



Guide de mise en œuvre

Cloud Migration Factory sur AWS



Cloud Migration Factory sur AWS: Guide de mise en œuvre

Copyright © 2024 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 la solution	1
Fonctionnalités et avantages	2
Cas d'utilisation	3
Concepts et définitions	3
Présentation de l'architecture	5
Diagramme d'architecture	5
Suivi de migration en option	6
AWS Considérations relatives à la conception de Well-Architected	7
Excellence opérationnelle	8
Sécurité	8
Fiabilité	8
Efficacité des performances	8
Optimisation des coûts	9
Durabilité	9
Détails de l'architecture	10
Serveur d'automatisation de la migration	10
API RestApis des services de migration	11
Services de connexion	11
Services d'administration	11
Services aux utilisateurs	12
Services d'outils	12
Interface Web de Migration Factory	13
AWS services inclus dans cette solution	13
Planifiez votre déploiement	18
Coût	18
(Facultatif/recommandé) Déployez une instance Amazon Elastic Compute Cloud pour aider à exécuter des scripts d'automatisation	20
Sécurité	21
Rôles IAM	21
Amazon Cognito	21
Amazon CloudFront	21
Amazon AWS WAF - Pare-feu pour applications Web	22
Régions AWS prises en charge	22
Quotas	24

Quotas pour AWS les services dans cette solution	24
Quotas AWS CloudFormation	24
Déployez la solution	25
Prérequis	25
Autorisations du serveur source	25
AWS Service de migration d'applications (AWS MGN)	25
Déploiement privé	25
AWS CloudFormation modèles	25
Vue d'ensemble du processus de déploiement	26
Étape 1 : Choisissez votre option de déploiement	27
Étape 2 : Lancez la pile	28
Étape 3 : Lancez la pile de comptes cible dans le AWS compte cible	37
Étape 4 : Création du premier utilisateur	38
Créez l'utilisateur initial et connectez-vous à la solution	38
Ajouter un utilisateur au groupe d'administrateurs	40
Identifiez l' CloudFront URL	40
Étape 5 : (Facultatif) Déployer le contenu statique d'une console Web privée	41
Étape 6 : mise à jour du schéma d'usine	42
Mettre à jour le aws_accountid pour MGN AWS	42
Étape 7 : Configuration d'un serveur d'automatisation de la migration	43
Création d'un serveur Windows Server 2016 ou version ultérieure	43
Installation du logiciel requis pour prendre en charge les automatisations	44
Configuration AWS des autorisations pour le serveur d'automatisation de la migration et installation de l'agent AWS Systems Manager (agent SSM)	45
Étape 8 : tester la solution à l'aide des scripts d'automatisation	50
Importer les métadonnées de migration dans l'usine	50
Accédez aux domaines	55
Procéder à un test de l'automatisation de la migration	56
Étape 9 : (Facultatif) Créez un tableau de bord de suivi des migrations	56
Définissez les QuickSight autorisations et les connexions	56
Création d'un tableau de bord	65
Étape 10 : (Facultatif) Configurer des fournisseurs d'identité supplémentaires dans Amazon Cognito	75
Surveillez la solution avec Service Catalog AppRegistry	78
Activer CloudWatch Application Insights	78
Confirmez les étiquettes de coût associées à la solution	80

Activer les balises de répartition des coûts associées à la solution	81
AWS Cost Explorer	82
Mettre à jour la solution	83
Résolution des problèmes	85
Contacter AWS Support	85
Créer un dossier	85
Comment pouvons-nous vous aider ?	85
Informations supplémentaires	85
Aidez-nous à résoudre votre cas plus rapidement	86
Résolvez maintenant ou contactez-nous	86
Désinstallez la solution	87
Videiement des compartiments Amazon S3	87
Utiliser leAWS Management Console pour supprimer la pile	87
UtilisationAWS Command Line Interface pour supprimer la pile	88
Guide de l'utilisateur	89
Gestion des métadonnées	89
Visualisation des données	89
Ajouter ou modifier un enregistrement	90
Supprimer un enregistrement	91
Exportation de données	91
Importation de données	92
Gestion des informations d'identification	96
Ajouter un secret	97
Modifier un secret	97
Suppression d'un secret	97
Exécuter l'automatisation depuis la console	97
Exécuter des automatisations à partir d'une invite de commande	100
Exécution manuelle d'un package d'automatisation	100
Création du FactoryEndpoints fichier .json	101
Lancez des jobs AWS MGN depuis Cloud Migration Factory	103
Activités préalables	103
Définition initiale	103
Initier une tâche	105
Replateforme vers EC2	106
Prérequis	107
Configuration initiale	107

Actions de déploiement	110
Gestion des scripts	111
Télécharger un nouveau package de script	112
Télécharger des packages de scripts	112
Ajouter une nouvelle version d'un package de script	113
Suppression de packages et de versions de scripts	113
Composer un nouveau package de script	113
Gestion des schémas	118
Ajouter/modifier un attribut	118
Gestion des autorisations	128
Politiques	130
Rôles	132
Manuel du développeur	133
Code source	133
Sujets supplémentaires	134
Liste des activités de migration automatisées à l'aide de la console Web d'usine	134
Vérifiez les prérequis	134
Installation des agents de réplication	135
Envoyez les scripts de post-lancement	136
Vérifiez l'état de la réplication	137
Valider le modèle de lancement	138
Lancer des instances à des fins de test	139
Vérifier l'état de l'instance cible	140
Marquer comme prêt pour le découpage	141
Arrêtez les serveurs sources concernés	142
Lancer des instances pour Cutover	143
Liste des activités de migration automatisées à l'aide d'une invite de commande	143
Vérifiez les prérequis	144
Installation des agents de réplication	146
Envoyez les scripts de post-lancement	148
Vérifiez l'état de la réplication	149
Vérifier l'état de l'instance cible	150
Arrêtez les serveurs sources concernés	152
Récupérez l'adresse IP de l'instance cible	152
Vérifiez les connexions au serveur cible	153
Référence	155

Collecte de données anonymisée	155
Ressources connexes	156
Collaborateurs	157
Révisions	158
Avis	162
.....	clxiii

Coordonnez et automatisez les migrations à grande échelle vers le AWS cloud à l'aide de la solution Cloud Migration Factory sur AWS

Date de publication : juin 2020 ([dernière mise à jour](#) : avril 2024)

La AWS solution Cloud Migration Factory on est conçue pour coordonner et automatiser les processus manuels pour les migrations à grande échelle impliquant un nombre important de serveurs. Cette solution aide les entreprises à améliorer leurs performances et à éviter les longues périodes de transition en fournissant une plate-forme d'orchestration permettant de migrer les charges de travail à grande échelle. AWS [AWS Les services professionnels](#), [AWS les partenaires](#) et d'autres entreprises ont déjà utilisé cette solution pour aider les clients à migrer des milliers de serveurs vers le AWS Cloud.

Cette solution vous permet de :

- Intégrez les nombreux types d'outils qui prennent en charge la migration, tels que les outils de découverte, les outils de migration et les outils de base de données de gestion des configurations (CMDB).
- Automatisez les migrations qui impliquent de nombreuses petites tâches manuelles, dont l'exécution prend du temps et qui sont lentes et difficiles à adapter.

Pour un guide de end-to-end déploiement complet utilisant cette solution, reportez-vous à la section [Automatisation des migrations de serveurs à grande échelle avec Cloud Migration Factory](#) du guide AWS prescriptive Guidance Cloud Migration Factory.

Ce guide de mise en œuvre décrit les considérations architecturales et les étapes de configuration pour déployer la AWS solution Cloud Migration Factory sur le cloud Amazon Web Services (AWS). Il inclut des liens vers des [AWS CloudFormation](#) modèles qui lancent et configurent les AWS services requis pour déployer cette solution en utilisant les AWS meilleures pratiques en matière de sécurité et de disponibilité.

Le guide est destiné aux architectes d'infrastructure informatique, aux administrateurs et aux DevOps professionnels ayant une expérience pratique de l'architecture dans le AWS Cloud.

Utilisez ce tableau de navigation pour trouver rapidement les réponses aux questions suivantes :

Si tu veux...	Lisez.
Connaissez le coût de fonctionnement de cette solution. Le coût d'exécution de cette solution dans la us-east-1 région est estimé à 14,31 dollars américains par mois pour les AWS ressources.	Coût
Comprenez les considérations de sécurité liées à cette solution.	Sécurité
Sachez comment planifier les quotas pour cette solution.	Quotas
Sachez quel Régions AWS support prend en charge cette solution.	Soutenu Régions AWS
Consultez ou téléchargez les AWS CloudFormation modèles inclus dans cette solution pour déployer automatiquement les ressources d'infrastructure (la « pile ») de cette solution.	AWS CloudFormation modèles

Fonctionnalités et avantages

La solution fournit les fonctionnalités suivantes :

Gérez, suivez et lancez la migration de votre charge de travail AWS depuis une interface Web unique, prenant en charge plusieurs cibles Comptes AWS et régions.

Fourni avec l'hébergement statique du site Web Amazon S3 ou dans le cadre d'un déploiement privé à partir d'une instance Amazon EC2 exécutant un serveur Web. Toutes les activités effectuées par la solution sont initiées à partir d'une seule interface Web, fournie par la solution. Consultez l'interface Web de Migration Factory pour plus de détails.

Tâches d'automatisation prédéfinies pour effectuer la plupart des tâches nécessaires à la migration complète des charges de travail à AWS l'aide du service de migration AWS d'applications.

La solution fournit toutes les tâches d'automatisation nécessaires à la migration de milliers de charges de travail AWS sans recourir à des scripts et avec des connaissances limitées pour démarrer. Toutes les automatisations peuvent être lancées depuis l'interface Web et, en arrière-plan, utiliser AWS System Manager pour lancer et exécuter les tâches d'automatisation sur le ou les serveurs d'automatisation fournis.

Personnalisez la solution avec des packages d'automatisation et des extensions de schéma d'attributs

La majorité des migrations nécessitent l'exécution de tâches d'automatisation personnalisées pour des applications et pour d'autres raisons spécifiques à l'environnement. Cloud Migration Factory AWS permet de personnaliser les scripts fournis par les utilisateurs ainsi que de charger des scripts personnalisés dans la solution. La solution permet également d'étendre le magasin de métadonnées de migration en quelques secondes, ce qui permet aux administrateurs d'ajouter et de supprimer des attributs au schéma qui doivent être suivis ou utilisés pendant la migration.

Intégration avec Service Catalog AppRegistry et AWS Systems Manager Application Manager

Cette solution inclut une AppRegistry ressource Service Catalog pour enregistrer le CloudFormation modèle de la solution et ses ressources sous-jacentes en tant qu'application à la fois dans [Service Catalog AppRegistry](#) et dans [AWS Systems Manager Application Manager](#). Grâce à cette intégration, vous pouvez gérer de manière centralisée les ressources de la solution et activer les actions de recherche, de reporting et de gestion des applications.

Cas d'utilisation

Migrez et gérez des migrations à grande échelle de charges de travail vers AWS

Offrez une vue d'ensemble unique des migrations de charges de travail à grande échelle vers AWS. Fournit une automatisation prédéfinie, des rapports et un accès basé sur les rôles via une interface Web unique conçue spécifiquement pour les migrations.

Concepts et définitions

Cette section décrit les concepts clés et définit la terminologie spécifique à cette solution :

application

Groupe de ressources constituant un service ou une application métier unique.

vague

Groupe d'applications qui seront migrées lors du même événement. Cela peut être basé sur l'affinité entre les uns et les autres, ou pour toute autre raison.

serveur

Serveur source à migrer.

database

Base de données source à migrer.

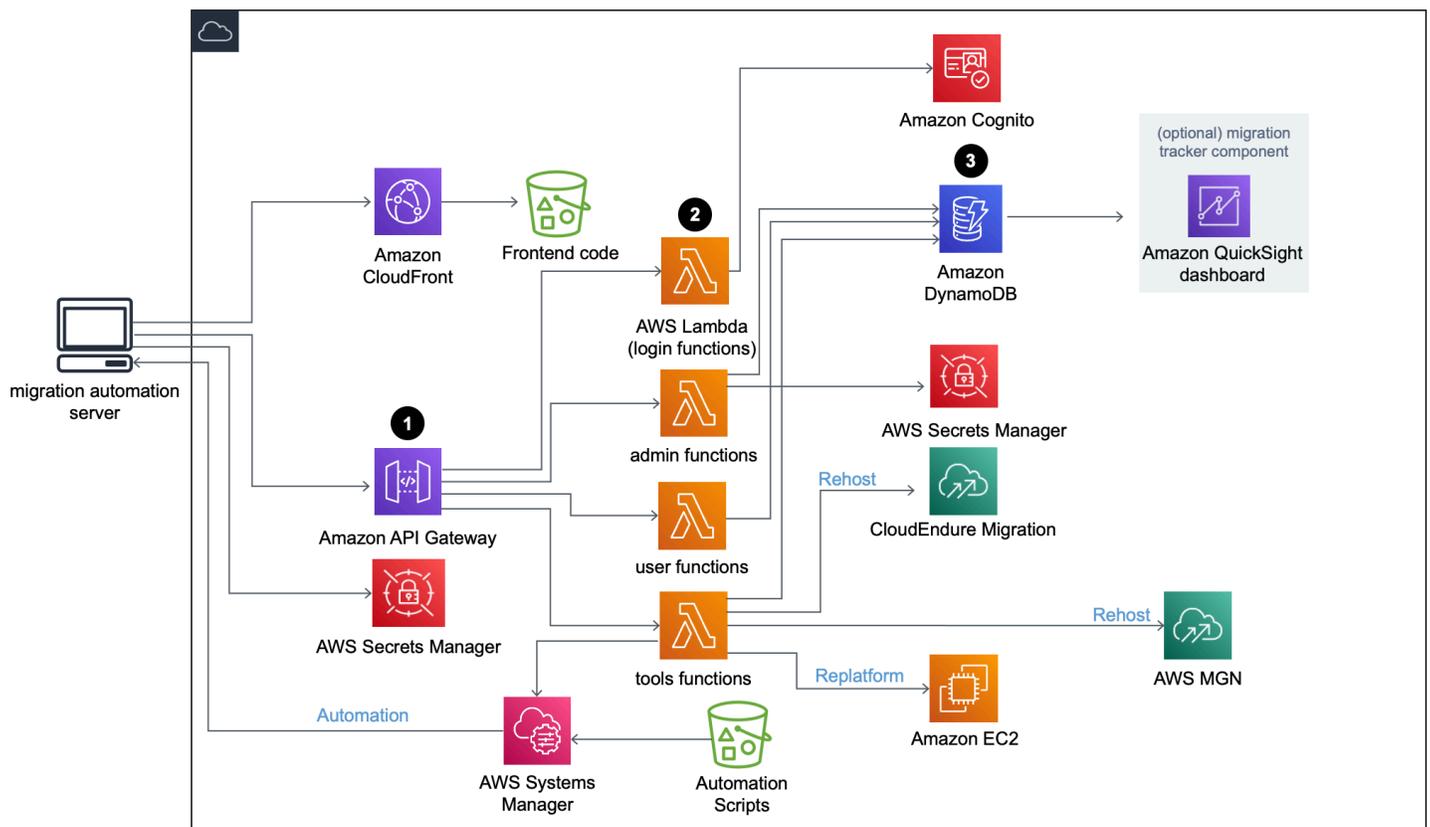
Pour une référence générale des AWS termes, reportez-vous au [AWS glossaire](#) de la référence AWS générale.

Présentation de l'architecture

Cette section fournit un schéma d'architecture d'implémentation de référence pour les composants déployés avec cette solution.

Diagramme d'architecture

Le déploiement de la solution par défaut permet de créer l'environnement sans serveur suivant dans le AWS cloud.



Cloud Migration Factory sur le schéma AWS d'architecture

Le AWS CloudFormation modèle de la solution lance les AWS services nécessaires pour aider les entreprises à migrer leurs serveurs.

Note

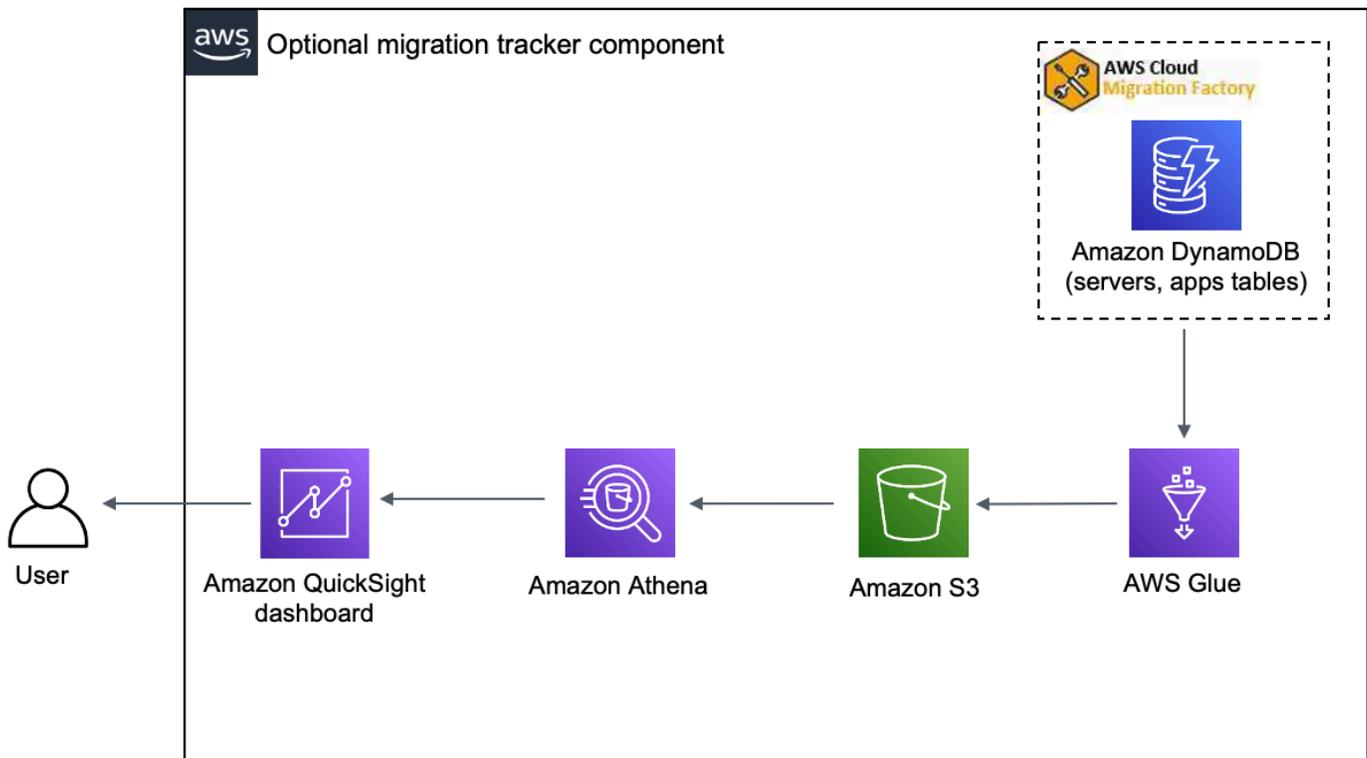
La AWS solution Cloud Migration Factory on utilise un serveur d'automatisation de la migration qui ne fait pas partie du AWS CloudFormation déploiement. Pour plus de détails

sur la création manuelle du serveur, reportez-vous à la section [Création d'un serveur d'automatisation de la migration](#).

1. [Amazon API Gateway](#) reçoit les demandes de migration du serveur d'automatisation de la migration via RestApis.
2. [AWS Lambda](#) les fonctions fournissent les services nécessaires pour vous connecter à l'interface Web, exécuter les fonctions administratives nécessaires pour gérer la migration et vous connecter à des API tierces pour automatiser le processus de migration.
 - [La fonction user Lambda intègre les métadonnées de migration dans une table Amazon DynamoDB](#). Les codes d'état HTTP standard vous sont renvoyés via le RestAPI depuis l'API Gateway. Un groupe d'utilisateurs [Amazon Cognito](#) est utilisé pour l'authentification des utilisateurs auprès de l'interface Web et des API Rest, et vous pouvez éventuellement le configurer pour qu'il s'authentifie auprès de fournisseurs d'identité SAML (Security Assertion Markup Language) externes.
 - Les fonctions tools Lambda traitent les API Rest externes et appellent le [service de CloudEndure migration et de migration AWS d'applications \(AWSMGN\)](#) pour la migration. AWS La fonction tools Lambda appelle également [Amazon EC2](#) pour lancer des instances EC2 et appelle [Systems AWS Manager](#) pour exécuter des scripts d'automatisation sur le serveur Migration Automation.
3. Les métadonnées de migration stockées dans Amazon DynamoDB sont acheminées vers l'API MGN pour lancer une AWS tâche de migration Rehost et lancer des serveurs. Si votre modèle de migration est Replatform vers EC2, la fonction tools Lambda lance des CloudFormation modèles de lancement dans le compte AWS cible pour lancer les instances Amazon EC2.

Suivi de migration en option

Cette solution déploie également un composant optionnel de suivi de migration qui suit la progression de votre migration.



Composant de suivi des migrations en option

Le CloudFormation modèle est déployé [AWS Glue](#) pour obtenir les métadonnées de migration à partir de la table DynamoDB de Cloud Migration Factory et exporte les métadonnées [vers Amazon Simple Storage Service \(Amazon S3\)](#) deux fois par jour (à 5 h 00 et 13 h 00 UTC). Une fois la AWS Glue tâche terminée, une requête de sauvegarde Amazon Athena est lancée et vous pouvez configurer Amazon QuickSight pour extraire les données des résultats de la requête Athena. Vous pouvez ensuite créer les visualisations et créer un tableau de bord qui répond aux besoins de votre entreprise. Pour obtenir des conseils sur la création de visuels et la création d'un tableau de bord, reportez-vous à la section [Création d'un tableau de bord de suivi des migrations](#).

Ce composant facultatif est géré par le paramètre Tracker du CloudFormation modèle. Par défaut, cette option est activée, mais vous pouvez la désactiver en modifiant le paramètre Tracker sur `false`.

AWS Considérations relatives à la conception de Well-Architected

Cette solution utilise les meilleures pratiques du [AWS Well-Architected Framework](#), qui aide les clients à concevoir et à exploiter des charges de travail fiables, sécurisées, efficaces et rentables dans le cloud.

Cette section décrit comment les principes de conception et les meilleures pratiques du Well-Architected Framework profitent à cette solution.

Excellence opérationnelle

Cette section décrit comment nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du [pilier de l'excellence opérationnelle](#).

- Ressources définies comme utilisant IaC CloudFormation.
- Toutes les actions et le journal d'audit sont envoyés à Amazon CloudWatch, ce qui permet de déployer des réponses automatisées.

Sécurité

Cette section décrit comment nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du [pilier de sécurité](#).

- IAM utilisé pour l'authentification et l'autorisation.
- Les autorisations de rôle ont été définies de manière à être aussi limitées que possible, bien que dans de nombreux cas, cette solution nécessite des autorisations génériques pour pouvoir agir sur toutes les ressources.
- Utilisation facultative du WAF pour renforcer la sécurité de la solution.
- Amazon Coginto et possibilité facultative de fédération avec des IdP externes.

Fiabilité

Cette section décrit comment nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du [pilier de fiabilité](#).

- Les services sans serveur permettent à la solution de fournir une architecture tolérante aux pannes.

Efficacité des performances

Cette section décrit comment nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du [pilier de l'efficacité des performances](#).

- Les services sans serveur permettent à la solution d'évoluer selon les besoins.

Optimisation des coûts

Cette section décrit comment nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du [pilier d'optimisation des coûts](#).

- Les services sans serveur vous permettent de payer uniquement pour ce que vous utilisez.

Durabilité

Cette section décrit comment nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du [pilier du développement durable](#).

- Les services sans serveur vous permettent d'augmenter ou de diminuer selon vos besoins.

Détails de l'architecture

Serveur d'automatisation de la migration

Cette solution s'appuie sur un serveur d'automatisation des migrations pour exécuter des migrations à l'aide d'API Rest. Ce serveur n'est pas automatiquement déployé avec la solution et doit être créé manuellement. Pour plus d'informations, reportez-vous à la section [Création d'un serveur d'automatisation de la migration](#). Nous vous recommandons de créer le serveur dans votre AWS environnement, mais vous pouvez également le créer sur site dans votre environnement réseau. Le serveur doit répondre aux exigences suivantes :

- Windows Server 2016 ou versions ultérieures
- Minimum 4 processeurs avec 8 Go de RAM
- Déployé en tant que nouvelle machine virtuelle sans application supplémentaire installée
- (Si intégré AWS) Dans la même Compte AWS région que Cloud Migration Factory

Une fois installé, le serveur a besoin d'un accès Internet et d'une connectivité réseau interne non restrictive avec les serveurs sources concernés (serveurs vers lesquels migrer). AWS

Si une restriction de port est requise entre le serveur d'automatisation de migration et les serveurs source, les ports suivants doivent être ouverts entre le serveur d'automatisation de migration et les serveurs source :

- Port SMB (TCP 445)
- Port SSH (TCP 22)
- Port WinRM (TCP 5985, 5986)

Nous recommandons que le serveur d'automatisation de la migration se trouve dans le même domaine Active Directory que les serveurs sources. Si les serveurs sources résident dans plusieurs domaines, la configuration de sécurité pour l'approbation du domaine dans chaque domaine détermine si vous avez besoin de plusieurs serveurs d'automatisation de la migration.

- Si la confiance de domaine existe dans tous les domaines dotés de serveurs source, un seul serveur d'automatisation de la migration pourra se connecter à tous les domaines et exécuter des scripts d'automatisation pour tous les domaines.

