comptes, voirRôle d'utilisateur IAM dans AMS.

Vérifier l'accès à la console

Une fois que vous avez configuré ADFS et que vous disposez de l'URL AMS à utiliser pour l'authentification, procédez comme suit.

Avec une configuration ADFS (Active Directory Federated Service), vous pouvez suivre les étapes suivantes :

1. Ouvrez une fenêtre de navigateur et accédez à la page de connexion qui vous a été fournie pour votre compte. La IdpInitiatedSignOnpage ADFS de votre compte s'ouvre.
2. Sélectionnez le bouton radio à côté de Se connecter à l'un des sites suivants. La liste de sélection du site de connexion devient active.
3. Choisissez le site signin.aws.amazon.com et cliquez sur Se connecter. Les options de saisie de vos informations d'identification sont ouvertes.
4. Entrez vos informations d'identification CORP et cliquez sur Se connecter. Les AWS Management Console ouvertures.
5. Collez dans la barre d'adresse l'URL de la console AMS et appuyez sur Entrée. La console AMS s'ouvre.

Vérifier l'accès à l'API

AMS utilise l'API AWS, avec certaines opérations spécifiques à AMS que vous pouvez consulter dans le manuel AMS API Reference.

AWS en fournit plusieurs SDKs auxquels vous pouvez accéder sur Tools for Amazon Web Services. Si vous ne souhaitez pas utiliser de SDK, vous pouvez effectuer des appels d'API directs. Pour plus d'informations sur l'authentification, consultez la section Signature des demandes d'API AWS. Si vous n'utilisez pas de SDK ou si vous effectuez des demandes d'API HTTP directes, vous pouvez utiliser l'AMS CLIs for Change Management (CM) et le SKMS.

Installez l'AMS CLIs

La CLI AWS est une condition préalable à l'utilisation de l'AMS CLIs (Change Management and 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).
2. Après l'installation, lancez aws help pour vérifier l'installation.
3. 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 des distribuables AMS et décompressez-le. Vous pouvez accéder aux distribuables de l'AMS CLI via le lien Documentation dans le menu de navigation de gauche de la console AMS, ou demander à votre responsable de prestation de services cloud (CSDM) de vous envoyer le fichier zip.

4. Ouvrez le répertoire Managed Cloud Distributables -> CLI -> Windows ou Managed Cloud Distributables -> CLI -> Linux/ macOS, selon votre système d'exploitation, et :
5. 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
6. Pour Mac/Linux, exécutez le fichier nommé : MC_CLI.sh 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.
7. 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.
8. Après l'installation, lancez `aws amscm help` et consultez `aws amsskms help` les commandes et les options.

MALZ : Intégration du compte d'application

Vous devez disposer d'un environnement AWS Managed Services (AMS) multi-comptes configuré avec des comptes principaux avant de demander un nouveau compte d'application. Voici les étapes à suivre après avoir configuré votre environnement.

Rubriques

- Demande d'un nouveau compte d'application
- Configuration d'Active Directory pour fédérer l'accès aux rôles AMS IAM
- Configuration de la mise en réseau avec le nouveau compte d'application
- Configuration de fonctionnalités supplémentaires VPCs dans le compte de l'application

Pour toute question relative à l'intégration, contactez votre responsable de prestation de services cloud (CSDM). Voir également Comptes d'applications : gérés par AMS, mode développement, gérés par le client. Pour des informations générales sur les modes, consultez la section Modes AMSGestion des services dans AWS Managed Services.

Pour plus d'informations sur les différents modes de comptes d'applications, voir Comptes d'applications : gérés par AMS, mode développement, gérés par le client. Pour des informations générales sur les modes, consultez la section Modes AMS.

Demande d'un nouveau compte d'application

Vous devez disposer d'un environnement AWS Managed Services (AMS) multi-comptes configuré avec des comptes principaux avant de demander un nouveau compte d'application. Pour plus d'informations sur la configuration d'un environnement multi-comptes avec des comptes principaux, consultezMALZ : Intégration du compte principal.

Vous pouvez choisir l'un des types Amazon VPC suivants pour le VPC initial dans le compte d'application :

- Privé : aucune passerelle Internet n'est attachée à ce VPC. Cela convient aux applications privées qui ne nécessitent aucun accès to/from à Internet.
- Public : ce VPC est connecté à une passerelle Internet et possède des sous-réseaux publics et privés. Cela convient aux applications publiques qui nécessitent un accès to/from à Internet.

Vous pouvez demander un nouveau compte d'application en soumettant une RFC de déploiement | Zone d'atterrissage gérée | Compte de gestion | Création d'un compte d'application (avec VPC) (ct-1zdasmc2ewzrs) et en fournissant les valeurs suivantes dans la RFC :

- Nom du compte : nom personnalisé pour le compte. Notez que le nom du compte a une longueur maximale de 50 caractères.
- Adresse e-mail du compte : adresse e-mail de la liste de distribution associée au compte. Cet identifiant e-mail est utilisé pour créer le compte AWS.
- Niveau de support : niveau de support AWS, Premium ou Plus.
- Nom du VPC : nom du VPC.
- Nombre de zones de disponibilité (AZs) : 2 ou 3.
- CIDR VPC : bloc d'adresse CIDR pour le VPC.
- Type d'itinéraire : Il peut s'agir de l'un `routable` ou de l'autre`isolated`. `Routable`signifie que l'application VPCs associée à la table de routage de l'application Transit Gateway (TGW) peut se connecter à ce VPC. `Isolated`signifie que l'application VPCs associée à la table de routage des applications TGW ne peut pas se connecter à ce VPC. L'argument par défaut est `routable`.

- Table de routage de l'application Transit Gateway : table de routage Transit Gateway à laquelle le compte d'application VPC doit être associé. Si aucune valeur n'est fournie, la valeur par défaut `defaultAppRouteDomain` est utilisée, ce qui signifie que ce compte pourra communiquer avec tous les autres comptes sous la même table de routage.
- PublicSubnet*<1-3>*CIDRCIDR AZ pour le sous-réseau public dans AZ 1 : CIDR pour le sous-réseau public dans la zone de disponibilité 1.
- PrivateSubnet*<1-10><I-3>*CIDRCIDR AZ pour le sous-réseau public dans AZ 1 : CIDR pour le sous-réseau public dans la zone de disponibilité 1.

À ce stade, AMS déploie un nouveau compte d'application dans votre compte de gestion AMS, avec la configuration VPC spécifiée.

Configuration d'Active Directory pour fédérer l'accès aux rôles AMS IAM

Fédérez votre annuaire avec les rôles AMS IAM pour permettre aux utilisateurs professionnels d'utiliser leurs informations d'identification professionnelles pour interagir avec la console AWS et AWS APIs, ainsi qu'avec la console AMS et AMS. APIs

Exemple de processus de fédération

Cet exemple utilise les services ADFS (Active Directory Federation Services). Cependant, toutes les technologies compatibles avec AWS IAM Federation sont prises en charge. Pour plus d'informations sur la fédération IAM prise en charge par AWS, consultez la section Partenaires IAM et fournisseurs d'identité et fédération. Votre CSDM vous aidera tout au long de ce processus, qui implique un effort conjoint avec votre équipe AD et AMS.

Pour obtenir des informations détaillées sur l'intégration de SAML pour l'accès aux API, consultez ce blog AWS intitulé Comment implémenter un accès fédéré aux API et aux CLI à l'aide de SAML 2.0 et d'AD FS.

Pour un exemple d'installation de l'interface de ligne de commande AMS et du protocole SAML, consultez l'annexe intitulée « Règle de réclamation AD FS et paramètres SAML » dans le guide de l'utilisateur d'AMS.

Configuration de la fédération sur la console AMS

Les rôles IAM et le fournisseur d'identité SAML (entité de confiance) détaillés dans le tableau suivant sont fournis dans votre nouveau compte d'application. Ces rôles vous permettent d'accéder au

nouveau compte et au nouveau fichier d'application RFCs, d'écrire dans des compartiments S3 et d'effectuer d'autres actions.

Rôle	Autorisations
AWSManagedServicesReadOnlyRole	Vous permet de consulter les ressources de votre nouveau compte d'application.
AWSManagedServicesCaseRole	Vous permet de consulter les ressources de votre nouveau compte d'application et de déposer des tickets AWS Support.
AWSManagedServicesChangeManagementRole	Vous permet de visualiser l'infrastructure AMS dans les comptes de l'application, d'archiver, de RFCs classer les tickets AWS Support, d'écrire dans des compartiments S3, de gérer les secrets de Secrets Manager et de gérer les instances réservées d'Amazon Elastic Compute Cloud (Amazon EC2).
AWSManagedServicesSecurityOpsRole	Vous permet de visualiser l'infrastructure AMS dans les comptes de l'application, de gérer les secrets de Secrets Manager, de gérer les règles du Web Application Firewall, de gérer les certificats et de déposer des tickets AWS Support.
AWSManagedServicesAdminRole	Vous permet de consulter l'infrastructure AMS dans les comptes d'applications, de gérer les abonnements Marketplace, de gérer les secrets de Secrets Manager, de gérer les règles du Web Application Firewall, de gérer les certificats, de créer RFCs, de gérer des EC2 instances Amazon réservées, d'écrire dans des compartiments S3, de déposer des tickets AWS Support et de gérer les accords AWS Artifacts.

Soumission de la demande de fédération à AMS

S'il s'agit de votre premier compte, collaborez avec votre ou vos architectes and/or cloud CSDM pour fournir le fichier XML de métadonnées à votre fournisseur d'identité.

Si vous créez un compte ou un fournisseur d'identité supplémentaire et que vous avez accès au compte de gestion ou au compte d'application souhaité, procédez comme suit.

1. Créez une demande de service depuis la console AMS.

   > **Note**
   >
   > - Si vous créez un fournisseur d'identité pour un compte d'application, soumettez cette demande depuis le compte d'application lui-même ou depuis le compte de gestion.
   > - Si vous créez un fournisseur d'identité pour un compte principal AMS, soumettez cette demande depuis le compte de gestion.
   > - Si vous créez un fournisseur d'identité pour le compte de gestion, soumettez cette demande depuis le compte de gestion ou contactez votre CSDM pour obtenir de l'aide.

   Dans la demande de service, fournissez les informations nécessaires pour ajouter le fournisseur d'identité :

   - AccountId du compte sur lequel le nouveau fournisseur d'identité sera créé.
   - Nom du fournisseur d'identité souhaité, s'il n'est pas fourni, le nom par défaut sera customer-saml ; il doit généralement correspondre aux paramètres configurés dans votre fournisseur de fédération.
   - Pour les comptes existants, indiquez si le nouveau fournisseur d'identité doit être étendu à tous les rôles de console existants ou fournissez une liste des rôles qui doivent faire confiance au nouveau fournisseur d'identité.
   - Joignez le fichier XML de métadonnées exporté par votre agent de fédération à la demande de service sous forme de pièce jointe.
2. À partir du compte sur lequel vous avez créé la demande de service, créez une nouvelle RFC à l'aide du CT-ID ct-1e1xtak34nx76 (Management | Other | Other | Create) avec les informations suivantes.

   - Titre : « Intégrer l'IDP SAML <Name>pour le compte < AccountId > ».

- AccountId du compte sur lequel le fournisseur d'identité sera créé.
- Nom du fournisseur d'identité.
- Pour les comptes existants : si le fournisseur d'identité doit être propagé à tous les rôles de console existants, ou liste des rôles qui doivent faire confiance au nouveau fournisseur d'identité.
- Numéro de dossier de la demande de service créée à l'étape 1, à laquelle le fichier XML de métadonnées est joint.

Vérifier l'accès à la console

Une fois que vous avez configuré AD FS et que vous disposez de l'URL AMS à utiliser pour l'authentification, vous pouvez effectuer la procédure suivante.

Avec une configuration Active Directory Federated Service (AD FS), vous pouvez suivre les étapes suivantes :

1. Ouvrez une fenêtre de navigateur et accédez à la page de connexion qui vous a été fournie pour votre compte. La IdpInitiatedSignOn page AD FS de votre compte s'ouvre.
2. Sélectionnez le bouton radio situé à côté de Se connecter à l'un des sites suivants. La liste des sites de connexion devient active.
3. Choisissez le site signin.aws.amazon.com, puis cliquez sur Se connecter. Les options de saisie de vos informations d'identification sont ouvertes.
4. Entrez vos informations d'identification CORP et choisissez Se connecter. La console de gestion AWS s'ouvre.
5. Collez dans la barre d'adresse l'URL de la console AMS et appuyez sur Entrée. La console AMS s'ouvre.

Vérifier l'accès à l'API

AMS utilise l'API AWS, avec certaines opérations spécifiques à AMS que vous pouvez consulter dans le manuel AMS API Reference.

AWS en fournit plusieurs SDKs auxquels vous pouvez accéder sur Tools for Amazon Web Services. Si vous ne souhaitez pas utiliser de SDK, vous pouvez effectuer des appels d'API directs. Pour plus d'informations sur l'authentification, consultez Signing AWS API Requests. . Si vous n'utilisez pas de

SDK ou si vous effectuez des demandes d'API HTTP directes, vous pouvez utiliser l'AMS CLIs for Change Management (CM) et le SKMS.

Configuration de la mise en réseau avec le nouveau compte d'application

La configuration du réseau pour le compte d'application inclut la configuration des règles de pare-feu et éventuellement la configuration de tables de routage Transit Gateway (TGW) supplémentaires.

Configuration de votre pare-feu

Pour utiliser les applications déployées dans votre environnement AMS, vous devez créer des règles de pare-feu. Vous n'avez pas besoin de ces règles pour accéder à vos instances, vous pouvez passer par les bastions pour accéder à vos instances.

Règles de pare-feu pour l'accès aux applications

Vous devez ouvrir les ports suivants pour le trafic passant par votre pare-feu :

- De votre réseau sur site à votre nouveau CIDRs VPC d'application, à la fois dans les directions d'entrée et de sortie.
- Du VPC de votre nouvelle application CIDRs à votre réseau sur site, à la fois en entrée et en sortie (si vos applications cloud doivent accéder à vos applications sur site).

Port	Protocole	Service	De/À	Depuis/vers
80	TCP	Accès Web HTTP	Réseau sur site	VPC d'application AMS
443	TCP	Accès Web HTTPS	Réseau sur site	VPC d'application AMS

Configuration de tables de routage supplémentaires pour les applications de passerelle de transit

Le réseau AWS Managed Services (AMS) est flexible et prend en charge de nombreux cas d'utilisation du réseau.

- Communication entre les applications VPCs d'un même compte.

- Communication entre les applications VPCs de différents comptes.
- Isolation entre les applications VPCs de différents comptes.
- Isolation entre les applications VPCs dans les mêmes comptes.

Si vous avez des unique/special exigences en matière de mise en réseau, contactez votre architecte du cloud AMS et il élaborera un plan pour répondre à vos exigences par l'architecture réseau AMS.

Sur la base de la décision de mise en réseau prise pour le compte d'application VPCs, vous pouvez créer plusieurs tables de routage de l'application Transit Gateway (TGW) en soumettant une RFC Deployment | Managed landing zone | Networking account | Create Transit Gateway Route Table (ct-3dscwaeyi6cup).

Le type de modification nécessite que vous spécifiiez `TransitGatewayRouteTableName` (un nom significatif pour la table de routage TGW)`TransitGatewayId`, et`TGWRouteTableType`.

> **Note**
>
> Si le createCustomRoute domaine est sélectionné pour TGWRouteTableType, la table de routage créée est vide. Vous devez déposer une RFC avec le type de changement Deployment | Managed landing zone | Networking account | Add static route (ct-3r2ckznmt0a59).

Configuration de fonctionnalités supplémentaires VPCs dans le compte de l'application

Vous pouvez demander un compte d'application (VPC) supplémentaire en soumettant un RFC de déploiement | Zone d'atterrissage gérée | Compte d'application | Créer un VPC (ct-1j3503fres5a5).

Cela fonctionne de la même manière que la configuration d'un VPC pour un nouveau compte d'application. Pour en savoir plus, consultez Demande d'un nouveau compte d'application.

Annexe : liste des points à considérer pour l'intégration dans une zone d'atterrissage multicompte (MALZ)

Vous devrez tenir compte d'un certain nombre de considérations clés lors de la planification du déploiement de votre zone d'atterrissage multi-comptes AMS. Vos choix fourniront à AMS les

informations dont elle a besoin pour déterminer les composants d'infrastructure dont vous aurez besoin. Votre architecte cloud (CA) vous fournira un questionnaire pour vous aider dans cette tâche.

Rubriques

- Configuration du compte de zone d'atterrissage multi-comptes AMS
- Alertes de surveillance de la zone d'atterrissage multi-comptes AMS
- Configuration réseau
- Configuration d'Active Directory
- Protection des terminaux Trend Micro (EPS)
- Accès : Bastions, SSH et RDP
- Fédération

> **Note**
>
> Pour plus d'informations sur les types d'instances, consultez Amazon EC2 Instance Types. Pour plus d'informations sur les types d'instances de base de données, consultez Types d'instances Amazon RDS.
> Si vous avez besoin de Direct Connect, consultez le guide d'intégration de la zone d'atterrissage à compte unique AMS pour créer une connexion Direct Connect.

Vous recevrez un questionnaire d'intégration de la part de votre responsable de prestation de services cloud (CSDM) contenant des questions sur les paramètres de configuration souhaités pour votre compte. Travaillez avec votre CSDM pour remplir le questionnaire avant de continuer.

Configuration du compte de zone d'atterrissage multi-comptes AMS

- Nouvel identifiant de compte

  L' Compte AWS identifiant que vous avez créé pour la zone de landing multi-comptes AMS. Ne doit pas faire partie d'une AWS organisation.

- Région de service

  Région principale dans laquelle l'environnement de zone d'atterrissage multi-comptes AMS sera déployé.

- Les e-mails du compte principal pour les notifications. (ils doivent tous être dans le même domaine). Indiquez une adresse e-mail pour chacun :
  - Compte Shared Services
  - Compte réseau
  - Compte de connexion
  - Compte de sécurité
- Votre type de service, Premium ou Plus

  Cela détermine les accords de niveau de service (SLAs) pour résoudre les problèmes dans votre environnement

Alertes de surveillance de la zone d'atterrissage multi-comptes AMS

AMS vous permet d'être directement alerté (plutôt que de recevoir des notifications du service AMS) pour certaines alertes de surveillance. Pour vous inscrire, assurez-vous que votre architecte cloud (CA) ou votre responsable de prestation de services cloud (CSDM) reçoit les informations suivantes :

Alertes directes par e-mail : il s'agit des adresses e-mail auxquelles vous souhaitez qu'AMS envoie certaines alertes basées sur les ressources. Pour plus de détails sur les alertes envoyées directement par e-mail, consultez la section Alertes issues de la surveillance de base dans AMS dans le guide de l'utilisateur avancé d'AMS. Pour plus d'informations sur la surveillance AMS, consultez la section Gestion de la surveillance dans le guide de l'utilisateur AMS pour la zone d'atterrissage à compte unique.

Configuration réseau

- Numéro ASN de Transit Gateway

  Il s'agit du numéro de système autonome (ASN) du côté AWS d'une session BGP (Border Gateway Protocol). Il doit être unique et ne peut pas être le même que celui utilisé pour votre Direct Connect ou votre VPN. La plage est comprise entre 64512 et 65534 (inclus) pour 16 bits. ASNs
- Vos gammes VPC CIDR d'infrastructure de zone d'atterrissage multi-comptes AMS.

  Ces plages d'adresses CIDR ne peuvent pas se chevaucher avec votre réseau sur site

  Vous pouvez soit inclure une plage d'adresse CIDR /22, soit fournir chaque adresse CIDR VPC individuellement. Notez que seules les plages CIDR suivantes sont autorisées :

  - 10.0.0.0 - 10.255.255.255 (préfixe 10/8)
  - 172.16.0.0 - 172.31.255.255 (préfixe 172.16/12)
  - 192.168.0.0 - 192.168.255.255 (préfixe 192.168/16)

  Notez que la plage d'adresses IP 198.18.0.0/15 ne peut pas être utilisée (elle est réservée par AWS Directory Service).
  - Gamme d'adresses CIDR VPC de l'infrastructure de base (plage /22 recommandée)
  - Gamme réseau VPC CIDR (plage /24 recommandée)
  - Plage d'adresses CIDR VPC Shared Services (plage /23 recommandée)
  - Gamme DMZ VPC CIDR (plage /25 recommandée)
- VPN ECMP (activer ou désactiver)

  Pour la prise en charge du protocole de VPN ECMP, choisissez activer si vous avez besoin d'une prise en charge du routage ECMP (Equal Cost Multipath) entre des connexions VPN. Si les connexions annoncent la même chose CIDRs, le trafic est réparti de manière égale entre elles.