- S'il n'existe pas d'approbation de domaine dans tous les domaines, vous devez créer un serveur d'automatisation de migration supplémentaire pour chaque domaine non fiable, ou pour chaque action à effectuer sur le serveur d'automatisation, des informations d'identification alternatives devront être fournies avec les autorisations appropriées sur les serveurs sources.

API RestApis des services de migration

La AWS solution Cloud Migration Factory on automatise le processus de migration à l'aide d'API Rest traitées par le biais de AWS Lambda fonctions, d'un Amazon API GatewayAWS Managed Services, d'AWS Application Migration Service (AWS MGN) et CloudEndure de Migration. Lorsque vous faites une demande ou initiez une transaction, par exemple en ajoutant un serveur ou en consultant une liste de serveurs ou d'applications, des appels d'API Rest sont envoyés à Amazon API Gateway, qui lance une AWS Lambda fonction pour exécuter la demande. Les services suivants détaillent les composants du processus de migration automatique.

Services de connexion

Les services de connexion incluent les fonctions login Lambda et Amazon Cognito. Une fois que vous êtes connecté à la solution à l'aide de l'loginAPI via l'API Gateway, la fonction valide les informations d'identification, récupère un jeton d'authentification auprès d'Amazon Cognito et vous renvoie les détails du jeton. Vous pouvez utiliser ce jeton d'authentification pour vous connecter aux autres services de cette solution.

Services d'administration

Les services d'administration incluent Amazon API Gateway, les fonctions admin Lambda et Amazon DynamoDB. Les administrateurs de la solution peuvent utiliser la fonction admin Lambda pour définir le schéma des métadonnées de migration, à savoir les attributs de l'application et du serveur. L'API des services d'administration fournit la définition du schéma de la table DynamoDB. Les données utilisateur, y compris les attributs de l'application et du serveur, doivent respecter cette définition de schéma. Les attributs typiques incluent les champs app_namewave_id, server_name, et les autres champs identifiés dans [Importer les métadonnées de migration dans l'usine](#). Par défaut, le AWS CloudFormation modèle déploie automatiquement un schéma commun, mais celui-ci peut être personnalisé après le déploiement.

Les administrateurs peuvent également utiliser les services d'administration pour définir les rôles de migration des membres de leur équipe de migration. L'administrateur dispose d'un contrôle

granulaire pour associer des rôles d'utilisateur spécifiques à des attributs et à des étapes de migration spécifiques. Une phase de migration est une période pendant laquelle certaines tâches de migration sont exécutées, par exemple une phase de création, une phase de test et une étape de transition.

Services aux utilisateurs

Les services aux utilisateurs incluent Amazon API Gateway, les fonctions `user` Lambda et Amazon DynamoDB. Les utilisateurs peuvent gérer les métadonnées de migration, ce qui leur permet de lire, de créer, de mettre à jour et de supprimer les données de vague, d'application et de serveur dans le pipeline de métadonnées de migration.

Remarque

Une vague de migration est un concept de regroupement d'applications avec une date de début, une date de fin ou une date limite. Les données des vagues incluent les applications candidates à la migration et les groupes d'applications prévus pour une vague de migration particulière.

Les services utilisateurs proposent une API permettant à l'équipe de migration de manipuler les données de la solution : créer, mettre à jour et supprimer les données à l'aide du script Python et des fichiers CSV source. Pour connaître les étapes détaillées, reportez-vous aux sections Activités de migration automatisées à l'aide de la console Web Migration Factory et Activités de migration automatisées à l'aide d'une invite de commande.

Services d'outils

Les services d'outils incluent Amazon API Gateway, les fonctions `tools` Lambda, Amazon DynamoDB, AWS Managed Services, le service de migration d'applications et la AWS migration. CloudEndure Vous pouvez utiliser ces services pour vous connecter à des API tierces et automatiser le processus de migration. À l'aide du service de CloudEndure migration et de migration d'AWS applications, l'équipe de migration peut orchestrer le processus de lancement du serveur en appuyant simplement sur un bouton pour lancer tous les serveurs d'une même vague composée d'un groupe d'applications et de serveurs ayant la même date de transition. Grâce à cette AWS solution AWS Managed Services, Cloud Migration Factory on automatise le processus RFC d'ingestion de charge de travail et réduit les efforts manuels nécessaires pendant le processus de migration.

Interface Web de Migration Factory

La solution inclut une interface Web Migration Factory qui peut être hébergée, par défaut, dans un compartiment Amazon S3 ou sur un serveur Web fourni (ne faisant pas partie du déploiement de la solution) qui vous permet d'effectuer les tâches suivantes à l'aide d'un navigateur Web :

- Mettez à jour les métadonnées des vagues, des applications et des serveurs depuis votre navigateur Web
- Gérer les définitions des schémas d'applications et de serveurs
- Exécutez des scripts d'automatisation pour automatiser les activités de migration telles que la vérification des conditions préalables et l'installation d'agents MGN
- Créez des informations d'identification de migration pour vous connecter aux serveurs sources
- Connectez-vous à des services tiers tels que le service de migration des AWS applications, CloudEndure la migration et AWS Managed Services pour automatiser le processus de migration

AWSservices inclus dans cette solution

AWS service	Description	
Amazon API Gateway	Noyau. Fournit des API REST à l'ensemble de la solution, utilisées pour accéder aux données du backend et lancer et gérer les tâches d'automatisation de la migration.	
AWS Lambda	Noyau. Fournissez les services nécessaires pour vous connecter à l'interface Web, exécuter les fonctions administratives nécessaires pour gérer la migration et vous connecter à des API tierces pour automatiser le processus de migration.	

AWS service	Description	
Amazon DynamoDB	Noyau. Stockage de métadonnées pour toutes les données gérées par les utilisateurs et le système, accessible via Amazon API Gateway et les fonctions Lambda.	
Amazon Cognito	Noyau. L'autorisation et l'authentification des utilisateurs, ainsi que la fédération facultative avec d'autres IdP, sont également possibles via Amazon Cognito.	
AWS Systems Manager	Soutenir. Prend en charge l'exécution de Cloud Migration Factory sur des packages AWS d'automatisation sur le serveur d'automatisation fourni par le client.	
Amazon EC2	Soutenir. Serveur d'automatisation exécutant AWS des agents Systems Manager pour permettre l'exécution de packages d'automatisation.	

AWS service	Description	
Amazon S3	Soutenir. Utilisé dans plusieurs domaines de la solution, 1/ en utilisant la fonctionnalité d'hébergement Web statique d'Amazon S3, il sert l'interface Web principale (via Amazon CloudFront), 2/ les journaux et autres sorties d'automatisation sont stockés dans Amazon S3 par la solution.	
AWS Secrets Manager	Soutenir. Lors de l'utilisation des fonctionnalités d'automatisation de la solution, AWS Secrets Manager il est utilisé pour stocker en toute sécurité les informations d'identification utilisées pour accéder aux ressources en migration afin d'exécuter des tâches et des actions visant à faciliter et à migrer les charges de travail.	
Amazon CloudFront	Facultatif. Pour les déploiements standard, Amazon CloudFront assure la distribution du contenu de l'interface Web à partir d'Amazon S3, ce qui le rend hautement disponible dans le monde entier et fournit un accès TLS sécurisé au contenu de l'interface Web depuis n'importe où.	

AWS service	Description	
AWSService de migration d'applications (AWSMGN)	Facultatif. Lorsque vous effectuez des migrations de réhébergement de charges de travail Windows ou Linux, Cloud Migration Factory on AWS utilise AWS MGN pour faciliter la migration du système vers Amazon EC2.	
Amazon QuickSight	Facultatif. Permet de créer des tableaux de bord de migration personnalisables en fonction des données stockées dans le métastore de migration conservé dans Amazon DynamoDB, fournissant aux équipes les données dont elles ont besoin pour suivre leurs migrations et en rendre compte.	
AWS Glue	Facultatif. Extrait régulièrement les données stockées dans Amazon DynamoDB vers Amazon S3, fournissant des données de reporting à utiliser dans Amazon Athena et les tableaux de bord Amazon QuickSight	

AWS service	Description	
Amazon Athena	Facultatif. Permet d'accéder aux données de reporting extraites par AWS Clue à partir des métadonnées de migration, ce qui permet de créer des tableaux de bord à l'aide d'Amazon QuickSight.	
AWS Pare-feu pour applications Web	Facultatif. Appliquez une sécurité supplémentaire aux points de terminaison pour Amazon API Gateway et Amazon CloudFront afin de restreindre l'accès à des appareils spécifiques en fonction de l'adresse IP source ou d'autres critères d'accès.	

Planifiez votre déploiement

Cette section vous aide à planifier les coûts, la sécurité, les régions AWS et les types de déploiement pour la solution Cloud Migration Factory sur AWS.

Coût

Vous êtes responsable du coût des AWS services utilisés lors de l'exécution de cette solution. À partir de cette révision, le coût estimé pour exécuter cette solution avec les paramètres par défaut dans la région de l'est des États-Unis (Virginie du Nord) et en supposant que vous migrez 200 serveurs par mois avec cette solution est d'environ 14,31\$ par mois. Le coût d'exécution de cette solution dépend de la quantité de données chargées, demandées, stockées, traitées et présentées, comme indiqué dans le tableau suivant.

AWS service	Facteurs	Coût/mois [USD]
Services de base		
Amazon API Gateway	10 000 demandes/mois x (3,50 dollars par million de dollars)	0,035\$
AWS Lambda	10 000 invocations/mois (durée moyenne de 3 000 ms et 128 Mo de mémoire)	\$0.065
Amazon DynamoDB	20 000 demandes d'écriture/mois x (1,25 million de dollars) 40 000 demandes de lecture par mois x (0,25 \$/million de dollars) Stockage de données : 1 Go x 0,25\$	0,035\$

AWS service	Facteurs	Coût/mois [USD]
Amazon S3	Stockage (10 Mo) et 50 000 demandes de réception par mois	0,25\$
Amazon CloudFront	<p>Transfert de données régional vers Internet : 10 premiers To</p> <p>Transfert de données régional vers le point d'origine : transfert de toutes les données</p> <p>Requêtes HTTPS : 50 000 demandes/mois X (0,01 \$/10 000 demandes)</p>	0,92\$
AWS Systems Manager	10 000 pas/mois	0,00\$
AWS Secrets Manager	5 secrets x durée de 30 jours	2,00\$
Amazon Cognito (connexion directe)	Jusqu'à 50 000 utilisateurs actifs (MAU) par mois couverts par le niveau gratuit d'AWS	0,00\$
Amazon Athena	10 Mo par jour x 5\$ par To de données numérisées	0,0015\$
Services optionnels		
AWS Glue(outil de suivi des migrations en option)	2 minutes par jour x 10 DPU par défaut x 0,44\$ par heure de processeur	4,40\$

AWS service	Facteurs	Coût/mois [USD]
AWS WAF	2 ACL Web de 5,00\$ par mois (au prorata horaire) 2 règles : 1,00\$ par mois (au prorata horaire) 10 000 demandes x (0,60\$ pour 1 million de demandes)	6,60\$
Amazon Cognito (connexion SAML)	Jusqu'à 50 MAU couvertes par le niveau gratuit d'AWS Au-dessus de 50 MAU, 0,015 \$/MAU	0,00\$
Au total :		~14,31 \$/mois

(Recommandé) Déployez une instance Amazon Elastic Compute Cloud pour aider à exécuter des scripts d'automatisation

Nous recommandons de déployer une instance Amazon Elastic Compute Cloud (Amazon EC2) pour automatiser la connexion aux API de la solution AWS et aux API Boto3 avec des rôles IAM. L'estimation des coûts suivante suppose que l'instance Amazon EC2 est située dans la us-east-1 région et fonctionne huit heures par jour, cinq jours par semaine.

AWS service	Facteurs	Coût/mois [USD]
Amazon EC2	176 heures par mois x 0,1108 \$/heure () t3.large	19,50\$
Amazon Elastic Block Store (Amazon EBS)	30 Go x 0,08 \$/Go par mois (gp3) x (176 heures/720 heures)	0,59\$
Au total :		~20,09 \$

Les prix sont susceptibles d'être modifiés. Pour plus de détails, consultez la page Web de tarification de chaque AWS service que vous utiliserez dans cette solution.

Sécurité

Lorsque vous créez des systèmes sur une AWS infrastructure, les responsabilités en matière de sécurité sont partagées entre vous et AWS. Ce [modèle partagé](#) peut réduire votre charge opérationnelle en AWS exploitant, en gérant et en contrôlant les composants, depuis le système d'exploitation hôte et la couche de virtualisation jusqu'à la sécurité physique des installations dans lesquelles les services fonctionnent. Pour plus d'informations sur la sécurité AWS, consultez [AWS Cloud Security](#).

Rôles IAM

AWS Identity and Access Management Les rôles (IAM) vous permettent d'attribuer des politiques d'accès et des autorisations détaillées aux services et aux utilisateurs dans le AWS cloud. Cette solution crée des rôles IAM qui accordent à la AWS Lambda fonction l'accès aux autres AWS services utilisés dans cette solution.

Amazon Cognito

L'utilisateur Amazon Cognito créé par cette solution est un utilisateur local autorisé à accéder uniquement aux API RestApis de cette solution. Cet utilisateur n'est pas autorisé à accéder aux autres services de votre AWS compte. Pour plus d'informations, reportez-vous à la section Groupes d'utilisateurs [Amazon Cognito dans le manuel](#) du développeur Amazon Cognito.

La solution prend éventuellement en charge la connexion SAML externe via la configuration de fournisseurs d'identité fédérés et la fonctionnalité d'interface utilisateur hébergée d'Amazon Cognito.

Amazon CloudFront

Cette solution par défaut déploie une console Web [hébergée](#) dans un compartiment Amazon S3. Pour réduire la latence et améliorer la sécurité, cette solution inclut une CloudFront distribution [Amazon dotée](#) d'une identité d'accès d'origine, c'est-à-dire un CloudFront utilisateur spécial qui permet de fournir un accès public au contenu du bucket du site Web de la solution. Pour plus d'informations, reportez-vous à la section [Restreindre l'accès au contenu Amazon S3 à l'aide d'une identité d'accès d'origine](#) dans le manuel Amazon CloudFront Developer Guide.

Si un type de déploiement privé est sélectionné lors du déploiement de la pile, CloudFront aucune distribution n'est déployée et nécessite l'utilisation d'un autre service d'hébergement Web pour héberger la console Web.

AWS WAF - Pare-feu pour applications Web

Si le type de déploiement sélectionné dans la pile est Public [AWS WAF](#), les ACL AWS WAF Web requises et les règles configurées pour protéger CloudFront les points de terminaison API Gateway et Cognito créés par la solution CMF CloudFormation seront déployés. Ces points de terminaison seront restreints pour autoriser uniquement les adresses IP sources spécifiées à accéder à ces points de terminaison. Lors du déploiement de la pile, deux plages CIDR doivent être fournies avec la fonctionnalité pour ajouter des règles supplémentaires après le déploiement via la AWS WAF console.

Régions AWS prises en charge

Cette solution utilise Amazon Cognito et Amazon QuickSight, qui ne sont actuellement disponibles que dans certaines AWS régions. Par conséquent, vous devez lancer cette solution dans une région où ces services sont disponibles. Pour connaître la disponibilité des services la plus récente par région, consultez la [liste des services AWS régionaux](#).

Note

Le transfert de données pendant le processus de migration n'est pas affecté par les déploiements régionaux.

Cloud Migration Factory sur AWS est disponible dans les régions AWS suivantes :

Noms des régions	
USA Est (Ohio)	Asie Pacifique (Tokyo)
USA Est (Virginie du Nord)	Canada (Centre)
USA Ouest (Californie du Nord)	Europe (Francfort)
USA Ouest (Oregon)	Europe (Irlande)

Noms des régions	
*Afrique (Le Cap)	Europe (Londres)
*Asie-Pacifique (Hong Kong)	*Europe (Milan)
*Asie-Pacifique (Hyderabad)	*Europe (Espagne)
*Asie-Pacifique (Jakarta)	Europe (Paris)
*Asie-Pacifique (Melbourne)	Europe (Stockholm)
Asie-Pacifique (Mumbai)	*Europe (Zurich)
Asie-Pacifique (Osaka)	*Moyen-Orient (Bahreïn)
Asie-Pacifique (Séoul)	*Moyen-Orient (Émirats arabes unis)
Asie-Pacifique (Singapour)	Israël (Tel Aviv)
Asie-Pacifique (Sydney)	Amérique du Sud (São Paulo)

Important

*Disponible uniquement pour le type de déploiement privé en raison de la journalisation des CloudFront accès à Amazon. Consultez [la section Configuration et utilisation des journaux standard \(journaux d'accès\)](#) dans le manuel Amazon CloudFront Developer Guide pour les derniers détails.

Cloud Migration Factory sur AWS n'est pas disponible dans les régions AWS suivantes :

Nom de la région	Service (s) ou option de service non disponible
AWS GovCloud (USA Est)	Amazon Cognito
AWS GovCloud (ouest des États-Unis)	Amazon Cognito

Quotas

Les quotas de service, également appelés limites, sont le nombre maximal de ressources ou d'opérations de service pour votre compte AWS.

Quotas pour AWS les services dans cette solution

Assurez-vous de disposer d'un quota suffisant pour chacun des [services mis en œuvre dans cette solution](#). Pour plus d'informations, reportez-vous à la section [Quotas AWS de service](#).

Sélectionnez l'un des liens suivants pour accéder à la page de ce service. Pour consulter les quotas de service pour tous les AWS services de la documentation sans changer de page, consultez plutôt les informations de la page [Points de terminaison et quotas du service](#) dans le PDF.

Quotas AWS CloudFormation

Vous avez un compte AWS CloudFormation des quotas dont vous devez tenir compte lorsque vous lancez la pile pour cette solution. En comprenant ces quotas, vous pouvez éviter les erreurs de limitation qui vous empêcheraient de déployer correctement cette solution. Pour plus d'informations, reportez-vous aux [AWS CloudFormation quotas](#) dans le Guide de l'AWS CloudFormation utilisateur.

Déployez la solution

Cette solution utilise des [AWS CloudFormation modèles et des piles](#) pour automatiser son déploiement. Le ou les CloudFormation modèles spécifient les AWS ressources incluses dans cette solution et leurs propriétés. La CloudFormation pile fournit les ressources décrites dans le ou les modèles.

Prérequis

Autorisations du serveur source

Un utilisateur de domaine disposant d'autorisations d'administrateur local sur les serveurs sources concernés par la migration est requis pour les serveurs Windows et Linux (autorisations sudo). Si les serveurs sources ne se trouvent pas dans un domaine, d'autres utilisateurs peuvent être utilisés, notamment un utilisateur LDAP avec des autorisations sudo/administrateur ou un utilisateur sudo/administrateur local. Avant de lancer cette solution, vérifiez que vous disposez des autorisations nécessaires ou que vous vous êtes concerté avec la personne compétente de votre organisation disposant des autorisations.

AWS Service de migration d'applications (AWS MGN)

Si vous utilisez AWS MGN pour cette solution, vous devez d'abord initialiser le service AWS MGN dans chaque compte et région cibles avant de lancer la pile de comptes cibles. Reportez-vous à la section [Initialisation du service de migration d'applications dans le guide de l'utilisateur du service](#) de migration d'applications pour plus de détails.

Déploiement privé

Si vous avez choisi de déployer une instance privée de CMF, déployez un serveur Web dans votre environnement avant de procéder au déploiement de la solution CMF.

AWS CloudFormation modèles

Cette solution permet AWS CloudFormation d'automatiser le déploiement de la AWS solution Cloud Migration Factory sur le AWS Cloud. Il inclut le AWS CloudFormation modèle suivant, que vous pouvez télécharger avant le déploiement.

View template

[aws-](#)

[cloud-migration-factory](#)-solution.template - Utilisez ce modèle pour lancer la solution Cloud Migration Factory sur la AWS solution et tous les composants associés. La configuration par défaut déploie des AWS Lambda fonctions, des tables Amazon DynamoDB, un Amazon API Gateway, Amazon, des compartiments Amazon S3 CloudFront, un groupe d' AWS Systems Manager utilisateurs Amazon Cognito, un [AWS Secrets Manager](#) document d'automatisation et des secrets, mais vous pouvez également personnaliser le modèle en fonction de vos besoins spécifiques.

View template

[aws-](#)

[cloud-migration-factory](#)- solution-target-account .template - Utilisez ce modèle pour lancer le ou les comptes cibles de la solution Cloud Migration Factory sur AWS. La configuration par défaut déploie des rôles IAM et un utilisateur, mais vous pouvez également personnaliser le modèle en fonction de vos besoins spécifiques.

Vue d'ensemble du processus de déploiement

Avant de lancer le déploiement automatique, passez en revue l'architecture, les composants et les autres considérations abordées dans ce guide. Suivez les step-by-step instructions de cette section pour configurer et déployer la AWS solution Cloud Migration Factory on dans votre compte.

Temps de déploiement : environ 20 minutes

Note

Si vous déployez cette solution dans des régions AWS autres que l'est des États-Unis (Virginie du Nord), la disponibilité de l' CloudFront URL de Migration Factory peut prendre plus de temps. Pendant ce temps, vous recevrez un message de refus d'accès lorsque vous accéderez à l'interface Web.

[Étape 1 : Choisissez votre option de déploiement](#)

[Étape 2 : Lancez la pile](#)

[Étape 3 : Lancer la pile de comptes cible dans le compte AWS cible](#)

[Étape 4 : Création du premier utilisateur](#)

[Étape 5 : \(Facultatif\) Déployer le contenu statique d'une console Web privée](#)

[Étape 6 : mise à jour du schéma d'usine](#)

[Étape 7 : Création d'un serveur d'automatisation de la migration](#)

[Étape 8 : tester la solution à l'aide des scripts d'automatisation](#)

[Étape 9 : \(Facultatif\) Créez un tableau de bord de suivi des migrations](#)

[Étape 10 : \(Facultatif\) Configurer des fournisseurs d'identité supplémentaires dans Amazon Cognito](#)

Important

Cette solution inclut une option permettant d'envoyer des métriques opérationnelles anonymisées à AWS. Nous utilisons ces données pour mieux comprendre comment les clients utilisent cette solution et les services et produits associés. AWS détient les données recueillies dans le cadre de cette enquête. La collecte de données est soumise à l'[avis AWS de confidentialité](#).

Pour désactiver cette fonctionnalité, téléchargez le modèle, modifiez la section de AWS CloudFormation mappage, puis utilisez la AWS CloudFormation console pour télécharger votre modèle mis à jour et déployer la solution. Pour plus d'informations, consultez la section [Collecte de données anonymisée](#) de ce guide.

Étape 1 : Choisissez votre option de déploiement

Il existe trois options pour le déploiement de la pile initiale et le choix de la bonne dépend des politiques de sécurité de l'environnement cible.

Ces options sont les suivantes :

- **Public (par défaut)** : toutes les applications Cloud Migration Factory sur les AWS terminaux sont accessibles au public grâce à l'authentification de l'utilisateur. Cette option déploie les points d'entrée suivants : CloudFront Public API Gateway Endpoints et Cognito.
- **Public avec AWS WAF** : l'accès aux points de terminaison Cloud Migration Factory est limité aux plages CIDR personnalisables. Cette option déploie les points d'entrée suivants : Public API

Gateway Endpoints CloudFront, Cognito, et AWS WAF restreint l'accès à des plages d'adresses CIDR spécifiques.

- Privé : tous les points de terminaison Cloud Migration Factory ne sont accessibles que depuis vos réseaux VPC et la console Web de Cloud Migration Factory AWS doit être hébergée sur un serveur Web privé déployé séparément. Cette option déploie les points d'entrée suivants : points de [terminaison d'API Gateway privés \(accessibles uniquement\)](#) au sein d'un VPC) et Cognito.

Étape 2 : Lancez la pile

Important

Cette solution inclut une option permettant d'envoyer des métriques opérationnelles anonymisées à AWS. Nous utilisons ces données pour mieux comprendre comment les clients utilisent cette solution et les services et produits associés. AWS détient les données recueillies dans le cadre de cette enquête. La collecte de données est soumise à la politique de [confidentialité d'AWS](#).

Pour désactiver cette fonctionnalité, téléchargez le modèle, modifiez la section de AWS CloudFormation mappage, puis utilisez la AWS CloudFormation console pour télécharger votre modèle et déployer la solution. Pour plus d'informations, reportez-vous à la [Collecte de données anonymisée](#) section de ce guide.

Ce AWS CloudFormation modèle automatisé déploie la solution Cloud Migration Factory sur AWS dans le AWS cloud.

Note

Vous êtes responsable du coût des AWS services utilisés lors de l'exécution de cette solution. Reportez-vous à la [Coût](#) section pour plus de détails. Pour plus de détails, consultez la page Web de tarification de chaque AWS service que vous utiliserez dans cette solution.

1. Connectez-vous au modèle AWS Management Console et sélectionnez le bouton pour lancer le `cloud-migration-factory-solution` AWS CloudFormation modèle.

[Launch solution](#)

Vous pouvez également [télécharger le modèle](#) comme point de départ pour votre propre implémentation.

2. Le modèle est lancé par défaut dans la région USA Est (Virginie du Nord). Pour lancer cette solution dans une autre AWS région, utilisez le sélecteur de région dans la barre de navigation de la console.

Note

Cette solution utilise Amazon Cognito et Amazon QuickSight, qui ne sont actuellement disponibles que dans certaines AWS régions. Par conséquent, vous devez lancer cette solution dans une AWS région où ces services sont disponibles. Pour connaître la disponibilité la plus récente par région, consultez la [liste des services AWS régionaux](#). Lorsqu'elle est déployée en public et en public avec des types de déploiement WAF, la solution utilise également la CloudFront journalisation d'Amazon sur Amazon S3. Aujourd'hui, la livraison de journaux d'Amazon CloudFront vers Amazon S3 n'est disponible que dans certaines régions. Reportez-vous à la section [Choisir un compartiment Amazon S3 pour vos journaux standard](#) afin de vérifier que votre région est prise en charge.

3. Sur la page Create stack, vérifiez que l'URL du modèle correct apparaît dans la zone de texte URL Amazon S3 et choisissez Next.
4. Sur la page Spécifier les détails de la pile, attribuez un nom à votre pile de solutions.
5. Sous Paramètres, passez en revue les paramètres du modèle et modifiez-les si nécessaire. Cette solution utilise les valeurs par défaut suivantes.

Paramètre	Par défaut	Description
Application name (Nom de l'application)	migration-factory	Entrez un préfixe à l'ID AWS CloudFormation physique qui identifie les AWS services déployés par cette solution.

Paramètre	Par défaut	Description
		<p> Note</p> <p><aws-resource>Le nom de l'application est utilisé comme préfixe pour identifier les AWS ressources déployées : <application-name>-<environment-name>-. Si vous modifiez le nom par défaut, nous vous recommandons de limiter les libellés de préfixes combinés à 40 caractères ou moins afin de ne pas dépasser les limites de caractères.</p>

Paramètre	Par défaut	Description
Nom de l'environnement	test	<p>Entrez un nom pour identifier l'environnement réseau dans lequel la solution est déployée. Nous recommandons un nom descriptif tel que testdev, ouprod.</p> <div data-bbox="1089 541 1507 1528" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p><aws-resource>Le nom de l'environnement est utilisé comme préfixe pour identifier les AWS ressources déployées : <application-name>-<environment-name>-. Si vous modifiez le nom par défaut, nous vous recommandons de limiter les libellés de préfixes combinés à 40 caractères ou moins afin de ne pas dépasser les limites de caractères.</p></div>
Suivi des migrations	true	Par défaut, le tableau de bord optionnel du suivi des migrations est activé, mais vous pouvez le désactiver en modifiant ce paramètre sur false.

Paramètre	Par défaut	Description
Replateforme EC2	<code>true</code>	Par défaut, la fonctionnalité Replatform EC2 est activée, mais vous pouvez la désactiver en modifiant ce paramètre sur <code>false</code>
ServiceAccountEmail	<code>serviceaccount@yourdomain.com</code>	Adresse e-mail du compte de service par défaut, les scripts d'automatisation de migration utilisent ce compte pour se connecter à l'API d'usine.
Autoriser la configuration d'un fournisseur d'identité supplémentaire dans Cognito	<code>false</code>	Par défaut, la solution utilise Amazon Cognito pour créer et gérer l'accès. La modification de ce paramètre <code>true</code> va configurer la solution pour autoriser l'ajout de fournisseurs d'identité SAML externes à Amazon Cognito et leur utilisation pour se connecter.

Paramètre	Par défaut	Description
Type de déploiement	Public	<p>Par défaut, le type de déploiement est Public, et tous les points de terminais on Cloud Migration Factory sont accessibles au public avec authentification utilisateur.</p> <p>Public avec AWS WAF : l'accès aux points de terminaison CMF est limité aux plages d'adresses CIDR personnalisables.</p> <p>Privé : tous les points de terminaison Cloud Migration Factory ne sont accessibles que depuis vos réseaux VPC et l'interface utilisateur Web de Cloud Migration Factory doit être hébergée sur un serveur Web privé déployé séparément.</p>

(Facultatif) Type de déploiement privé uniquement

Paramètre	Par défaut	Description
URL complète utilisée pour accéder à l'interface utilisateur Web	[not set]	<p>Obligatoire lorsque le type de déploiement est défini sur Privé. Spécifiez l'URL de l'interface Web de Migration Factory qui diffusera le contenu Web statique. Exemple https://cmf.yourdomain.local.</p> <div data-bbox="1089 638 1510 1604" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Important</p><ul style="list-style-type: none">• N'ajoutez pas de barre oblique à l'URL, cela provoquerait l'échec de l'interface Web lors du chargement.• Dans les déploiements privés, un serveur Web est requis pour héberger le contenu statique et doit être déployé avant le déploiement du CloudFormation modèle.</div>

Paramètre	Par défaut	Description
ID VPC pour héberger les points de terminaison API Gateway	[not set]	Obligatoire lorsque le type de déploiement est défini sur Privé. Spécifiez un seul VPC ID où les points de terminaison API Gateway privés seront créés.
Sous-réseaux pour héberger les points de terminaison de l'interface API Gateway	[not set]	Obligatoire lorsque le type de déploiement est défini sur Privé. Spécifiez deux ID de sous-réseau dans lesquels les points de terminaison privés de l'API Gateway seront créés. Les ID de sous-réseau spécifiés doivent se trouver dans le VPC spécifié ci-dessus.
(Facultatif) Public avec type de AWS WAF déploiement uniquement		

Paramètre	Par défaut	Description
CIDR autorisé	[not set]	Obligatoire lorsque le type de déploiement est défini sur Public avec AWS WAF. Spécifiez deux plages d'adresses CIDR à partir desquelles les utilisateurs et le serveur d'automatisation accéderont aux points de terminaison. <div data-bbox="1089 684 1510 1413" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px; margin-top: 10px;"><p> Important</p><ul style="list-style-type: none">• Vous devez spécifier 2 plages CIDR.• Une fois déployée, il est possible d'ajouter des plages et des restrictions supplémentaires aux AWS WAF règles selon les besoins.</div>

6. Choisissez Next (Suivant).
7. Sur la page Configurer les options de pile, choisissez Suivant.
8. Sur la page Vérification, vérifiez et confirmez les paramètres. Cochez les cases indiquant que le modèle créera des ressources [AWS Identity and Access Management](#)(IAM) et qu'il peut nécessiter la fonctionnalité CAPABILITY_AUTO_EXPAND.
9. Choisissez Submit pour déployer la pile.

Vous pouvez consulter l'état de la pile dans la AWS CloudFormation console dans la colonne État. Vous devriez recevoir le statut CREATE_COMPLETE dans environ 20 minutes.

⚠ Important

Si vous utilisez le AWS MGN, vous devez remplir les conditions requises pour le AWS MGN avant de passer à l'étape 3.

Étape 3 : Lancez la pile de comptes cible dans le AWS compte cible

Ce AWS CloudFormation modèle automatique déploie les rôles IAM dans le AWS compte cible pour permettre au compte d'usine d'assumer des rôles et d'effectuer des actions MGN sur le compte cible. Répétez cette étape pour chaque compte cible. Si la pile d'usine de l'étape précédente est un compte cible, cette pile cible devra être déployée sur celui-ci.

📘 Note

Le compte cible doit être initialisé pour le service de migration AWS d'applications avant de lancer cette pile. Pour plus de détails, reportez-vous à la section [Initialisation du service de migration](#) d'applications du guide de l'utilisateur du service de migration d'applications.

La pile de comptes cible doit être lancée dans la même région que la pile d'usine à l'étape précédente, quelle que soit la région qui sera utilisée comme région cible de migration. Cette pile est réservée aux autorisations entre comptes.

1. Connectez-vous à la [console AWS CloudFormation](#). Choisissez Créer une pile, puis sélectionnez Avec de nouvelles ressources pour démarrer le déploiement du modèle. Vous pouvez également [télécharger le modèle](#) comme point de départ pour votre propre implémentation.
2. Sur la page Spécifier les détails de la pile, attribuez un nom à votre pile de solutions.
3. Sous Paramètres, passez en revue les paramètres du modèle et modifiez-les si nécessaire. Cette solution utilise les valeurs par défaut suivantes.

Paramètre	Par défaut	Description
Usine AWSAccountId	111122223333	Entrez un identifiant de compte sur lequel la

Paramètre	Par défaut	Description
		Migration Factory a été déployée. <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>Lancez cette pile dans la même région AWS que la pile Migration Factory.</p> </div>
Recréation de plateforme	Yes	Activez cette option si vous prévoyez d'utiliser le module Replatform EC2 de cette solution
Réhéberger MGN	Yes	Activez cette option si vous prévoyez d'utiliser le module Rehost MGN de cette solution

4. Choisissez Next (Suivant).
5. Sur la page Configurer les options de pile, choisissez Suivant.
6. Sur la page Vérification, vérifiez et confirmez les paramètres. Cochez la case indiquant que le modèle créera des ressources [AWS Identity and Access Management](#)(IAM).
7. Choisissez Submit pour déployer la pile.

Vous pouvez consulter l'état de la pile dans la AWS CloudFormation console dans la colonne État. Vous devriez recevoir le statut CREATE_COMPLETE dans environ 5 minutes.

Étape 4 : Création du premier utilisateur

Créez l'utilisateur initial et connectez-vous à la solution

Pour créer l'utilisateur initial, procédez comme suit.

1. Accédez à la [console Amazon Cognito](#).
2. Dans le volet de navigation, sélectionnez Groupes d'utilisateurs.
3. Sur la page Groupes d'utilisateurs, choisissez le groupe d'utilisateurs qui commence par le migration-factory préfixe.
4. Sélectionnez l'onglet Utilisateurs, puis choisissez Créer un utilisateur.
5. Dans la section Informations utilisateur de l'écran Créer un utilisateur, procédez comme suit :
 1. Vérifiez que l'option Envoyer une invitation est sélectionnée.
 2. Entrez une adresse e-mail.

 Important

Cette adresse e-mail doit être différente de celle que vous avez utilisée dans le ServiceAccountEmail paramètre, que la solution utilise lors du déploiement du CloudFormation modèle principal.

3. Sélectionnez Définir un mot de passe.
4. Dans le champ Mot de passe, entrez un mot de passe.

 Note

Le mot de passe doit comporter au moins huit caractères, y compris des lettres majuscules et minuscules, des chiffres et des caractères spéciaux.

6. Choisissez Create user (Créer un utilisateur).

 Note

Vous recevrez un e-mail contenant le mot de passe temporaire. Jusqu'à ce que vous changiez le mot de passe temporaire, le statut du compte de cet utilisateur s'affichera comme Forcer le changement de mot de passe. Vous pouvez mettre à jour le mot de passe ultérieurement au cours du déploiement.

Ajouter un utilisateur au groupe d'administrateurs

Dans la console Amazon Cognito, suivez la procédure suivante pour ajouter un utilisateur au groupe d'administrateurs par défaut.

1. Accédez à la console Amazon Cognito.
2. Dans le menu de navigation, sélectionnez Groupes d'utilisateurs.
3. Sur la page Groupes d'utilisateurs, choisissez le groupe d'utilisateurs qui commence par le `migration-factory` préfixe.
4. Sélectionnez l'onglet Groupes et ouvrez le groupe nommé admin en sélectionnant le nom.
5. Choisissez Ajouter un utilisateur au groupe, puis sélectionnez le nom d'utilisateur à ajouter.
6. Choisissez Ajouter.

L'utilisateur choisi sera désormais ajouté à la liste des membres du groupe. Ce groupe d'administrateurs par défaut autorise l'utilisateur à gérer tous les aspects de la solution.

Note

Après avoir créé les utilisateurs initiaux, vous pouvez gérer l'appartenance aux groupes dans l'interface utilisateur de la solution en sélectionnant Administration, Autorisations, puis Groupes.

Identifier l' CloudFront URL (publique et publique pour les AWS WAF déploiements uniquement)

Utilisez la procédure suivante pour identifier l' CloudFront URL Amazon de la solution. Cela vous permet de vous connecter et de modifier le mot de passe.

1. Accédez à la [AWS CloudFormation console](#) et sélectionnez la pile de la solution.
2. Sur la page Stacks, sélectionnez l'onglet Sorties et sélectionnez la valeur de l'MigrationFactoryURL.

Note

Si vous avez lancé la solution dans une AWS région autre que l'est des États-Unis (Virginie du Nord), le déploiement CloudFront peut prendre plus de temps et

l'MigrationFactoryURL risque de ne pas être accessible immédiatement (vous recevrez un message d'erreur de refus d'accès). Jusqu'à quatre heures peuvent s'écouler avant que l'URL ne soit disponible. L'URL inclut `cloudfront.net` dans la chaîne.

3. Connectez-vous avec votre nom d'utilisateur et votre mot de passe temporaire, puis créez un nouveau mot de passe et choisissez `Changer le mot de passe`.

 Note

Le mot de passe doit comporter au moins huit caractères, y compris des lettres majuscules et minuscules, des chiffres et des caractères spéciaux.

Étape 5 : (Facultatif) Déployer le contenu statique d'une console Web privée

Si vous avez sélectionné le type de déploiement privé lors du déploiement de la pile, vous devez déployer manuellement le code de la console Web CMF sur le serveur Web que vous avez créé, puis spécifié dans URL complète utilisée pour accéder au paramètre d'interface utilisateur Web de la pile. Pour tous les autres types de déploiement, ignorez cette étape.

Les instructions d'installation et de configuration pour chaque serveur Web étant différentes, ce guide ne fournit que des instructions génériques sur l'emplacement à partir duquel copier le contenu. Vous devez configurer le serveur Web selon vos propres besoins avant de mettre à jour le contenu.

1. Assurez-vous que le serveur Web a accès à S3 et que l'interface de ligne de commande AWS est installée et configurée. Vous pouvez également télécharger le contenu du bucket frontal et le copier sur le serveur Web à l'aide d'un autre appareil.
2. À l'aide de l'interface de ligne de commande AWS, exécutez la commande suivante en remplaçant le nom de l'environnement par celui spécifié lors du déploiement de la pile, l'ID du compte AWS dans lequel la pile a été déployée et le répertoire cible par celui du répertoire racine par défaut du serveur Web. Cela copiera le code statique de la console Web Cloud Migration Factory ainsi que la configuration spécifique requise pour le déploiement de cette solution Cloud Migration Factory :

Exemple Windows :

```
aws s3 cp --recursive s3://migration-factory-<environment name>-<AWS Account Id>-front-end/ C:\inetpub\wwwroot --recursive
```

Exemple de Linux :

```
aws s3 cp s3://migration-factory-<environment name>-<AWS Account Id>-front-end/ /var/www/html --recursive
```

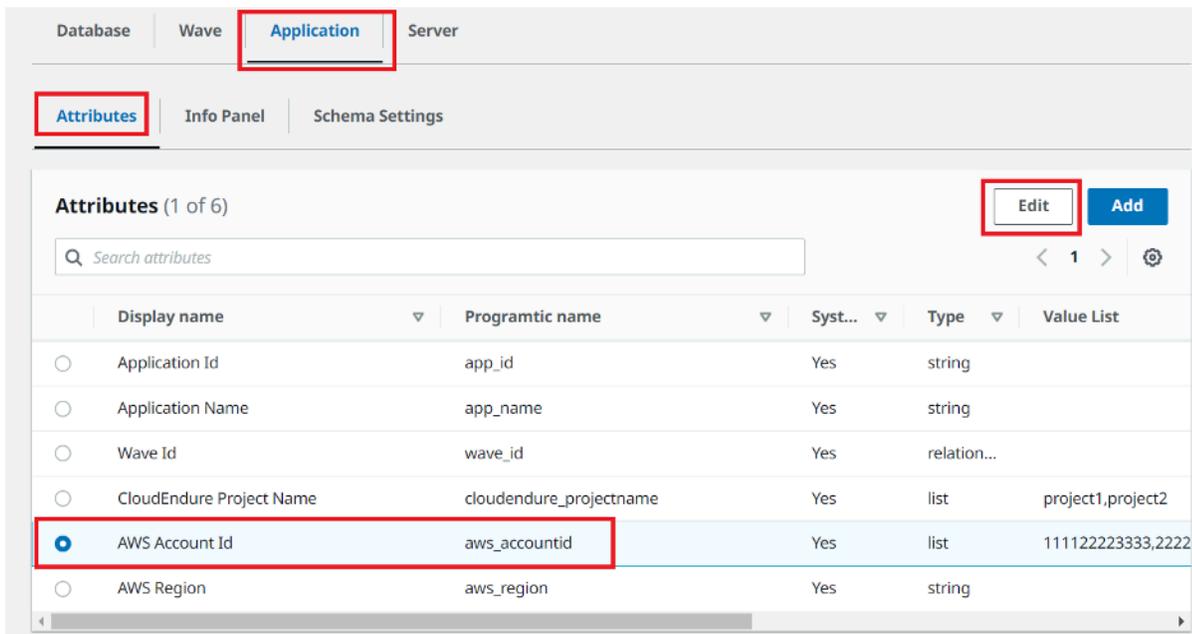
Note

Si une mise à jour est apportée aux paramètres de la pile, il est nécessaire de remplacer les fichiers sur le serveur Web à partir du compartiment frontal pour garantir que toutes les modifications de configuration sont disponibles sur la console Web.

Étape 6 : mise à jour du schéma d'usine

Mettre à jour l'identifiant de compte AWS cible pour les AWS migrations MGN

1. Sur l'interface Web de Migration Factory, sélectionnez Administration, puis Attributs.
2. Sur la page Configuration des attributs, sélectionnez Application, puis Attributs.
3. Sélectionnez l'ID de compte AWS, puis choisissez Modifier.



- Sur la page Modifier l'attribut, mettez à jour la liste des valeurs avec vos identifiants de compte AWS cibles et choisissez Enregistrer.

Note

Si vous avez plusieurs identifiants de AWS compte, séparez-les par des virgules.

Étape 7 : Configuration d'un serveur d'automatisation de la migration

Le serveur d'automatisation de la migration est utilisé pour exécuter l'automatisation de la migration.

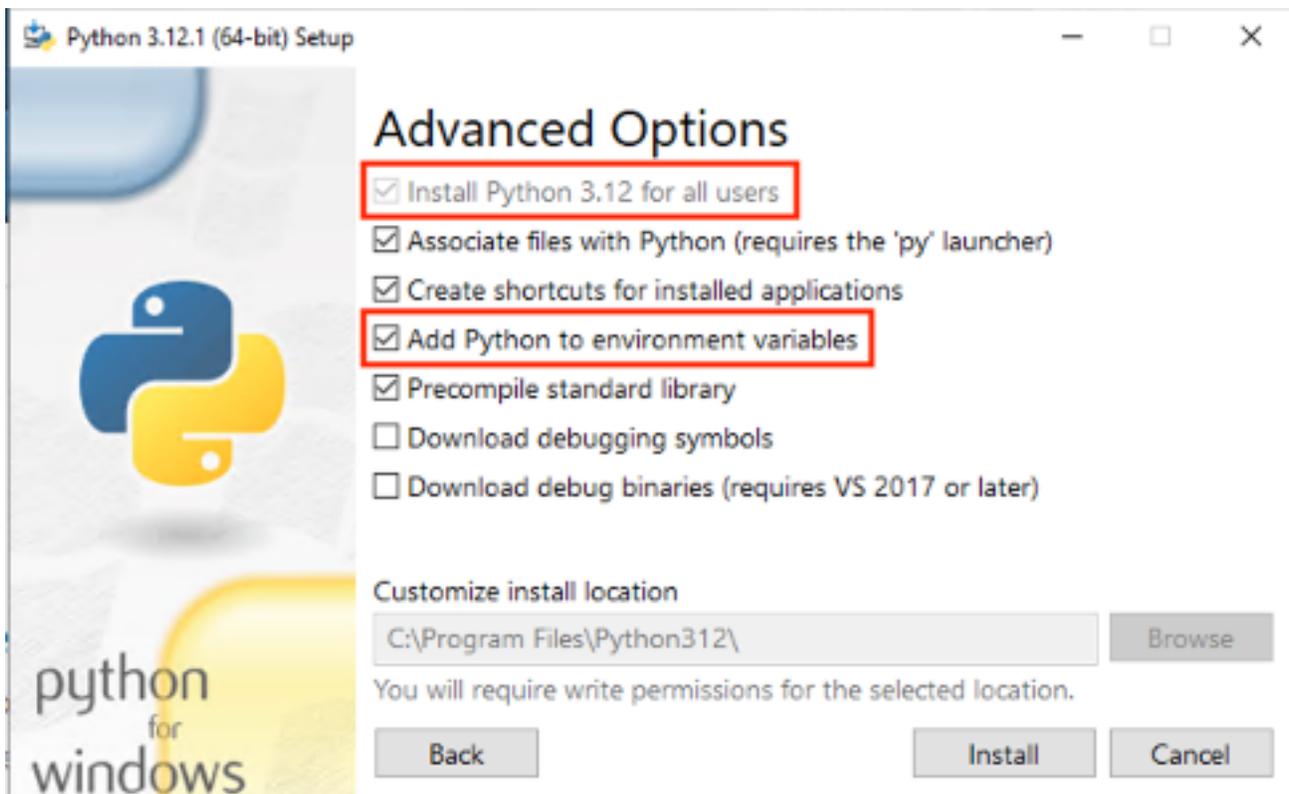
Création d'un serveur Windows Server 2016 ou version ultérieure

Nous vous recommandons de créer le serveur dans votre compte AWS, mais il peut également être créé dans votre environnement sur site. S'il est intégré à un compte AWS, il doit se trouver dans le même compte AWS et dans la même région que Cloud Migration Factory. Pour connaître les exigences du serveur, reportez-vous à la section [Serveur d'automatisation de la migration](#).

Quel que soit l'endroit où vous déployez l'instance Windows, celle-ci doit être déployée en tant qu'installation standard de Windows 2016 ou version ultérieure répondant à vos exigences opérationnelles et de sécurité.

Installation du logiciel requis pour prendre en charge les automatisations

1. Téléchargez [Python v3.12.1](#).
2. Connectez-vous en tant qu'administrateur et installez Python v3.12.1, puis choisissez Personnaliser l'installation.
3. Choisissez Next, puis sélectionnez Installer pour tous les utilisateurs et Ajouter Python aux variables d'environnement. Choisissez Installer.



4. Vérifiez que vous disposez des privilèges d'administrateur `cmd . exe`, ouvrez et exécutez les commandes suivantes pour installer les packages Python un par un :

```
python -m pip install requests
python -m pip install paramiko
python -m pip install boto3
```

Si l'une de ces commandes échoue, mettez à niveau pip en exécutant la commande suivante :

```
python -m pip install --upgrade pip
```

5. Installez [AWS CLI \(interface de ligne de commande\)](#).

6. Effectuez l'installation [PowerShell à l'aide du module for AWS](#), en vous assurant que le AllUsers paramètre -Scope est inclus dans la commande.

```
Install-Module -Name AWSPowerShell -Scope AllUsers
```

7. Ouvrez l'exécution du PowerShell script en ouvrant la PowerShell CLI en tant qu'administrateur et en exécutant la commande suivante :

```
Set-ExecutionPolicy RemoteSigned
```

Configuration AWS des autorisations pour le serveur d'automatisation de la migration et installation de l'agent AWS Systems Manager (agent SSM)

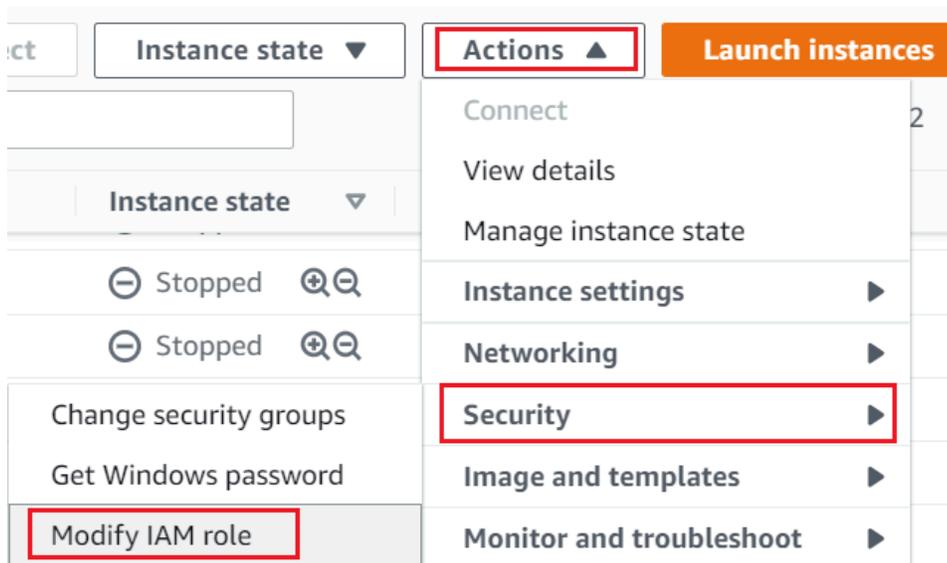
Selon l'endroit où vous déployez le serveur d'exécution de la migration, choisissez l'une des options ci-dessous pour configurer AWS les autorisations pour le serveur d'automatisation de la migration. Le rôle ou la politique IAM fournit l'autorisation au serveur d'automatisation et l'accès à AWS Secrets Manager pour obtenir les clés d'installation des agents et les informations d'identification des comptes de service d'usine. Vous pouvez déployer le serveur d'automatisation de la migration en AWS tant qu'instance EC2 ou sur site.

Option 1 : utilisez la procédure suivante pour configurer les autorisations pour le serveur d'automatisation de la migration dans Amazon EC2 et dans le même compte AWS et dans la même région que l'usine.

1. Accédez à la [AWS CloudFormation console](#) et sélectionnez la pile de la solution.
2. Sélectionnez l'onglet Sorties, sous la colonne Clé, localisez AutomationServerIAMRole et enregistrez la valeur à utiliser ultérieurement dans le déploiement.