Liste de contrôle d'accès réseau (NACL)

Une liste de contrôle d'accès réseau (NACL) est une couche de sécurité facultative 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 de landing multi-comptes 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 principaux de la zone de landing zone multi-comptes : gestion, mise en réseau, services partagés, journalisation et sécurité.
- NACLs sont pris en charge dans les comptes d'applications de zone de landing zone multi-comptes tant qu'ils ne sont utilisés que comme liste « à refuser ». En outre, l'option « Tout autoriser » doit être configurée pour garantir les opérations de surveillance et de gestion de l'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 de landing multi-comptes AMS pour séparer le trafic réseau entre les différents comptes. VPCs

Configuration d'Active Directory

Nom de domaine complet pour Active Directory géré par AMS

Protection des terminaux Trend Micro (EPS)

- Tailles d'instance pour vos EC2 instances et vos groupes Auto Scaling

  Trend Micro Endpoint Protection (EPS) est le principal composant d'AMS pour la sécurité du système d'exploitation. Le système est composé d' EC2 instances de Deep Security Manager (DSM), d' EC2 instances de relais et d'un agent présent dans l'ensemble du plan de données AMS et dans vos EC2 instances.

  - Type d'instance de relais (le minimum pris en charge par AMS est m5.large)
  - Taille de l'instance de base de données (200 Go recommandés)
  - Type d'instance RDS (seuls db.m5.large ou db.m5.xlarge sont autorisés)
- Type de licence DSM (Marketplace ou BYOL)

  Si vous possédez déjà une licence, choisissez BYOL (apportez votre propre licence). AMS vous contactera pour obtenir les informations nécessaires sur la licence.
- AWS Nom de ressource Amazon (ARN) utilisateur ou rôle IAM pour l'abonnement à Trend Micro Deep Security (rôle ARN : arn:aws:iam : ::role/) *ACCOUNT_ID ROLE_NAME*

  Fournissez-nous un rôle IAM, un ARN ou un ARN d'utilisateur IAM à partir de l'un de vos rôles existants Comptes AWS auxquels vous avez accès. AMS crée un rôle IAM ; dans votre compte Shared Services de zone de landing zone multi-comptes AMS et ajoute le rôle ou l'utilisateur fourni en toute confiance à un rôle IAM dans Shared Services afin que vous puissiez assumer le rôle pour vous abonner à Trend Micro Deep Security dans. AWS Marketplace

Accès : Bastions, SSH et RDP

- Paramètres de SSH Bastion

  AMS fournit des bastions SSH dans votre compte Shared Services pour accéder aux hôtes de l'environnement AMS. Pour accéder au réseau AMS en tant qu'utilisateur SSH, vous devez utiliser

SSH Bastions comme point d'entrée. Le chemin réseau provient du réseau sur site, passe par DX/VPN la passerelle de transit (TGW), puis est acheminé vers le VPC Shared Services. Une fois que vous êtes en mesure d'accéder au bastion, vous pouvez accéder à d'autres hôtes de votre environnement AMS, à condition que la demande d'accès appropriée ait été accordée.

- Nombre d'instances souhaité (2 recommandées)
- Nombre maximum d'instances (4 recommandées)
- Nombre minimum d'instances (2 recommandées)
- Type d'instance (m5.large recommandé)
- Entrée CIDRs : plages d'adresses IP à partir desquelles les utilisateurs de votre réseau accèderont aux bastions SSH (plage d'adresses IP 1, plage d'adresses IP 2, plage d'adresses IP 3,... etc.)

- Paramètres du Bastion RDP

  AMS fournit éventuellement des bastions RDP dans votre compte Shared Services pour accéder aux hôtes de l'environnement AMS. Pour accéder au réseau AMS en tant qu'utilisateur RDP, vous devez utiliser RDP Bastions comme point d'entrée. Le chemin réseau provient du réseau sur site, passe par le TGW, puis est acheminé DX/VPN 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 appropriée ait été accordée.

  - Type d'instance (t3.medium recommandé)
  - Séances minimales souhaitées (2 recommandées)
  - Nombre maximum de sessions souhaitées (10 recommandées)

- Type de configuration RDP Bastion, standard partagé ou haute disponibilité partagée (la valeur par défaut est Shared Standard)

  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 il peut se connecter et deux utilisateurs peuvent se connecter au même bastion en même temps.

Fédération

Nom du fournisseur d'identité (IDP)

La valeur par défaut est `customer-saml`.

Intégration à la zone d'atterrissage à compte unique (SALZ) AMS

Processus d'intégration d'AMS SALZ

Pour intégrer des comptes de zone d'atterrissage à compte unique (SALZ) AMS, vous devez suivre les étapes suivantes :

1. Créez un nouveau compte AWS qu'AMS configure comme compte réseau pour héberger le pare-feu. Créez le nouveau compte au sein de votre organisation AWS, si vous en avez un. AMS suivra la procédure de création d'un compte AMS normal. Toutes les informations requises doivent donc être collectées (par exemple, le CIDR, les licences EPS et les utilisateurs). Remarque : une allocation CIDR de /24 est une bonne chose.
2. Spécifiez si vous souhaitez supprimer les passerelles Internet (IGWs) des comptes de trafic de sortie.
3. Déterminez vos domaines approuvés. AMS permet le filtrage des destinations en conservant une liste de domaines approuvés ; la liste peut être modifiée ultérieurement.
4. Confirmez la taille d'instance que vous souhaitez utiliser en fonction du débit attendu. Par défaut, l'instance est créée dans une instance m4.xlarge où nous avons constaté que le débit du pare-feu est de 350 Mbps. AMS peut augmenter la taille jusqu'à une instance C4.8xLarge dont le débit attendu est de 1,25 Gbit/s.
5. Configurez la mise en réseau entre AMS et votre réseau privé. Plusieurs tâches sont impliquées :
    a. Allouer de l'espace IP
    b. Établissez une connectivité réseau privée avec AWS
    c. Configurez votre pare-feu
    d. Configuration de la gestion des accès
    e. Planifier des sauvegardes
6. Donnez accès au compte créé à AMS.
7. Vérifiez que le service AMS fonctionne correctement.

AMS sera en mesure de créer le compte (intégration) de votre compte dans un délai de 2 semaines (10 jours ouvrables) à compter de la date de demande initiale. Toute activité de suivi peut être effectuée à l'aide d'AMS Planned Event Management (PEM).

Note

- 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)

De nouvelles régions sont ajoutées fréquemment. Pour obtenir la liste la plus récente, consultez la section Régions et zones de disponibilité AWS.

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. VPCsLes 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 Directory Service et interagir avec les contrôleurs de 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 instances Amazon EC2.

SALZ : Créez un nouveau AWS compte pour AMS

Les cinq étapes pour créer un nouveau AWS compte pour AWS Managed Services (AMS) sont les suivantes :

1. Créez un Compte AWS
2. Configurez la facturation consolidée : associez le nouveau compte au compte du payeur
3. Configurez votre accès Compte AWS pour AMS
4. Sécurisez le nouveau compte avec l'authentification multifactorielle (MFA) pour l'utilisateur root dans AMS
5. Abonnez-vous à AWS Marketplace for EPS

Veuillez contacter votre responsable de la prestation du service client (CSDM) si vous avez des questions.

Créez un Compte AWS

Le programme AMS nécessite la création d'un nouveau compte Amazon Web Services (AWS). Des instructions détaillées sont disponibles dans la vidéo suivante : Comment créer et activer un nouveau compte Amazon Web Services ? Les étapes simples sont les suivantes :

Inscrivez-vous pour un Compte AWS

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

Pour vous inscrire à un Compte AWS

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

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

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

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

Création d'un utilisateur doté d'un accès administratif

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

Sécurisez votre Utilisateur racine d'un compte AWS

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

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

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

Création d’un utilisateur doté d’un accès administratif

1. Activez IAM Identity Center.

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

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

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

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

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

Attribution d’un accès à d’autres utilisateurs

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

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

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

> **Note**
>
> Si vous avez déjà un compte, rendez-vous sur la page AWS des tarifs et cliquez sur Créer un compte gratuit. Assurez-vous de vous inscrire au moins au service EC2. L'inscription à un service vous permet d'accéder à tous les services de AWS. Seuls les services que vous utilisez vous sont facturés.
> Si vous envisagez de lier votre nouveau compte à un compte payeur à des fins de facturation consolidée, vous n'avez pas besoin de saisir les informations relatives au mode de paiement lorsque vous y êtes invité. Au lieu de cela, une fois que vous avez atteint l'écran pour saisir les informations de votre carte de crédit, il vous suffit de naviguer. Vous aurez besoin de l'adresse e-mail associée au compte payeur pour envoyer une demande de billing/linked compte consolidé, qui est détaillée dans la section suivante.

> **Important**
>
> Il est essentiel de vous assurer qu'une adresse e-mail et un numéro de téléphone sont associés au compte afin de recevoir des réponses aux éventuels incidents de sécurité.
> Le numéro de téléphone et l'adresse e-mail du compte ne peuvent pas être modifiés sans réinitialiser le mot de passe du compte, ce qui est une tâche importante pour un compte root AMS. Pour garantir la stabilité de ces valeurs, il est essentiel de sélectionner des informations de contact non associées à des personnes, qui peuvent changer. Choisissez un alias d'e-mail pouvant pointer vers un groupe. Suivez la même bonne pratique pour sélectionner un numéro de téléphone : choisissez un numéro qui peut pointer vers un groupe ou vers un numéro appartenant à l'entreprise et non à un individu.

Configurez la facturation consolidée : associez le nouveau compte au compte du payeur

Si vous souhaitez que votre nouvelle Compte AWS facture gérée par AMS soit intégrée au paiement d'un compte de AWS Organizations gestion existant, vous devez configurer une facturation consolidée et associer les comptes. Pour plus de détails sur cette procédure, voir

- Facturation consolidée AWS Organizations et stratégie de facturation AWS multi-comptes.
- Inviter un Compte AWS homme à rejoindre votre organisation

> **Note**
>
> Vous pouvez effectuer ces étapes avant de transférer le compte à AMS. Après le transfert, les étapes pour rejoindre votre organisation (indiquées ci-dessus) peuvent être effectuées dans le cadre du processus de gestion du changement. Consultez votre responsable de prestation de services cloud (CSDM) ou votre architecte cloud (CA) si vous avez besoin d'aide.

Pour obtenir des informations générales sur la facturation, y compris la gestion de la facturation consolidée, voir Qu'est-ce que AWS la facturation. Pour obtenir des AWS Organizations informations générales sur la manière dont les comptes peuvent fonctionner ensemble, consultez la section Qu'est-ce que c'est AWS Organizations. Pour obtenir des conseils prescriptifs sur les comptes AWS Organizations de gestion, voir Le compte de gestion, l'accès sécurisé et les administrateurs délégués

Configurez votre accès Compte AWS pour AMS

Une fois les étapes ci-dessus terminées, vous avez sécurisé avec succès vos nouveaux frais Compte AWS et vous êtes assuré que les coûts associés sont facturés de manière appropriée. La dernière étape du processus consiste à autoriser AMS à accéder au nouveau compte pour la configuration initiale de la pile et pour répondre aux demandes de modification et de provisionnement en cours. Pour plus de détails, consultez la section Accès délégué entre AWS comptes à l'aide de rôles IAM. Les étapes de base sont décrites dans cette section.

Activer l'accès au AWS site Web

Pour permettre à vos utilisateurs IAM d'accéder aux informations et aux outils de facturation de votre compte, vous devez activer cette fonctionnalité.

Procédez comme suit :

1. Connectez-vous à l' AWS Management Console aide des informations d'identification de votre compte root (l'adresse e-mail et le mot de passe que vous avez utilisés pour créer votre compte Compte AWS). Ne vous connectez pas avec vos informations d'identification utilisateur IAM.

   La page AWS Management Console d'accueil s'ouvre.
2. Dans la barre de navigation supérieure, ouvrez le menu déroulant correspondant au nom de votre compte, puis sélectionnez Mon compte.

La page d'accueil de facturation s'ouvre.

3. Faites défiler la page jusqu'à la zone Accès des utilisateurs IAM aux informations de facturation, puis cliquez sur Modifier sur le côté droit. *The area does not appear unless you are logged in with root credentials*.

   Une zone d'accès Activate IAM s'ouvre.

4. Cochez la case et cliquez sur Mettre à jour.

   Vous pouvez désormais utiliser des politiques IAM pour contrôler les pages auxquelles un utilisateur peut accéder.

Pour plus de détails sur ce processus dans AWS, voir Présentation de la gestion des autorisations d'accès.

Création d'un rôle IAM avec accès au site Web AWS

Gestion des identités et des accès AWS (IAM) est un service Web qui vous permet de contrôler en toute sécurité l'accès aux AWS ressources pour vos utilisateurs. Vous utilisez IAM pour contrôler qui peut utiliser vos AWS ressources (authentification), quelles ressources ils peuvent utiliser et de quelle manière (autorisation).

1. Accédez à la console de gestion IAM, cliquez sur Rôles dans le volet de navigation de gauche.

   La page de gestion des rôles s'ouvre avec des informations sur les rôles IAM, une option Créer un rôle et une liste des rôles existants.

2. Cliquez sur Créer un rôle.

   La page Créer un rôle Sélectionnez le type d'entité de confiance s'ouvre. Cliquez sur Autre Compte AWS et une zone de paramètres s'ouvre ci-dessous.

   Entrez l'identifiant de compte sécurisé AMS qui vous a été fourni par AMS. Laissez les options Exiger External ID et Exiger MFA désélectionnées.

3. Cliquez sur Next: Permissions (Suivant : Autorisations).

   La page Créer un rôle Joindre des politiques d'autorisation s'ouvre avec des options permettant de créer une nouvelle politique, d'actualiser la page et de

rechercher des politiques existantes. Une liste des politiques existantes est fournie.

4. Sélectionnez la AdministratorAccesspolitique, puis cliquez sur Suivant : Révision.

   La page Créer une révision de rôle s'ouvre.

5. Nommez le nouveau rôle aws_managedservices_onboarding_role et saisissez « AMS Onboarding Role » pour la description du rôle. Vérifiez les paramètres du nouveau rôle et, si vous êtes satisfait, cliquez sur Créer un rôle.

   La page de gestion des rôles s'ouvre avec votre nouveau rôle répertorié.

Abonnez-vous à AWS Marketplace for EPS

Les récentes modifications apportées à AMS Endpoint Security (EPS) nécessitent que vous vous abonniez à TrendMicro Deep Security par le biais des conditions du logiciel AWS Marketplace et que vous les acceptiez.

TrendMicro propose deux modèles de licence : Per Protected Instance Hour et Bring your own License (BYOL).

- PAR OL :
  1. Vous utilisez votre propre licence que vous avez achetée par le biais de canaux externes.
  2. Vous devez fournir toutes les clés de licence à AMS pour créer l'infrastructure EPS. Vous pouvez fournir un code d'activation qui octroie une licence à tous les modules, ou des codes d'activation individuels qui octroient une licence à un certain ensemble de modules. AMS crée uniquement les fichiers de licence correspondant aux codes d'activation que vous fournissez. Étant donné que l'activation de la licence a lieu lors de l'intégration, en présence d'un ingénieur principal d'AMS et d'un CSDM, vous pouvez ensuite partager ces informations.
  3. De plus, vous devez souscrire à l'abonnement AMI BYOL TrendMicro Market Place. Voir Trend Micro Deep Security (BYOL).
- Par heure d'instance protégée :
  1. Dans le cadre de cet abonnement, il n'est pas nécessaire que vous possédiez une licence Trend précédemment achetée.

2. Cependant, vous devez souscrire à l'abonnement Marketplace.
3. Aucun partage de clé de licence avec AMS n'est requis dans ce modèle, car l'utilisation de Trend est mesurée automatiquement, y compris la licence logicielle et l'utilisation de l' EC2 infrastructure. Voir Trend Micro Deep Security.

Pour vous abonner à Trend Micro, procédez comme suit :

1. Connectez-vous à votre Compte AWS.
2. Accédez à la page produit de Trend Micro Deep Security (BYOL ou Per Protected Instance Hour).
3. Cliquez sur Continuer pour vous abonner dans le panneau de droite.
4. Cliquez sur Accepter les conditions dans le coin supérieur droit.

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.

Étape suivante : Sécurisez le nouveau compte avec l'authentification multifactorielle (MFA) pour l'utilisateur root dans AMS

S'abonner à AWS Marketplace pour CentOS 7.6

AMS fournit désormais le CentOS 7 (x86_64), avec les mises à jour HVM vendues par CentOS.org, en tant qu'AMI AMS. Pour utiliser cette AMI, vous devez souscrire à la licence FREE Cent OS et accepter la licence sur tous vos comptes AMS.

Pour vous abonner, rendez-vous sur les instructions d'inscription AWS Marketplaceet suivez-les.

Vous n'aurez pas à payer de frais logiciels pour l'utilisation de ce produit, mais vous êtes toujours responsable des autres AWS frais, y compris EC2 l'utilisation. S'il s'agit d'un produit « Bring Your Own License », vous devez disposer d'une licence logicielle valide pour pouvoir l'utiliser.

Vous pouvez consulter les informations relatives à ce logiciel sur CentOS 7 (x86_64) - avec Updates HVM.

Sécurisez le nouveau compte avec l'authentification multifactorielle (MFA) pour l'utilisateur root dans 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.

SALZ : Configuration de la mise en réseau

Plusieurs processus doivent être effectués pour configurer le réseau pour AWS Managed Services (AMS) :

1. Allocation d'espace IP pour votre environnement AMS
2. Établissement d'une connectivité réseau privée avec AWS
3. Configuration de votre pare-feu pour autoriser les opérations AMS

Allouez de l'espace IP à votre environnement AMS

AMS a été conçu et testé en utilisant un bloc CIDR /16 comme allocation réseau recommandée. Il est important que le réseau sécurisé connecté à AMS utilise un bloc d'adresse CIDR qui ne chevauche pas le bloc d'adresse CIDR attribué à AMS. Ces adresses sont nécessaires pour configurer votre cloud privé virtuel (VPC) et vos sous-réseaux. Pour plus d'informations sur AWS VPCs, consultez Amazon VPC Limits et Amazon VPC. FAQs

Bien qu'un bloc CIDR /16 puisse sembler être un grand nombre d'adresses IP, un VPC, une fois créé, ne peut pas être étendu. Cette allocation garantit donc que votre VPC géré par AMS peut fonctionner

pendant une période considérable. Dans le bloc CIDR, vous devez allouer des plages d'adresses IP pour au moins deux sous-réseaux privés et deux sous-réseaux publics.

AWS accepte la connectivité à l'environnement AMS via la fonctionnalité native du réseau privé virtuel (VPN) AWS. De votre côté, cela peut être réalisé via AWS Direct Connect (DX), un VPN matériel ou un VPN logiciel. Du côté AMS, nous utilisons la fonctionnalité Virtual Gateway de VPCs.

Composants de base de l'environnement

Options de Network-to-Amazon connectivité VPC utilisateur	
VPN matériel	Établit une connexion VPN matérielle entre votre équipement réseau sur un réseau distant et l'équipement réseau géré par AMS connecté à votre VPC.
AWS Direct Connect (DX)	Établit une connexion privée, logique (ou cryptée si elle est utilisée avec un VPN) entre votre réseau distant et Amazon VPC, en tirant parti d'AWS Direct Connect.
Logiciel VPN	Établit une connexion VPN entre votre équipement sur un réseau distant et une appliance VPN logicielle gérée par l'utilisateur exécutée au sein d'un Amazon VPC.

> **Note**
>
> AMS recommande des connexions VPN privées redondantes vers DX. Votre responsable de la prestation du service client (CSDM) vous aidera à le configurer au moment de l'enregistrement de votre compte.

Établissez une connectivité réseau privée avec AWS

Ajoutez AMS à l'Active Directory de votre entreprise pour établir la connectivité. Vous souhaiterez peut-être effectuer des actions administratives ou accéder aux utilisateurs via une connexion réseau privée. AWS propose à la fois une connectivité VPN et des lignes dédiées via Direct Connect.

Les étapes suivantes expliquent comment utiliser AMS pour établir l'un ou l'autre des moyens de connectivité (ou les deux).

Configuration du VPN

Cette section décrit les étapes de base pour configurer un VPN pour communiquer entre votre VPC géré par AMS et votre réseau interne.

> **Note**
>
> Pour mieux comprendre l'utilisation d'un VPN avec les services AWS, reportez-vous à la section Qu'est-ce qu'un Site-to-Site VPN AWS et à tout savoir sur votre passerelle client (votre appliance VPN).

Suivez les sections Getting Started and Testing the Site-to-Site VPN User Guide d'AWS pour effectuer les étapes suivantes.

- Étape 1 : dans votre VPC AWS, créez une passerelle client
- Étape 2 : dans votre VPC AWS, créez une passerelle privée virtuelle
- Étape 3 : Dans votre VPC AWS, activez la propagation de routes dans votre table de routage
- Étape 4 : Dans votre VPC AWS, mettez à jour votre groupe de sécurité pour activer l'accès SSH, RDP et ICMP entrant
- Étape 5 : Dans votre réseau interne, créez une connexion VPN et configurez la passerelle client
- Étape 6 : tester la connectivité VPN entre le VPC et votre réseau interne

Direct Connect Configuration

Cette section décrit les étapes de base pour configurer un Direct Connect (DX) pour communiquer entre votre VPC géré par AMS et votre réseau interne.

> **Note**
>
> Pour plus d'informations sur l'utilisation d'un DX avec les services AWS, consultez Getting Started at an Direct Connect Location.

Pour configurer une connexion DX, vous devez suivre les étapes suivantes :

1. Inscrivez-vous à Amazon Web Services
2. Soumettre une demande de connexion AWS Direct Connect
3. Terminez le Cross Connect
4. (Facultatif) Configurer des connexions redondantes avec AWS Direct Connect
5. Réalisé par AMS : Création d'une interface virtuelle
6. Réalisé par AMS : Télécharger la configuration du routeur
7. Vérifiez votre interface virtuelle

Configurez votre pare-feu

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.

Options d'AMS Bastion lors de la migration/de l'intégration des applications

Afin de vous offrir la meilleure expérience possible lors des efforts de migration, voici les options potentielles qu'AMS pourrait actuellement exploiter :

- Option 1 : Contourner les bastions uniquement pour les efforts de migration (vous devez vous y opposer pour des raisons de sécurité à titre de mesure temporaire).

  Remarque : Les fonctionnalités d'audit seront toujours en place pour garantir à AMS une visibilité sur chaque demande.
- Option 2 : Tunneling SSH avec un outil de choix, par exemple, PuTTy, comme illustré.

  Les composants de l'environnement décrits devraient déjà être en place pour cette option.

  AMS fournirait des notes et des instructions supplémentaires.

Étapes du tunneling SSH avec Pu : TTy

Dans PuTTY, vous devez créer une session SSH, avec l'adresse IP publique de l'hôte bastion, fournir la clé PEM dans la section AUTH, puis créer un tunnel. Le port source du tunnel doit être un port local inutilisé (par exemple 5000) et l'adresse IP doit être l'adresse IP de l'hôte de destination (le boîtier

Windows que vous essayez d'atteindre) avec le port RDP ajouté (3389). Veillez à enregistrer votre configuration, car vous ne voulez pas avoir à le faire à chaque fois que vous vous connectez à la boîte. Connectez-vous à l'hôte Bastion, puis connectez-vous. Démarrez ensuite une session RDP pour localhost:5000 (ou le port que vous choisissez).

1. Définir le nom d'hôte ou l'adresse IP publique de l'hôte bastion

2. Dans SSH ->Auth, définissez le fichier de clé privée au format .ppk

3. Dans SSH ->Tunnels, ajoutez le nouveau port transféré. Le port source doit être le port inutilisé arbitraire, et la destination doit être l'adresse IP du serveur de destination situé derrière l'hôte du bastion, avec le port RDP ajouté.

4. Connectez-vous à l'hôte Bastion via PuTTY et connectez-vous.

5. Démarrez une session RDP sur localhost:5000 pour atteindre le serveur de destination.

SALZ : Configuration de la gestion des accès

L'utilisation d'un réseau géré par AWS Managed Services (AMS) signifie donner à AMS un accès pour gérer votre infrastructure cloud. Vous devez configurer un moyen de connexion sécurisée entre votre réseau privé et AMS. Cela commence par certaines décisions concernant les types d'accès que vous souhaitez fournir :

- Pour l'accès à AMS API/CLI et à la console : vous devez installer l'AMS CLI (les instructions sont fournies dans ce document). Vous utilisez l'API de gestion des modifications AMS pour envoyer des demandes de modification à AMS et l'API AMS SKMS pour en savoir plus sur vos ressources gérées par AMS. À l'aide d'Active Directory Federation Services (AD FS), vous pouvez accéder à la console AMS.

> **Note**
>
> Si vous configurez votre propre ITSM, vous devrez utiliser l'API AWS Support (SAPI) pour les demandes de service et les rapports d'incidents. Le SAPI est documenté dans le AWS Support API Reference.

- Pour l'accès des utilisateurs : que vous gériez les utilisateurs avec Windows Active Directory (AD) ou une Linux/LDAP solution, la connectivité doit être établie entre AD du côté AMS (via les services d'annuaire) et votre annuaire.
- Pour l'accès aux instances : l'accès au niveau de l'instance s'effectue via une configuration Forest Trust unidirectionnelle. Les services d'annuaire font confiance aux informations d'identification de leur CORP AD, ce qui permet aux piles situées du côté AMS de permettre la connexion avec les informations d'identification CORP.

  Notez que l'Active Directory (AD) dans lequel AMS configure la confiance doit être l'annuaire contenant les comptes des utilisateurs que vous avez autorisés à accéder à vos ressources AWS.

> **Important**
>
> Pour configurer un Forest Trust, AMS a besoin de votre contrôleur de domaine : politiques locales -> options de sécurité -> accès au réseau : canaux nommés accessibles de manière anonyme, dont les canaux Netlogon et lsarpc sont répertoriés. Ces canaux sont répertoriés par défaut, mais sont parfois supprimés pour des raisons de sécurité. Une fois la confiance établie, ils peuvent à nouveau être retirés de la liste.

Établir une relation de confiance Active Directory (AD)

Avant de commencer à établir une approbation Active Directory (AD) pour votre compte AWS Managed Services (AMS), assurez-vous que les ports de pare-feu appropriés sont ouverts.

La confiance accordée par Active Directory géré par AMS et votre service d'annuaire d'entreprise vous permet d'utiliser vos informations d'identification gérées par l'entreprise pour accéder à des instances gérées par AMS afin d'effectuer des fonctions de développement, de test ou d'administration.

La création d'un lien de confiance est un exercice en deux parties :

Tout d'abord, configurez un transfert conditionnel, une configuration DNS afin que les requêtes DNS sachent vers quel serveur DNS se rendre.

Ensuite, configurez un trust, une construction Active Directory (AD) permettant aux utilisateurs d'un domaine d'utiliser les ressources d'un autre domaine.

Configuration du redirecteur conditionnel

Suivez cet article de Microsoft AD Attribuer un redirecteur conditionnel pour un nom de domaine, puis utilisez les paramètres et les choix suivants :

1. Dans le gestionnaire DNS AD -> Créer un nouveau redirecteur conditionnel, sous Domaine DNS : utilisez le nom de domaine AMS qui vous a été fourni ; par exemple,*A523434123.amazonaws.com*.
2. Sous Adresses IP des serveurs principaux : ajoutez les adresses IP fournies par AMS. Assurez-vous qu'il n'y a aucun problème de connexion en validant les deux adresses.
3. Sélectionnez Stocker ce redirecteur conditionnel dans Active Directory et répliquez comme suit : Tous les serveurs DNS de ce domaine, puis appuyez sur OK.

Configuration de la confiance

Pour configurer l'approbation de votre compte AWS Managed Services (AMS), suivez cet article MicroSoft AD Create a one-way, Incoming, forest trust for one side of the trust, en utilisant les paramètres et les choix décrits dans cette section.

1. Ouvrez la boîte de dialogue Démarrer -> Outils d'administration -> Domaines et approbations Active Directory. Cliquez avec le bouton droit sur le nœud de domaine du domaine avec lequel vous souhaitez établir une approbation, puis cliquez sur Propriétés -> Approbations -> Nouvelle approbation pour ouvrir l'assistant de nouvelle approbation. Entrez le nom de domaine qui vous a été fourni par AMS pour le nom de confiance et appuyez sur Suivant.
2. Sous Type de confiance, sélectionnez Forest Trust. Appuyez sur Next (Suivant).
3. Sous Direction de la confiance, sélectionnez Unidirectionnel : entrant. Appuyez sur Next (Suivant).
4. Sous Sides of Trust, sélectionnez Ce domaine uniquement. Appuyez sur Next (Suivant).
5. Sous Trust Password, saisissez le mot de passe de votre choix. Appuyez sur Next (Suivant).
6. Pour que les sélections de confiance soient terminées et que la création de la confiance soit terminée, appuyez simplement sur Suivant.
7. Sous Confirmer la confiance entrante, sélectionnez Non, ne pas confirmer la confiance entrante. Appuyez sur Next (Suivant).
8. Sous Terminer le nouvel assistant de confiance, sélectionnez Terminer, puis OK pour fermer.

9. Fournissez le mot de passe de confiance (contactez-nous via le numéro de téléphone de votre CSDM pour des raisons de sécurité). AMS achèvera la configuration de confiance.

Sites et services Active Directory

Pour réduire la latence de connexion, ajoutez la plage d'adresses CIDR VPC à vos sites et services Active Directory (Démarrer -> Outils d'administration -> Sites et services Active Directory). Ajoutez la plage d'adresses CIDR VPC à un site Active Directory contenant les contrôleurs de domaine les plus proches d'AWS.

Routage des suffixes de noms Active Directory

Une fois le trust forestier à sens unique établi, veuillez suivre les étapes supplémentaires.

1. Sous Démarrer > Tous les programmes > Outils d'administration, cliquez sur Domaines et approbations Active Directory.

   La console Active Directory Domains and Trusts s'ouvre.
2. Cliquez avec le bouton droit sur votre domaine d'entreprise, puis cliquez sur Propriétés

   La boîte de dialogue Propriétés de ce domaine s'ouvre.
3. Cliquez sur l'onglet Trusts.

   La page Trusts s'ouvre.
4. Cliquez sur le nom de domaine Amazon, puis sur Propriétés.

   La page Propriétés du domaine Amazon Trust s'ouvre.
5. Cliquez sur Name Suffix Routing, puis sur Actualiser.

   Ces étapes garantissent que les noms principaux du service (SPNs) peuvent être résolus au-delà de la confiance.

Dépannage

Voici quelques conseils à essayer en cas de problème :

- Le groupe de sécurité sortant Active Directory géré par AMS doit être autorisé à se connecter via votre bloc CIDR (par exemple 10.27.0.0/16) à votre contrôleur de domaine.

- Tracez l'itinéraire dans la console AWS d'un contrôleur de domaine à un autre en vérifiant tous les groupes de sécurité en cours de route.
- Assurez-vous de pouvoir envoyer un ping aux contrôleurs de domaine Active Directory gérés par AMS si le protocole ICMP (Internet Control Message Protocol) est autorisé.
- Assurez-vous que votre contrôleur de domaine peut communiquer avec AWS Directory Services.
- Assurez-vous que les redirecteurs conditionnels sont résolus et validés.
- Si Forest Trust n'apparaît pas dans l'assistant New Trust, cela signifie que vos redirecteurs conditionnels ne fonctionnent peut-être pas correctement :
  - Utiliser nslookup pour tester la résolution
  - Essayez de redémarrer le contrôleur de domaine

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 gérera 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.

Fédérez votre Active Directory avec les rôles AMS Gestion des identités et des accès AWS

L'objectif de la fédération de votre annuaire avec les rôles AMS IAM est de permettre aux utilisateurs de l'entreprise d'utiliser leurs informations d'identification d'entreprise pour interagir avec AWS Management Console et, par conséquent AWS APIs, avec la console AMS et. APIs

Exemple de processus de fédération

Cet exemple utilise les services de fédération Active Directory (AD FS) ; toutefois, toute technologie prenant en charge la Gestion des identités et des accès AWS fédération est prise en charge. Pour plus d'informations sur la fédération IAM AWS prise en charge, consultez la section Partenaires IAM, fournisseurs d'identité et fédération. Votre CSDM vous aidera tout au long de ce processus, qui implique un effort conjoint avec votre équipe AD et AMS.

Pour obtenir des informations détaillées sur l'intégration de SAML pour l'accès aux API, consultez ce AWS blog, Comment implémenter un accès fédéré aux API et aux CLI à l'aide de SAML 2.0 et d'AD FS.

> **Note**
>
> Pour un exemple d'installation de l'interface de ligne de commande AMS et du protocole SAML, consultez. Annexe : règle de réclamation des services de ActiveDirectory fédération (ADFS) et paramètres SAML

Configuration de la fédération sur la console AMS (SALZ)

Les rôles IAM et le fournisseur d'identité SAML (entité de confiance) détaillés dans le tableau suivant ont été fournis dans le cadre de l'intégration de votre compte. Ces rôles vous permettent de soumettre et de surveiller RFCs les demandes de service et les rapports d'incidents, ainsi que d'obtenir des informations sur vous VPCs et vos stocks.

Rôle	Fournisseur d'identité	Autorisations
Client_ _Rôle ReadOnly	SAML	Pour les comptes AMS standard. Vous permet de soumettre RFCs pour apporter des modifications à l'infrastructure gérée par AMS, ainsi que de créer des demandes de service et des incidents.
customer_managed_ad_user_role	SAML	Pour les comptes Active Directory gérés par AMS. Vous permet de vous connecter à la console AMS pour créer des demandes de service et des incidents (non RFCs).

Pour la liste complète des rôles disponibles sous différents comptes, voirRôle d'utilisateur IAM dans AMS.

Un membre de l'équipe d'intégration télécharge le fichier de métadonnées de votre solution de fédération vers le fournisseur d'identité préconfiguré. Vous utilisez un fournisseur d'identité SAML lorsque vous souhaitez établir un lien de confiance entre un IdP compatible SAML (fournisseur d'identité) tel que Shibboleth ou Active Directory Federation Services, afin que les utilisateurs de votre organisation puissent accéder aux ressources AWS. Les fournisseurs d'identité SAML dans IAM sont utilisés comme principaux dans une politique de confiance IAM avec les rôles ci-dessus.

Alors que d'autres solutions de fédération fournissent des instructions d'intégration pour AWS, AMS propose des instructions distinctes. À l'aide du billet de blog suivant, Enabling Federation to AWS Using Windows Active Directory, AD FS et SAML 2.0, ainsi que les modifications ci-dessous,

permettront aux utilisateurs de votre entreprise d'accéder à plusieurs comptes AWS à partir d'un seul navigateur.

Après avoir créé la confiance de la partie utilisatrice conformément au billet de blog, configurez les règles de réclamation de la manière suivante :

- NameId: Suivez le billet de blog.
- RoleSessionName: utilisez les valeurs suivantes :
  - Nom de la règle de réclamation : RoleSessionName
  - Magasin d'attributs : Active Directory
  - Attribut LDAP : SAM-Account-Name
  - Type de réclamation sortante : https://aws.amazon.com/SAML/ Attributs/ RoleSessionName
- Obtenir des groupes AD : suivez le billet de blog.
- Affirmation de rôle : suivez le billet de blog, mais pour la règle personnalisée, utilisez ceci :

```
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/"));
```

Lorsque vous utilisez AD FS, vous devez créer des groupes de sécurité Active Directory pour chaque rôle au format indiqué dans le tableau suivant (customer_managed_ad_user_role est réservé aux comptes AD gérés par AMS uniquement) :

Groupe	Rôle
AWS- [AccountNo] ReadOnly -Customer_ _Role	Client_ _Rôle ReadOnly
AWS- [AccountNo] -customer_managed_ ad_user_role	customer_managed_ad_user_role

Pour plus d'informations, voir Configuration des assertions SAML pour la réponse d'authentification.

> **Tip**
>
> Pour vous aider à résoudre les problèmes, téléchargez le plug-in de traçage SAML pour votre navigateur.

Soumission de la demande de fédération à AMS

S'il s'agit de votre premier compte, collaborez avec votre ou vos architectes and/or cloud CSDM pour fournir le fichier XML de métadonnées à votre fournisseur d'identité.

Si vous créez un compte ou un fournisseur d'identité supplémentaire et que vous avez accès au compte de gestion ou au compte d'application souhaité, procédez comme suit.

1. Créez une demande de service depuis la console AMS, fournissez les informations nécessaires pour ajouter le fournisseur d'identité :
   - AccountId du compte sur lequel le nouveau fournisseur d'identité sera créé.
   - Nom du fournisseur d'identité souhaité, s'il n'est pas fourni, le nom par défaut sera customer-saml ; il doit généralement correspondre aux paramètres configurés dans votre fournisseur de fédération.
   - Pour les comptes existants, indiquez si le nouveau fournisseur d'identité doit être étendu à tous les rôles de console existants ou fournissez une liste des rôles qui doivent faire confiance au nouveau fournisseur d'identité.
   - Joignez le fichier XML de métadonnées exporté par votre agent de fédération à la demande de service sous forme de pièce jointe.
2. À partir du compte sur lequel vous avez créé la demande de service, créez une nouvelle RFC à l'aide du CT-ID ct-1e1xtak34nx76 (Management | Other | Other | Create) avec les informations suivantes.
   - Titre : « Intégrer l'IDP SAML <Name>pour le compte < AccountId > ».
   - AccountId du compte sur lequel le fournisseur d'identité sera créé.
   - Nom du fournisseur d'identité.
   - Pour les comptes existants : si le fournisseur d'identité doit être propagé à tous les rôles de console existants, ou liste des rôles qui doivent faire confiance au nouveau fournisseur d'identité.

- Numéro de dossier de la demande de service créée à l'étape 1, à laquelle le fichier XML de métadonnées est joint.

Vérifier l'accès à la console

Une fois que vous avez configuré ADFS et que vous disposez de l'URL AMS à utiliser pour l'authentification, procédez comme suit.

Avec une configuration ADFS (Active Directory Federated Service), vous pouvez suivre les étapes suivantes :

1. Ouvrez une fenêtre de navigateur et accédez à la page de connexion qui vous a été fournie pour votre compte. La IdpInitiatedSignOnpage ADFS de votre compte s'ouvre.
2. Sélectionnez le bouton radio à côté de Se connecter à l'un des sites suivants. La liste de sélection du site de connexion devient active.
3. Choisissez le site signin.aws.amazon.com et cliquez sur Se connecter. Les options de saisie de vos informations d'identification sont ouvertes.
4. Entrez vos informations d'identification CORP et cliquez sur Se connecter. Les AWS Management Console ouvertures.
5. Collez dans la barre d'adresse l'URL de la console AMS et appuyez sur Entrée. La console AMS s'ouvre.

Vérifier l'accès à l'API

AMS utilise l'API AWS, avec certaines opérations spécifiques à AMS que vous pouvez consulter dans le manuel AMS API Reference.

AWS en fournit plusieurs SDKs auxquels vous pouvez accéder sur Tools for Amazon Web Services. Si vous ne souhaitez pas utiliser de SDK, vous pouvez effectuer des appels d'API directs. Pour plus d'informations sur l'authentification, consultez Signing AWS API Requests. Si vous n'utilisez pas de SDK ou si vous effectuez des demandes d'API HTTP directes, vous pouvez utiliser l'AMS CLIs for Change Management (CM) et le SKMS.

Installation de l'AMS CLIs

Pour un exemple d'installation de la CLI AWS Managed Services (AMS) à utiliser avec SAML, consultezAnnexe : règle de réclamation des services de ActiveDirectory fédération (ADFS) et paramètres SAML.

Si vous avez besoin d'un accès temporaire, pour obtenir et installer AWS Managed Services (AMS) SDKs, consultez la section Accès temporaire à la console AMS.

> **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`

Planification des sauvegardes AMS au niveau du VPC

La planification des sauvegardes AWS Managed Services (AMS) dans le VPC, où les instances cibles sont allouées, est créée lors de l'enregistrement du compte avec une balise par défaut dans le schéma de création du VPC. Le système de sauvegarde planifie l'exécution des instantanés en fonction de cette balise VPC. La modification de l'horaire peut être effectuée en créant une demande de service. Pour plus d'informations, consultez la section Balises VPC et paramètres par défaut.

Pour les valeurs de sauvegarde par défaut, voir Comprendre les valeurs par défaut d'AMS

SALZ : paramètres par défaut

Votre réseau AWS Managed Services (AMS) est configuré de manière standardisée avec des valeurs par défaut pour la plupart des services.