Outputs (10)		
<input type="text" value="Search outputs"/>		
Key	Value	Description
AutomationServerIAMPolicy	migration-factory-test-AutomationInstancePolicy	IAM Policy for Migration Automation Server
AutomationServerIAMRole	migration-factory-test-automation-server	IAM Role for Migration Automation Server

3. Accédez à la console [Amazon Elastic Compute Cloud](#).
4. Dans le volet de navigation de gauche, sélectionnez Instances.
5. Sur la page Instances, utilisez le champ Filtrer les instances et entrez le nom du serveur d'exécution de la migration pour rechercher l'instance.
6. Sélectionnez l'instance et sélectionnez Actions dans le menu.
7. Sélectionnez Sécurité dans la liste déroulante, puis sélectionnez Modifier le rôle IAM.

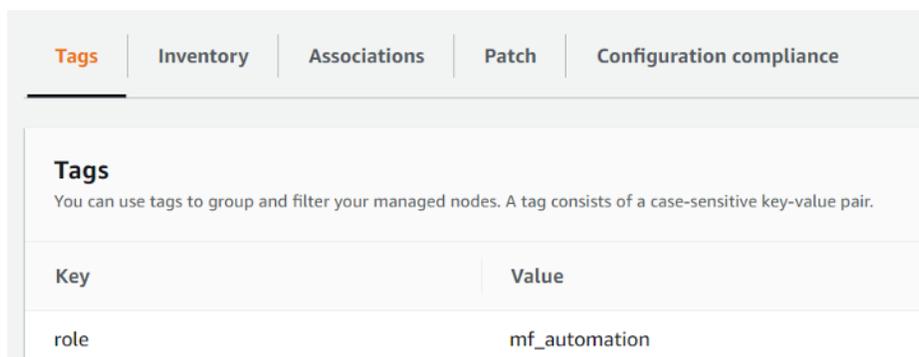


8. Dans la liste des rôles IAM, recherchez et sélectionnez le rôle IAM contenant la valeur **AutomationServerIAMRole** que vous avez enregistré à l'étape 2, puis choisissez Enregistrer.
9. Utilisez votre protocole RDP (Remote Desktop Protocol) pour vous connecter au serveur d'automatisation de la migration.
10. Téléchargez et installez l'[agent SSM](#) sur le serveur d'automatisation de la migration.

Note

Par défaut, l'agent AWS Systems Manager est préinstallé sur le serveur Windows 2016 Amazon Machine Images. Effectuez cette étape uniquement si l'agent SSM n'est pas installé.

11. Ajoutez la balise suivante à l'instance EC2 du serveur d'automatisation de la migration : Key = role et Value =mf_automation.

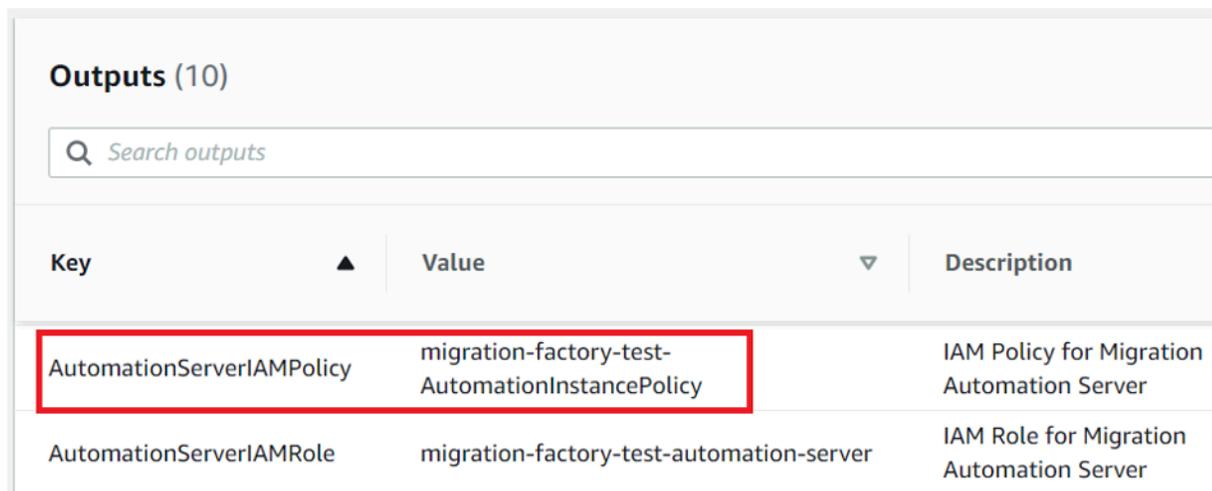


Key	Value
role	mf_automation

12. Ouvrez la console AWS Systems Manager et choisissez Fleet Manager. Vérifiez l'état du serveur d'automatisation et assurez-vous que l'état du ping de l'agent SSM est en ligne.

Option 2 : utilisez la procédure suivante pour configurer les autorisations pour le serveur d'automatisation de la migration sur site.

1. Accédez à la [AWS CloudFormation console](#) et sélectionnez la pile de la solution.
2. Sélectionnez l'onglet Sorties, sous la colonne Clé, localisez AutomationServerIAMPolicy et enregistrez la valeur à utiliser ultérieurement dans le déploiement.



Key	Value	Description
AutomationServerIAMPolicy	migration-factory-test-AutomationInstancePolicy	IAM Policy for Migration Automation Server
AutomationServerIAMRole	migration-factory-test-automation-server	IAM Role for Migration Automation Server

3. Accédez à la [console Identity and Access Management](#).
4. Dans le volet de navigation de gauche, sélectionnez Utilisateurs, puis Ajouter des utilisateurs.
5. Dans le champ Nom d'utilisateur, créez un nouvel utilisateur.
6. Choisissez Suivant.
7. Sur la page Définir les autorisations, sous Options d'autorisations, sélectionnez Joindre directement les politiques. La liste des politiques s'affiche.
8. Dans la liste des politiques, recherchez et sélectionnez la politique contenant la valeur `AutomationServerIAMPolicy` que vous avez enregistrée à l'[étape 2](#).
9. Choisissez Next, puis vérifiez que la bonne politique est sélectionnée.
10. Choisissez Create user (Créer un utilisateur).
11. Après avoir été redirigé vers la page Utilisateurs, choisissez l'utilisateur que vous avez créé à l'étape précédente, puis cliquez sur l'onglet Informations d'identification de sécurité.
12. Dans la section Clés d'accès, choisissez Créer une clé d'accès.

Note

Les clés d'accès se composent d'un ID de clé d'accès et d'une clé d'accès secrète, qui servent à signer les demandes par programme auprès des services AWS. Si vous n'avez pas de clés d'accès, vous pouvez en créer à l'aide de la console de gestion AWS. Une bonne pratique consiste à ne pas utiliser de clés d'accès d'utilisateur racine en lien avec des tâches pour l'exécution desquelles elles ne sont pas requises. Au lieu de cela, [créez un utilisateur IAM administrateur](#) avec des clés d'accès pour vous-même.

La seule fois où vous pouvez voir ou télécharger la clé d'accès secrète est lors de sa création. Vous pouvez pas la récupérer par la suite. En revanche, vous pouvez créer des clés d'accès à tout moment. Vous devez également disposer d'autorisations pour effectuer les actions IAM requises. Pour plus d'informations, consultez la section [Autorisations requises pour accéder aux ressources IAM](#) dans le Guide de l'utilisateur IAM.

13. Pour afficher la nouvelle clé d'accès, choisissez Show (Afficher). Vous ne pourrez pas accéder à la clé d'accès secrète à nouveau une fois que cette boîte de dialogue se sera fermée. Vos informations d'identification s'afficheront comme suit :
- Access key ID: AKIAIOSFODNN7EXAMPLE
 - Secret access key: wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY

14. Pour télécharger la paire de clés, choisissez Télécharger le fichier .csv. Stockez les clés dans un emplacement sûr. Vous ne pourrez pas accéder à la clé d'accès secrète à nouveau une fois que cette boîte de dialogue se sera fermée.

⚠ Important

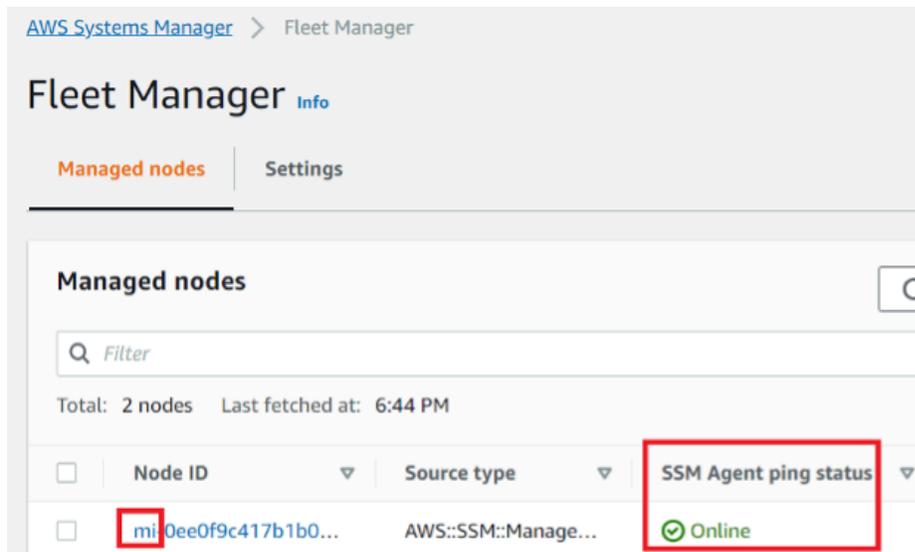
Gardez les clés confidentielles pour protéger votre compte AWS et ne les envoyez jamais par e-mail. Ne les partagez pas en dehors de votre organisation, même si une demande semble provenir d'AWS ou d'Amazon.com. Aucun véritable représentant d'Amazon ne vous demandera jamais de lui fournir votre clé secrète.

15. Après avoir téléchargé le fichier .csv, choisissez Close (Fermer). Lorsque vous créez une clé d'accès, la paire de clés est activée par défaut et vous pouvez utiliser la paire immédiatement.
16. Utilisez votre protocole RDP (Remote Desktop Protocol) pour vous connecter au serveur d'exécution de la migration.
17. Connectez-vous en tant qu'administrateur, ouvrez une invite de commande (CMD.exe).
18. Exécutez la commande suivante pour configurer les AWS informations d'identification sur le serveur. Remplacez <your_access_key_id><your_secret_access key>, et <your_region>par vos valeurs :

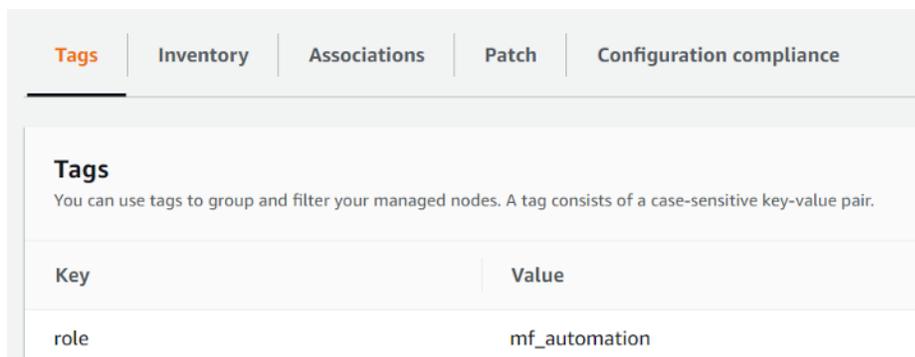
```
SETX /m AWS_ACCESS_KEY_ID <your_access_key_id>  
SETX /m AWS_SECRET_ACCESS_KEY <your_secret_access key>  
SETX /m AWS_DEFAULT_REGION <your_region>
```

19. Redémarrez le serveur d'automatisation.
20. Installez l'agent AWS Systems Manager en mode hybride (serveurs sur site).
 - a. Créez une activation hybride ; consultez la section [Créer une activation \(console\)](#) dans le guide de l'utilisateur d'AWS Systems Manager. Au cours de ce processus, lorsqu'on vous demande de fournir un rôle IAM, sélectionnez un rôle IAM existant et choisissez le rôle avec le suffixe -automation-server qui a été automatiquement créé lors du déploiement de la stack Cloud Migration Factory.
 - b. Connectez-vous au serveur d'automatisation de la migration en tant qu'administrateur.
 - c. Installez l'agent AWS Systems Manager (agent SSM) ; consultez la section [Installation de l'agent SSM pour un environnement hybride et multicloud](#) dans le guide de l'utilisateur d'AWS Systems Manager. Utilisez l'activation hybride créée à l'étape 20.a.

- d. Une fois l'agent installé avec succès, dans la console AWS Systems Manager, sélectionnez Fleet Manager. Identifiez l'ID du nœud avec le préfixe mi- avec le statut en ligne.



- e. Sélectionnez l'ID du nœud et assurez-vous que le rôle IAM est celui que vous avez sélectionné avec le suffixe de serveur d'automatisation.
- f. Ajoutez la balise suivante pour ce nœud hybride : Key = `role` et Value = `mf_automation`. Tout en minuscules.



Étape 8 : tester la solution à l'aide des scripts d'automatisation

Importer les métadonnées de migration dans l'usine

Pour démarrer le processus de migration, téléchargez le [server-list.csv](#) fichier depuis le GitHub référentiel. Le `server-list.csv` fichier est un exemple de formulaire de demande de migration du service AWS MGN permettant d'importer les attributs des serveurs source concernés.

Note

Le fichier .csv et les exemples de scripts d'automatisation faisaient partie du package provenant du même GitHub référentiel.

Vous pouvez personnaliser le formulaire pour votre migration en remplaçant les exemples de données par des données spécifiques à votre serveur et à votre application. Le tableau suivant détaille les données à remplacer pour personnaliser cette solution en fonction de vos besoins de migration.

Nom de champ	Obligatoire ?	Description
nom_onde	Oui	Le nom de la vague est basé sur la priorité et les dépendances du serveur d'applications. Obtenez cet identifiant dans votre plan de migration.
app_name	Oui	Les noms des applications concernées par la migration . Vérifiez que votre groupe d'applications inclut toutes les applications partageant les mêmes serveurs.
aws_account id	Oui	Un identifiant à 12 chiffres qui Compte AWS se trouve dans le profil de votre compte. Pour y accéder, sélectionnez le profil de votre compte dans le coin supérieur droit du, AWS Management Console puis sélectionnez Mon compte dans le menu déroulant.
aws_region	Oui	Région AWS code. Par exemple, us-east-1 .

Nom de champ	Obligatoire ?	Description
		Consultez la liste complète des codes de région .
nom_serveur	Oui	Nom des serveurs locaux concernés par la migration.
server_os_family	Oui	Système d'exploitation (OS) qui s'exécute sur les serveurs sources concernés. Utilisez Windows ou Linux, car cette solution ne prend en charge que ces systèmes d'exploitation.
version du système d'exploitation du serveur	Oui	Version du système d'exploitation exécutée sur les serveurs source concernés.

 **Note**

Utilisez la version du système d'exploitation, pas la version du noyau. Par exemple, utilisez RHEL 7.1, Windows Server 2012 R2 ou CentOS 7.5, 7.6. N'utilisez pas Linux 3.xx, 4.xx ou Windows 8.1.x.

Nom de champ	Obligatoire ?	Description
server_fqdn	Oui	Le nom de domaine complet du serveur source, qui est le nom du serveur suivi du nom de domaine. Par exemple, server123.company.com.
niveau du serveur	Oui	Étiquette permettant d'identifier si le serveur source est un serveur Web, d'application ou de base de données. Nous recommandons de désigner le serveur source comme application s'il fonctionne à plusieurs niveaux, par exemple s'il exécute simultanément les niveaux Web, d'application et de base de données.
environnement_serveur	Oui	Une étiquette pour identifier l'environnement du serveur. Par exemple, dev, test, prod, QA ou pre-prod.
r_type	Oui	Une étiquette pour identifier la stratégie de migration. Par exemple, Retire, Retain, Relocalise, Rehost, Redpurchase, Replatform, Rearchitect, TBC.
ID de sous-réseau	Oui	L'ID de sous-réseau de l'instance Amazon EC2 cible pour la migration après le passage.

Nom de champ	Obligatoire ?	Description
Identifiants du groupe de sécurité	Oui	L'ID du groupe de sécurité pour l'instance Amazon EC2 cible pour la migration après le passage.
Sous-réseau IDS_Test	Oui	ID de sous-réseau cible pour le serveur source qui sera testé.
Groupe de sécurité _IDS_Test	Oui	ID du groupe de sécurité cible pour le serveur source qui sera testé.
instanceType	Oui	Type d'instance Amazon EC2 identifié lors de l'effort de découverte et de planification. Pour plus d'informations sur les types d'instances EC2, reportez-vous à la section Types d'instances Amazon EC2 .
location	Oui	Le type de location, qui est identifié lors des efforts de découverte et de planification. Utilisez l'une des valeurs suivantes pour identifier la location : hôte partagé, dédié ou dédié. Vous pouvez utiliser Shared comme valeur par défaut, sauf si la licence d'une application nécessite un type spécifique.

Nom de champ	Obligatoire ?	Description
Balises	Non	Les balises pour les ressources du serveur, telles que CostCenter =123 ; BU=IT ; Location=US
private_ip	Non	L'adresse IP privée de l'instance cible. Si elle n'est pas incluse, l'instance obtiendra une adresse IP du DHCP.
Je suis un rôle	Non	Rôle IAM pour l'instance cible. S'il n'est pas inclus, aucun rôle IAM ne sera attaché à l'instance cible.

1. Connectez-vous à la console Web Cloud Migration Factory.
2. Sous Gestion de la migration, sélectionnez Importer, puis sélectionnez Sélectionner un fichier. Sélectionnez le formulaire d'admission que vous avez rempli précédemment, puis cliquez sur Suivant.
3. Passez en revue les modifications et assurez-vous qu'aucune erreur ne s'affiche (le message d'information est normal), puis choisissez Next.
4. Choisissez Upload to upload servers.

Accédez aux domaines

Les exemples de scripts d'automatisation inclus dans cette solution se connectent aux serveurs sources concernés pour automatiser les tâches de migration, telles que l'installation de l'agent de réplication et l'arrêt des serveurs sources. Pour tester la solution, un utilisateur de domaine disposant d'autorisations d'administrateur local sur les serveurs source est requis, pour les serveurs Windows et Linux (autorisation sudo). Si Linux n'est pas dans le domaine, d'autres utilisateurs tels qu'un utilisateur LDAP avec des autorisations sudo ou un utilisateur sudo local peuvent être utilisés. Pour plus d'informations sur les tâches de migration automatisées, reportez-vous aux sections Activités

de migration automatisées à l'aide de la console Web Migration Factory et [Activités de migration automatisées à l'aide d'une invite de commande](#).

Procéder à un test de l'automatisation de la migration

Cette solution vous permet de tester l'automatisation de la migration. À l'aide de scripts d'automatisation, le processus de migration importe les données du fichier CSV de migration dans la solution. Des vérifications préalables sont effectuées pour les serveurs sources, l'agent de réplication est envoyé aux serveurs sources, l'état de réplication est vérifié et le serveur cible est lancé depuis l'interface Web de Migration Factory. Pour step-by-step obtenir des instructions sur l'exécution d'un test, reportez-vous aux sections [Activités de migration automatisées à l'aide de la console Web Migration Factory](#) et [Activités de migration automatisées à l'aide d'une invite de commande](#).

Étape 9 : (Facultatif) Créez un tableau de bord de suivi des migrations

Si vous avez déployé le composant optionnel de suivi des migrations, vous pouvez configurer un QuickSight tableau de bord qui visualisera les métadonnées de migration stockées dans la table Amazon DynamoDB.

Utilisez les procédures suivantes pour :

1. [Définissez les QuickSight autorisations et les connexions](#)
2. [Création d'un tableau de bord](#)

Note

Si la Migration Factory est vide et qu'il n'y a aucune donnée sur les vagues, les applications et les serveurs, il n'y aura aucune donnée pour créer un QuickSight tableau de bord.

Définissez les QuickSight autorisations et les connexions

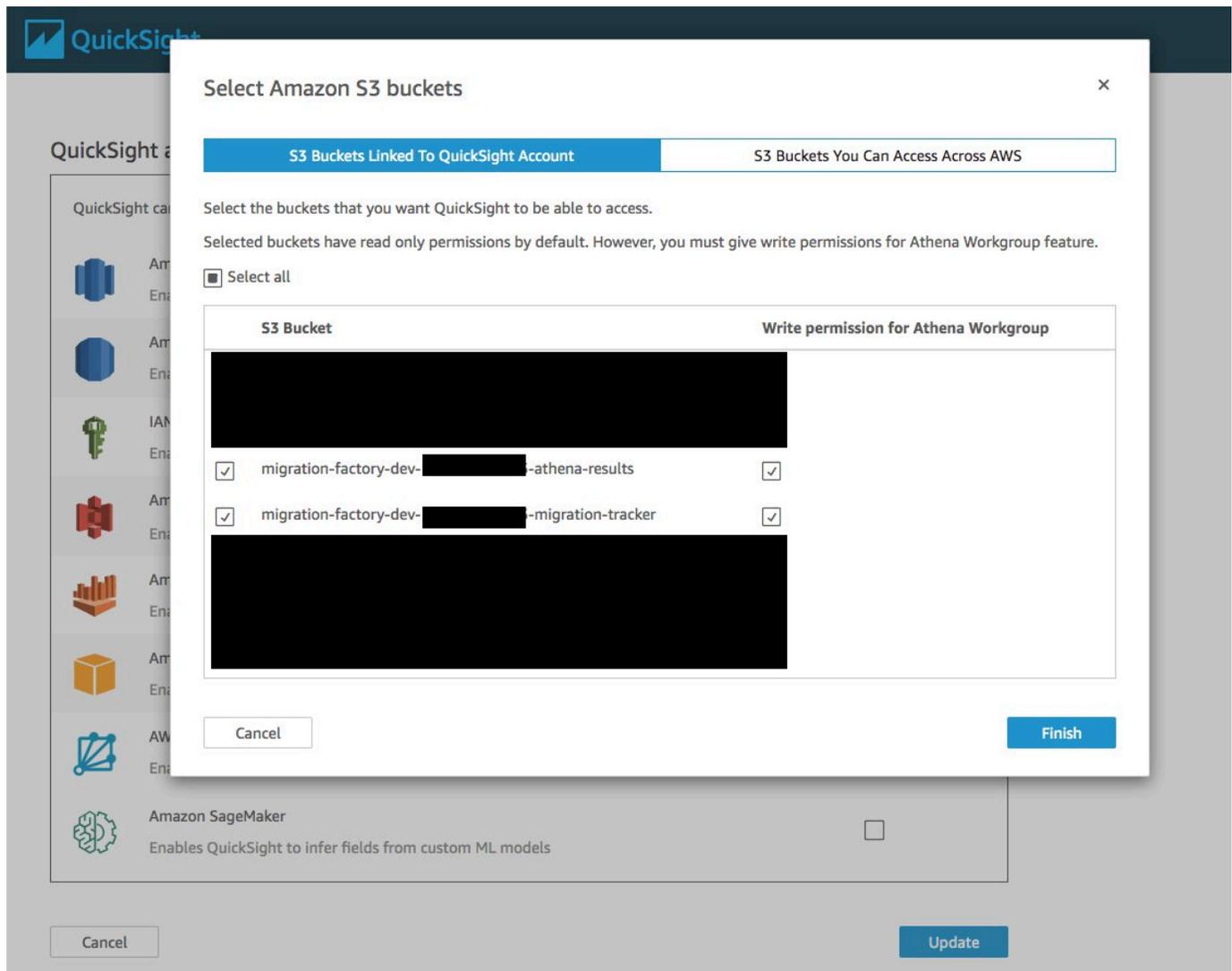
Si vous n'avez pas configuré Amazon QuickSight dans votre compte AWS, reportez-vous à la section [Configuration d'Amazon QuickSight](#) dans le guide de QuickSight l'utilisateur Amazon. Après avoir configuré un QuickSight abonnement, utilisez la procédure suivante pour définir les autorisations et les connexions entre QuickSight et cette solution.

 Note

Cette solution utilise une licence Amazon QuickSight Enterprise. Toutefois, si vous ne souhaitez pas recevoir les rapports par e-mail, les informations et l'actualisation des données toutes les heures, vous pouvez opter pour une licence standard, qui peut également être utilisée avec le suivi des migrations.

Connectez-vous d'abord QuickSight au compartiment Amazon S3 :

1. Accédez à la [console QuickSight](#).
2. Sur la QuickSightpage, cliquez sur l'icône représentant une personne dans le coin supérieur droit, puis sur Gérer. QuickSight
3. Sur la page Nom du compte, dans le volet de menu de gauche, sélectionnez Sécurité et autorisations.
4. Sur la page Sécurité et autorisations, dans la section QuickSight Accès aux services AWS, sélectionnez Gérer.
5. Sur la page d'QuickSight accès aux services AWS, cochez la case Amazon S3.
6. Dans la boîte de dialogue Sélectionner les compartiments Amazon S3, vérifiez que vous êtes dans l'onglet Compartiments S3 liés au QuickSight compte et cochez les cases de droite et de gauche pour les compartiments S3 athena-results et migration-tracker.

**Note**

Si vous l'utilisez déjà QuickSight pour d'autres analyses de données S3, décochez et recochez l'option Amazon S3 pour afficher la boîte de dialogue de sélection du compartiment.

7. Choisissez Finish (Terminer).

Configurez ensuite les autorisations pour Amazon Athena :

1. Sur la page QuickSight d'accès aux services AWS, cochez la case Amazon Athena.
2. Dans la boîte de dialogue des autorisations Amazon Athena, choisissez Next.

3. Dans la boîte de dialogue des ressources Amazon Athena, vérifiez que vous êtes dans l'onglet Compartiments S3 liés au QuickSight compte et vérifiez que les mêmes compartiments S3 sont cochés : athena-results et migration-tracker.

Select Amazon S3 buckets ×

S3 Buckets Linked To QuickSight Account | **S3 Buckets You Can Access Across AWS**

Select the buckets that you want QuickSight to be able to access.
Selected buckets have read only permissions by default. However, you must give write permissions for Athena Workgroup feature.

Select all

S3 Bucket	Write permission for Athena Workgroup
[redacted]	<input type="checkbox"/>
[redacted]	<input type="checkbox"/>
<input checked="" type="checkbox"/> migration-factory [redacted]-athena-results	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> migration-factory [redacted]-migration-tracker	<input checked="" type="checkbox"/>
[redacted]	<input type="checkbox"/>
[redacted]	<input type="checkbox"/>
[redacted]	<input type="checkbox"/>

4. Choisissez Finish (Terminer).
5. Sur la page d'QuickSight accès aux services AWS, sélectionnez Enregistrer.

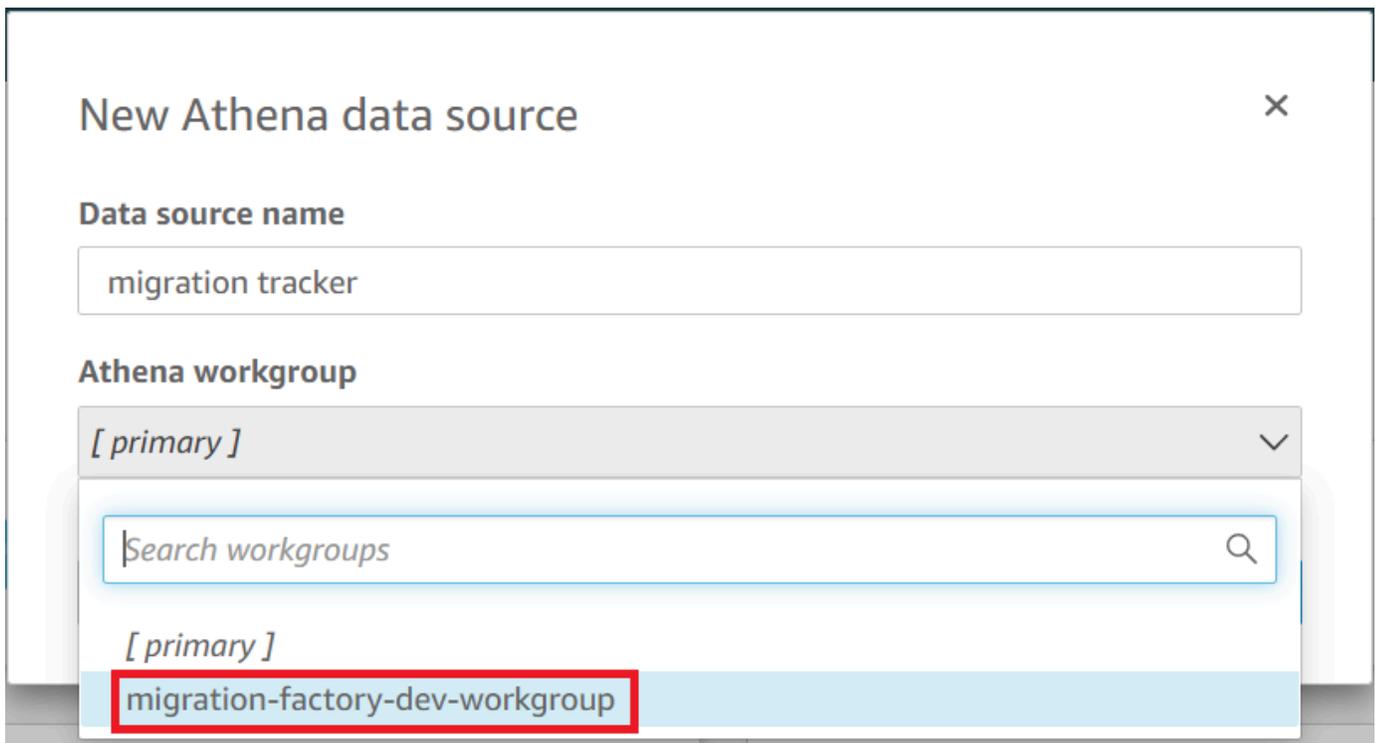
Ensuite, configurez une nouvelle analyse :

1. Sélectionnez le QuickSight logo pour revenir à la QuickSight page d'accueil.
2. Sur la page Analyse, sélectionnez Nouvelle analyse.
3. Choisissez Nouveau jeu de données.
4. Sur la page Créer un ensemble de données, choisissez Athena.
5. Dans la boîte de dialogue de la source de données New Athena, effectuez les actions suivantes :

- a. Dans le champ Nom de la source de données, entrez le nom de la source de données
- b. <migration-factory> Dans le champ Athena workgroup, sélectionnez le -workgroup approprié.

Note

Si vous avez déployé cette solution à plusieurs reprises, il y aura plusieurs groupes de travail. Sélectionnez celui qui a été créé pour votre déploiement actuel.



6. Choisissez Valider la connexion pour vous assurer qu' QuickSight elle peut communiquer avec Athena.
7. Une fois la connexion validée, choisissez Create data source.
8. Dans la boîte de dialogue suivante, Choisissez votre table, effectuez les actions suivantes :
 - a. Dans la liste du catalogue, sélectionnez AwsDataCatalog.
 - b. Dans la liste des bases de données, choisissez <Athena-table>-tracker.
 - c. Dans la liste Tables, choisissez <tracker-name>-general-view.
 - d. Choisissez Select (Sélectionner).

Choose your table ×

migration tracker

Catalog: contain sets of databases.

AwsDataCatalog ▾

Database: contain sets of tables.

migration-factory-dev-tracker ▾

Tables: contain the data you can visualize.

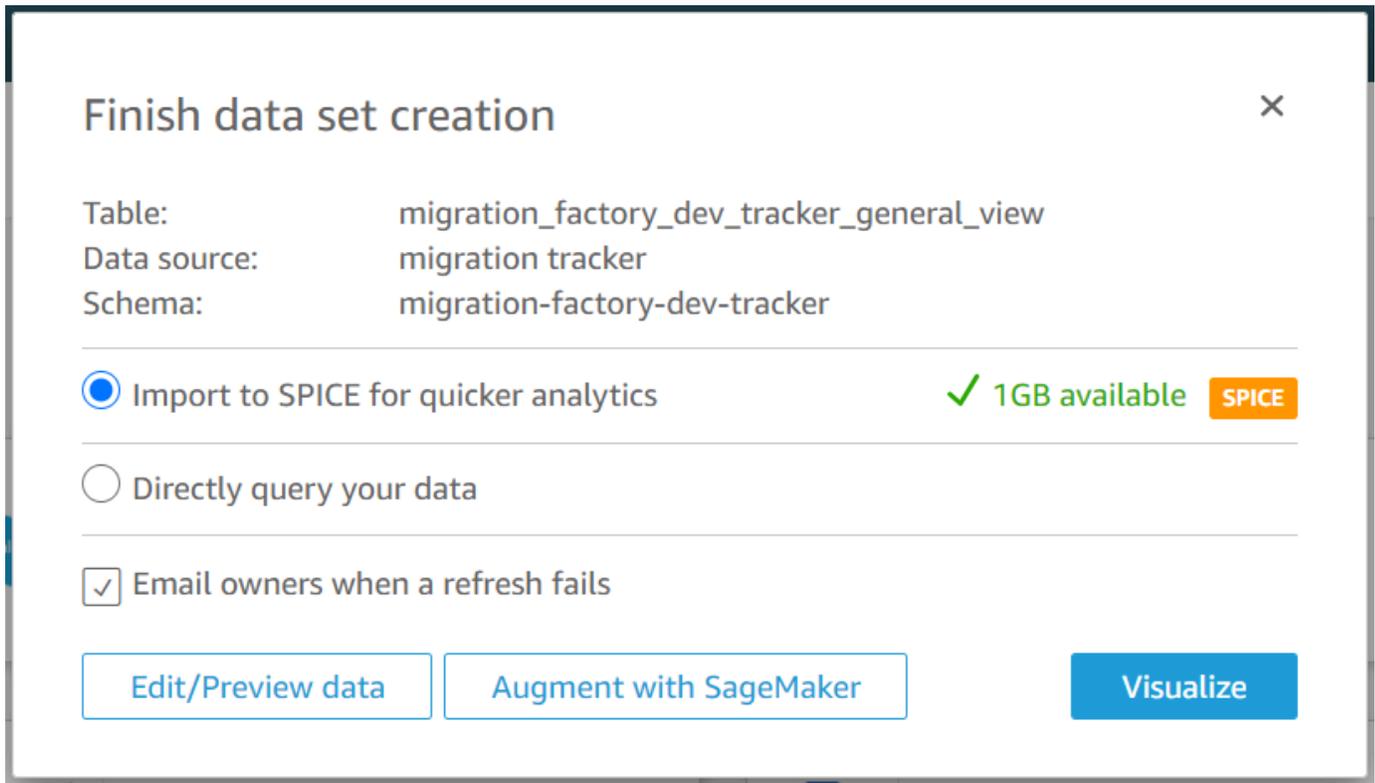
migration_factory_dev_apps

migration_factory_dev_servers

migration_factory_dev_tracker_general_view

[Edit/Preview data](#) [Use custom SQL](#) [Select](#)

9. Dans la boîte de dialogue suivante, Terminer la création du jeu de données, sélectionnez Visualiser.



10. Dans Nouvelle feuille, choisissez Feuille interactive, puis Créer.

Une fois les données importées, vous serez redirigé vers la page Analyse. Toutefois, avant de créer vos visuels, définissez un calendrier pour actualiser votre jeu de données.

1. Accédez à la QuickSight page d'accueil.
2. Dans le volet de navigation, sélectionnez Datasets.
3. Sur la page Ensembles de données, sélectionnez le jeu de données <migration-factory>-general-view.

QuickSight

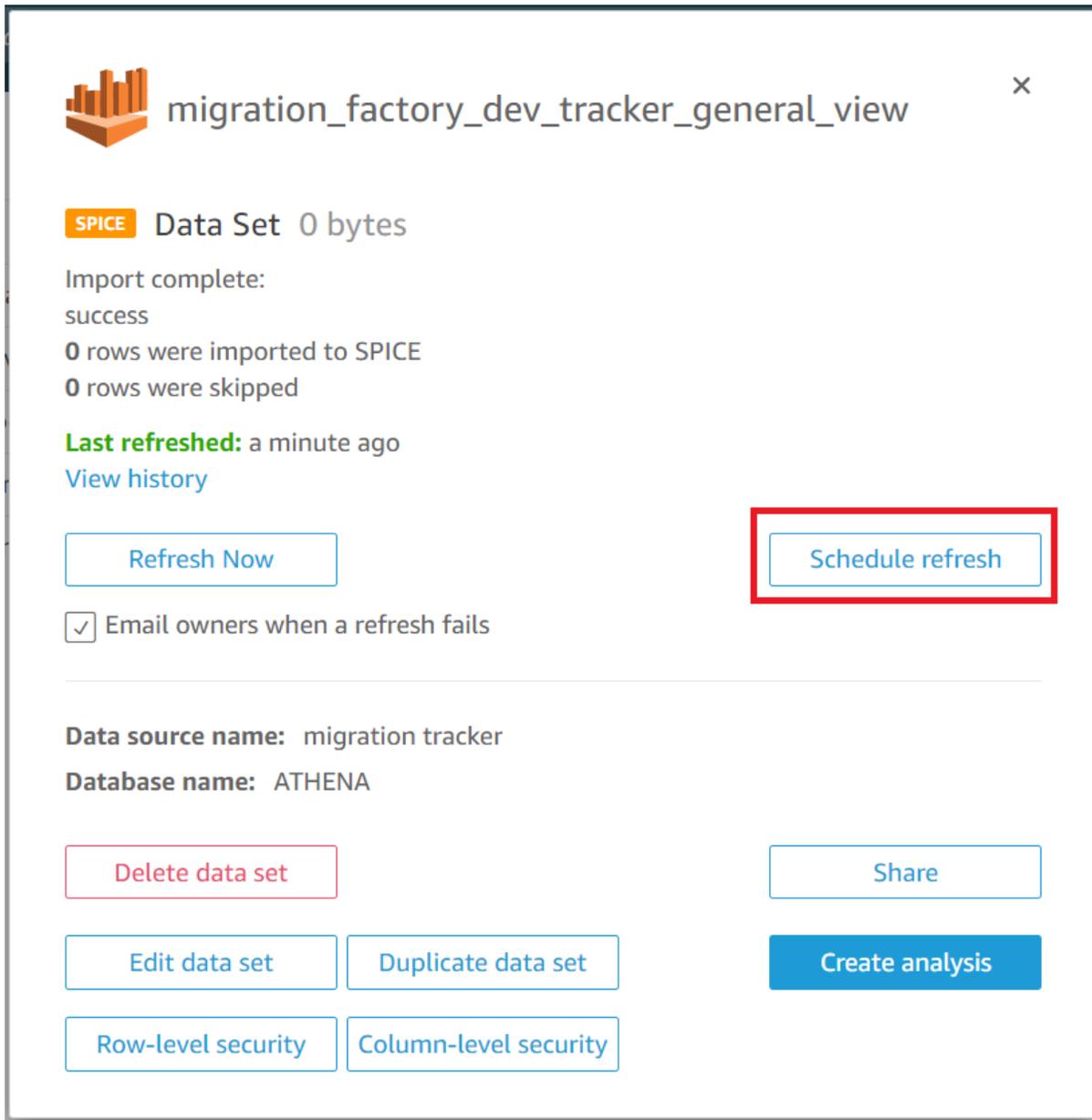
Search for analyses, data sets, and dashboards

- ★ Favorites
- 🕒 Recent
- 📁 My folders
- 📁 Shared folders
- 📊 Dashboards
- 📈 Analyses
- 📄 Datasets**

Datasets

Name	SPICE
migration_factory_dev_tracker_general_view	SPICE
Business Review	SPICE
Web and Social Media Analytics	SPICE
People Overview	SPICE
Sales Pipeline	SPICE

4. Sur la page Ensembles de données -general-view, choisissez l'onglet Actualiser. <migration-factory>



migration_factory_dev_tracker_general_view ×

SPICE Data Set 0 bytes

Import complete:
success
0 rows were imported to SPICE
0 rows were skipped

Last refreshed: a minute ago
[View history](#)

[Refresh Now](#) [Schedule refresh](#)

Email owners when a refresh fails

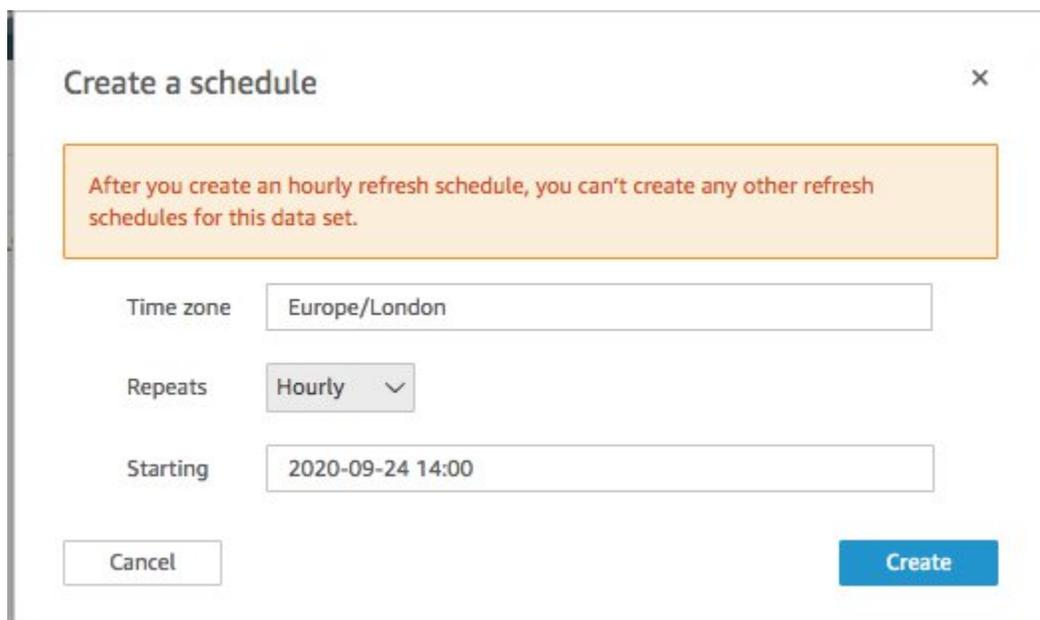
Data source name: migration tracker
Database name: ATHENA

[Delete data set](#) [Share](#)

[Edit data set](#) [Duplicate data set](#) [Create analysis](#)

[Row-level security](#) [Column-level security](#)

5. Choisissez Ajouter un nouveau calendrier.
6. Sur la page Créer un calendrier d'actualisation, sélectionnez Actualisation complète, sélectionnez le fuseau horaire approprié, entrez une heure de début et sélectionnez la fréquence.
7. Choisissez Enregistrer.



Create a schedule ×

After you create an hourly refresh schedule, you can't create any other refresh schedules for this data set.

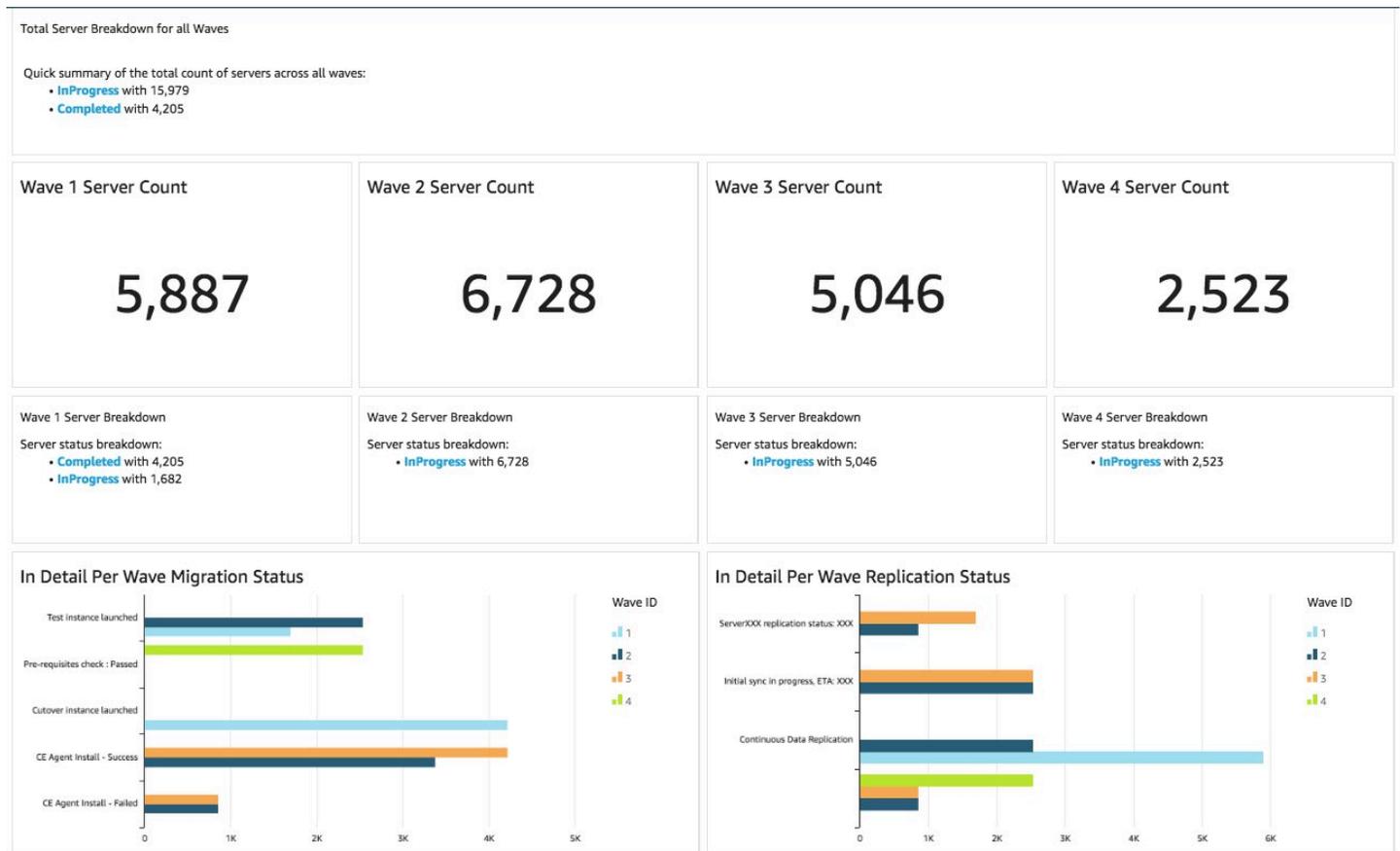
Time zone

Repeats ▾

Starting

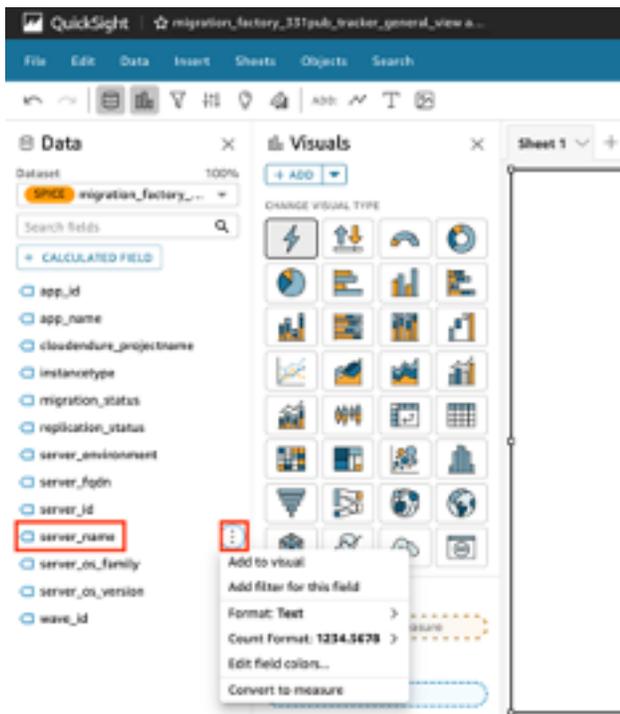
Création d'un tableau de bord

Amazon QuickSight offre la flexibilité de créer un tableau de bord personnalisé qui vous aide à visualiser les métadonnées de votre migration. Le didacticiel suivant crée un tableau de bord contenant un visuel indiquant le nombre de serveurs par vagues et des diagrammes à barres indiquant l'état de la migration. Vous pouvez personnaliser ce tableau de bord pour répondre aux besoins de votre entreprise.

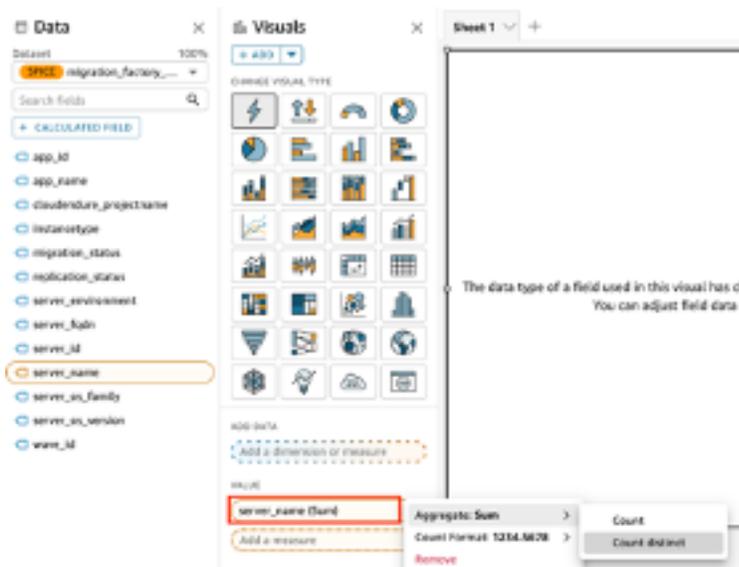


Suivez les étapes ci-dessous pour créer une vue d'ensemble du nombre par vagues de migration. Cette vue compte tous les serveurs du jeu de données regroupés par vague, fournissant ainsi une vue granulaire du nombre total de serveurs dans une vague. Pour créer cette vue, vous allez convertir le nom_serveur en une mesure, ce qui vous permet de compter les noms de serveurs distincts. Ensuite, vous allez créer un filtre vague par onde.

1. Accédez à la QuickSight page d'accueil.
2. Dans le volet de navigation, sélectionnez Analyses.
3. Sélectionnez <migration-factory>-general-view.
4. Sur la page Visualiser, passez le curseur sur le nom du serveur et choisissez les points de suspension sur la droite.



5. Sélectionnez Convertir en mesure pour convertir le jeu de données d'une dimension en mesure. Le texte server_name devient vert pour indiquer que le jeu de données a été converti en mesure.
6. Sélectionnez server_name pour visualiser l'image. Le visuel contiendra un message d'erreur indiquant que les types de données des champs doivent être mis à jour.
7. Dans le volet Visuels, sélectionnez le nom du serveur (Sum), sous Valeur, sélectionnez Aggregate : Sum, puis sélectionnez Count distinct.