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

Pour un exemple de coûts d'infrastructure, voir Composants de base.

Les règles de pare-feu sont fournies dans Configurez votre pare-feu

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 communica tion 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

Paramètre	Par défaut
Dérive maximale autorisée (différence) entre les heures des serveurs	Illimité
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.

Paramètre	Par défaut
Source de mise à jour	Serveur de mise à jour Trend Micro (https://ipv6-iaus.trendmicro.com/iau_server.dll/)
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

Paramètre	Par défaut
	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 Tous les Day/All jours (24 heures)	Mettez en quarantaine tous les virus suspects. IntelliTrap Activation et spyware/grayware protection. 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

Paramètre	Par défaut	Remarques
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.
Spyware ou grayware autorisés	Aucune	N/A
Notification d'événement local	Oui	N/A

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 console AWS EC2 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,	TCP	80/ 443 (Source : 0,0,0,0/0)	SentinelDefaultSecurityGroupPublic (ne limite pas le trafic sortant)

Type	Protocole	Plage de ports	Source
SSH, RDP		L'accès SSH et RDP est autorisé depuis les bastions	
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

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 console AWS EC2 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

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 (managed automation)` modification (ct-1oxx2g2d7hc90).

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-2019s9y3nfml4]

> **Note**
>
> Lorsque vous utilisez le mode manuel 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 console EC2. 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`.

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-instance-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`	`AMSInstanceProfileBYOEPSPolicy` : Permet aux instances Ec2 d'utiliser AMS pour apporter votre propre EPS.
	`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.
	`AMSInstanceProfileS3WritePolicy` : Permet aux instances Ec2 d'accéder read/write aux compartiments S3 du client.

SALZ

Il existe un profil d'instance par défaut AMS`customer-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 `aws:iam::*:role/customer-*` et `aws:iam::*:role/customer_*` .
Instance pour télécharger les événements du journal	Autorisation	Créer un groupe de journaux	Permet de créer des journaux dans : `aws:logs:*:*:log-group:i-*`
		Créer un flux de journal	Permet de diffuser les journaux vers : `aws:logs:*:*:log-group:i-*`

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 : `aws:logs:*:*:log-group:/mc/*`
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, ListMultipartUploadPorts, 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. `aws:s3:::mc-*-internal-*/aws/ssm*`
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 `aws:s3:::mc-*-logs-*/encrypted/app/*`

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 `aws:s3:::awsms-a*-patch-data-*`
Téléchargement de vos propres journaux vers S3	Autorisation	PutObject	Permet aux EC2 applications de télécharger des journaux personnalisés vers : `aws:s3:::mc-a*-logs-*/aws/instances/*/${aws:userid}/*`
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 : `aws:s3:::mc-*-logs-*/encrypted/mc*` , `aws:s3:::mc-*-logs-*/mc/*`, `aws:s3:::mc-a*-logs-*-audit/*`

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 : `aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-tenant-id*` , `arn:aws:secretsmanager:*:*: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*`
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.

Valeurs par défaut des métriques surveillées

Le tableau suivant indique ce qui est surveillé et les seuils d'alerte par défaut. Vous pouvez modifier les valeurs par défaut à l'aide d'une demande de modification (RFC) de gestion des modifications.

> **Note**
>
> CloudWatch a lancé la rétention prolongée des indicateurs le 1er novembre 2016. Pour plus d'informations, consultez Limites CloudWatch .

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 directeme nt à votre adresse e-mail (si vous avez souscrit à la rubrique Direct-Customer-Alerts SNS).			
Instance d'Applica tion 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.
Applicati on 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 enregistr ées.
Instance Amazon EC2 — 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	CloudWatch événement. Émis lorsqu'un point de restauration de sauvegarde est supprimé.

Service	Alerte de sécurité	Nom de l'alerte et condition de déclenchement	Remarques
		supprimé un point de AWS Backup récupération.	
AWS Outposts	Oui	AMSOutpostsInstanceFamilyCapacityAvailability 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.
		AMSOutpostsInstanceTypeCapacityAvailability TypeCapacityAvailability = 80 % pendant 5 minutes, 12 fois consécutives.	CloudWatch alarme sur le type d'instance (capacité, disponibilité de la AWS Outposts ressource).
		AMSOutpostsConnectedStatusConnectedStatus < 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.
		AMSOutpostsCapacityExceptionCapacityExceptions 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) .

Service	Alerte de sécurité	Nom de l'alerte et condition de déclenchement	Remarques
Instance EC2 : toutes OSs	Non	CPUUtilization* >= 95 % pendant 5 minutes, 6 fois de suite, si l'instance ne répond pas à une commande d'interrogation de Systems Manager.	CloudWatch alarme. L'utilisation 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.
		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/managedservices/latest/ctref/management-monitoring-cloudwatch-enable-non-root-volumes-monitoring.html#management-monitoring-cloudwatch-enable-non-root-volumes-monitoring-info.	

Service	Alerte de sécurité	Nom de l'alerte et condition de déclenchement	Remarques
		Sans mémoire* MemoryFree < 5 % pendant 5 minutes, 6 fois de suite.	
	Oui	Logiciel malveillant EPS Malware détecté sur l'instance.	CloudWatch événement.
Instance Amazon EC2 - Linux	Non	Utilisation de l'inode du volume racine Moyenne >= 95 % pendant 5 minutes, 6 fois de suite.	CloudWatch alarme. Appliqué aux instances Linux uniquement.
		Swap gratuit* Échange de mémoire < 5 % pendant 5 minutes, 6 fois de suite.	
ElastiCache Cluster	Non	CurrConnections = 65000	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.

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 cluster	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 réplicas ne sont pas alloués 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 réplica 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.
Instance d'Elastic Load Balancing	Non	SurgeQueueLength > 100 pendant 1 minute, 15 fois de suite.	CloudWatch alarme si un nombre excessif de demandes sont en attente de routage.
		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	Tableau de bord AWS Health	Des notifications sont envoyées en cas de modification du statut des événements Tableau de bord AWS Health (AWS Health) par rapport aux services de base pris en charge par AMS nécessitant une action de la part d'AMS Operations. 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.

Service	Alerte de sécurité	Nom de l'alerte et condition de déclenchement	Remarques
		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.
		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 du statut 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 instantan é.

Service	Alerte de sécurité	Nom de l'alerte et condition de déclenchement	Remarques
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.
		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 IDs 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 retentera 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 ne peut pas 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 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 retentera 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 de santé 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 Analyzing Amazon Macie Findings. Notez que Macie n'est pas activé pour tous les comptes.

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 pendant 10 ans 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.

Paramètres par défaut de gestion de la continuité

Cette section décrit les paramètres par défaut de gestion de la continuité AMS ; pour plus d'informations sur les sauvegardes AMS, consultez le chapitre sur la gestion de la continuité du guide de l'utilisateur AMS.

La configuration de sauvegarde est effectuée au moment de l'intégration. Il s'agit des paramètres de sauvegarde par défaut (recommandés).

Tag VPC et valeurs par défaut

Pour obtenir les informations les plus récentes sur la sauvegarde AMS, consultez la section Gestion de la continuité.

> **Important**
>
> Par défaut, les sauvegardes par EC2 pile sont désactivées (Backup = False). Vous pouvez activer les sauvegardes d' EC2 instance au moment de la création en ajoutant une balise `Key: Backup, Value: True` lorsque vous demandez une EC2 pile via une RFC (CT ct-14027q0sjyt1h). Si vous souhaitez ajouter la balise une fois l'instance créée, soumettez une RFC avec Management | Advanced stack components | EC2 instance stack | Update CT (ct-38s4s4tm4ic4u).

EC2 balise d'instance et valeurs par défaut

La balise de sauvegarde de la EC2 pile indique si la pile nécessite ou non un instantané des volumes EBS attachés.

```
Tag  Key: Backup

Tag  Value: True, False
```

Par défaut, la valeur est que `False` la balise de sauvegarde n'est pas présente et qu'aucune sauvegarde n'est planifiée dans la pile.

Modifiez la balise `Key: Backup Value: True` pour activer les sauvegardes, qui sont ensuite effectuées selon le calendrier défini avec la balise de sauvegarde VPC.

> **Note**
>
> Le cadre de la valeur de l'étiquette (valeur uniquement) est insensible, donc True/true ou False/false est tout à fait acceptable.

Sauvegarde et paramètres par défaut de l'instance RDS

Les valeurs par défaut d'Amazon Relational Database Service (RDS) sont définies dans les modèles de pile :

```
 Backup: Yes

 Backup Window: 22:00-23:00 (RDS local time zone)

 Retention Period: 7 (7 snapshots stored)
```

Paramètres par défaut des correctifs

Cette section décrit les paramètres par défaut des correctifs AMS ; pour plus d'informations sur les correctifs AMS, consultez le chapitre sur la gestion des correctifs du guide de l'utilisateur AMS.

Les versions d'AMS sont AMIs corrigées tous les mois ; toutes les nouvelles demandes de pile doivent être configurées avec la dernière AMI AMS.

> **Important**
>
> AMS Patch Orchestrator, un système de correctifs basé sur des balises, utilise la fonctionnalité AWS Systems Manager (SSM) pour vous permettre de baliser ou de faire étiqueter des instances par AMS pour vous et de faire appliquer des correctifs à ces

instances à l'aide d'une ligne de base et d'une fenêtre que vous configurez. Pour en savoir plus, voir Patch Orchestrator : un modèle d'application de correctifs basé sur des balises.

Correctifs conformes à la norme AMS, basés sur les comptes : pour chaque compte dont les piles reçoivent des correctifs sur place, une notification des correctifs applicables à venir est envoyée peu après le « mardi des correctifs ». La notification contient une liste de toutes les piles et des correctifs applicables, ainsi que la fenêtre de correctifs suggérée. Pour les correctifs critiques, la fenêtre n'est pas définie plus de 10 jours à l'avance, et pour les correctifs standard, pas plus de 14 jours à l'avance. Si vous ne répondez pas à la notification, aucun correctif n'est appliqué. Si vous souhaitez exclure certains correctifs, répondez à la notification ou envoyez une demande de service. Si vous répondez en acceptant l'application de correctifs, mais que vous ne demandez pas spécifiquement un calendrier différent, les correctifs sont appliqués comme décrit dans la notification que vous recevez.

> **Note**
>
> La notification du service de correctifs est un e-mail envoyé aux contacts du compte et contient un lien vers la console AWS Support. Vous pouvez répondre via la console AWS Support ou via la page de demande de service AMS, où la notification apparaît sous forme de notification de service.

Au moment du processus d'application des correctifs conformes à la norme AMS, AMS effectue les opérations suivantes :

1. Vous recevez une notification du service de correctifs quatorze jours avant la fenêtre de correctifs proposée. La notification du service de correctifs est envoyée par e-mail à l'adresse e-mail de contact que vous avez enregistrée pour votre compte.
2. Identifie toutes les EC2 instances accessibles de la pile en fonction de la liste des piles fournie dans la notification d'application des correctifs. Dans ce cas, « Accessible » désigne les instances qui sont dans l' EC2 état « En cours d'exécution » et dont l'agent EC2 Run Command est pleinement opérationnel.
3. AMS exécute les correctifs de manière à garantir qu'un nombre suffisant d' EC2 instances s'exécutent simultanément (configurées via le `healthy-host-threshold` paramètre) afin que la pile reste saine.
4. Une fois l'opération de correction terminée pour toutes les EC2 instances, AMS met à jour la RFC avec l'état du correctif : réussite, réussite partielle ou échec. Dans le cas d'un statut autre

que Success, un ticket est créé pour qu'un opérateur puisse suivre les résultats des correctifs et prendre des mesures correctives.

Valider le service AMS (SALZ)

Pour vérifier que le service AWS Managed Services (AMS) fonctionne comme prévu, certains exercices que vous pouvez effectuer sont décrits dans ce chapitre.

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 se *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 saml`, 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 saml`, 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 saml`, 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 saml`, 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 Backupservice 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.

Recherche d'un ID d'instance ou d'une adresse IP

Vous avez besoin d'une adresse IP d'instance pour vous connecter à l'instance.

- 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 saml`, 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-s6xvs000000000000",
        "CreatedTime": "1486584508416",
        "Name": "Amazon"
    }
}
```

Noms de bastion 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)*.A*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)*.A*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

Trouver les adresses IP des 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.

Instances EC2 : création

Vous pouvez utiliser la console AMS ou API/CLI créer un Amazon EC2 et un Amazon EC2 avec des volumes supplémentaires.

Créer une pile

Création d'une instance EC2 avec la console

Ce qui suit montre ce type de modification dans la console AMS.

Fonctionnement :

1. Accédez à la page Créer une RFC : Dans le volet de navigation de gauche de la console AMS, cliquez RFCspour 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 instance EC2 avec la CLI

Fonctionnement :

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 (évitez 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-14027q0sjyt1h" --change-type-version "4.0"
 --title "EC2-Create-RFC" --execution-parameters "{\"Description\": \"Create a new
 EC2 Instance stack\",\"VpcId\": \"vpc-0a60eb65b4EXAMPLE\",\"Name\": \"My-EC2\",
\"TimeoutInMinutes\": 60,\"Parameters\": {\"InstanceAmiId\": \"ami-1234567890EXAMPLE\",
\"InstanceDetailedMonitoring\": false,\"InstanceEBSOptimized\": false,\"InstanceProfile
\": \"customer-mc-ec2-instance-profile\",\"InstanceRootVolumeIops\": 3000,
\"InstanceRootVolumeType\": \"gp3\",\"InstanceType\": \"t2.large\",\"InstanceUserData
\": \"\",\"InstanceSubnetId\": \"subnet-0bb1c79de3EXAMPLE\",\"EnforceIMDSV2\":
 \"false\"}}"
```

CRÉATION DU MODÈLE :

1. Exportez les paramètres d'exécution de ce type de modification dans un fichier JSON ; cet exemple le nomme Create EC2 Params.json :

   ```
   aws amscm get-change-type-version --change-type-id "ct-14027q0sjyt1h" --query
    "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateEC2Params.json
   ```

2. Modifiez et enregistrez le fichier Create EC2 Params. Par exemple, vous pouvez remplacer le contenu par quelque chose comme ceci :

```
{
  "Description": "Create a new EC2 Instance stack",
  "VpcId": "vpc-0a60eb65b4EXAMPLE",
  "Name": "My-EC2",
  "TimeoutInMinutes": 60,
  "Parameters": {
    "InstanceAmiId": "ami-1234567890EXAMPLE",
    "InstanceDetailedMonitoring": false,
    "InstanceEBSOptimized": false,
    "InstanceProfile": "customer-mc-ec2-instance-profile",
    "InstanceRootVolumeIops": 3000,
    "InstanceRootVolumeType": "gp3",
    "InstanceType": "t2.large",
    "InstanceUserData": "",
    "InstanceSubnetId": "subnet-0bb1c79de3EXAMPLE",
    "EnforceIMDSV2": "false"
  }
}
```

3. Exportez le modèle RFC dans un fichier de votre dossier actuel ; cet exemple le nomme Create EC2 RFC.json :

```
aws amscm create-rfc --generate-cli-skeleton > CreateEC2Rfc.json
```

4. Modifiez et enregistrez le fichier Create EC2 RFC.json. Par exemple, vous pouvez remplacer le contenu par quelque chose comme ceci :.

```
{
"ChangeTypeVersion":    "4.0",
"ChangeTypeId":         "ct-14027q0sjyt1h",
"Title":                "EC2-Create-RFC"
}
```

5. Créez le RFC en spécifiant le fichier Create EC2 Rfc et le fichier Create EC2 Params :

```
aws amscm create-rfc --cli-input-json file://CreateEC2Rfc.json  --execution-
parameters file://CreateEC2Params.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.

Conseils

Groupes de sécurité

À partir de la version 3.0 de ce type de modification, AMS n'attache pas les groupes de sécurité AMS par défaut si vous spécifiez vos propres groupes de sécurité. Si vous ne spécifiez pas vos propres groupes de sécurité dans la demande, AMS joint les groupes de sécurité AMS par défaut. Dans les versions précédentes, AMS associait les groupes de sécurité par défaut, que vous ayez fourni ou non vos propres groupes de sécurité. Actuellement, si vous spécifiez des groupes de sécurité personnalisés, vous devez également spécifier les groupes IDs de sécurité AMS par défaut pour votre compte, `mc-initial-garden-SG-name` et`mc-initial-garden-SG-name`.

Types d'instances

AMS ne recommande pas les types t2.micro/t3.micro et t2.nano/t3.nano. Il s'agit de types d'instances plus petits qui peuvent dégrader les performances de votre application et des outils AMS. Les instances EC2 ont besoin d'une capacité suffisante pour prendre en charge les outils AMS tels que EPS, SSM et Cloudwatch, en plus de la charge de travail des applications. Pour plus d'informations, consultez Choisir le type d'instance EC2 adapté à votre application.

Pour créer une pile EC2 avec des volumes supplémentaires, voir EC2 Stack | Create (with Additional Volumes).

Vous pouvez ajouter jusqu'à 50 balises, mais pour cela, vous devez activer la vue Configuration supplémentaire.

Si nécessaire, consultez EC2 instance stack create fail.

Créer une pile (avec des volumes supplémentaires)

Création d'une instance EC2 et de volumes supplémentaires avec la console

Ce qui suit montre ce type de modification dans la console AMS.

Fonctionnement :

1. Accédez à la page Créer une RFC : Dans le volet de navigation de gauche de la console AMS, cliquez RFCspour 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 instance EC2 et de volumes supplémentaires avec la CLI

Fonctionnement :

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 (évitez les guillemets lorsque vous fournissez des paramètres d'exécution en ligne), puis soumettez l'ID RFC renvoyé (l'exemple montre uniquement les paramètres requis). Par exemple, vous pouvez remplacer le contenu par quelque chose comme ceci :

```
aws amscm create-rfc --change-type-id "ct-1aqsjf86w6vxg" --change-type-version "4.0"
 --title "EC2-Create-A-V-QC" --execution-parameters "{\"Description\":\"My EC2 stack
 with addl vol\",\"VpcId\":\"VPC_ID\",\"Name\":\"My Stack\",\"StackTemplateId\":
\"stm-nn8v8ffhcal611bmo\",\"TimeoutInMinutes\":60,\"Parameters\":{\"InstanceAmiId\":
\"AMI_ID\",\"InstanceSubnetId\":\"SUBNET_ID\"}}
```

CRÉATION DU MODÈLE :

1. Exportez les paramètres d'exécution de ce type de modification dans un fichier JSON nommé Create EC2 AVParams .json.

```
aws amscm get-change-type-version --change-type-id "ct-1aqsjf86w6vxg" --query
 "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateEC2AVParams.json
```

2. Modifiez et enregistrez le EC2 AVParams fichier Create (l'exemple montre la plupart des paramètres). Par exemple, vous pouvez remplacer le contenu par quelque chose comme ceci :

```
{
"Description":      "EC2-Create-1-Addl-Volumes",
"VpcId":            "VPC_ID",
"StackTemplateId":  "stm-nn8v8ffhcal611bmo",
"Name":             "My-EC2-1-Addl-Volume",
"TimeoutInMinutes": 60,
"Parameters":   {
    "InstanceAmiId":    "AMI_ID",
    "InstanceSecurityGroupIds": "SECURITY_GROUP_ID",
    "InstanceCoreCount": 1,
    "InstanceThreadsPerCore": 2,
    "InstanceDetailedMonitoring": "true",
    "InstanceEBSOptimized": "false",
    "InstanceProfile": "customer-mc-ec2-instance-profile",
    "InstanceRootVolumeIops": 100,
    "InstanceRootVolumeName": "/dev/xvda",
    "InstanceRootVolumeSize": 50,
    "InstanceRootVolumeType": "io1",
    "RootVolumeKmsKeyId": "default",
    "InstancePrivateStaticIp": "10.27.0.100",
    "InstanceSecondaryPrivateIpAddressCount": 0,
    "InstanceTerminationProtection": "false",
    "InstanceType": "t3.large",
    "CreditSpecification": "unlimited",
    "InstanceUserData": "echo $",
    "Volume1Encrypted": "true",
    "Volume1Iops":      "IOPS"
    "Volume1KmsKeyId":  "KMS_MASTER_KEY_ID",
    "Volume1Name":      "xvdh"
    "Volume1Size":      "2 GiB",
    "Volume1Snapshot":  "SNAPSHOT_ID",
    "Volume1Type":      "iol",
    "InstanceSubnetId": "SUBNET_ID"
    }
```

```
}
```

3. Exportez le modèle RFC dans un fichier de votre dossier actuel ; cet exemple le nomme Create EC2 AVRfc .json :

```
aws amscm create-rfc --generate-cli-skeleton > CreateEC2AVRfc.json
```

4. Modifiez et enregistrez le fichier Create EC2 AVRfc .json. Par exemple, vous pouvez remplacer le contenu par quelque chose comme ceci :

```
{
"ChangeTypeVersion":    "4.0",
"ChangeTypeId":         "ct-1aqsjf86w6vxg",
"Title":                "EC2-Create-1-Addl-Volume-RFC"
}
```

5. Créez la RFC en spécifiant le fichier de création et le EC2 AVRfc fichier de création EC2 AVParams :

```
aws amscm create-rfc --cli-input-json file://CreateEC2AVRfc.json  --execution-
parameters file://CreateEC2AVParams.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.