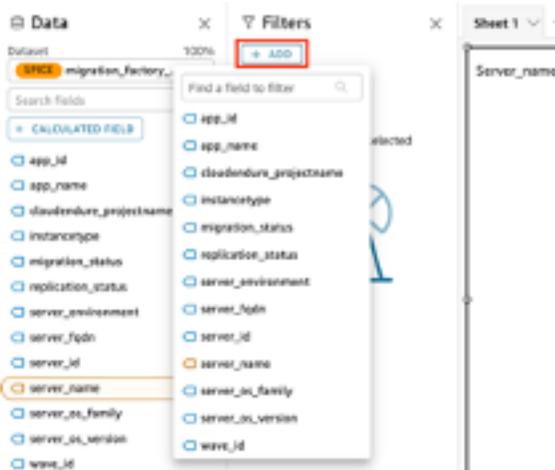
Le décompte du nombre de noms de serveurs uniques présents dans votre ensemble de données s'affiche. Vous pouvez redimensionner la visualisation selon vos besoins pour vous assurer qu'elle affiche clairement les informations sur votre écran.

Note

Il se peut que vous deviez reconvertir votre jeu de données en dimension lorsque vous créez un autre visuel.

Ajoutez ensuite des filtres à la visualisation pour identifier le nombre de serveurs pour chaque vague de migration. Les étapes suivantes appliqueront un filtre `wave_id` à votre visualisation.

1. Vérifiez que la visualisation est sélectionnée. Dans le volet de navigation supérieur, sélectionnez **Filtrer**.
2. Dans le volet Filtres de gauche, choisissez **ADD** et sélectionnez `wave_id` dans la liste.

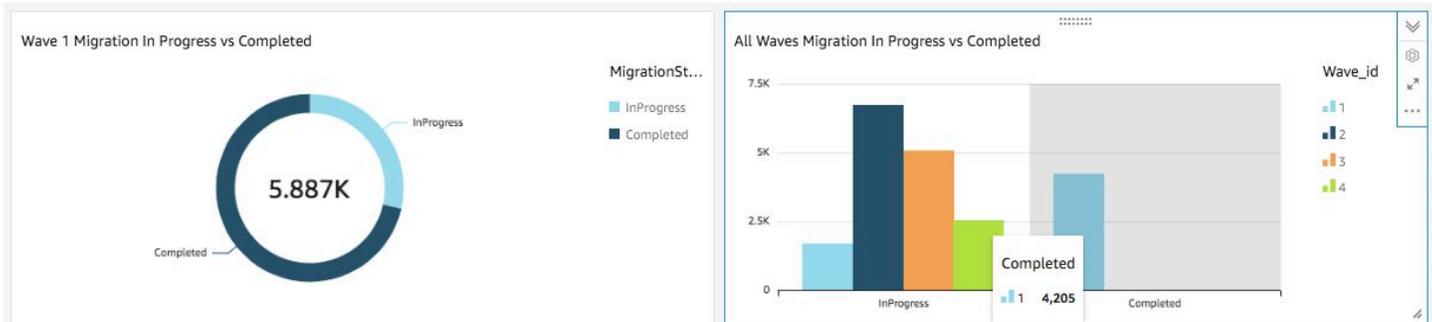


3. Choisissez `wave_id` dans la liste des filtres.
4. Dans le volet Filtre, sous Valeurs de recherche, cochez la case à côté de la valeur 1.
5. Choisissez Appliquer.
6. Dans la visualisation, remplacez le titre par Wave 1 Server Count en double-cliquant sur le titre actuel.

Répétez ces étapes pour les autres vagues visualisées dans votre tableau de bord.

Modifier le volet du filtre

La prochaine visualisation que nous ajouterons au tableau de bord est un graphique en forme de beignet montrant les serveurs en cours de migration par rapport à ceux qui ont terminé la migration. Ce graphique utilise des requêtes SPICE (moteur de calcul parallèle en mémoire) ultrarapides en créant une nouvelle colonne dans l'ensemble de données qui détermine qu'un statut incomplet sera identifié comme étant en cours. Toutes les valeurs de l'ensemble de données qui ne sont pas complétées sont combinées et classées comme en cours.



Note

Par défaut, lorsqu'aucune requête personnalisée n'est appliquée à l'ensemble de données, jusqu'à cinq statuts de migration/réplication peuvent être affichés. Pour cette solution, une MigrationStatusSummary requête est créée dans une nouvelle colonne : `ifelse(migration_status = 'Cutover instance launched', 'Completed', 'InProgress')`

Cette requête combine les valeurs des statuts pour créer une colonne utilisée pour la visualisation. Pour plus d'informations sur la création d'une requête, reportez-vous à la section [Utilisation de l'éditeur de requêtes](#) dans le guide de QuickSight l'utilisateur Amazon.

Procédez comme suit pour créer la MigrationStatusSummary colonne :

1. Accédez à la QuickSight page d'accueil.
2. Dans le volet de navigation, sélectionnez Datasets.
3. Sur la page Ensembles de données, sélectionnez le `<migration-factory>-general-view` jeu de données.
4. Sur la page du jeu de données, choisissez Modifier le jeu de données.

The screenshot shows the Amazon QuickSight interface. On the left, the 'Datasets' menu item is highlighted with a red box. The main panel displays the configuration for a data set named 'migration_factory_dev_tracker_general_view'. The data set is of type 'SPICE' and has 0 bytes. It shows 'Import complete: success' with 0 rows imported and 0 rows skipped. The last refresh was 'a minute ago'. There are buttons for 'Refresh Now', 'Schedule refresh', 'Delete data set', 'Edit data set', 'Duplicate data set', 'Row-level security', 'Column-level security', 'Share', and 'Create analysis'. The 'Edit data set' button is highlighted with a red box. The data source is 'migration tracker' and the database is 'ATHENA'.

5. Dans le volet Champs, choisissez +, puis sélectionnez Ajouter un champ calculé.
6. Sur la page Ajouter un champ calculé, entrez le nom de votre requête SQL, par exemple MigrationStatusSummary.
7. Entrez la requête SQL suivante dans l'éditeur SQL :

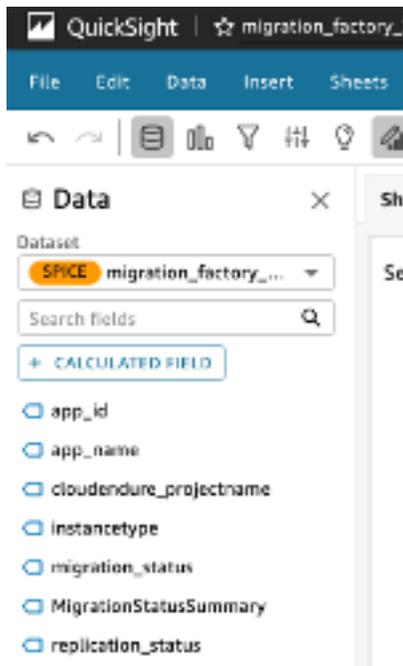
```
ifelse(migration_status = 'Cutover instance launched', 'Completed', 'InProgress')
```

8. Choisissez Enregistrer.

The screenshot shows the 'Add calculated field' dialog in Amazon QuickSight. The dialog title is 'MigrationStatusSummary'. The SQL query 'ifelse(migration_status = 'Cutover instance launched', 'Completed', 'InProgress')' is entered in the editor. The 'Save' button is highlighted.

9. Sur la page Ensemble de données, choisissez Enregistrer et publier.

La requête que vous venez d'ajouter sera répertoriée dans la liste des champs de l'ensemble de données.



Ensuite, créez le tableau de bord.

1. Accédez à la QuickSight page d'accueil.
2. Choisissez Analyses, puis choisissez les analyses migration_factory créées précédemment.
3. Assurez-vous qu'aucun graphique n'est sélectionné dans la feuille 1.
4. Dans le volet Ensemble de données, passez le curseur sur les points de suspension situés à droite MigrationStatusSummary et choisissez les points de suspension.
5. Choisissez Ajouter au visuel.
6. Choisissez ensuite wave_id.
7. Dans le volet Visuels, sélectionnez et déplacez la dimension MigrationStatusSummary vers l'axe X et sélectionnez wave_name comme GROUP/COLOR.

Si vous possédez une licence d'entreprise pour Amazon QuickSight, des informations seront générées une fois les colonnes personnalisées créées. Vous pouvez personnaliser vos récits en fonction de chaque aperçu. Par exemple :



Vous pouvez également personnaliser les données en décomposant les métadonnées en vagues. Par exemple :



(Facultatif) Afficher les informations sur le QuickSight tableau de bord

Note

Vous pouvez utiliser la procédure suivante si vous possédez une licence d'entreprise pour Amazon QuickSight.

Suivez les étapes suivantes pour ajouter un aperçu à votre tableau de bord qui montre le détail des migrations terminées et en cours.

1. Dans le volet de navigation supérieur, sélectionnez Insights.
2. Sur la page Informations, dans la section Nombre d'enregistrements PAR MIGRATIONSTATUSSUMMARY, passez le curseur sur l' MigrationSummaryélément Top 2 et choisissez le + pour ajouter un aperçu au visuel.

Filter

TOP 3 SERVER_IDS

Top 3 server_ids for total count of records are:
2 with 1
4 with 1
5 with 1

Parameters

TOP 3 REPLICATION_STATUSS

Top 3 replication_status for total count of records are:
Continuous Data Replication with 2
Initial sync in progress, ETA: 24 Minutes with 1
Initial sync in progress, ETA: 14 Minutes with 1

Actions

Themes

Settings

COUNT OF RECORDS BY MIGRATIONSTATUSSUMMARY

TOP 2 MIGRATIONSTATUSSUMMARYS

Top 2 MigrationStatusSummary for total count of records are:
Completed with 2
InProgress with 1

3. Personnalisez les informations nécessaires à votre analyse en choisissant Personnaliser le récit sur le visual.

Top ranked

Top 2 MigrationStatusSummary for total count of server_name are:

- **InProgress** with 15,979
- **Completed** with 4,205

Total Server Breakdown for all Waves

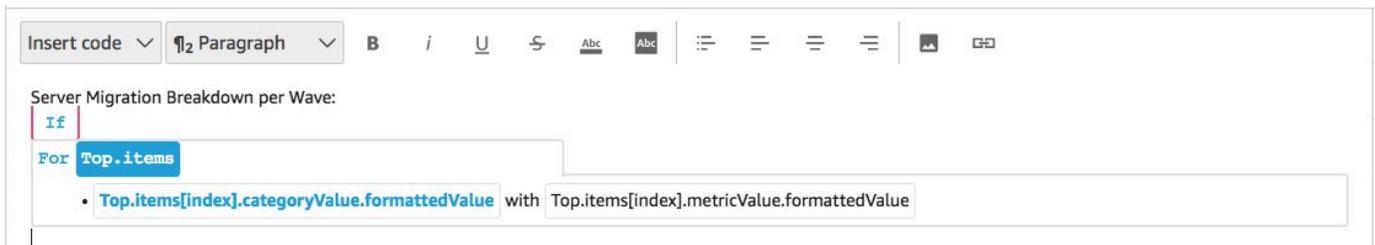
Insert code | Paragraph | B | i | U | | Abc | Abc | | | | | | |

Top If `Top.itemsCount > 1` `Top.itemsCount` `Top.categoryField.name` for total count of `Top.metricField.name` If `Top.itemsCount > 1` are: If `Top.itemsCount < 2` is:

For `Top.items`

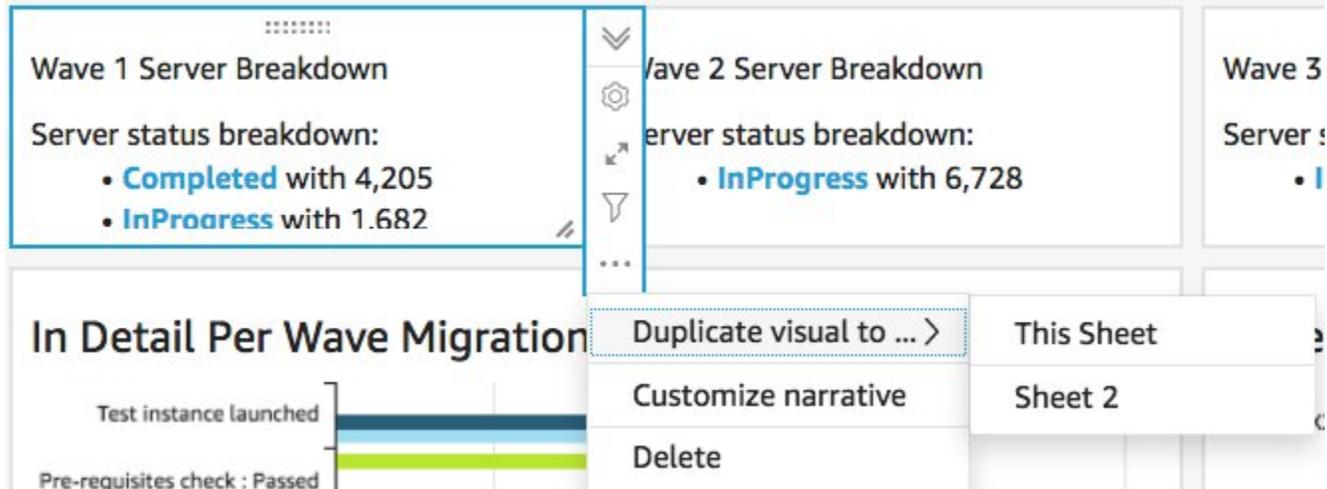
- `Top.items[index].categoryValue.formattedValue` with `Top.items[index].metricValue.formattedValue`

4. Modifiez le récit en fonction de votre cas d'utilisation et choisissez Enregistrer. Par exemple :



Retournez au tableau de bord et filtrez-le pour afficher chaque vague :

5. Dans le volet de menu de gauche, choisissez Filtrer.
6. Cliquez sur le bouton + et sélectionnez wave_id.
7. Sélectionnez une vague à visualiser, puis choisissez Appliquer.
8. Pour visualiser toutes les vagues de migration, dupliquez les visuels en choisissant les points de suspension sur le côté gauche du visuel et en sélectionnant Dupliquer le visuel.



9. Modifiez le filtre pour chaque visuel afin d'afficher une ventilation pour chaque vague de migration.

Ces informations personnalisées résument le nombre total de serveurs sur toutes les vagues. Pour plus d'informations et un guide sur la façon de personnaliser les informations, reportez-vous à la section [Utilisation des informations](#) dans le guide de QuickSight l'utilisateur. Vous pouvez accéder à ce QuickSight tableau de bord depuis n'importe quel appareil et l'intégrer facilement dans vos applications, portails et sites Web. Pour plus d'informations sur les QuickSight tableaux de bord, consultez la section [Travailler avec des tableaux](#) de bord dans le guide de QuickSight l'utilisateur Amazon.

Étape 10 : (Facultatif) Configurer des fournisseurs d'identité supplémentaires dans Amazon Cognito

Si vous avez sélectionné `true` le paramètre facultatif Autoriser la configuration d'un fournisseur d'identité supplémentaire dans Cognito lors du lancement de la pile, vous pouvez en configurer un autre IdPs dans Amazon Cognito pour autoriser la connexion à l'aide de l'IdP SAML existant. Le processus de configuration de l'IdP externe varie selon les fournisseurs. Cette section décrit la configuration d'Amazon Cognito et les étapes génériques pour configurer l'IdP externe.

Procédez comme suit pour collecter des informations auprès d'Amazon Cognito afin de les fournir à l'IdP externe :

1. Accédez à la [CloudFormation console AWS](#) et sélectionnez la pile Cloud Migration Factory sur AWS.
2. Sélectionnez l'onglet Outputs (Sorties).
3. Dans la colonne Clé, recherchez UserPoolId et enregistrez la valeur à utiliser ultérieurement lors de la configuration.
4. Accédez à la [console Amazon Cognito](#).
5. Choisissez le groupe d'utilisateurs qui correspond à l'ID du groupe d'utilisateurs dans la sortie de la pile de solutions.
6. Choisissez l'onglet Intégration des applications et enregistrez le domaine Cognito à utiliser ultérieurement lors de la configuration.

Effectuez les étapes suivantes dans l'interface de gestion de votre IdP existant :

Note

Ces instructions sont génériques et peuvent varier d'un fournisseur à l'autre. Consultez la documentation de votre IdP pour plus de détails sur la configuration des applications SAML.

1. Accédez à l'interface de gestion de votre IdP.
2. Choisissez l'option permettant d'ajouter des applications ou de configurer l'authentification SAML pour une application, puis de créer ou d'ajouter une nouvelle application.
3. Lors de la configuration de cette application SAML, les valeurs suivantes vous seront demandées :

- a. Identifiant (ID d'entité) ou quelque chose de similaire. Entrez la valeur suivante :

```
urn:amazon:cognito:sp:<UserPoolId recorded earlier>
```

- b. URL de réponse (URL d'Assertion Consumer Service) ou quelque chose de similaire. Entrez la valeur suivante :

```
https://<Amazon Cognito domain recorded earlier>/saml2/idpresponse
```

- c. Attributs et revendications ou quelque chose de similaire. Assurez-vous au minimum qu'un identifiant ou un objet unique est configuré avec un attribut fournissant l'adresse e-mail de l'utilisateur.
4. Il y aura soit une URL de métadonnées, soit la possibilité de télécharger un fichier XML de métadonnées. Téléchargez une copie du fichier ou enregistrez l'URL fournie pour une utilisation ultérieure lors de l'installation.
5. Dans le cadre de la configuration, configurez la liste d'accès des utilisateurs de l'IdP autorisés à se connecter à l'application CMF. Tous les utilisateurs autorisés à accéder à l'application dans l'IdP bénéficieront automatiquement d'un accès en lecture seule à la console CMF.

Procédez comme suit pour ajouter le nouvel IdP au groupe d'utilisateurs Amazon Cognito créé lors du déploiement de la pile :

1. Accédez à la [console Amazon Cognito](#).
2. Choisissez le groupe d'utilisateurs qui correspond à l'ID du groupe d'utilisateurs dans la sortie de la pile de solutions.
3. Choisissez l'onglet Sign-in experience (Expérience de connexion).
4. Choisissez Ajouter un fournisseur d'identité, puis choisissez SAML comme fournisseur tiers.
5. Entrez un nom pour le fournisseur ; celui-ci sera affiché à l'utilisateur sur l'écran de connexion au CMF.
6. Dans la section Source du document de métadonnées, fournissez l'URL des métadonnées capturée à partir de la configuration SAML de l'IDP ou téléchargez le fichier XML de métadonnées.
7. Dans la section Attributs de la carte, choisissez Ajouter un autre attribut.
8. Choisissez e-mail pour la valeur de l'attribut du groupe d'utilisateurs. Pour l'attribut SAML, entrez le nom de l'attribut auquel votre IdP externe fournira l'adresse e-mail.
9. Choisissez Ajouter un fournisseur d'identité pour enregistrer cette configuration.

10. Choisissez l'onglet App integration (Intégration d'applications).
11. Dans la section Liste des clients d'applications, choisissez le client d'application Migration Factory (il ne devrait y en avoir qu'un seul) en cliquant sur son nom.
12. Dans la section Interface utilisateur hébergée, choisissez Modifier.
13. Mettez à jour les fournisseurs d'identité sélectionnés en sélectionnant le nouveau nom d'IdP que vous avez ajouté à l'étape 5 et en désélectionnant Cognito User Pool.

 Note

Le pool d'utilisateurs Cognito n'est pas obligatoire car il est intégré à l'écran de connexion au CMF et s'il est sélectionné, il s'affichera deux fois.

14. Sélectionnez Enregistrer les modifications.

La configuration est maintenant terminée. Sur la page de connexion au CMF, vous verrez le bouton Se connecter avec votre identifiant d'entreprise. Le choix de cette option permet d'afficher le fournisseur que vous avez configuré précédemment. Les utilisateurs qui choisissent cette option seront invités à se connecter, puis à revenir à la console CMF une fois connectés avec succès.

Surveillez la solution avec Service Catalog AppRegistry

Cette solution inclut une AppRegistry ressource Service Catalog pour enregistrer le CloudFormation modèle et les ressources sous-jacentes en tant qu'application dans [Service Catalog AppRegistry](#) et [AWS Systems Manager Application Manager](#).

AWS Systems Manager Application Manager vous donne une vue d'ensemble de cette solution et de ses ressources au niveau de l'application, afin que vous puissiez :

- Surveillez ses ressources, les coûts des ressources déployées sur plusieurs piles et Comptes AWS les journaux associés à cette solution à partir d'un emplacement central.
- Affichez les données opérationnelles relatives aux ressources de cette solution (telles que l'état du déploiement, les CloudWatch alarmes, les configurations des ressources et les problèmes opérationnels) dans le contexte d'une application.

La figure suivante illustre un exemple de vue d'application pour la pile de solutions dans Application Manager.

The screenshot displays the AWS Systems Manager Application Manager console. On the left, a sidebar shows a tree view under 'Components (2)' with 'AWS-Systems-Manager-Application-Manager' selected. The main content area is titled 'AWS-Systems-Manager-Application-Manager' and includes a 'Start runbook' button. Below the title is the 'Application information' section, which contains a 'View in AppRegistry' button and details such as 'Application type: AWS-AppRegistry', 'Name: AWS-Systems-Manager-Application-Manager', and 'Application monitoring: Not enabled'. A description states: 'Service Catalog application to track and manage all your resources for the solution'. A navigation bar below this section includes tabs for Overview, Resources, Instances, Compliance, Monitoring, OpsItems, Logs, Runbooks, and Cost. At the bottom, there are two summary cards: 'Insights and Alarms' with a 'View all' button and 'Cost' with a 'View all' button. The cost card shows 'Cost (USD)'.

Pile de solutions dans le gestionnaire d'applications

Activer CloudWatch Application Insights

1. Connectez-vous à la [console Systems Manager](#).

2. Dans le volet de navigation, choisissez Application Manager.
3. Dans Applications, recherchez le nom de l'application pour cette solution et sélectionnez-la.

Le nom de l'application indiquera App Registry dans la colonne Source de l'application et comportera une combinaison du nom de la solution, de la région, de l'ID de compte ou du nom de la pile.

4. Dans l'arborescence des composants, choisissez la pile d'applications que vous souhaitez activer.
5. Dans l'onglet Surveillance, dans Application Insights, sélectionnez Configurer automatiquement Application Insights.

Overview | Resources | Provisioning | Compliance | **Monitoring** | Opsitems | Logs | Runbooks | Cost

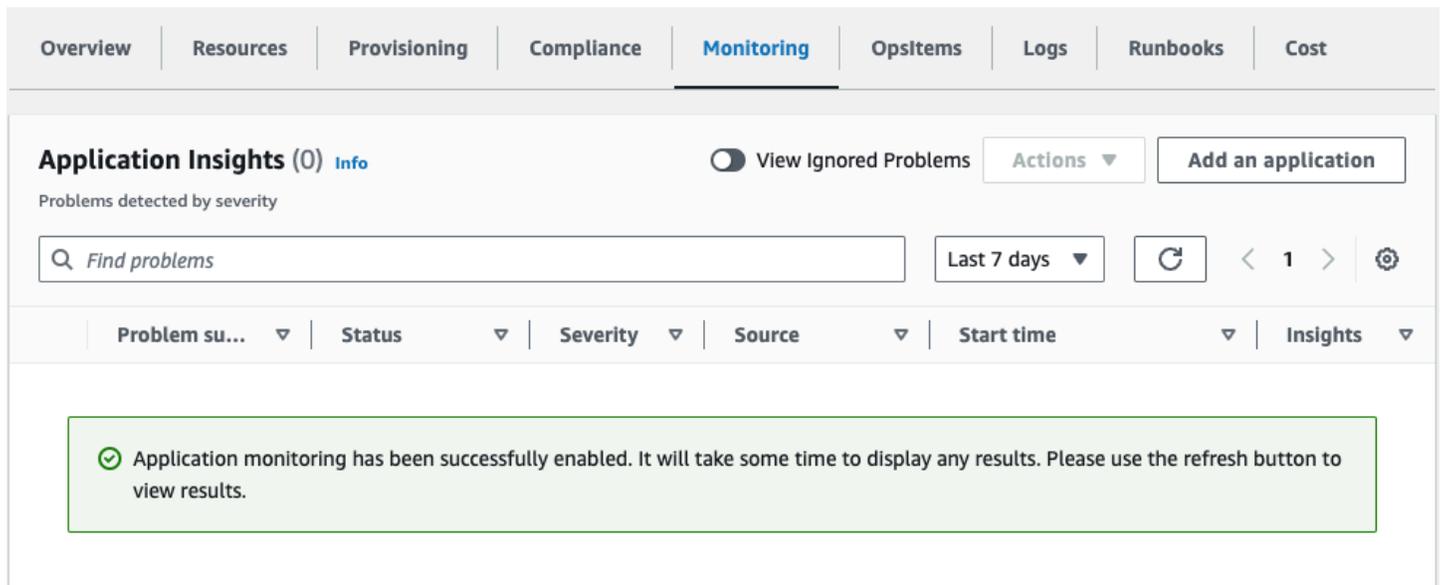
Application Insights (0) [Info](#) View Ignored Problems [Actions](#) [Add an application](#)

Problems detected by severity

Last 7 days < 1 >

Problem su...	Status	Severity	Source	Start time	Insights
Advanced monitoring is not enabled					
<p>When you onboard your first application, a service-linked role (SLR) is created in your account. The SLR is predefined by CloudWatch Application Insights and includes the permissions the service requires to monitor AWS services on your behalf.</p> <p>Auto-configure Application Insights</p>					

La surveillance de vos applications est désormais activée et la boîte de statut suivante apparaît :



Overview | Resources | Provisioning | Compliance | **Monitoring** | OpsItems | Logs | Runbooks | Cost

Application Insights (0) [info](#) View Ignored Problems **Actions** ▾ **Add an application**

Problems detected by severity

Last 7 days ▾ < 1 >

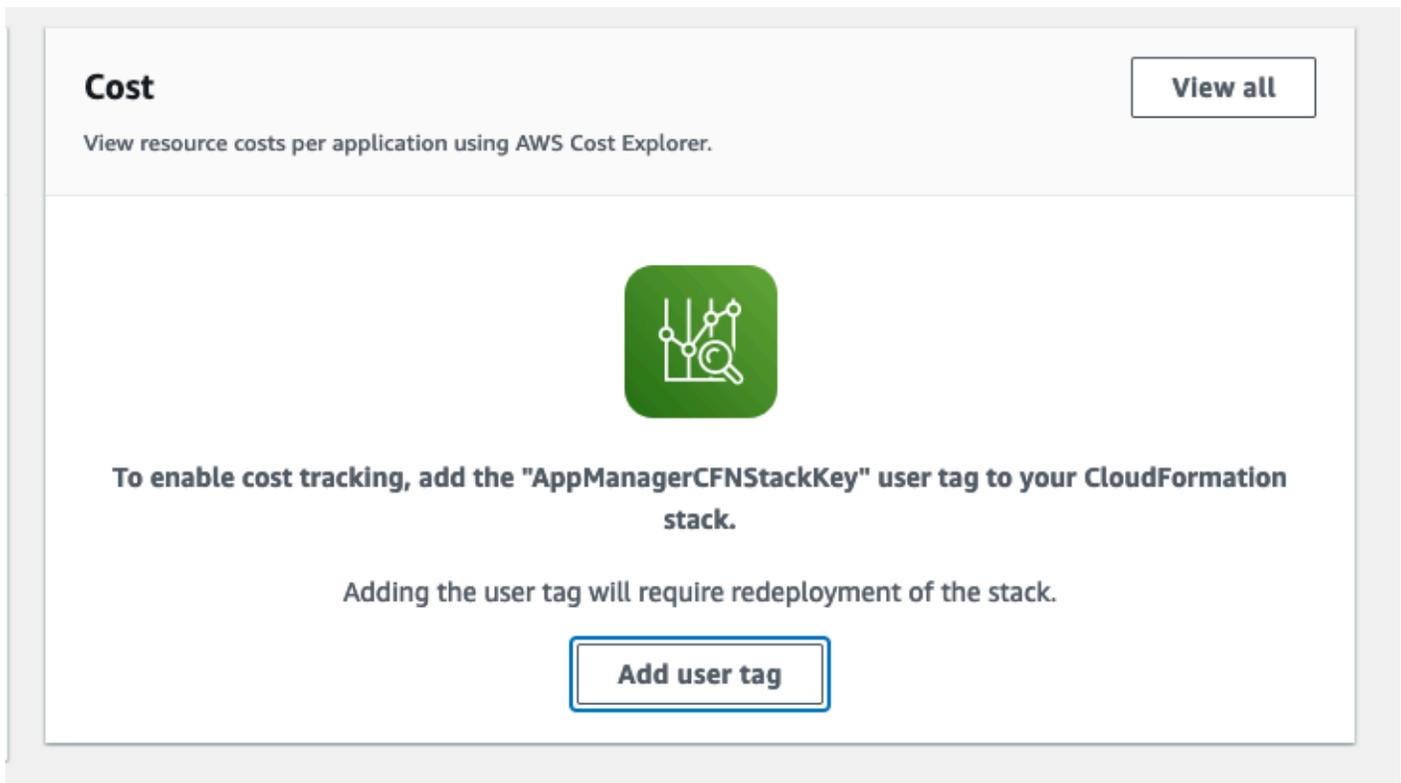
Problem su... ▾ | **Status** ▾ | **Severity** ▾ | **Source** ▾ | **Start time** ▾ | **Insights** ▾

✔ Application monitoring has been successfully enabled. It will take some time to display any results. Please use the refresh button to view results.

Confirmez les étiquettes de coût associées à la solution

Après avoir activé les balises de répartition des coûts associées à la solution, vous devez confirmer les balises de répartition des coûts pour connaître les coûts de cette solution. Pour confirmer les balises de répartition des coûts :

1. Connectez-vous à la [console Systems Manager](#).
2. Dans le volet de navigation, choisissez Application Manager.
3. Dans Applications, choisissez le nom de l'application pour cette solution, puis sélectionnez-la.
4. Dans l'onglet Aperçu, dans Coût, sélectionnez Ajouter un tag utilisateur.



Cost View all

View resource costs per application using AWS Cost Explorer.



To enable cost tracking, add the "AppManagerCFNStackKey" user tag to your CloudFormation stack.

Adding the user tag will require redeployment of the stack.

Add user tag

5. Sur la page Ajouter un tag utilisateur, entrez `confirm`, puis sélectionnez Ajouter un tag utilisateur.

Le processus d'activation peut prendre jusqu'à 24 heures et les données du tag peuvent apparaître.

Activer les balises de répartition des coûts associées à la solution

Après avoir confirmé les étiquettes de coût associées à cette solution, vous devez activer les balises de répartition des coûts pour voir les coûts de cette solution. Les balises de répartition des coûts ne peuvent être activées qu'à partir du compte de gestion de l'organisation.

Pour activer les balises de répartition des coûts :

1. Connectez-vous à la [console AWS Billing and Cost Management and Cost Management](#).
2. Dans le volet de navigation, sélectionnez Balises de répartition des coûts.
3. Sur la page Balises de répartition des coûts, filtrez le `AppManagerCFNStackKey` tag, puis sélectionnez-le parmi les résultats affichés.
4. Choisissez Activer.

AWS Cost Explorer

Vous pouvez consulter l'aperçu des coûts associés à l'application et aux composants de l'application dans la console Application Manager grâce à l'intégration à AWS Cost Explorer. Cost Explorer vous aide à gérer les coûts en fournissant une vue des coûts et de l'utilisation de vos ressources AWS au fil du temps.

1. Connectez-vous à la [console de gestion des AWS coûts](#).
2. Dans le menu de navigation, sélectionnez Cost Explorer pour visualiser les coûts et l'utilisation de la solution au fil du temps.

Mettre à jour la solution

Si vous avez déjà déployé la solution, suivez cette procédure pour mettre à jour la CloudFormation pile de solutions Cloud Migration Factory on AWS afin d'obtenir la dernière version du framework de la solution.

1. Connectez-vous à la [AWS CloudFormation console](#), sélectionnez votre Cloud Migration Factory existant dans la CloudFormation pile de AWS solutions, puis sélectionnez Mettre à jour.
2. Sélectionnez Remplacer le modèle actuel.
3. Sous Spécifier le modèle :
 - a. Sélectionnez l'URL Amazon S3.
 - b. Copiez le lien vers le [dernier modèle](#).
 - c. Collez le lien dans le champ URL d'Amazon S3.
 - d. Vérifiez que l'URL du modèle s'affiche correctement dans la zone de texte URL Amazon S3, puis choisissez Next. Choisissez Suivant à nouveau.
4. Sous Paramètres, passez en revue les paramètres du modèle et modifiez-les si nécessaire. Reportez-vous à [l'étape 2. Lancez le Stack](#) pour plus de détails sur les paramètres.
5. Choisissez Next (Suivant).
6. Sur la page Configurer les options de pile, choisissez Suivant.
7. Sur la page Vérification, vérifiez et confirmez les paramètres. Assurez-vous de cocher la case indiquant que le modèle est susceptible de créer des ressources AWS Identity and Access Management (IAM).
8. Choisissez Afficher l'ensemble de modifications et vérifiez les modifications.
9. Choisissez Mettre à jour la pile pour déployer la pile.

Vous pouvez consulter l'état de la pile dans la AWS CloudFormation console dans la colonne État. Vous devriez recevoir le statut UPDATE_COMPLETE dans environ 10 minutes.

Après avoir mis à jour la pile, il est nécessaire de redéployer les API API Gateway : admin, login, tools et user. Cela garantit que toutes les modifications apportées à la configuration sont disponibles pour toutes les API.

1. Connectez-vous à la [console Amazon API Gateway](#), sélectionnez les API dans le menu de navigation de gauche, puis sélectionnez l'API CMF.

2. Dans les ressources d'API, sélectionnez Actions, puis sélectionnez Déployer l'API.
3. Sélectionnez l'étape de déploiement du produit, puis choisissez Deploy.
4. Répétez les étapes 1 à 3 pour chacune des API Cloud Migration Factory sur AWS.

 Note

La mise à jour de la solution ajoute les versions actuelles des scripts inclus à la pile déployée, mais les versions par défaut des scripts ne seront pas définies sur la dernière version. La raison en est que nous ne voulons pas remplacer les personnalisations qui auraient pu être appliquées à la solution.

Pour utiliser les dernières versions des scripts :

1. Accédez à Cloud Migration Factory sur la console AWS.
2. Dans le menu de navigation, sélectionnez Automatisation, puis Scripts.
3. Sur la page Scripts d'automatisation, pour chaque script, vous souhaitez que la dernière version soit la version par défaut :
 - a. Sélectionnez le script.
 - b. Dans Actions, sélectionnez Modifier la version par défaut.
 - c. Dans Version par défaut du script, choisissez le dernier numéro de version disponible.
 - d. Choisissez Enregistrer.

Résolution des problèmes

Si vous avez besoin d'aide avec cette solution, contactez-nous AWS Support pour ouvrir un dossier d'assistance pour cette solution.

Contacteur AWS Support

Si vous bénéficiez d'[AWS Developer Support](#), d'[AWS Business Support](#) ou d'[AWS Enterprise Support](#), vous pouvez utiliser le Centre de support pour obtenir l'assistance d'experts concernant cette solution. Les sections suivantes fournissent des instructions.

Créer un dossier

1. Connectez-vous au [Centre de Support](#).
2. Choisissez Create case (Créer une demande).

Comment pouvons-nous vous aider ?

1. Choisissez Technique.
2. Dans le champ Service, sélectionnez Solutions.
3. Dans Catégorie, sélectionnez Autres solutions.
4. Pour Severity, sélectionnez l'option qui correspond le mieux à votre cas d'utilisation.
5. Lorsque vous entrez le service, la catégorie et la gravité, l'interface contient des liens vers des questions de dépannage courantes. Si vous ne parvenez pas à résoudre votre question à l'aide de ces liens, sélectionnez Étape suivante : Informations supplémentaires.

Informations supplémentaires

1. Dans le champ Objet, saisissez un texte résumant votre question ou problème.
2. Dans le champ Description, décrivez le problème en détail.
3. Choisissez Joindre des fichiers.
4. Joignez les informations dont AWS Support a besoin pour traiter la demande.

Aidez-nous à résoudre votre cas plus rapidement

1. Entrez les informations demandées.
2. Choisissez Next step: Solve now or contact us (Étape suivante : résolvez maintenant ou contactez-nous).

Résolvez maintenant ou contactez-nous

1. Passez en revue les solutions Solve now.
2. Si vous ne parvenez pas à résoudre votre problème avec ces solutions, choisissez Contactez-nous, entrez les informations demandées, puis choisissez Soumettre.

Désinstallez la solution

Vous pouvez désinstaller la solution Cloud Migration Factory on AWS à partir de l'AWS Management Console ou en utilisant l'AWS Command Line Interface. Vous devez vider manuellement tous les compartiments Amazon Simple Storage Service (Amazon S3) créés par cette solution. Les implémentations de solutions ne suppriment pas automatiquement les compartiments S3 au cas où vous auriez stocké des données à conserver.

Videiement des compartiments Amazon S3

Si vous décidez de supprimer la pile AWS CloudFormation, cette solution est configurée pour conserver le compartiment Amazon S3 créé (à déployer dans une région optionnelle) afin d'éviter toute perte de données accidentelle. Vous devez vider manuellement tous les compartiments S3 avant de supprimer complètement la pile. Suivez les étapes ci-après pour vider le compartiment Amazon S3.

1. Connectez-vous à la [console Amazon S3](#).
2. Dans le volet de navigation de gauche, choisissez Compartiments.
3. Localisez les <stack-name>compartiments S3.
4. Sélectionnez le compartiment S3 et choisissez Vide.

Pour supprimer le compartiment S3 à l'aide de l'AWS CLI, exécutez la commande suivante :

```
aws s3 rm s3://<bucket-name> --recursive
```

Utiliser l'AWS Management Console pour supprimer la pile

1. Connectez-vous à la [console AWS CloudFormation](#).
2. Sur la page Stacks, sélectionnez la pile d'installation de cette solution.
3. Choisissez Delete (Supprimer).

Utilisation AWS Command Line Interface pour supprimer la pile

Déterminez si AWS Command Line Interface (AWS CLI) est disponible dans votre environnement. Pour obtenir des instructions d'installation, reportez-vous à la section [What AWS Command Line Interface Is the](#) in the AWS CLI User Guide. Après avoir vérifié la disponibilité de la AWS CLI, exécutez la commande suivante :

```
aws cloudformation delete-stack --stack-name <installation-stack-name>
```

Guide de l'utilisateur

Les sections suivantes fournissent des conseils sur l'utilisation des différentes fonctionnalités disponibles dans une instance Cloud Migration Factory sur AWS déployée dans le cadre d'une migration à grande échelle vers AWS.

Gestion des métadonnées

La AWS solution Cloud Migration Factory on fournit une banque de données extensible qui permet d'ajouter, de modifier et de supprimer des enregistrements depuis l'interface utilisateur. Toutes les mises à jour des données stockées dans la banque de données sont auditées à l'aide d'estampilles d'audit de niveau record, qui fournissent des horodatages de création et de mise à jour ainsi que des informations sur l'utilisateur. Tous les accès aux mises à jour des enregistrements sont contrôlés par les groupes et les politiques associées assignés à l'utilisateur connecté. Pour plus de détails sur l'octroi d'autorisations aux utilisateurs, reportez-vous à la section [Gestion des autorisations](#).

Visualisation des données

Dans le volet de navigation Migration Management, vous pouvez sélectionner les types d'enregistrements (application, vague, base de données, serveur) conservés dans la banque de données. Après avoir sélectionné une vue, un tableau des enregistrements existants pour le type d'enregistrement choisi s'affiche. Le tableau de chaque type d'enregistrement affiche un ensemble de colonnes par défaut qui peut être modifié par l'utilisateur. Les modifications sont persistantes entre les sessions et sont stockées dans le navigateur et l'ordinateur utilisés pour effectuer les modifications.

Modification des colonnes par défaut affichées dans les tableaux

Pour modifier les colonnes par défaut, sélectionnez l'icône des paramètres située dans le coin supérieur droit de n'importe quel tableau de données, puis sélectionnez les colonnes à afficher. À partir de cet écran, vous pouvez également modifier le nombre de lignes à afficher par défaut et activer l'habillage des lignes pour les colonnes contenant de grandes quantités de données.

Afficher un enregistrement

Pour afficher un enregistrement spécifique dans un tableau, vous pouvez cliquer n'importe où sur la ligne ou cocher la case à côté de la ligne. Si vous sélectionnez plusieurs lignes, aucun

enregistrement ne sera affiché. Cela affichera ensuite l'enregistrement en mode lecture seule sous le tableau de données en bas de l'écran. Les tables par défaut suivantes seront disponibles pour l'enregistrement affiché.

Détails — Il s'agit d'une vue récapitulative des attributs et valeurs requis pour le type d'enregistrement.

Tous les attributs — Cela affiche une liste complète de tous les attributs et de leurs valeurs.

D'autres onglets peuvent être présents en fonction du type d'enregistrement sélectionné pour fournir des données et des informations connexes. Par exemple, les enregistrements d'application comporteront un onglet Serveurs affichant un tableau des serveurs associés à l'application sélectionnée.

Ajouter ou modifier un enregistrement

Les opérations sont contrôlées par type d'enregistrement via les autorisations des utilisateurs. Si un utilisateur n'a pas l'autorisation requise pour ajouter ou modifier un type d'enregistrement spécifique, les boutons Ajouter et/ou Modifier sont grisés et désactivés.

Pour ajouter un nouvel enregistrement :

1. Choisissez Ajouter dans le coin supérieur droit du tableau pour le type d'enregistrement que vous souhaitez créer.

Par défaut, l'écran Ajouter une application affiche les sections Détails et Audit, mais selon le type et les éventuelles personnalisations du schéma, d'autres sections peuvent également s'afficher.

2. Une fois que vous avez rempli le formulaire et résolu toutes les erreurs, choisissez Enregistrer.

Pour modifier un enregistrement existant :

1. Sélectionnez un enregistrement dans le tableau que vous souhaitez modifier, puis choisissez Modifier.
2. Modifiez l'enregistrement et assurez-vous qu'aucune erreur de validation n'existe, puis choisissez Enregistrer.

Supprimer un enregistrement

Si un utilisateur n'est pas autorisé à supprimer un type d'enregistrement spécifique, le bouton Supprimer est grisé et désactivé.

Important

Les enregistrements supprimés de la banque de données ne sont pas récupérables. Nous vous recommandons d'effectuer des sauvegardes régulières de la table DynamoDB ou d'exporter les données pour garantir la présence d'un point de restauration en cas de problème.

Pour supprimer un ou plusieurs enregistrements :

1. Sélectionnez un ou plusieurs enregistrements dans le tableau.
2. Choisissez Delete (Supprimer) et confirmez l'action.

Exportation de données

La majorité des données stockées dans la AWS solution Cloud Migration Factory peuvent être exportées vers des fichiers Excel (.xlsx). Vous pouvez exporter des données au niveau du type d'enregistrement ou une sortie complète de toutes les données et de tous les types.

Pour exporter un type d'enregistrement spécifique :

1. Accédez au tableau pour exporter.
2. Facultatif : Sélectionnez le ou les enregistrements à exporter vers une feuille Excel. Si aucun n'est sélectionné, tous les enregistrements seront exportés.
3. Cliquez sur l'icône Exporter dans le coin supérieur droit de l'écran du tableau de données.

Un fichier Excel portant le nom du type d'enregistrement (par exemple, `servers.xlsx`) sera téléchargé vers l'emplacement de téléchargement par défaut du navigateur.

Pour exporter toutes les données :

1. Accédez à Gestion des migrations, puis sélectionnez Exporter.

2. Cochez Télécharger toutes les données.

Un fichier Excel portant le nom `all-data.xlsx` sera téléchargé dans l'emplacement de téléchargement par défaut du navigateur. Ce fichier Excel contient un onglet par type d'enregistrement, et tous les enregistrements de chaque type seront exportés.

Note

Les fichiers exportés peuvent contenir de nouvelles colonnes car Excel a une limite de 32 767 caractères pour le texte des cellules. Par conséquent, l'exportation tronque le texte de tous les champs contenant plus de données que celles prises en charge par Excel. Pour tous les champs tronqués, une nouvelle colonne avec le nom d'origine ajouté au texte [`truncated - Excel max chars 32767`] est ajoutée à l'exportation. De plus, dans la cellule tronquée, vous verrez également le texte [`n characters truncated, first x provided`]. Le processus de troncature protège contre le scénario dans lequel un utilisateur exporte puis importe le même fichier Excel et, par conséquent, remplace les données par les valeurs tronquées.

Importation de données

La AWS solution Cloud Migration Factory on fournit une fonctionnalité d'importation de données qui permet d'importer des structures d'enregistrement simples dans le magasin de données, par exemple une liste de serveurs. Il peut également importer des données relationnelles plus complexes, par exemple créer un nouvel enregistrement d'application et plusieurs serveurs contenus dans le même fichier et les relier les uns aux autres dans le cadre d'une seule tâche d'importation. Cela permet d'utiliser un processus d'importation unique pour tous les types de données devant être importés. Le processus d'importation valide les données en utilisant les mêmes règles de validation que celles utilisées lorsque l'utilisateur modifie les données dans l'interface utilisateur.

Téléchargement d'un modèle

Pour télécharger des modèles de formulaires d'admission depuis l'écran d'importation, sélectionnez le modèle requis dans la liste des actions. Les deux modèles par défaut suivants sont disponibles.

Modèle avec uniquement les attributs obligatoires : il ne contient que les attributs marqués comme obligatoires. Il fournit l'ensemble minimal d'attributs requis pour importer des données pour tous les types d'enregistrements.

Modèle avec tous les attributs : il contient tous les attributs du schéma. Ce modèle contient des informations d'assistance de schéma supplémentaires pour chaque attribut afin d'identifier le schéma dans lequel il a été trouvé. Ces préfixes auxiliaires des en-têtes de colonne peuvent être supprimés si nécessaire. Si elles sont laissées en place lors d'une importation, les valeurs de la colonne ne seront chargées que dans le type d'enregistrement spécifique et ne seront pas utilisées pour les valeurs relationnelles. Reportez-vous à la section Aide à l'importation du schéma d'en-tête pour plus de détails.

Importation d'un fichier

Les fichiers d'importation peuvent être créés au format .xlsx ou .csv. Pour le format CSV, il doit être enregistré en utilisant le codage UTF8, sinon le fichier apparaîtra vide lors de l'affichage du tableau de validation avant le téléchargement.

Pour importer un fichier :

1. Accédez à Gestion des migrations, puis sélectionnez Importer.
2. Choisissez Sélectionner un fichier. Par défaut, vous ne pouvez sélectionner que des fichiers portant l'.xlsx extension .csv ou. Si le fichier est lu avec succès, le nom et la taille du fichier seront affichés.
3. Choisissez Suivant.
4. L'écran de validation préalable au téléchargement montre le résultat du mappage des en-têtes du fichier aux attributs du schéma, ainsi que la validation des valeurs fournies.
 - Les mappages des en-têtes de colonnes du fichier sont affichés sur les noms des colonnes des tables à l'écran. Pour vérifier quel en-tête de colonne de fichier a été mappé, sélectionnez le nom extensible dans l'en-tête pour plus d'informations sur le mappage, y compris l'en-tête du fichier d'origine et le nom du schéma auquel il a été mappé. Vous verrez un avertissement dans la colonne Validation pour tout en-tête de fichier non mappé ou s'il existe des noms dupliqués dans plusieurs schémas.
 - Tous les en-têtes valident les valeurs de chaque ligne du fichier par rapport aux exigences relatives à l'attribut mappé. Tout avertissement ou erreur dans le contenu du fichier est affiché dans la colonne Validation.
5. Une fois qu'aucune erreur de validation n'est présente, choisissez Next.
6. L'étape Charger les données donne un aperçu des modifications qui seront apportées une fois ce fichier chargé. Pour tout élément pour lequel une modification sera effectuée lors du téléchargement, vous pouvez sélectionner Détails sous le type de mise à jour spécifique pour afficher les modifications qui seront effectuées.

7. Une fois la révision terminée, choisissez Upload pour valider ces modifications dans les données en temps réel.

Un message apparaît en haut du formulaire si le téléchargement est réussi. Toutes les erreurs survenues lors du téléchargement sont affichées sous Aperçu du téléchargement.

Outils d'aide à l'importation du schéma d'en-tête

Par défaut, les en-têtes de colonne du fichier d'admission doivent être définis sur le nom d'un attribut de n'importe quel schéma. Le processus d'importation recherche tous les schémas et tente de faire correspondre le nom de l'en-tête à un attribut. Si un attribut est trouvé dans plusieurs schémas, un avertissement s'affiche, en particulier pour les attributs de relation qui peuvent être ignorés dans la plupart des cas. Toutefois, si l'intention est de mapper une colonne spécifique à un attribut de schéma spécifique, vous pouvez annuler ce comportement en préfixant l'en-tête de colonne par un préfixe d'assistance au schéma. Ce préfixe est au format `{schema name}{attribute name}`, où `{schema name}` est le nom du schéma basé sur son nom système (wave, application, serveur, base de données) et le `{attribute name}` nom système de l'attribut dans le schéma. Si ce préfixe est présent, toutes les valeurs ne seront renseignées que dans les enregistrements de ce schéma spécifique, même si le nom de l'attribut est présent dans d'autres schémas.

Comme le montre la figure suivante, l'en-tête de la colonne C a été préfixé par `[database]` ce qui oblige l'attribut à correspondre à `database_typeattribut` du schéma de base de données.

	B	C	D	E	F	G	H	I
1	database_name	[database]database_type	wave_name	aws_accountid	server_name	server_os_family	server_os_version	server_fqdn
2	importdb1	mssql	importwave1	123456789012	importserver1	linux	RH	importserver1

Aide à l'importation du schéma d'en-tête

Format d'importation d'attributs

Le tableau suivant fournit un guide pour mettre en forme les valeurs d'un fichier d'importation afin de les importer correctement dans les attributs de Cloud Migration Factory.

Type	Format d'importation pris en charge	Exemple
Chaîne	Accepte les caractères alphanumériques et spéciaux.	123456AbCd . !

Type	Format d'importation pris en charge	Exemple
Chaîne à valeurs multiples	Liste de type chaîne, délimitée par un point-virgule.	Item1;Item2;Item3
Mot de passe	Accepte les caractères alphanumériques et spéciaux.	123456AbCd.!
Date	MM/DD/YYYY HH : mm	01/30/2023 10:00
Checkbox	Valeur booléenne, sous forme de chaîne, TRUE pour sélectionné et FALSE pour non sélectionné.	TRUE ou FALSE
Zone de texte	Type de chaîne avec prise en charge des flux en ligne et des retours en chariot.	Test line1 ou Testline 2
Tag	Les balises doivent être mises en forme car key=value; plusieurs balises doivent être séparées par un point-virgule.	TagKey1=Tagvalue1; TagKey2=tagvalue2;
Liste	Si vous définissez un attribut de liste à valeurs uniques, utilisez le même formatage que le type de chaîne, s'il s'agit d'une liste de sélection multiple, alors, selon le type de chaîne à valeurs multiples.	Selection1;Selecti on2;

Type	Format d'importation pris en charge	Exemple
Relation	Accepte les caractères alphanumériques et spéciaux qui doivent correspondre à une valeur basée sur la clé définie dans la définition de l'attribut.	Application1

Gestion des informations d'identification

La AWS solution Cloud Migration Factory propose un gestionnaire d'informations d'identification qui s'intègre à AWS Secrets Manager dans le compte sur lequel l'instance est déployée. Cette fonctionnalité permet aux administrateurs d'enregistrer les informations d'identification du système dans AWS Secrets Manager pour les utiliser dans des scripts d'automatisation sans permettre aux utilisateurs d'accéder directement aux informations d'identification, ni avoir besoin de fournir aux utilisateurs l'accès à AWS Secrets Manager. Les utilisateurs peuvent sélectionner les informations d'identification stockées en fonction de leur nom et de leur description lorsqu'elles les fournissent à une tâche d'automatisation. La tâche d'automatisation récupérera alors uniquement les informations d'identification demandées lors de son exécution sur le serveur d'automatisation, et à ce stade, le rôle IAM attribué à l'instance EC2 sera utilisé pour accéder aux secrets requis.