Conseils

> **Important**
>
> Il existe une nouvelle version de ce type de modification, v 4.0, qui utilise un autre StackTemplateId (stm-nn8v8ffhcal611bmo). Ceci est important si vous soumettez la RFC avec ce type de modification sur la ligne de commande. La nouvelle version introduit deux nouveaux paramètres (RootVolumeKmsKeyIdet CreditSpecification) et modifie la valeur par défaut d'un paramètre existant (InstanceType).

Types d'instances

- Si vous choisissez de spécifier le nombre de cœurs ou de threads, vous devez spécifier des valeurs pour les deux. Utilisez les paramètres `InstanceCoreCount` et`InstanceThreadsPerCore`. Pour trouver des combinaisons valides de cœurs/threads, consultez la section Nombre de cœurs de processeur et de threads par cœur de processeur et par type d'instance.
- AMS ne recommande pas les types d'instance t2.micro/t3.micro ou t2.nano/t3.nano. Ils sont trop petits pour prendre en charge les outils AMS tels que EPS, SSM et Cloudwatch en plus de la charge de travail de votre entreprise. Pour plus d'informations, consultez Choisir le type d'instance EC2 adapté à votre application.
- Dans la version 4.0, le type par défaut est passé de t2.large à t3.large. Les instances T3 sont lancées avec des « crédits illimités » par défaut. Vous ne subirez aucun ralentissement du processeur même si l'instance consomme tous les crédits du processeur. Vous pouvez plutôt choisir des instances T2 et utiliser l'option CreditSpecification illimitée.
- Pour plus d'informations sur Amazon EC2, notamment les recommandations relatives à la taille, consultez la documentation Amazon Elastic Compute Cloud.

Pour mettre à jour votre pile EC2 avec des volumes supplémentaires après leur création, voir Pile d'instances EC2 : mise à jour (avec volumes supplémentaires)

Accès, demande

Demande d'accès administratif

Demande d'accès administrateur via la console

Ce qui suit montre ce type de modification dans la console AMS.

Fonctionnement :

1. Accédez à la page Créer une RFC : Dans le volet de navigation de gauche de la console AMS, cliquez RFCspour 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 le RFC ou en créer une copie avec les options en haut de la page.

Demande d'accès administrateur à l'aide de la CLI

Fonctionnement :

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 (évitez 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 --profile saml amscm create-rfc --change-type-id "ct-1dmlg9g1l91h6" --change-type-
version "3.0" --title "Stack-Admin-Access-QC" --execution-parameters "{\"DomainFQDN
\":\"TEST.com\",\"StackIds\":[\"stack-01234567890abcdef\"],\"TimeRequestedInHours\":1,
\"Usernames\":[\"TEST\"],\"VpcId\":\"VPC_ID\"}"
```

CRÉATION DU MODÈLE :

1. Afficher le schéma JSON des paramètres d'exécution pour ce type de modification dans un fichier ; cet exemple le nomme GrantAdminAccessParams .json :

   ```
   aws amscm get-change-type-version --change-type-id "ct-1dmlg9g1l91h6"
    --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
    GrantAdminAccessParams.json
   ```

Modifiez et enregistrez le GrantAdminAccessParams fichier. Par exemple, vous pouvez remplacer le contenu par quelque chose comme ceci :

```
{
"DomainFQDN":           "mycorpdomain.acme.com",
"StackIds":             [STACK_ID, STACK_ID],
"TimeRequestedInHours": 12,
"Username":             ["USERNAME", "USERNAME"],
"VpcId":                "VPC_ID"
}
```

Notez que l'`TimeRequestedInHours`option est définie par défaut sur une heure. Vous pouvez demander jusqu'à douze heures.

2. Exportez le modèle RFC dans un fichier de votre dossier actuel ; cet exemple le nomme GrantAdminAccessRfc .json :

```
aws amscm create-rfc --generate-cli-skeleton > GrantAdminAccessRfc.json
```

3. Modifiez et enregistrez le fichier GrantAdminAccessRfc .json. Par exemple, vous pouvez remplacer le contenu par quelque chose comme ceci :

```
{
"ChangeTypeId":         "ct-1dmlg9g1l91h6",
"ChangeTypeVersion":    "3.0",
"Title":                "Request-Admin-Access-to-EC2-RFC"
}
```

4. Créez la RFC en spécifiant le GrantAdminAccessRfc fichier et le GrantAdminAcessParams fichier :

```
aws amscm create-rfc --cli-input-json file://GrantAdminAccessRfc.json --execution-
parameters file://GrantAdminAccessParams.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 vous connecter à l'instance via un bastion, suivez la procédure suivante, intitulée Exemples d'accès aux instances.

Conseils

> **Note**
>
> Vous pouvez mettre à jour votre demande d'accès avant son expiration. Pour plus d'informations, voir Stack Admin Access | Update.
> Pour vous connecter à une instance faisant partie d'un ASG, vous demandez l'accès à la pile ASG, qui vous donne accès à toutes les instances associées.

Pour un exemple de demande ReadOnly d'accès, voir ReadOnly accès : demande.

Demande d' ReadOnly accès

Demande ReadOnly d'accès via la console

Ce qui suit montre ce type de modification dans la console AMS.

Fonctionnement :

1. Accédez à la page Créer une RFC : Dans le volet de navigation de gauche de la console AMS, cliquez RFCspour 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 le RFC ou en créer une copie avec les options en haut de la page.

Demande ReadOnly d'accès avec la CLI

Fonctionnement :

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 (évitez 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 --profile saml amscm create-rfc --change-type-id "ct-199h35t7uz6jl" --change-type-
version "3.0" --title "Stack-RO-Access-QC" --execution-parameters "{\"DomainFQDN\":
\"TEST.com\",\"StackIds\":[\"stack-01234567890abcdef\"],\"TimeRequestedInHours\":1,
\"Usernames\":[\"TEST\"],\"VpcId\":\"VPC_ID\"}"
```

CRÉATION DU MODÈLE :

1. Afficher le schéma JSON des paramètres d'exécution pour ce type de modification dans un fichier ; cet exemple le nomme GrantReadOnlyAccessParams .json :

   ```
   aws amscm get-change-type-version --change-type-id "ct-199h35t7uz6jl"
    --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
    GrantReadOnlyAccessParams.json
   ```

   Modifiez et enregistrez le GrantReadOnlyAccessParams fichier. Par exemple, vous pouvez remplacer le contenu par quelque chose comme ceci :

   ```
   {
   "DomainFQDN":           "mycorpdomain.acme.com",
   "StackIds":             [STACK_ID, STACK_ID],
   "TimeRequestedInHours": 12,
   "Usernames":             ["USERNAME", "USERNAME"],
   "VpcId":                "VPC_ID"
   }
   ```

   Notez que l'`TimeRequestedInHours`option est définie par défaut sur une heure. Vous pouvez demander jusqu'à douze heures.

2. Exportez le modèle RFC dans un fichier de votre dossier actuel ; cet exemple le nomme GrantReadOnlyAccessRfc .json :

```
aws amscm create-rfc --generate-cli-skeleton > GrantReadOnlyAccessRfc.json
```

3. Modifiez et enregistrez le fichier GrantReadOnlyAccessRfc .json. Par exemple, vous pouvez remplacer le contenu par quelque chose comme ceci :

```
{
"ChangeTypeId":          "ct-199h35t7uz6jl",
"ChangeTypeVersion":     "3.0",
"Title":                 "Request-ReadOnly-Access-to-EC2-RFC"
}
```

4. Créez la RFC en spécifiant le GrantReadOnlyAccessRfc fichier et le GrantReadOnlyAcessParams fichier :

```
aws amscm create-rfc --cli-input-json file://GrantReadOnlyAccessRfc.json --
execution-parameters file://GrantReadOnlyAccessParams.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 vous connecter à l'instance via un bastion, suivez la procédure suivante, intitulée Exemples d'accès aux instances.

Conseils

> **Note**
>
> Vous pouvez mettre à jour votre demande d'accès avant son expiration. Pour plus de détails, voir Stack Read-Only Access | Update.
> Pour vous connecter à une instance faisant partie d'un groupe EC2 Auto Scaling (ASG), vous demandez l'accès à la pile ASG, qui vous donne accès à toutes les instances associées.

Pour une présentation détaillée de la demande d'accès administrateur, voir Accès administrateur : demande.

Autre | Autre RFC, création (CLI)

Cet exemple montre comment demander une modification qui ne contient aucune CTs adresse disponible, en utilisant le CT Management | Other | Other | Create (ct-1e1xtak34nx76).

Utilisez ce scanner lorsque vous ne trouvez pas de type de modification correspondant à ce que vous recherchez ; toutefois, si vous n'êtes pas sûr de spécifier les paramètres d'un scanner existant, il est préférable de soumettre une demande de service pour obtenir de l'aide. Pour plus d'informations sur la soumission de demandes de service, consultez les exemples de demandes de service.

Ce type de RFC nécessite une approbation, ce qui signifie qu'il nécessite l'approbation de l'AMS avant de pouvoir être mis en œuvre. Après avoir soumis le RFC, un opérateur AMS vous contactera pour discuter de la pile que vous souhaitez déployer.

> **Note**
>
> Lorsque vous utilisez le mode manuel 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.

DONNÉES REQUISES :

- `Comment`: À quoi sert le RFC.
- `ChangeTypeId`et `ChangeTypeVersion` : utilisez Other | Create (`ct-1e1xtak34nx76`) pour demander de nouvelles ressources, utilisez Other | Update (`ct-0xdawir96cy7k`) pour modifier les ressources existantes ; les deux le sont`v1`.

DONNÉES FACULTATIVES `Priority` : Les valeurs acceptables sont `High`, `Medium`, ou`Low`.

CRÉATION EN LIGNE :

- Émettez la commande create RFC avec les paramètres d'exécution fournis en ligne (évitez les guillemets lorsque vous fournissez des paramètres d'exécution en ligne). L'exemple utilise Autre | Créer.

```
aws amscm create-rfc --change-type-id "ct-1e1xtak34nx76" --change-type-version "1.0"
 --title "TITLE" --execution-parameters "{\"Comment\": \"What you want created\"}"
```

- Soumettez le RFC à l'aide de l'ID RFC renvoyé lors de l'opération de création du RFC. Jusqu'à ce qu'elle soit soumise, la RFC reste en l'`Editing`état et ne fait l'objet d'aucune action.

```
aws amscm submit-rfc --rfc-id RFC_ID
```

- Surveillez l'état de la RFC et visualisez le résultat de l'exécution :

```
aws amscm get-rfc --rfc-id RFC_ID
```

CRÉATION D'UN MODÈLE :

1. Créez et enregistrez un fichier JSON pour les paramètres d'exécution ; l'exemple le nomme OtherParams .json et inclut le `Priority` paramètre facultatif :

```
{
"Comment":          "What you want created",
"Priority":         "Medium"
}
```

2. Créez et enregistrez un fichier JSON pour les paramètres RFC ; l'exemple le nomme OtherRfc .json.

```
{
"ChangeTypeId":         "ct-1e1xtak34nx76",
"ChangeTypeVersion":    "1.0",
"Title":                "TITLE"
}
```

3. Créez la RFC en spécifiant le OtherRfc fichier et le OtherParams fichier :

```
aws amscm create-rfc --cli-input-json file://OtherRfc.json  --execution-parameters
 file://OtherParams.json
```

Vous recevez le code RfcId de la nouvelle RFC dans la réponse. Par exemple :

```
{
```

```
"RfcId": "RFC-ID"
}
```

4. Soumettez le RFC :

```
aws amscm submit-rfc --rfc-id RFC-ID
```

Si aucune erreur n'est signalée, cela signifie que l'opération a réussi.

5. Pour surveiller l'état de la demande et consulter le résultat de l'exécution, procédez comme suit :

```
aws amscm get-rfc --rfc-id RFC-ID
```

N'importe quelle pile : suppression, redémarrage, démarrage, arrêt

Vous pouvez utiliser la console AMS ou API/CLI pour supprimer, redémarrer, démarrer ou arrêter une pile AMS.

Supprimer la pile

Supprimer une pile à l'aide de la console

Capture d'écran de ce type de modification dans la console AMS :

Fonctionnement :

1. Accédez à la page Créer une RFC : Dans le volet de navigation de gauche de la console AMS, cliquez RFCspour 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 le RFC ou en créer une copie avec les options en haut de la page.

Supprimer une pile à l'aide de la CLI

Fonctionnement :

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 (évitez 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-0q0bic0ywqk6c" --change-type-version "1.0" --
title "Delete My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

CRÉATION D'UN MODÈLE :

1. Exportez le modèle RFC dans un fichier de votre dossier actuel ; cet exemple le nomme DeleteStackRfc .json :

   ```
   aws amscm create-rfc --generate-cli-skeleton > DeleteStackRfc.json
   ```

2. Modifiez et enregistrez le fichier DeleteStackRfc .json.

   Les guillemets internes de l'extension ExecutionParameters JSON doivent être masqués par une barre oblique inverse (\). Exemple sans heure de début et de fin :

   ```
   {
   "ChangeTypeVersion":    "1.0",
   "ChangeTypeId":         "ct-0q0bic0ywqk6c",
   "Title":                "Delete-My-Stack-RFC"
   "ExecutionParameters":  "{
           \"StackId\":\"STACK_ID\"}"
   }
   ```

3. Créez le RFC :

```
aws amscm create-rfc --cli-input-json file://DeleteStackRfc.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.

Conseils

> **Note**
>
> Si vous supprimez un compartiment S3, il doit d'abord être vidé de ses objets.

> **Important**
>
> La suppression de piles peut avoir des conséquences indésirables et imprévues. Pour les mises en garde importantes, consultez la section Dépannage des RFC RFCs pour Delete Stack.

Redémarrer la pile

Redémarrer une pile à l'aide de la console

Capture d'écran de ce type de modification dans la console AMS :

Fonctionnement :

1. Accédez à la page Créer une RFC : Dans le volet de navigation de gauche de la console AMS, cliquez RFCspour 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 le RFC ou en créer une copie avec les options en haut de la page.

Redémarrer une pile à l'aide de la CLI

Fonctionnement :

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 (évitez 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-02u0hoaa9grat" --change-type-version "1.0" --
title "Reboot My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

CRÉATION D'UN MODÈLE :

1. Exportez le modèle RFC dans un fichier de votre dossier actuel. Cet exemple le nomme RebootStackRfc .json. Notez qu'étant donné qu'il n'existe qu'un seul paramètre d'exécution pour arrêter (redémarrer ou démarrer) une instance, le paramètre d'exécution peut se trouver dans le fichier JSON du schéma lui-même et il n'est pas nécessaire de créer un fichier JSON de paramètres d'exécution distinct.

   ```
   aws amscm create-rfc --generate-cli-skeleton > StopInstanceRfc.json
   ```

2. Modifiez et enregistrez le fichier RebootStackRfc .json.

   Les guillemets internes de l'extension `ExecutionParameters` JSON doivent être masqués par une barre oblique inverse (\). Exemple :

   ```
   {
   ```

```
"ChangeTypeId":          "ct-02u0hoaa9grat",
"Title":                 "Reboot-My-EC2-RFC",
"TimeoutInMinutes":      60,
"ExecutionParameters":   "{
        \"StackId\":\"STACK_ID\"
    }"
}
```

3. Créez le RFC :

```
aws amscm create-rfc --cli-input-json file://RebootStackRfc.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.

Conseils

Pour plus d'informations sur les équilibreurs de charge d'application, voir Équilibreurs de charge d'application.

Start Stack

Démarrer une pile avec la console

Capture d'écran de ce type de modification dans la console AMS :

Fonctionnement :

1. Accédez à la page Créer une RFC : Dans le volet de navigation de gauche de la console AMS, cliquez RFCspour 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 le RFC ou en créer une copie avec les options en haut de la page.

Démarrage d'une pile avec la CLI

Fonctionnement :

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 (évitez 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-1h5xgl9cr4bzy" --change-type-version "1.0" --
title "Start My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

CRÉATION D'UN MODÈLE :

1. Exportez le modèle RFC dans un fichier de votre dossier actuel. Cet exemple le nomme StartInstanceRfc .json. Notez qu'étant donné qu'il n'existe qu'un seul paramètre d'exécution pour démarrer une pile, le paramètre d'exécution peut se trouver dans le fichier JSON du schéma lui-même et il n'est pas nécessaire de créer un fichier JSON de paramètres d'exécution distinct.

   ```
   aws amscm create-rfc --generate-cli-skeleton > StartStackRfc.json
   ```

2. Modifiez et enregistrez le fichier StartStackRfc .json. Par exemple, vous pouvez remplacer le contenu par quelque chose comme ceci :

   ```
   {
   "ChangeTypeId":          "ct-1h5xgl9cr4bzy",
   "Title":                 "Start-My-EC2-RFC",
   "TimeoutInMinutes":      60,
   ```

```
"ExecutionParameters":  "{
        \"StackId\":\"STACK_ID\"
    }"
}
```

3. Créez le RFC :

```
aws amscm create-rfc --cli-input-json file://StartStackRfc.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.

Conseils

Pour plus d'informations sur les équilibreurs de charge d'application, voir Équilibreurs de charge d'application.

Arrêter la pile

Arrêter une pile à l'aide de la console

Capture d'écran de ce type de modification dans la console AMS :

Fonctionnement :

1. Accédez à la page Créer une RFC : Dans le volet de navigation de gauche de la console AMS, cliquez RFCspour 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 le RFC ou en créer une copie avec les options en haut de la page.

Arrêter une pile à l'aide de la CLI

Fonctionnement :

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 (évitez 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-3dgbnh6gpst4d" --change-type-version "1.0" --
title "Stop My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

CRÉATION D'UN MODÈLE :

1. Exportez le modèle RFC dans un fichier de votre dossier actuel. Cet exemple le nomme StopStackRfc .json. Notez qu'étant donné qu'il n'existe qu'un seul paramètre d'exécution pour arrêter (redémarrer ou démarrer) une instance, le paramètre d'exécution peut se trouver dans le fichier JSON du schéma lui-même et il n'est pas nécessaire de créer un fichier JSON de paramètres d'exécution distinct.

   ```
   aws amscm create-rfc --generate-cli-skeleton > StopStackRfc.json
   ```

2. Modifiez et enregistrez le fichier StopStackRfc .json. Par exemple, vous pouvez remplacer le contenu par quelque chose comme ceci :

   ```
   {
   "ChangeTypeId":          "ct-3dgbnh6gpst4d",
   "Title":                 "Stop-My-EC2-RFC",
   "TimeoutInMinutes":      60,
   "ExecutionParameters":   "{
           \"StackId\":\"STACK_ID\"
   ```

```
    }"
}
```

3. Créez le RFC :

```
aws amscm create-rfc --cli-input-json file://StopInstanceRfc.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.

Conseils

Les instances arrêtées restent arrêtées sauf si vous avez planifié des redémarrages à l'aide du planificateur de ressources AMS.

Si nécessaire, consultez la section EC2 instance Stack Stop Fail.

Exemples d'accès

Ces exemples montrent comment se connecter à une instance via un bastion une fois que l'accès vous a été accordé via une RFC. Pour plus de détails sur l'obtention de l'accès, consultez la section Demandes d'accès.

> **Note**
>
> Une EC2 instance créée par le biais d'un groupe Auto Scaling aura une adresse IP qui entre et sort et vous devrez utiliser votre EC2 console pour trouver cette adresse IP.

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. Trouver les adresses IP des bastions
- Nom d'utilisateur (par exemple username@customerdomain.com) et mot de passe : informations d'identification du compte.
- Adresse IP de pile : pour ce faire, consultez la page Stacks de la console AMS pour trouver la pile à laquelle vous souhaitez vous connecter, puis en filtrant cet ID de pile dans la EC2 console de

votre compte. Pour une EC2 instance unique, vous pouvez également utiliser la commande AMS SKMS. Pour la référence de l'API AMS SKMS, consultez l'onglet Rapports de la console AWS Artifact. Pour trouver l'ID de pile, puis pour la référence de l'API AMS SKMS, consultez l'onglet Rapports de la console AWS Artifact pour trouver l'adresse IP de la pile.

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.

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 choisissez 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, consultezNoms 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 sympathiques des bastions, consultezNoms 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).AAMSAccountNumber.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).AAMSAccountNumber.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 sympathiques des bastions, consultezNoms 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, consultezNoms 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)`*`.A`*`AMSAccountNumber`*`.amazonaws.com`, ce qui ressemblerait à ceci si votre numéro de compte est 123456789123 et que vous choisissez 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).AAMSAccountNumber.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.

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
```

Signaler un incident

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 rouvert.
- 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 affectée. 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 Soumettre.

   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.

Création d'une demande de service

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 Soumettre.

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, utilisez la catégorie Autre dans la console AMS, `ChangeTypeId ct-1e1xtak34nx76` dans l'API AMS CM ou `IssueType=AMS` dans l'API AWS Support.

Étapes postérieures à l'intégration

Maintenant que vous avez créé un compte AMS, vous voudrez lire davantage de documentation AMS. Consultez ces documents :

- Les didacticiels d'utilisation du HA Two-Tier Stack CT pour créer une WordPress pile entièrement fonctionnelle offrent ensuite une expérience AMS complète.
- Guide de l'utilisateur AMS : Le guide de l'utilisateur AMS décrit les fonctionnalités d'AMS, répertorie les termes clés, les opérations, les interfaces et fournit une vue d'ensemble d'une architecture d'infrastructure gérée AMS typique. En outre, les détails de gestion des accès et les paramètres par défaut d'AMS sont fournis. Des descriptions détaillées de l'utilisation du système de gestion des modifications AMS sont également fournies et plusieurs procédures pas à pas sont fournies. D'autres concepts de gestion sont également décrits.

- Référence d'API AMS : Cette référence d'API fournit des descriptions de tous les appels d'API, y compris les demandes, les réponses et les exemples.
- Guide des applications AMS : Le guide des applications AMS décrit les différentes options et méthodes de déploiement et de maintenance de vos applications dans AMS.

Didacticiels

Les didacticiels suivants décrivent les étapes de création d'une pile à deux niveaux avec le CT (avancé) à haute disponibilité (ct-06mjngx5flwto), à l'aide de la CLI et de la console. Un tutoriel est fourni pour déployer un groupe Linux Auto Scaling (ASG) et pour déployer un ASG Windows.

Les descriptions de toutes les options de tomodensitométrie, y compris, se ChangeTypeId trouvent dans le manuel AMS Change Type Reference.

Tutoriel CLI : Stack à deux niveaux de haute disponibilité (Linux/RHEL)

Cette section décrit comment déployer une pile à deux niveaux de haute disponibilité (HA) dans un environnement AMS à l'aide de la CLI AMS.

> **Note**
>
> Cette procédure de déploiement a été testée dans les environnements AMZN Linux et RHEL.

Résumé des tâches et des exigences RFCs :

1. Création d'une infrastructure (pile HA à deux niveaux)
2. Création d'un compartiment S3 pour les CodeDeploy applications
3. Créez le bundle WordPress d'applications et chargez-le dans le compartiment S3
4. Déployez l'application avec CodeDeploy
5. Accédez au WordPress site et connectez-vous pour valider le déploiement

Avant de commencer

Deployment | Advanced Stack Components | High Availability Two Tier Stack Advanced | Create CT crée un groupe Auto Scaling, un équilibreur de charge, une base de données, ainsi qu'un nom d'

CodeDeploy application et un groupe de déploiement (avec le même nom que celui que vous donnez à l'application). Pour plus d'informations, CodeDeploy voir Qu'est-ce que c'est CodeDeploy ?

Cette procédure pas à pas utilise une RFC de haute disponibilité à deux niveaux (avancée) qui inclut UserData et décrit également comment créer un WordPress bundle pouvant CodeDeploy être déployé.

L'exemple `UserData` illustré permet d'obtenir les métadonnées d'instance telles que l'ID d'instance, la région, etc., à partir d'une instance en cours d'exécution en interrogeant le service de métadonnées d' EC2 instance disponible sur http://169.254.169.254/latest/meta-data/. Cette ligne du script de données utilisateur :`REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/ | sed 's/[a-z]$//')`, extrait le nom de la zone de disponibilité du service de métadonnées dans la variable $REGION pour nos régions prises en charge, et l'utilise pour compléter l'URL du compartiment S3 dans lequel l' CodeDeploy agent est téléchargé. L'IP 169.254.169.254 est routable uniquement au sein du VPC (tout le monde peut interroger le service). VPCs Pour plus d'informations sur le service, consultez la section Métadonnées d'instance et données utilisateur. Notez également que les scripts saisis UserData sont exécutés en tant qu'utilisateur « root » et n'ont pas besoin d'utiliser la commande « sudo ».

Cette procédure pas à pas laisse les paramètres suivants à la valeur par défaut (illustrée) :

- Groupe Auto Scaling :`Cooldown=300, DesiredCapacity=2, EBSOptimized=false, HealthCheckGracePeriod=600, IAMInstanceProfile=customer-mc-ec2-instance-profile, InstanceDetailedMonitoring=true, InstanceRootVolumeIops=0, InstanceRootVolumeType=standard, InstanceType=m3.medium, MaxInstances=2, MinInstances=2, ScaleDownPolicyCooldown=300, ScaleDownPolicyEvaluationPeriods=4, ScaleDownPolicyPeriod=60, ScaleDownPolicyScalingAdjustment=-1, ScaleDownPolicyStatistic=Average, ScaleDownPolicyThreshold=35, ScaleMetricName=CPUUtilization, ScaleUpPolicyCooldown=60, ScaleUpPolicyEvaluationPeriods=2, ScaleUpPolicyPeriod=60, ScaleUpPolicyScalingAdjustment=2, ScaleUpPolicyStatistic=Average, ScaleUpPolicyThreshold=75`.
- Load Balancer :. `HealthCheckInterval=30, HealthCheckTimeout=5`
- Base de données :`BackupRetentionPeriod=7, Backups=true, InstanceType=db.m3.medium, IOPS=0, MultiAZ=true, PreferredBackupWindow=22:00-23:00, PreferredMaintenanceWindow=wed:03:32-wed:04:02, StorageEncrypted=false, StorageEncryptionKey="", StorageType=gp2`.

- Application :`DeploymentConfigName=CodeDeployDefault.OneAtATime`.
- Seau S3 :`AccessControl=Private`.

PARAMÈTRES SUPPLÉMENTAIRES :

`RequestedStartTime`et `RequestedEndTime` si vous souhaitez planifier votre RFC : vous pouvez utiliser Time.is pour déterminer l'heure UTC correcte. Les exemples fournis doivent être adaptés de manière appropriée. Une RFC ne peut pas continuer si l'heure de début est dépassée. Vous pouvez également omettre ces valeurs pour créer une RFC ASAP qui s'exécute dès que les approbations sont passées.

> **Note**
>
> Il existe de nombreux paramètres que vous pouvez choisir de définir différemment de ceux illustrés. Les valeurs des paramètres présentés dans l'exemple ont été testées mais ne vous conviennent peut-être pas.

Création de l'infrastructure

La collecte des données suivantes avant de commencer accélérera le déploiement.

LES DONNÉES REQUISES ONT UNE PILE :

- AutoScalingGroup:
  - `UserData`: Cette valeur est fournie dans ce didacticiel. Il inclut des commandes permettant de configurer la ressource pour l' CodeDeploy agent CodeDeploy et de le démarrer.
  - `AMI-ID`: Cette valeur détermine le type d' EC2 instances que votre groupe Auto Scaling (ASG) va créer. Assurez-vous de sélectionner une AMI dans votre compte qui commence par « customer- » et qui utilise le système d'exploitation que vous souhaitez. Trouvez l'AMI à l' IDs aide de la référence For the AMS SKMS API, consultez l'onglet Rapports de l'opération AWS Artifact Console (CLI : list-amis) ou sur la page de détails de la console AMS ->. VPCs VPCs Cette procédure pas à pas est destinée aux ASGs personnes configurées pour utiliser une AMI Linux.
- Base de données :
  - Ces paramètres, `DBEngineEngineVersion`, et `LicenseModel` doivent être définis en fonction de votre situation, bien que les valeurs indiquées dans l'exemple aient été testées.

  - Ces paramètres,`RDSSubnetIds`, `DBNameMasterUsername`, et `MasterUserPassword` sont obligatoires lors du déploiement du bundle d'applications. Pour RDSSubnet les identifiants, utilisez deux sous-réseaux privés.
- LoadBalancer:
  - Ces paramètres, `DBEngineEngineVersion`, et `LicenseModel` doivent être définis en fonction de votre situation, bien que les valeurs indiquées dans l'exemple aient été testées.
  - `ELBSubnetIds`: utilisez deux sous-réseaux publics.
- Application : la `ApplicationName` valeur définit le nom de l' CodeDeploy application et le nom du groupe de CodeDeploy déploiement. Vous l'utilisez pour déployer votre application. Il doit être unique dans le compte. Pour vérifier les CodeDeploy noms de votre compte, consultez la CodeDeploy console. L'exemple utilise « WordPress » mais, si vous voulez utiliser cette valeur, assurez-vous qu'elle n'est pas déjà utilisée.

Cette procédure utilise le CT à deux niveaux (avancé) à haute disponibilité (ct-06mjngx5flwto) et le CT Create S3 storage (ct-1a68ck03fn98r). À partir de votre compte authentifié, suivez ces étapes sur la ligne de commande.

1. Lancez la pile d'infrastructure.

   a. Exportez le schéma JSON des paramètres d'exécution pour la pile HA à deux niveaux CT dans un fichier de votre dossier actuel nommé CreateStackParams .json.

   ```
   aws amscm get-change-type-version --change-type-id "ct-06mjngx5flwto"
    --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
    CreateStackParams.json
   ```

   b. Modifiez le schéma. Remplacez-le *`variables`* comme il convient. Par exemple, utilisez le système d'exploitation que vous souhaitez pour les EC2 instances que l'ASG créera. Enregistrez-le `ApplicationName` tel que vous l'utiliserez ultérieurement pour déployer l'application. Notez que vous pouvez ajouter jusqu'à 50 balises.

   ```
   {
   "Description":      "HA two tier stack for WordPress",
   "Name":             "WordPressStack",
   "TimeoutInMinutes":  360,
   "Tags": [
           {
               "Key": "ApplicationName",
   ```

```
            "Value": "WordPress"
        }
    ],
"AutoScalingGroup": {
            "AmiId":    "AMI-ID",
            "UserData": "#!/bin/bash \n
            REGION=$(curl 169.254.169.254/latest/meta-data/placement/
availability-zone/ | sed 's/[a-z]$//') \n
            yum -y install ruby httpd \n
            chkconfig httpd on \n
            service httpd start \n
            touch /var/www/html/status \n
            cd /tmp \n
            curl -O https://aws-codedeploy-$REGION.s3.amazonaws.com/latest/
install \n
            chmod +x ./install \n
            ./install auto \n
            chkconfig codedeploy-agent on \n
            service codedeploy-agent start"
    },
    "LoadBalancer": {
        "Public":               true,
        "HealthCheckTarget":    "HTTP:80/status"
    },
    "Database":     {
        "DBEngine":             "MySQL",
        "DBName":               "wordpress",
        "EngineVersion":        "8.0.16 ",
        "LicenseModel":         "general-public-license",
        "MasterUsername":       "admin",
        "MasterUserPassword":   "p4ssw0rd"
    },
    "Application":  {
    "ApplicationName":  "WordPress"
        }
}
```

c. Exportez le modèle CreateRfc JSON dans un fichier de votre dossier actuel nommé CreateStackRfc .json :

```
aws amscm create-rfc --generate-cli-skeleton > CreateStackRfc.json
```

d. Modifiez le modèle RFC comme suit et enregistrez-le, vous pouvez supprimer et remplacer le contenu. Notez que `RequestedStartTime` et `RequestedEndTime` sont désormais facultatifs ; leur exclusion crée une RFC ASAP qui s'exécute dès qu'elle est approuvée (ce qui se produit généralement automatiquement). Pour soumettre une RFC planifiée, ajoutez ces valeurs.

```
{
"ChangeTypeVersion":    "3.0",
"ChangeTypeId":         "ct-06mjngx5flwto",
"Title":                "HA-Stack-For-WP-RFC"
}
```

e. Créez la RFC en spécifiant le fichier CreateStackRfc .json et le fichier de paramètres d'exécution CreateStackParams .json :

```
aws amscm create-rfc --cli-input-json file://CreateStackRfc.json --execution-
parameters file://CreateStackParams.json
```

Vous recevez l'identifiant RFC dans la réponse. Enregistrez l'identifiant pour les étapes suivantes.

f. Soumettez le RFC :

```
aws amscm submit-rfc --rfc-id  RFC_ID
```

Si la RFC réussit, vous ne recevrez aucune sortie.

g. Pour vérifier l'état de la RFC, exécutez

```
aws amscm get-rfc --rfc-id RFC_ID
```

Notez l'identifiant RFC.

2. Lancer un compartiment S3

La collecte des données suivantes avant de commencer accélérera le déploiement.

BUCKET S3 DE DONNÉES REQUIS :

- `VPC-ID`: Cette valeur détermine l'emplacement de votre compartiment S3. Utilisez le même ID VPC que celui que vous avez utilisé précédemment.
- `BucketName`: Cette valeur définit le nom du compartiment S3, vous l'utilisez pour télécharger votre bundle d'applications. Il doit être unique dans la région du compte et ne peut pas contenir de majuscules. Il n' BucketName est pas obligatoire d'inclure votre identifiant de compte, mais cela permet d'identifier plus facilement le compartiment ultérieurement. Pour voir quels noms de compartiment S3 existent dans le compte, accédez à la console Amazon S3 de votre compte.

a. Exportez le schéma JSON des paramètres d'exécution pour le stockage S3 create CT dans un fichier JSON nommé CreateS3 StoreParams .json.

```
aws amscm get-change-type-version --change-type-id "ct-1a68ck03fn98r"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 CreateS3StoreParams.json
```

b. Modifiez le schéma comme suit, vous pouvez supprimer et remplacer le contenu. Remplacez *`VPC_ID`* de manière appropriée. Les valeurs de l'exemple ont été testées, mais elles ne vous conviennent peut-être pas.

> **Tip**
>
> Ils `BucketName` doivent être uniques dans la région du compte et ne peuvent pas inclure de majuscules. Il n' BucketName est pas obligatoire d'inclure votre identifiant de compte, mais cela permet d'identifier plus facilement le compartiment ultérieurement. Pour voir quels noms de compartiment S3 existent dans le compte, accédez à la console Amazon S3 de votre compte.

```
{
"Description":      "S3BucketForWordPressBundle",
"VpcId":            "VPC_ID",
"StackTemplateId":  "stm-s2b72beb000000000",
"Name":             "S3BucketForWP",
"TimeoutInMinutes":  60,
"Parameters":   {
    "AccessControl":    "Private",
```

```
    "BucketName":       "ACCOUNT_ID-BUCKET_NAME"
    }
}
```

c. Exportez le modèle JSON CreateRfc pour dans un fichier, dans votre dossier actuel, nommé CreateS3 StoreRfc .json :

```
aws amscm create-rfc --generate-cli-skeleton > CreateS3StoreRfc.json
```

d. Modifiez et enregistrez le fichier CreateS3 StoreRfc .json, vous pouvez supprimer et remplacer le contenu. Notez que `RequestedStartTime` et `RequestedEndTime` sont désormais facultatifs ; leur exclusion crée une RFC ASAP qui s'exécute dès qu'elle est approuvée (ce qui se produit généralement automatiquement). Pour soumettre une RFC planifiée, ajoutez ces valeurs.

```
{
"ChangeTypeVersion":    "1.0",
"ChangeTypeId":         "ct-1a68ck03fn98r",
"Title":                "S3-Stack-For-WP-RFC"
}
```

e. Créez la RFC en spécifiant le fichier CreateS3 StoreRfc .json et le fichier de paramètres d'exécution StoreParams CreateS3 .json :

```
aws amscm create-rfc --cli-input-json file://CreateS3StoreRfc.json  --
execution-parameters file://CreateS3StoreParams.json
```

Vous recevez RfcId le nouveau RFC dans la réponse. Enregistrez l'identifiant pour les étapes suivantes.

f. Soumettez le RFC :

```
aws amscm submit-rfc --rfc-id RFC_ID
```

Si la RFC réussit, vous ne recevrez aucune sortie.

g. Pour vérifier l'état de la RFC, exécutez

```
aws amscm get-rfc --rfc-id RFC_ID
```

Création, téléchargement et déploiement de l'application

Créez d'abord un bundle d' WordPress applications, puis utilisez-le CodeDeploy CTs pour créer et déployer l'application.

1. Téléchargez WordPress, extrayez les fichiers et créez un. répertoire /scripts.

   Commande Linux :

   ```
   wget https://github.com/WordPress/WordPress/archive/master.zip
   ```

   Windows : collez `https://github.com/WordPress/WordPress/archive/master.zip` le fichier dans une fenêtre de navigateur et téléchargez le fichier zip.

   Créez un répertoire temporaire dans lequel assembler le package.

   Linux :

   ```
   mkdir /tmp/WordPress
   ```

   Windows : Créez un répertoire WordPress « », vous utiliserez le chemin du répertoire ultérieurement.

2. Extrayez la WordPress source dans le répertoire WordPress « » et créez un fichier. répertoire / scripts.

   Linux :

   ```
   unzip master.zip -d /tmp/WordPress_Temp
   cp -paf /tmp/WordPress_Temp/WordPress-master/* /tmp/WordPress
   rm -rf /tmp/WordPress_Temp
   rm -f master
   cd /tmp/WordPress
   mkdir scripts
   ```

   Windows : Accédez au répertoire « WordPress » que vous avez créé et créez-y un répertoire « scripts ».

   Si vous êtes dans un environnement Windows, veillez à définir le type de rupture des fichiers de script sur Unix (LF). Dans Notepad ++, il s'agit d'une option en bas à droite de la fenêtre.

3. Créez le fichier CodeDeploy appspec.yml dans le WordPress répertoire (si vous copiez l'exemple, vérifiez l'indentation, chaque espace compte). IMPORTANT : Assurez-vous que le chemin « source » est correct pour copier les WordPress fichiers (dans ce cas, dans votre WordPress répertoire) vers la destination prévue (/var/www/html/WordPress). Dans l'exemple, le fichier appspec.yml se trouve dans le répertoire contenant les WordPress fichiers, donc seul «/» est nécessaire. De plus, même si vous avez utilisé une AMI RHEL pour votre groupe Auto Scaling, laissez la ligne « os : linux » telle quelle. Exemple de fichier appspec.yml :

```
version: 0.0
os: linux
files:
  - source: /
    destination: /var/www/html/WordPress
hooks:
  BeforeInstall:
    - location: scripts/install_dependencies.sh
      timeout: 300
      runas: root
  AfterInstall:
    - location: scripts/config_wordpress.sh
      timeout: 300
      runas: root
  ApplicationStart:
    - location: scripts/start_server.sh
      timeout: 300
      runas: root
  ApplicationStop:
    - location: scripts/stop_server.sh
      timeout: 300
      runas: root
```

4. Créez des scripts de fichiers bash dans le WordPress . répertoire /scripts.

   Commencez `config_wordpress.sh` par créer avec le contenu suivant (si vous préférez, vous pouvez modifier directement le fichier wp-config.php).

   > **Note**
   >
   > Remplacez *DBName* par la valeur indiquée dans la RFC HA Stack (par exemple,`wordpress`).

Remplacez *DB_MasterUsername* par la `MasterUsername` valeur indiquée dans la RFC HA Stack (par exemple,`admin`).
Remplacez *DB_MasterUserPassword* par la `MasterUserPassword` valeur indiquée dans la RFC HA Stack (par exemple,`p4ssw0rd`).
*DB_ENDPOINT*Remplacez-le par le nom DNS du point de terminaison dans les sorties d'exécution de la HA Stack RFC (par exemple,`srt1cz23n45sfg.clgvd67uvydk.us-east-1.rds.amazonaws.com`). Vous pouvez le trouver dans l'GetRfcopération (CLI : get-rfc --rfc-id RFC_ID) ou dans la page de détails de la RFC de la console AMS pour la RFC HA Stack que vous avez précédemment soumise.

```
#!/bin/bash
chmod -R 755 /var/www/html/WordPress
cp /var/www/html/WordPress/wp-config-sample.php /var/www/html/WordPress/wp-
config.php
cd /var/www/html/WordPress
sed -i "s/database_name_here/DBName/g" wp-config.php
sed -i "s/username_here/DB_MasterUsername/g" wp-config.php
sed -i "s/password_here/DB_MasterUserPassword/g" wp-config.php
sed -i "s/localhost/DB_ENDPOINT/g" wp-config.php
```

5. Dans le même répertoire, créez `install_dependencies.sh` avec le contenu suivant :

```
#!/bin/bash
yum install -y php
yum install -y php-mysql
yum install -y mysql
service httpd restart
```

> **Note**
>
> Le protocole HTTPS est installé dans les données utilisateur au lancement afin de permettre aux contrôles de santé de fonctionner dès le départ.

6. Dans le même répertoire, créez `start_server.sh` avec le contenu suivant :

   - Pour les instances Amazon Linux, utilisez ceci :

```
#!/bin/bash
```

```
service httpd start
```

- Pour les instances RHEL, utilisez ceci (les commandes supplémentaires sont des politiques qui autorisent SELINUX à accepter) : WordPress

```
#!/bin/bash
setsebool -P  httpd_can_network_connect_db 1
setsebool -P  httpd_can_network_connect 1
chcon -t httpd_sys_rw_content_t /var/www/html/WordPress/wp-content -R
restorecon -Rv /var/www/html
service httpd start
```

7. Dans le même répertoire, créez `stop_server.sh` avec le contenu suivant :

```
#!/bin/bash
service httpd stop
```

8. Créez le bundle zip.

   Linux :

```
$ cd /tmp/WordPress
$ zip -r wordpress.zip .
```

   Windows : Accédez à votre répertoire WordPress « », sélectionnez tous les fichiers et créez un fichier zip. N'oubliez pas de le nommer wordpress.zip.

1. Téléchargez le bundle d'applications dans le compartiment S3.

   Le bundle doit être en place pour continuer à déployer la pile.

   Vous avez automatiquement accès à toutes les instances de compartiment S3 que vous créez. Vous pouvez y accéder via vos bastions ou via la console S3, et télécharger le WordPress bundle avec le fichier zip drag-and-drop ou en le recherchant et en le sélectionnant.

   Vous pouvez également utiliser la commande suivante dans une fenêtre shell ; assurez-vous que le chemin d'accès au fichier zip est correct :

```
aws s3 cp wordpress.zip s3://BUCKET_NAME/
```

2. Déployez le bundle WordPress d'applications.

La collecte des données suivantes avant de commencer accélérera le déploiement.

DONNÉES REQUISES :

- `VPC-ID`: Cette valeur détermine l'emplacement de votre compartiment S3. Utilisez le même ID VPC que celui que vous avez utilisé précédemment.
- `CodeDeployApplicationNameet CodeDeployApplicationName` : La `ApplicationName` valeur que vous avez utilisée dans la RFC HA 2-Tier Stack définit le CodeDeployApplicationName et le. CodeDeployDeploymentGroupName L'exemple utilise « WordPress », mais vous avez peut-être utilisé une valeur différente.
- `S3Location`: Pour`S3Bucket`, utilisez celui `BucketName` que vous avez créé précédemment. Les `S3BundleType` et `S3Key` proviennent du bundle que vous avez ajouté à votre boutique S3.

a. Exportez le schéma JSON des paramètres d'exécution pour le déploiement de CodeDeploy l'application CT dans un fichier JSON nommé Deploy CDApp Params.json.

```
aws amscm get-change-type-version --change-type-id "ct-2edc3sd1sqmrb"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 DeployCDAppParams.json
```

b. Modifiez le schéma comme suit et enregistrez-le sous le nom, vous pouvez supprimer et remplacer le contenu.

```
{
"Description":                          "DeployWPCDApp",
"VpcId":                                "VPC_ID",
"Name":                                 "WordPressCDAppDeploy",
"TimeoutInMinutes":                     60,
"Parameters":   {
    "CodeDeployApplicationName":                "WordPress",
    "CodeDeployDeploymentGroupName":            "WordPress",
    "CodeDeployIgnoreApplicationStopFailures":   false,
    "CodeDeployRevision": {
      "RevisionType": "S3",
      "S3Location": {
        "S3Bucket":     "BUCKET_NAME",
        "S3BundleType": "zip",
        "S3Key":        "wordpress.zip" }
```

```
        }
    }
}
```

c. Exportez le modèle JSON CreateRfc pour dans un fichier, dans votre dossier actuel, nommé Deploy CDApp RFC.json :

```
aws amscm create-rfc --generate-cli-skeleton > DeployCDAppRfc.json
```

d. Modifiez et enregistrez le fichier Deploy CDApp RFC.json, vous pouvez supprimer et remplacer le contenu. Notez que `RequestedStartTime` et `RequestedEndTime` sont désormais facultatifs ; leur exclusion crée une RFC ASAP qui s'exécute dès qu'elle est approuvée (ce qui se produit généralement automatiquement). Pour soumettre une RFC planifiée, ajoutez ces valeurs.

```
{
"ChangeTypeVersion":    "1.0",
"ChangeTypeId":         "ct-2edc3sd1sqmrb",
"Title":                "CD-Deploy-For-WP-RFC"
}
```

e. Créez le RFC en spécifiant le fichier Deploy CDApp Rfc et le fichier de paramètres d'exécution de Deploy CDApp Params :

```
aws amscm create-rfc --cli-input-json file://DeployCDAppRfc.json  --execution-
parameters file://DeployCDAppParams.json
```

Vous recevez RfcId le nouveau RFC dans la réponse. Enregistrez l'identifiant pour les étapes suivantes.

f. Soumettez le RFC :

```
aws amscm submit-rfc --rfc-id RFC_ID
```

Si la RFC réussit, vous ne recevrez aucune sortie.

g. Pour vérifier l'état de la RFC, exécutez

```
aws amscm get-rfc --rfc-id RFC_ID
```

Valider le déploiement de l'application

Accédez au point de terminaison (ELB CName) de l'équilibreur de charge créé précédemment, avec le WordPress chemin déployé :/. WordPress Exemples :

```
http://stack-ID-FOR-ELB.us-east-1.elb.amazonaws.com/WordPress
```

Démanteler le déploiement de l'application

Une fois que vous aurez terminé le didacticiel, vous souhaiterez réduire le déploiement afin de ne pas avoir à vous facturer les ressources.

Voici une opération générique de suppression de pile. Vous devez le soumettre deux fois, une fois pour la pile HA à 2 niveaux et une fois pour la pile de compartiments S3. Enfin, soumettez une demande de service demandant que tous les instantanés du compartiment S3 (incluez l'ID de pile du compartiment S3 dans la demande de service) soient supprimés. Ils sont automatiquement supprimés au bout de 10 jours, mais leur suppression anticipée permet d'économiser un peu d'argent.

Cette procédure pas à pas fournit un exemple d'utilisation de la console AMS pour supprimer une pile S3 ; cette procédure s'applique à la suppression de toute pile à l'aide de la console AMS.

> **Note**
>
> Si vous supprimez un compartiment S3, il doit d'abord être vidé de ses objets.

DONNÉES REQUISES :

- `StackId`: La pile à utiliser. Vous pouvez le trouver en consultant la page AMS Console Stacks, disponible via un lien dans le menu de navigation de gauche. À l'aide de l'API/CLI AMS SKMS, exécutez la référence For the AMS SKMS API, voir l'onglet Rapports dans l'opération AWS Artifact Console (dans l'interface de ligne de commande). `list-stack-summaries`
- L'identifiant du type de modification pour cette procédure pas à pas est « 1.0 ». Pour connaître la dernière version, exécutez cette commande : `ct-0q0bic0ywqk6c`

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=ct-0q0bic0ywqk6c
```

CRÉATION EN LIGNE :

- Émettez la commande create RFC avec les paramètres d'exécution fournis en ligne (évitez les guillemets lorsque vous fournissez des paramètres d'exécution en ligne). E

```
aws amscm create-rfc --change-type-id "ct-0q0bic0ywqk6c" --change-type-version "1.0"
 --title "Delete My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

- Soumettez le RFC à l'aide de l'ID RFC renvoyé lors de l'opération de création du RFC. Jusqu'à ce qu'elle soit soumise, la RFC reste en l'`Editing`état et ne fait l'objet d'aucune action.

```
aws amscm submit-rfc --rfc-id RFC_ID
```

- Surveillez l'état de la RFC et visualisez le résultat de l'exécution :

```
aws amscm get-rfc --rfc-id RFC_ID
```

CRÉATION D'UN MODÈLE :

1. Exportez le modèle RFC dans un fichier de votre dossier actuel ; l'exemple le nomme DeleteStackRfc .json :

   ```
   aws amscm create-rfc --generate-cli-skeleton > DeleteStackRfc.json
   ```

2. Modifiez et enregistrez le fichier DeleteStackRfc .json. Comme la suppression d'une pile ne comporte qu'un seul paramètre d'exécution, les paramètres d'exécution peuvent se trouver dans le fichier DeleteStackRfc .json lui-même (il n'est pas nécessaire de créer un fichier JSON distinct avec les paramètres d'exécution).

   Les guillemets internes de l'extension ExecutionParameters JSON doivent être masqués par une barre oblique inverse (\). Exemple sans heure de début et de fin :

   ```
   {
   "ChangeTypeVersion":    "1.0",
   "ChangeTypeId":         "ct-0q0bic0ywqk6c",
   "Title":                "Delete-My-Stack-RFC"
   "ExecutionParameters":  "{
           \"StackId\":\"STACK_ID\"}"
   }
   ```

3. Créez le RFC :

```
aws amscm create-rfc --cli-input-json file://DeleteStackRfc.json
```

Vous recevez le code RfcId de la nouvelle RFC dans la réponse. Exemples :

```
{
"RfcId": "daaa1867-ffc5-1473-192a-842f6b326102"
}
```

Enregistrez l'identifiant pour les étapes suivantes.

4. Soumettez le RFC :

```
aws amscm submit-rfc --rfc-id RFC_ID
```

Si le RFC réussit, vous ne recevez aucune confirmation sur la ligne de commande.

5. Pour surveiller l'état de la demande et consulter le résultat de l'exécution, procédez comme suit :

```
aws amscm get-rfc --rfc-id RFC_ID --query "Rfc.
{Status:Status.Name,Exec:ExecutionOutput}" --output table
```

Tutoriel sur console : pile à deux niveaux de haute disponibilité (Linux/RHEL)

Cette section décrit comment déployer un WordPress site haute disponibilité (HA) dans un environnement AMS à l'aide de la console AMS.

> **Note**
>
> Cette procédure de déploiement a été testée dans les environnements AMZN Linux et RHEL.

Résumé des tâches et des exigences RFCs :

1. Création d'une infrastructure (pile HA à deux niveaux)
2. Création d'un compartiment S3 pour les CodeDeploy applications
3. Créez le bundle WordPress d'applications et chargez-le dans le compartiment S3
4. Déployez l'application avec CodeDeploy

5. Accédez au WordPress site et connectez-vous pour valider le déploiement
6. Démanteler le déploiement

Les descriptions de toutes les options de tomodensitométrie ChangeTypeId, y compris, se trouvent dans AMS Change Type Reference.

Avant de commencer

Le Deployment | Advanced Stack Components | High Availability Two Tier Stack | Create CT crée un groupe Auto Scaling, un équilibreur de charge, une base de données, ainsi qu'un nom d' CodeDeploy application et un groupe de déploiement (avec le même nom que celui que vous avez donné à l'application). Pour plus d'informations sur la CodeDeploy section Qu'est-ce que c'est CodeDeploy ?

Cette procédure pas à pas utilise une RFC à deux niveaux de haute disponibilité qui inclut `UserData` et décrit également comment créer un WordPress bundle pouvant CodeDeploy être déployé.

L'exemple `UserData` illustré permet d'obtenir les métadonnées d'instance telles que l'ID d'instance, la région, etc., à partir d'une instance en cours d'exécution en interrogeant le service de métadonnées d' EC2 instance disponible sur http://169.254.169.254/latest/meta-data/. Cette ligne du script de données utilisateur :`REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/ | sed 's/[a-z]$//')`, extrait le nom de la zone de disponibilité du service de métadonnées dans la variable $REGION pour nos régions prises en charge, et l'utilise pour compléter l'URL du compartiment S3 dans lequel l' CodeDeploy agent est téléchargé. L'adresse IP 169.254.169.254 est routable uniquement au sein du VPC (tout le monde peut interroger le service). VPCs Pour plus d'informations sur le service, consultez la section Métadonnées d'instance et données utilisateur. Notez également que les scripts saisis en tant que UserData sont exécutés en tant qu'utilisateur « root » et n'ont pas besoin d'utiliser la commande « sudo ».

Cette procédure pas à pas laisse les paramètres suivants à la valeur par défaut (illustrée) :

- Groupe Auto Scaling :`Cooldown=300, DesiredCapacity=2, EBSOptimized=false, HealthCheckGracePeriod=600, IAMInstanceProfile=customer-mc-ec2-instance-profile, InstanceDetailedMonitoring=true, InstanceRootVolumeIops=0, InstanceRootVolumeType=standard, InstanceType=m3.medium, MaxInstances=2, MinInstances=2, ScaleDownPolicyCooldown=300, ScaleDownPolicyEvaluationPeriods=4, ScaleDownPolicyPeriod=60, ScaleDownPolicyScalingAdjustment=-1, ScaleDownPolicyStatistic=Average, ScaleDownPolicyThreshold=35, ScaleMetricName=CPUUtilization,`

`ScaleUpPolicyCooldown=60, ScaleUpPolicyEvaluationPeriods=2, ScaleUpPolicyPeriod=60, ScaleUpPolicyScalingAdjustment=2, ScaleUpPolicyStatistic=Average, ScaleUpPolicyThreshold=75`.

- Load Balancer :. `HealthCheckInterval=30, HealthCheckTimeout=5`
- Base de données :`BackupRetentionPeriod=7, Backups=true, InstanceType=db.m3.medium, IOPS=0, MultiAZ=true, PreferredBackupWindow=22:00-23:00, PreferredMaintenanceWindow=wed:03:32-wed:04:02, StorageEncrypted=false, StorageEncryptionKey="", StorageType=gp2`.
- Candidature :`DeploymentConfigName=CodeDeployDefault.OneAtATime`.

Paramètres variables :

La console fournit une option ASAP pour l'heure de début et cette procédure pas à pas recommande de l'utiliser. ASAP entraîne l'exécution de la RFC dès que les approbations sont passées.

> **Note**
>
> Il existe de nombreux paramètres que vous pouvez choisir de définir différemment de ceux illustrés. Les valeurs des paramètres présentés dans l'exemple ont été testées, mais elles ne vous conviennent peut-être pas. Seules les valeurs obligatoires sont indiquées dans les exemples. Les valeurs de *`replaceable`* police doivent être modifiées car elles sont propres à votre compte.

Création de l'infrastructure

Cette procédure utilise le Stack CT à deux niveaux à haute disponibilité suivi du CT de stockage Create S3.

La collecte des données suivantes avant de commencer accélérera le déploiement.

LES DONNÉES REQUISES ONT UNE PILE :

- AutoScalingGroup:
  - UserData: Cette valeur est fournie dans ce didacticiel. Il inclut des commandes permettant de configurer la ressource pour l' CodeDeploy agent CodeDeploy et de le démarrer.

  - AMI-ID : cette valeur détermine le système d'exploitation des EC2 instances que votre groupe Auto Scaling (ASG) créera. Sélectionnez une AMI dans votre compte qui commence par « customer- » et qui utilise le système d'exploitation que vous souhaitez. Trouvez l'AMI IDs dans la console AMS VPCs -> page de VPCs détails. Cette procédure pas à pas est destinée aux ASGs personnes configurées pour utiliser une AMI Amazon Linux ou RHEL.
- Base de données :
  - Ces paramètres, DBEngineEngineVersion, et LicenseModeldoivent être définis en fonction de votre situation, bien que les valeurs indiquées dans l'exemple aient été testées. Le didacticiel utilise les valeurs suivantes, respectivement :*MySQL*,*8.0.16*,*general-public-license*.
  - Ces paramètres, DBNameMasterUserPassword, et MasterUsernamesont obligatoires lors du déploiement du bundle d'applications. Le didacticiel utilise les valeurs suivantes, respectivement :*wordpressDB*,*p4ssw0rd*,*admin*. Notez qu'il ne DBName peut contenir que des caractères alphanumériques.
  - Lorsque vous entrez le code MasterUsernamepour la base de données RDS, il apparaît en texte clair. Connectez-vous à la base de données dès que possible et modifiez le mot de passe pour garantir votre sécurité.
  - Pour RDSSubnetles identifiants, utilisez deux sous-réseaux privés. Entrez-les un par un en appuyant sur « Entrée » après chaque. Trouvez un sous-réseau IDs avec la référence For the AMS SKMS API, consultez l'onglet Rapports dans l'opération AWS Artifact Console (CLI list-subnet-summaries :) ou sur la page de détails de la console AMS VPCs -> VPC.
- LoadBalancer:
  - Définissez ce paramètre Public sur true car le didacticiel utilise des sous-réseaux ELB publics.
  - ELBSubnetIdentifiants : utilisez deux sous-réseaux publics. Entrez-les un par un en appuyant sur « Entrée » après chaque. Trouvez un sous-réseau IDs avec la référence For the AMS SKMS API, consultez l'onglet Rapports dans l'opération AWS Artifact Console (CLI list-subnet-summaries :) ou sur la page de détails de la console AMS VPCs -> VPC.
- Application : la ApplicationNamevaleur définit le nom de l' CodeDeploy application et le nom du groupe de CodeDeploy déploiement. Vous l'utilisez pour déployer votre application. Il doit être unique dans le compte. Pour vérifier les CodeDeploy noms de votre compte, consultez la CodeDeploy console. L'exemple utilise *WordPress* mais, si vous voulez utiliser cette valeur, assurez-vous qu'elle n'est pas déjà utilisée.

1. Lancez la pile de haute disponibilité.

a. Sur la page Create RFC, sélectionnez la catégorie Deployment, la sous-catégorie Standard Stacks, l'article High Availability two-tier stack et operation Create dans la liste.

b. IMPORTANT : Choisissez Avancé et définissez les valeurs comme indiqué.

   Il vous suffit de saisir des valeurs pour les options marquées d'un astérisque (*). Les valeurs testées sont indiquées dans l'exemple ; vous pouvez laisser les options vides non obligatoires vides vides.

c. Pour la section Description de la RFC :

```
Subject: WP-HA-2-Tier-RFC
```

d. Dans la section Informations sur les ressources, définissez les paramètres de la base de données AutoScalingGroupLoadBalancer, de l'application et des balises.

   De plus, le but de la touche de balise AppName « » est de vous permettre de rechercher facilement les instances ASG dans la EC2 console ; vous pouvez appeler cette clé de balise « Nom » ou tout autre nom de clé de votre choix. Notez que vous pouvez ajouter jusqu'à 50 balises.

```
UserData:
    #!/bin/bash
    REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/
 | sed 's/[a-z]$//')
    yum -y install ruby httpd
    chkconfig httpd on
    service httpd start
    touch /var/www/html/status
    cd /tmp
    curl -O https://aws-codedeploy-$REGION.s3.amazonaws.com/latest/install
    chmod +x ./install
    ./install auto
    chkconfig codedeploy-agent on
    service codedeploy-agent start
AmiId:              AMI-ID
Description:        WP-HA-2-Tier-Stack

Database:
    LicenseModel:    general-public-license (USE RADIO BUTTON)
    EngineVersion:   8.0.16
    DBEngine:        MySQL
```

```
    RDSSubnetIds:     PRIVATE_AZ1 PRIVATE_AZ2 (ENTER ONE AT A TIME PRESSING
 "ENTER" AFTER EACH)
    MasterUserPassword:  p4ssw0rd
    MasterUsername:      admin
    DBName:              wordpressDB

LoadBalancer:
    Public:              true (USE RADIO BUTTON)
    ELBSubnetIds:        PUBLIC_AZ1 PUBLIC_AZ2

Application:
    ApplicationName:     WordPress

Tags:
    Name:                WP-Rhel-Stack
```

e. Cliquez sur Soumettre lorsque vous avez terminé.

2. Connectez-vous à la base de données que vous avez créée et modifiez le mot de passe.
3. Lancez une pile de compartiments S3.

   La collecte des données suivantes avant de commencer accélérera le déploiement.

   BUCKET S3 DE DONNÉES REQUIS :

   - VPC-ID : cette valeur détermine l'emplacement de votre compartiment S3. Trouvez un VPC à l' IDs aide de la référence pour l'API For the AMS SKMS, consultez l'onglet Rapports dans l'opération AWS Artifact Console (CLI : list-vpc-summaries) ou sur la page de la console AMS. VPCs
   - BucketName: Cette valeur définit le nom du compartiment S3, vous l'utilisez pour télécharger votre bundle d'applications. Il doit être unique dans la région du compte et ne peut pas contenir de majuscules. Il n' BucketName est pas obligatoire d'inclure votre identifiant de compte, mais cela permet d'identifier plus facilement le compartiment ultérieurement. Pour voir quels noms de compartiment S3 existent dans le compte, accédez à la console Amazon S3 de votre compte.

   a. Sur la page Create RFC, sélectionnez la catégorie Deployment, la sous-catégorie Advanced Stack Components, l'élément S3 storage et l'opération Create dans la liste de sélection RFC CT.

   b. Conservez l'option Basic par défaut et définissez les valeurs comme indiqué.

```
Subject:              S3-Bucket-WP-HA-RFC
Description:          S3BucketForWordPressBundles
BucketName:           ACCOUNT_ID-BUCKET_NAME
AccessControl:        Private
VpcId:                VPC_ID
Name:                 S3-Bucket-WP-HA-Stack
TimeoutInMinutes:     60
```

c. Cliquez sur Soumettre lorsque vous avez terminé. Le bucket déployé avec ce type de modification permet un read/write accès complet à l'ensemble du compte.

Création, téléchargement et déploiement de l'application

Créez d'abord un bundle d' WordPress applications, puis utilisez-le CodeDeploy CTs pour créer et déployer l'application.

1. Téléchargez WordPress, extrayez les fichiers et créez un. répertoire /scripts.

   Commande Linux :

   ```
   wget https://github.com/WordPress/WordPress/archive/master.zip
   ```

   Windows : collez `https://github.com/WordPress/WordPress/archive/master.zip` le fichier dans une fenêtre de navigateur et téléchargez le fichier zip.

   Créez un répertoire temporaire dans lequel assembler le package.

   Linux :

   ```
   mkdir /tmp/WordPress
   ```

   Windows : Créez un répertoire WordPress « », vous utiliserez le chemin du répertoire ultérieurement.

2. Extrayez la WordPress source dans le répertoire WordPress « » et créez un fichier. répertoire / scripts.

   Linux :

   ```
   unzip master.zip -d /tmp/WordPress_Temp
   ```

```
cp -paf /tmp/WordPress_Temp/WordPress-master/* /tmp/WordPress
rm -rf /tmp/WordPress_Temp
rm -f master
cd /tmp/WordPress
mkdir scripts
```

Windows : Accédez au répertoire « WordPress » que vous avez créé et créez-y un répertoire « scripts ».

Si vous êtes dans un environnement Windows, veillez à définir le type de rupture des fichiers de script sur Unix (LF). Dans Notepad ++, il s'agit d'une option en bas à droite de la fenêtre.

3. Créez le fichier CodeDeploy appspec.yml dans le WordPress répertoire (si vous copiez l'exemple, vérifiez l'indentation, chaque espace compte). IMPORTANT : Assurez-vous que le chemin « source » est correct pour copier les WordPress fichiers (dans ce cas, dans votre WordPress répertoire) vers la destination prévue (/var/www/html/WordPress). Dans l'exemple, le fichier appspec.yml se trouve dans le répertoire contenant les WordPress fichiers, donc seul «/» est nécessaire. De plus, même si vous avez utilisé une AMI RHEL pour votre groupe Auto Scaling, laissez la ligne « os : linux » telle quelle. Exemple de fichier appspec.yml :

```
version: 0.0
os: linux
files:
  - source: /
    destination: /var/www/html/WordPress
hooks:
  BeforeInstall:
    - location: scripts/install_dependencies.sh
      timeout: 300
      runas: root
  AfterInstall:
    - location: scripts/config_wordpress.sh
      timeout: 300
      runas: root
  ApplicationStart:
    - location: scripts/start_server.sh
      timeout: 300
      runas: root
  ApplicationStop:
    - location: scripts/stop_server.sh
      timeout: 300
      runas: root
```

4. Créez des scripts de fichiers bash dans le WordPress . répertoire /scripts.

   Commencez `config_wordpress.sh` par créer avec le contenu suivant (si vous préférez, vous pouvez modifier directement le fichier wp-config.php).

   > **Note**
   >
   > Remplacez *DBName* par la valeur indiquée dans la RFC HA Stack (par exemple,`wordpress`).
   > Remplacez *DB_MasterUsername* par la `MasterUsername` valeur indiquée dans la RFC HA Stack (par exemple,`admin`).
   > Remplacez *DB_MasterUserPassword* par la `MasterUserPassword` valeur indiquée dans la RFC HA Stack (par exemple,`p4ssw0rd`).
   > *DB_ENDPOINT*Remplacez-le par le nom DNS du point de terminaison dans les sorties d'exécution de la HA Stack RFC (par exemple,`srt1cz23n45sfg.clgvd67uvydk.us-east-1.rds.amazonaws.com`). Vous pouvez le trouver dans l'GetRfcopération (CLI : get-rfc --rfc-id RFC_ID) ou dans la page de détails de la RFC de la console AMS pour la RFC HA Stack que vous avez précédemment soumise.

```
#!/bin/bash
chmod -R 755 /var/www/html/WordPress
cp /var/www/html/WordPress/wp-config-sample.php /var/www/html/WordPress/wp-
config.php
cd /var/www/html/WordPress
sed -i "s/database_name_here/DBName/g" wp-config.php
sed -i "s/username_here/DB_MasterUsername/g" wp-config.php
sed -i "s/password_here/DB_MasterUserPassword/g" wp-config.php
sed -i "s/localhost/DB_ENDPOINT/g" wp-config.php
```

5. Dans le même répertoire, créez `install_dependencies.sh` avec le contenu suivant :

```
#!/bin/bash
yum install -y php
yum install -y php-mysql
yum install -y mysql
service httpd restart
```

> **Note**
>
> Le protocole HTTPS est installé dans les données utilisateur au lancement afin de permettre aux contrôles de santé de fonctionner dès le départ.

6. Dans le même répertoire, créez `start_server.sh` avec le contenu suivant :

   - Pour les instances Amazon Linux, utilisez ceci :

   ```
   #!/bin/bash
   service httpd start
   ```

   - Pour les instances RHEL, utilisez ceci (les commandes supplémentaires sont des politiques qui autorisent SELINUX à accepter) : WordPress

   ```
   #!/bin/bash
   setsebool -P  httpd_can_network_connect_db 1
   setsebool -P  httpd_can_network_connect 1
   chcon -t httpd_sys_rw_content_t /var/www/html/WordPress/wp-content -R
   restorecon -Rv /var/www/html
   service httpd start
   ```

7. Dans le même répertoire, créez `stop_server.sh` avec le contenu suivant :

   ```
   #!/bin/bash
   service httpd stop
   ```

8. Créez le bundle zip.

   Linux :

   ```
   $ cd /tmp/WordPress
   $ zip -r wordpress.zip .
   ```

   Windows : Accédez à votre répertoire WordPress « », sélectionnez tous les fichiers et créez un fichier zip. N'oubliez pas de le nommer wordpress.zip.

1. Téléchargez le bundle d'applications dans le compartiment S3

Le package doit être en place pour continuer à déployer la pile.

Vous avez automatiquement accès à toutes les instances de compartiment S3 que vous créez. Vous pouvez y accéder via vos Bastions (voir Accès aux instances) ou via la console S3, et télécharger le CodeDeploy package avec drag-and-drop, ou en naviguant vers le fichier et en le sélectionnant.

Vous pouvez également utiliser la commande suivante dans une fenêtre shell ; assurez-vous que le chemin d'accès au fichier zip est correct :

```
aws s3 cp wordpress/wordpress.zip s3://BUCKET_NAME/
```

2. Déployer le bundle WordPress CodeDeploy d'applications

DÉPLOIEMENT DE L'APPLICATION DE DÉPLOIEMENT DU CODE DE DONNÉES REQUIS :

- CodeDeployApplicationName: le nom que vous avez donné à l' CodeDeploy application.
- CodeDeployGroupName: Étant donné que l' CodeDeploy application et le groupe ont tous deux été créés à partir du nom que vous avez donné à l' CodeDeploy application dans la RFC de la pile HA, il s'agit du même nom que le CodeDeployApplicationName.
- S3Bucket : nom que vous avez donné au compartiment S3.
- S3 BundleType et S3Key : ils font partie du bundle d' WordPress applications que vous avez déployé.
- VpcId: Le VPC concerné.

a. Sur la page Créer une RFC, sélectionnez la catégorie Déploiement, la sous-catégorie Applications, l'article CodeDeploy application et l'opération Deploy dans la liste de sélection RFC CT.

b. Conservez l'option Basic par défaut et définissez les valeurs comme indiqué.

> **Note**
>
> Référencez l' CodeDeploy application, CodeDeploy le groupe de déploiement, le compartiment S3 et le bundle créés précédemment.

```
Subject:                                WP-CD-Deploy-RFC
Description:                            DeployWordPress
S3Bucket:                               BUCKET_NAME
S3Key:                                  wordpress.zip
S3BundleType:                           zip
CodeDeployApplicationName:              WordPress
CodeDeployDeploymentGroupName:          WordPress
CodeDeployIgnoreApplicationStopFailures: false
RevisionType:                           S3



VpcId:                                  VPC_ID
Name:                                   WP-CD-Deploy-Op
TimeoutInMinutes:                       60
```

c. Cliquez sur Soumettre lorsque vous avez terminé.

Valider le déploiement de l'application

Accédez au point de terminaison (LoadBalancerCName) de l'équilibreur de charge créé précédemment, avec le chemin WordPress déployé :/. WordPress Par exemple :

```
http://stack-ID-FOR-ELB.us-east-1.elb.amazonaws.com/WordPress
```

Vous devriez voir une page comme celle-ci :

Arrêtez le déploiement de la haute disponibilité

Pour réduire le déploiement, vous soumettez le Delete Stack CT à la pile HA à deux niveaux et au compartiment S3, et vous pouvez demander la suppression des instantanés RDS (ils sont supprimés automatiquement au bout de dix jours, mais ils coûtent peu cher pendant leur séjour). Rassemblez la pile IDs pour la pile HA et le compartiment S3, puis procédez comme suit. Voir Stack | Delete.

Annexe : Questionnaire d'intégration de la SALZ

Rubriques

- Récapitulatif du déploiement
- Considérations relatives à l'architecture environnementale
- Alertes de surveillance des zones d'atterrissage à compte unique
- Fenêtre de maintenance
- Étapes suivantes

Voici certaines des informations auxquelles vous devrez réfléchir avant de créer un compte.

Récapitulatif du déploiement

Description du déploiement. Exemples :

- Ce compte est destiné au déploiement d'une Line-of-Business application (par opposition au déploiement d'une application de produit).
- Le déploiement implique un ARP (proxy inverse authentifié) à mise à l'échelle automatique au sein du sous-réseau public ou DMZ du compte.
- Les serveurs Web et d'applications seront déployés dans le sous-réseau privé du compte.
- Une instance RDS (Amazon Relational Database Service) sera également déployée dans le sous-réseau privé du compte.
- Les serveurs (ARP, Web, application, base de données, équilibreur de charge, etc.) sont séparés en groupes de sécurité distincts.
- Le compte nécessite une conception HA (haute disponibilité) répartie sur les zones de disponibilité (AZs), c'est-à-dire « multi-AZ ».

Considérations relatives à l'architecture environnementale

Tenez compte des critères suivants pour déterminer comment configurer votre environnement et votre architecture.

- Votre centre de données virtuel sera-t-il reconnecté à votre réseau d'entreprise ?
  - Disposez-vous d'un AWS DirectConnect service existant ou avez-vous besoin d'un nouveau DirectConnect service ?
  - Disposez-vous d'une connexion VPN existante ou avez-vous besoin d'un nouveau service VPN ?
- Quelle est la plage de blocs d'adresses internes CIDR disponibles que vous pourriez allouer ? (/16 recommandé, ne doit pas chevaucher les plages du réseau de l'entreprise)

- Votre centre de données virtuel aura-t-il besoin d'un accès à Internet ?
- Quelle (s) région (s) comptez-vous utiliser ? (Sydney/N. Virginia/Dublin)
- Aurez-vous besoin d'un sous-réseau Shared Services pour héberger des applications connectées à tous les autres sous-réseaux ?
- Quelles sont les divisions de votre organisation que vous aimeriez voir hébergées sous forme de sous-réseaux distincts ? Pour chacun d'entre eux :
  - De quelle connectivité aux autres sous-réseaux avez-vous besoin ?
  - Le sous-réseau nécessite-t-il un accès à Internet ?
  - Existe-t-il des restrictions de déploiement d'applications sur ce sous-réseau ?
  - Existe-t-il des exigences réseau particulières pour ce sous-réseau ?
- Souhaitez-vous des environnements de and/or test de développement distincts ? (Inclura un duplicata des services partagés pour un accès à tout moment)
- Quelles sont vos exigences en matière de sauvegarde de snapshots ?
- Disposez-vous d'un processus de maintenance existant ou d'une ou de plusieurs fenêtres de correctifs que vous souhaiteriez conserver ?
- Quelles sont les exigences relatives à l'enregistrement de votre domaine ?
- Avez-vous des exigences en matière d'authentification unique ? (par exemple, AD, LDAP)
- Quels sont vos besoins globaux en matière de système d'exploitation et de capacité prévus ?

Alertes de surveillance des zones d'atterrissage à compte unique

AMS vous permet d'être directement alerté (plutôt que de recevoir des notifications du service AMS) pour certaines alertes de surveillance. Pour vous inscrire, assurez-vous que votre architecte cloud (CA) ou votre responsable de prestation de services cloud (CSDM) reçoit les informations suivantes :

Alertes directes par e-mail : il s'agit des adresses e-mail auxquelles vous souhaitez qu'AMS envoie certaines alertes basées sur les ressources. Pour plus de détails sur les alertes envoyées directement par e-mail, consultez la section Alertes issues de la surveillance de base dans AMS dans le guide de l'utilisateur d'AMS pour la zone d'atterrissage à compte unique. Pour plus d'informations sur la surveillance AMS, consultez la section Gestion de la surveillance dans le guide de l'utilisateur AMS pour la zone d'atterrissage à compte unique.

Fenêtre de maintenance

Vous souhaiterez créer une fenêtre de maintenance prenant en compte les différents besoins des applications, ainsi que les différentes périodes de stress. Régions AWS C'est dans votre fenêtre de maintenance qu'AMS appliquera les correctifs. Voici quelques directives :

- Pour limiter l'impact sur les utilisateurs, planifiez votre fenêtre de maintenance en fonction de l' Région AWS endroit où vos environnements sont déployés.
- Planifiez une période en dehors des heures normales de bureau et au moment où le moins de trafic est attendu sur les serveurs de production.
- En général, les infrastructures nécessitent des mises à jour mensuelles.
- Planifiez une fenêtre de maintenance d'au moins 300 minutes. L'application de correctifs au système d'exploitation prend 60 à 90 minutes, tandis que l'application de correctifs à la pile d'infrastructure prend 180 à 300 minutes.

Étapes suivantes

L'équipe d'intégration d'AMS vous aidera à chaque étape de l'intégration de votre compte chez AMS. Voici les exigences d'intégration :

- Fournissez un nouveau Compte AWS à utiliser pour AMS et fournissez un Compte AWS identifiant.
- Inscrivez-vous pour obtenir le niveau de Support souhaité.
- Créez un rôle IAM entre comptes pour accorder l'accès au compte de provisionnement AMS et fournissez le nom du rôle à AMS.
- Ajoutez le compte 753102745277 en tant qu'entité de confiance.

Annexe : règle de réclamation des services de ActiveDirectory fédération (ADFS) et paramètres SAML

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 Distributables -> CLI -> Windows ou Managed Cloud Distributables -> 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 installer beautifulsoup4
9. Copiez le script dans home/ec2-user

   Définissez les autorisations requises

   Exécutez le script : samlapi.py

Historique du document

Le tableau suivant décrit les modifications importantes apportées à la documentation depuis la dernière version d'AMS.

- Version de l'API : 2019-05-21
- Dernière mise à jour de la documentation : 23 septembre 2025

Modifier	Description	Date
Mise à jour des paramètres par défaut de conservation et de rotation des journaux dans SALZ : section Paramètres par défaut	Valeurs par défaut de conservation et de rotation des journaux. Informations mises à jour sur AWS CloudTrail les journaux.	11 février 2026
Type de modification mis à jour pour le dimensionnement automatique des terminaux dans l' SageMaker IA dans la section FAQ d'AWS Managed Services	Utilisez AMS SSP pour configurer Amazon SageMaker AI sur votre compte AMS. Soumettez une RFC avec Management | Advanced stack components | Identity and Access Management (IAM) | Modifier le type d'entité ou de politique (automatisation gérée) (ct-27tuth19k52b4) pour augmenter les autorisations de dimensionnement automatiq ue temporairement ou définitivement, car le dimensionnement automatique nécessite un accès permissif au service. CloudWatch	25 septembre 2025
Références précises sur les types de modifications	Créez, modifiez ou supprimez des groupes de sécurité. Pour ajouter un utilisateur : Soumettre une RFC en utilisant Management | Directory Service | Utilisateurs et groupes | Ajouter un utilisateur au groupe [ct-24pi85mjtza8k] et pour supprimer un utilisateur : Soumettre une RFC en utilisant	8 août 2025

Modifier	Description	Date
	Management | Directory Service | Utilisateurs et groupes | Supprimer un utilisateur du groupe [ct-2019s9y3nfml4]	
Lien vers la table des matières supprimé	Le lien vers le AWS glossaire de la table des matières a été supprimé.	8 août 2025
Ajout d'un lien pour obtenir des conseils de prescription	Configurez la facturation consolidée : associez le nouveau compte au compte du payeur.	8 mai 2025
Instructions mises à jour pour activer l'accès IAM au AWS Management Console	Clarification des instructions pour activer l'accès IAM au AWS Management Console.	Activer l'accès IAM à la console AWS
Nombre actualisé d'interfaces virtuelles de transit autorisées sur les connexions dédiées Direct Connect	Les connexions dédiées Direct Connect sont désormais limitées à 4 interfaces virtuelles de transit par connexion	Connexion de Direct Connect à Transit Gateway
Améliorez le libellé.	Spécifie que « uniquement utilisée comme liste de refus » » doit inclure « Tout autoriser » pour garantir les opérations de surveillance et de gestion d'AMS.	Configuration réseau
Informations supplémentaires sur l'utilisation de l'AMS CLI.	« Notez également que l'`--region`option peut être nécessaire pour certaines commandes CLI »	Installation de l'AMS CLIs
Mise à jour : pour des raisons de cohérence et de lisibilité, les titres des chapitres ont été déplacés vers des sections plus appropriées	« Modes de gestion du changement » est le nouveau titre de « Gestion du changement »	Modes de gestion des modifications

Modifier	Description	Date
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.	Mode RFC.
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 raccourcie et contient des liens vers les sections du guide de l'utilisateur avancé d'AMS sur les modes ajoutés.	Modes AMS.
MALZ : schéma d'architecture réseau mis à jour	Architecture des comptes réseaum	16 juin 2022
Liste des sujets déplacée en dessous des paragraphes d'ouverture	Présentation de l'intégration à AWS Managed Services	16 juin 2022
Contenu actualisé, initiative linguistique inclusive	« Compte de gestion » et non « Compte principal ».	Rôle d'utilisateur IAM dans AMS, section « Exemples de politiques »
Contenu mis à jour, outils, comptes, noms de rôles	Nom de rôle mis CustomerMigrationAccessRole à jour en AWSManagedServices MigrationRole.	AWS Service de migration d'applications (AWS MGN)
SALZ : Valeurs par défaut de gestion de la continuité	Lien mis à jour et suppression des informations obsolètes de Tag VPC et valeurs par défaut	28 février 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.