La zone d'administration du Credentials Manager n'est visible que pour les utilisateurs membres du groupe d'administrateurs au sein d'Amazon Cognito. Les utilisateurs non administrateurs ne pourront consulter les noms et les descriptions des informations d'identification que s'ils sont référencés par le biais d'une automatisation ou d'une autre relation d'enregistrement.

Les trois types de secrets suivants peuvent être enregistrés dans AWS Secrets Manager via Credentials Manager.

Informations d'identification du système d'exploitation — Sous la forme d'un, `username` et `password`.

Clé/valeur secrète — Sous la forme d'un `key` et `value`

Texte brut — Sous la forme d'une chaîne de texte brut unique.

Ajouter un secret

1. Choisissez Ajouter dans la liste des secrets du Credential Manager.
2. Sélectionnez le type de secret à ajouter.
3. Entrez un nom secret. Il s'agira du même nom qui sera affiché dans AWS Secrets Manager pour le nom du secret.
4. Entrez une description secrète. Il s'agira de la même description qui sera affichée dans AWS Secrets Manager pour la description du secret.
5. Entrez les informations d'identification pour le type de secret.

Note

Pour le type secret des informations d'identification du système d'exploitation, il existe une option permettant de sélectionner le type de système d'exploitation qui peut être référencé dans des scripts personnalisés.

Modifier un secret

À l'exception du nom et du type du secret, vous pouvez modifier toutes les propriétés du secret à l'aide de l'interface utilisateur du Credentials Manager.

Suppression d'un secret

Dans la vue Credentials Manager, sélectionnez le secret que vous souhaitez supprimer et choisissez Supprimer. La suppression du secret sera programmée dans AWS Secrets Manager, ce qui peut prendre quelques minutes. Toute tentative d'ajout d'un nouveau secret portant le même nom pendant cette période échouera.

Exécuter l'automatisation depuis la console

La AWS solution Cloud Migration Factory on fournit un moteur d'automatisation permettant aux utilisateurs d'exécuter des tâches sous forme de scripts sur l'inventaire de la banque de données. Grâce à cette fonctionnalité, vous pouvez gérer, personnaliser et déployer toutes les automatisations nécessaires pour mener à bien les activités de end-to-end migration.

Les tâches initiées par AWS CMF sont exécutées sur des serveurs d'automatisation qui peuvent être hébergés sur site AWS Cloud ou sur site. Ces serveurs doivent exécuter Windows avec l'agent AWS SSM installé, ainsi que Python et Microsoft PowerShell. Vous pouvez également installer d'autres frameworks selon les besoins pour les automatisations personnalisées. Reportez-vous à [l'étape 6. Créez un serveur d'automatisation de la migration](#) pour obtenir des informations détaillées sur la création du serveur d'automatisation. Au moins un serveur d'automatisation est requis pour exécuter des tâches depuis la console AWS CMF.

Lors du déploiement, vous pouvez utiliser des scripts pour les tâches les plus courantes nécessaires au réhébergement des charges de travail à l'aide AWS de MGN. Téléchargez les scripts depuis l'interface Web et utilisez-les comme point de départ pour des scripts personnalisés. Pour plus de détails sur la création de scripts d'automatisation personnalisés, reportez-vous à la section [Gestion des scripts](#).

Pour lancer une tâche depuis la console, sélectionnez une vague sur laquelle exécuter l'automatisation, puis sélectionnez Actions, puis choisissez Exécuter l'automatisation. Vous pouvez également sélectionner une tâche sur laquelle exécuter l'automatisation, puis sélectionner Actions, puis choisir Exécuter l'automatisation.

À partir de Run Automation :

1. Entrez le nom du Job. Cela sera utilisé pour identifier la tâche dans le journal.

Note

Les noms des tâches ne doivent pas nécessairement être uniques, car toutes les tâches se voient également attribuer un identifiant unique et des horodatages pour mieux les identifier.

2. Sélectionnez le nom du script dans la liste. Il s'agit d'une liste de tous les scripts qui ont été chargés dans l'instance AWS CMF. Lorsque le travail est soumis, la version par défaut du script sélectionné est exécutée. Pour vérifier les détails du script, y compris la version par défaut actuelle, choisissez Détails connexes sous le nom du script. Reportez-vous à la section Modifier la version par défaut du package de script pour plus de détails sur la mise à jour de la version par défaut des scripts. Lorsque vous sélectionnez le script à exécuter, les paramètres requis sont affichés sous Arguments du script.
3. Dans l'ID d'instance, sélectionnez le serveur d'automatisation pour la tâche dans la liste.

Note

La liste n'affichera que les instances sur lesquelles l'agent SSM est installé et où la balise Managed Instance de est définie sur l'instance EC2 ou pour les serveurs d'automatisation non hébergés par EC2. `role mf_automation`

4. Dans Arguments du script, entrez les arguments d'entrée requis pour le script.
5. Une fois que vous avez saisi tous les paramètres requis et que vous les avez vérifiés, choisissez Submit Automation Job.

Lorsque vous soumettez la tâche d'automatisation, le processus suivant est lancé :

1. Un enregistrement de tâche sera créé avec la vue des tâches de AWS Cloud Migration Factory contenant les détails de la tâche et son statut actuel.
2. Une tâche d'automatisation AWS Systems Manager sera créée et commencera à exécuter le document d'automatisation SSM de AWS Cloud Migration Factory sur le serveur d'automatisation fourni via l'ID d'instance. Le document d'automatisation :
 - a. Télécharge la version par défaut actuelle du package de script depuis le bucket S3 de AWS Cloud Migration Factory vers le serveur d'automatisation dans le `C:\migration\scripts` répertoire.
 - b. Décompresse et vérifie le colis.
 - c. Lance le script python du fichier principal spécifié dans le fichier `package-structure.yml` inclus dans le zip.
3. Une fois que le script python du fichier principal a été lancé, toute sortie du script est capturée par l'agent SSM et introduite CloudWatch. Il est ensuite capturé régulièrement et stocké dans la banque de données AWS Cloud Migration Factory avec l'enregistrement de tâche d'origine, fournissant ainsi un audit complet de l'exécution du travail.
 - a. Si le script nécessite des informations d'identification pour AWS Cloud Migration Factory, il contactera AWS Secrets Manager pour obtenir les informations d'identification du compte de service. Si les informations d'identification sont incorrectes ou absentes, le script renverra un échec.
 - b. Si le script doit accéder à d'autres secrets stockés à l'aide de la fonctionnalité AWS Cloud Migration Factory Credentials Manager, il contactera AWS Secrets Manager pour accéder à ces informations d'identification. Si cela n'est pas possible, le script renverra un échec.

4. Une fois le script python du fichier principal terminé, le résultat de ce script déterminera le statut fourni à l'enregistrement de tâche AWS Cloud Migration Factory. Un retour différent de zéro sera défini sur `Job Status.Failed`

Note

Actuellement, si un échec survient lors de l'exécution initiale du document AWS SSM, il n'apparaît pas dans l'interface Web. Les échecs ne sont enregistrés qu'une fois que le fichier principal python est lancé.

Toutes les tâches lancées depuis la console expireront au bout de 12 heures si elles n'ont pas renvoyé un statut de réussite ou d'échec.

Exécuter des automatisations à partir d'une invite de commande

Bien que nous vous recommandions d'exécuter des tâches d'automatisation via l'interface Web, vous pouvez exécuter des scripts d'automatisation manuellement à partir d'une ligne de commande sur le serveur d'automatisation. Cela fournit des options supplémentaires lorsque les entreprises ne peuvent ou ne veulent pas utiliser la combinaison de AWS CMF Credentials Manager, AWS Secrets Manager et AWS Systems Manager dans l'environnement, ou si les AWS utilisateurs de Cloud Migration Factory doivent fournir des codes d'accès uniques à authentification multifactorielle (MFA) pour se connecter à Cloud Migration Factory. AWS

Lorsque les scripts sont exécutés depuis la ligne de commande, l'historique des tâches et les journaux ne sont pas disponibles dans la vue Tâches de l'interface Web. La sortie du journal sera uniquement dirigée vers la sortie de la ligne de commande. Les scripts peuvent toujours accéder à Cloud Migration Factory sur les AWS API pour lire et mettre à jour les enregistrements, ainsi qu'à d'autres fonctions disponibles via les API.

Nous vous recommandons de stocker les scripts dans la bibliothèque de scripts ou dans un autre emplacement central pour vous assurer que vous accédez à la dernière version du script ou à la version dont l'utilisation est actuellement approuvée et que vous l'utilisez.

Exécution manuelle d'un package d'automatisation

Cette section décrit les étapes à suivre pour télécharger un package depuis Cloud Migration Factory AWS et l'exécuter manuellement sur le serveur d'automatisation. Vous pouvez également suivre le

processus pour les autres emplacements de source de script en remplaçant les étapes 1 et 2 par les étapes de téléchargement spécifiques à la source.

1. Si les scripts sont stockés dans Cloud Migration Factory sur AWS, suivez les étapes décrites dans [Télécharger les packages de scripts](#) pour obtenir le fichier zip du package d'automatisation.
2. Copiez le fichier zip vers un emplacement sur le serveur d'automatisation, par exemple : `\migrations\scripts`, et décompressez le contenu.
3. Copiez le `FactoryEndpoints.json` fichier dans chacun des dossiers de scripts décompressés. Configurez le fichier avec les points de terminaison d'API spécifiques pour l'instance Cloud Migration Factory qui contient les serveurs ou les autres enregistrements auxquels cette tâche d'automatisation fera référence. Reportez-vous à la section [Création du fichier FactoryEndpoints.json](#) pour plus d'informations sur la création de ce fichier.
4. Sur la ligne de commande, assurez-vous que vous vous trouvez dans le répertoire racine du package décompressé, puis exécutez la commande suivante :

```
python [package master script file] [script arguments]
```

fichier de script principal du package — celui-ci peut être obtenu à partir du `Package-Structure.yml` dessous de la `MasterFileName` clé.

arguments du script : les informations relatives aux arguments sont fournies `Package-Structure.yml` sous la `Arguments` clé.

5. Les scripts demanderont les informations d'identification requises pour Cloud Migration Factory sur les AWS API et le serveur distant. Toutes les informations d'identification saisies manuellement sont mises en cache dans la mémoire pendant toute la durée de ce processus afin d'éviter de saisir à nouveau les mêmes informations d'identification. Si vous entrez des arguments de script pour accéder aux secrets stockés à l'aide de la fonctionnalité Credentials Manager, l'accès à AWS Secrets Manager et aux secrets associés est requis. Si la récupération du secret échoue pour une raison quelconque, le script demandera les informations d'identification de l'utilisateur.

Création du FactoryEndpoints fichier .json

Nous vous recommandons de créer ce fichier une seule fois lors du déploiement de la solution Cloud Migration Factory sur AWS, car le contenu ne change pas après le déploiement initial, et de le stocker dans un emplacement central sur le serveur d'automatisation. Ce fichier fournit les scripts

d'automatisation avec les points de terminaison de l'API Cloud Migration Factory sur AWS et d'autres paramètres clés. Voici un exemple du contenu par défaut du fichier :

```
{
  "UserApiUrl":
  "https://cmfuserapi.execute-api.us-east-1.amazonaws.com",
  "Region": "us-east-1",
  "UserPoolId": "us-east-1_AbCdEfG",
  "UserPoolClientId": "123456abcdef7890ghijk",
  "LoginApiUrl":
  "https://cmfloginapi.execute-api.us-east-1.amazonaws.com"
}
```

Note

La plupart des informations requises pour composer ce fichier pour une instance AWS Cloud Migration Factory déployée sont disponibles dans l'onglet AWS CloudFormation Sorties de la pile déployée, à l'exception du `UserPoolClientId`. Obtenez cette valeur en suivant les étapes suivantes :

1. Accédez à la console Amazon Cognito.
2. Ouvrez la configuration du groupe d'utilisateurs.
3. Sélectionnez Intégration des applications, qui fournira la configuration du client de l'application.

```
{
  "UserApiUrl": <UserApi-value>,
  "Region": <Region-value>,
  "UserPoolId": <UserPoolId-value>,
  "UserPoolClientId": <Amazon-Cognito-user-pool-app-clients-console>,
  "LoginApiUrl": <LoginApi-value>
}
```

Remplacez *< LoginApi -value>*, *< UserApi -value>* et *< UserPoolId -value>* *<Region-value>* par les valeurs correspondantes que vous avez extraites de la console Outputs. **AWS CloudFormation** N'ajoutez pas de barre oblique (/) à la fin des URL.

Le fichier possède une `DefaultUser` clé facultative. Vous pouvez définir la valeur de cette clé sur l'ID utilisateur par défaut à utiliser pour accéder à Cloud Migration Factory sur AWS instance afin

d'éviter d'avoir à saisir à chaque fois. Lorsque vous êtes invité à saisir l'ID utilisateur de Cloud Migration Factory, vous pouvez saisir un ID utilisateur ou utiliser la valeur par défaut en appuyant sur la touche Entrée. Vous ne pouvez le faire que lorsque les scripts sont exécutés manuellement.

Lancez des jobs AWS MGN depuis Cloud Migration Factory

La AWS solution Cloud Migration Factory on a intégré l'automatisation pour initier et gérer la migration de Rehost à l'aide de AWS MGN. Ces automatisations permettent aux équipes de migration de gérer tous les aspects de leur migration à partir d'une interface utilisateur unique, en combinant les actions clés disponibles dans la console de service AWS MGN avec la bibliothèque d'automatisation AWS Cloud Migration Factory qui étend les fonctionnalités avec des scripts prédéfinis pour les migrations de masse, ce qui contribue à accélérer les activités de migration. Reportez-vous à la section Liste des activités de migration automatisées pour le service de migration d' AWS applications (AWS MGN) pour obtenir la liste complète des tâches d'automatisation AWS MGN disponibles. L'utilisation de AWS Cloud Migration Factory permet également des migrations multicomptes fluides à l'aide de AWS MGN, car Cloud Migration Factory a la capacité d'assumer automatiquement des rôles dans différents comptes cibles en fonction de l'application Cloud Migration Factory et des définitions de serveur en cours de migration.

Activités préalables

1. Compte cible AWS CMF CloudFormation déployé dans chaque compte cible. Pour plus d'informations, consultez la section [AWS CloudFormation modèles](#) de ce document.
2. [AWS Le MGN est initialisé dans chaque compte cible.](#)

Définition initiale

La définition de l'inventaire sur site s'effectue par la création d'éléments de vague, d'application et de serveur à l'aide de l'interface utilisateur ou de l'importation d'un formulaire d'admission au format CSV. Ces définitions sont utilisées pour fournir les identités des serveurs sur site ainsi que les paramètres EC2 cibles, ainsi que d'autres données requises pour gérer l'activité de migration.

Définition de l'interface utilisateur

Pour utiliser la fonctionnalité AWS MGN, vous devez créer un enregistrement wave, avec les enregistrements d'application associés, et enfin un ou plusieurs enregistrements de serveur associés aux applications. L'enregistrement wave est utilisé pour regrouper les applications et ne fournit pas

de paramètres à l'automatisation, tandis que l'enregistrement d'application définit l' Compte AWS ID cible et Région AWS vers lequel l'application sera migrée. Les enregistrements du serveur fournissent les actions d'automatisation et l'intégration AWS MGN, les paramètres cibles pour les instances EC2, tels que le type d'instance, les sous-réseaux, les groupes de sécurité, etc.

Lors de la définition d'un serveur dans la banque de données AWS CMF à utiliser avec la fonctionnalité AWS MGN, le serveur doit être configuré avec une stratégie de migration de type Rehost. Une fois que Rehost est sélectionné, les attributs supplémentaires requis pour cette fonctionnalité s'affichent à l'écran. Les attributs suivants doivent être renseignés pour lancer avec succès une tâche de migration AWS MGN :

Obligatoire

Famille de systèmes d'exploitation de serveur : définissez Linux ou Windows selon la famille de systèmes d'exploitation.

Version du système d'exploitation du serveur : définissez la version détaillée du système d'exploitation exécutée sur le serveur.

Type d'instance : type d'instance EC2 à utiliser.

Location — Hébergement partagé, hôte dédié.

Identifiants des groupes de sécurité : liste des groupes de sécurité qui seront attribués à l'instance lorsque le transfert final sera lancé.

Identifiants des groupes de sécurité - Test — Liste des groupes de sécurité qui seront attribués à l'instance lorsque le test sera lancé.

Conditionnel

Identifiants de sous-réseau : ID de sous-réseau auquel attribuer cette instance EC2 lorsque le passage final est lancé. (non applicable lorsque l'ID d'interface réseau est spécifié)

Identifiants de sous-réseau - Test — ID de sous-réseau auquel attribuer cette instance EC2 lorsque le test est lancé. (non applicable lorsque l'ID d'interface réseau -Test est spécifié)

ID d'interface réseau — ID ENI à utiliser lors du lancement de la transition finale.

ID d'interface réseau - Test - ID ENI à utiliser lors du lancement du test.

ID d'hôte dédié : ID d'hôte dédié sur lequel l'instance sera lancée. (applicable uniquement lorsque la location est définie sur Hôte dédié).

Facultatif

Tags : balises d'instance EC2 à appliquer à l'instance.

Tous les autres attributs non répertoriés ici n'ont aucune incidence sur les tâches AWS MGN initiées depuis la solution AWS CMF.

Définition du formulaire d'admission

Les formulaires d'admission peuvent contenir les informations nécessaires pour créer ou mettre à jour plusieurs types d'enregistrements avec la banque de données sur une seule ligne du fichier csv, ce qui permet l'importation de données connexes. Dans l'exemple ci-dessous, les enregistrements de vague, d'application et de serveur seront créés et liés les uns aux autres automatiquement lors de l'importation.

Pour importer le formulaire d'admission, suivez le même processus que les autres importations de données dans le Cloud Migration Factory sur la AWS solution décrite dans la section [Importation de données](#).

Initier une tâche

Le lancement d'une tâche AWS MGN à partir de AWS CMF est effectué contre une vague, dans la vue de la liste des vagues, sélectionnez la vague, puis dans les Actions, sélectionnez Rehost > MGN.

Cet écran demande à l'utilisateur de faire les choix suivants avant de pouvoir soumettre le travail.

1. Sélectionnez l'action AWS MGN à exécuter sur les applications et les serveurs de la vague. Ces actions reproduisent principalement celles disponibles dans la console de service et l'API AWS MGN, à l'exception du modèle de validation de lancement (voir ci-dessous pour plus de détails sur cette action). Pour plus de détails sur les effets de chaque action, reportez-vous au guide de l'utilisateur de AWS MGN.
2. Sélectionnez la vague contre laquelle lancer l'action.
3. Sélectionnez les applications dans la vague sur laquelle l'action sera exécutée. Cette liste affiche uniquement les applications associées à la vague sélectionnée.
4. Une fois que toutes les options sont correctes, choisissez Soumettre.

L'automatisation lancera désormais l'action sélectionnée contre la cible de chaque application sélectionnée Compte AWS, comme indiqué dans l'enregistrement de l'application. Les résultats de l'action seront affichés dans le message de notification, y compris les éventuelles erreurs.

Valider le modèle de lancement

Cette action est utilisée pour valider la validité des données de configuration stockées dans le CMF pour chaque serveur avant de tenter des activités de transfert. Pour exécuter cette action, vous devez avoir correctement déployé les agents AWS MGN sur le serveur source.

Les validations effectuées pour chaque serveur sont les suivantes :

- Vérifiez que le type d'instance est valide.
- Vérifiez que le profil d'instance IAM existe.
- Des groupes de sécurité existent à la fois pour le test et pour le live.
- Des sous-réseaux existent à la fois pour le test et pour le live (si l'ENI n'est pas spécifié).
- Un hôte dédié existe (si spécifié).
 - Si un hôte dédié est spécifié, les vérifications suivantes sont effectuées :
 - L'hôte dédié prend-il en charge le type d'instance spécifié ?
 - L'hôte dédié dispose-t-il d'une capacité disponible pour répondre à toutes les exigences de cette vague, en fonction des types d'instances requis ?
- L'ENI existe (si spécifié).

Les résultats de l'action seront affichés dans le message de notification, y compris les éventuelles erreurs.

Replateforme vers EC2

La AWS solution Cloud Migration Factory on permet de lancer automatiquement des groupes d'instances EC2 à partir de configurations définies dans sa banque de données, en déployant des instances EC2 auxquelles des volumes EBS sont attachés. Cela permet de fournir de nouvelles instances EC2, ce qui permet la replatforme et le réhébergement de serveurs sur site avec AWS MGN au sein d'une seule interface utilisateur CMF. AWS CloudFormation Avant de pouvoir utiliser cette fonctionnalité, la banque de données doit contenir la définition des serveurs. Une fois ce problème résolu, les serveurs doivent être connectés à une vague. Lorsque la décision est prise de lancer les instances EC2, l'utilisateur peut lancer les actions suivantes contre la vague :

- Validation des entrées EC2
- Modèle CF EC2 Generate
- Déploiement EC2

Prérequis

Autorisations permettant d'ajouter l'accès à l'attribut Replatform.

Configuration initiale

La configuration des nouvelles instances EC2 s'effectue par la création de nouveaux éléments de serveur à l'aide de l'interface utilisateur ou par l'importation d'un formulaire d'admission CSV contenant les éléments du serveur. Ces définitions sont converties en modèles de AWS Cloud formation stockés dans un compartiment S3 au sein duquel Compte AWS l'instance AWS CMF est déployée.

Définition de l'interface utilisateur

Lors de la définition d'un serveur dans la banque de données AWS Cloud Migration Factory à utiliser avec la fonctionnalité Replatform to EC2, le serveur doit être configuré avec une stratégie de migration de Replatform. Une fois que Replatform est sélectionné, les attributs supplémentaires requis pour cette fonctionnalité s'affichent à l'écran. Les attributs suivants doivent être renseignés pour que la fonctionnalité fonctionne :

Attributs requis

ID AMI : ID de l'image machine Amazon utilisée pour lancer l'instance EC2.

Zone de disponibilité — AZ dans laquelle l'instance EC2 sera déployée.

Taille du volume racine : taille en Go du volume racine de l'instance.

Type d'instance : type d'instance EC2 à utiliser.

ID des groupes de sécurité : liste des groupes de sécurité assignés à l'instance.

Identifiants de sous-réseau : ID de sous-réseau auquel attribuer cette instance EC2.

Location — Actuellement, la seule option prise en charge pour l'intégration de la replateforme vers EC2 est Shared. Toute autre option sera remplacée par Shared lors de la génération du modèle.

Attributs facultatifs

Activer la surveillance détaillée : cochez cette case pour activer la surveillance détaillée.

Noms de volumes supplémentaires : liste des noms de volumes EBS supplémentaires. Chaque élément de la liste doit être mappé sur la même ligne que les listes Taille et Type.

Tailles de volume supplémentaires — Liste des tailles de volume EBS supplémentaires. Chaque élément de la liste doit être mappé sur la même ligne que les listes de noms et de types.

Types de volumes supplémentaires : liste des types de volumes EBS supplémentaires. Chaque élément de la liste doit être mappé sur la même ligne que les listes de noms et de tailles. S'il n'est pas spécifié, la valeur par défaut est gp2 pour tous les volumes.

ID de clé EBS KMS pour le chiffrement des volumes — Si les volumes EBS doivent être chiffrés, spécifiez l'ID de clé, l'ARN de clé, l'alias de clé ou l'ARN d'alias.

Activer EBS Optimized — Sélectionnez cette option pour activer EBS Optimized.

Nom du volume racine : sélectionnez l'une des options proposées. Si ce n'est pas le cas, l'ID sera utilisé.

Type de volume racine — Indiquez le type EBS du volume à créer. S'il n'est pas spécifié, la valeur par défaut est gp2.

Définition du formulaire d'admission

Les formulaires d'admission peuvent contenir les informations nécessaires pour créer ou mettre à jour plusieurs types d'enregistrements avec la banque de données sur une seule ligne du fichier csv, ce qui permet l'importation de données connexes. Dans l'exemple suivant, les enregistrements de vague, d'application et de serveur seront créés et liés les uns aux autres automatiquement lors de l'importation.

Exemple : formulaire d'admission

Nom de la colonne	Exemple de données	Obligatoire	Remarques
nom_onda	vague 1	Oui	
app_name	app1	Oui	
aws_account id	1234567890	Oui	

Nom de la colonne	Exemple de données	Obligatoire	Remarques
nom_serveur	Serveur 1	Oui	
server_fqdn	Serveur 1	Oui	
server_os_family	linux	Oui	
version du système d'exploitation du serveur	Amazon	Oui	
niveau du serveur	Web	Non	
environnement_serveur	Développeur	Non	
ID de sous-réseau	sous-réseau-xxxxxxx	Oui	
Identifiants du groupe de sécurité	sg-yyyyyyyyyyy	Oui	
instanceType	m5.large	Oui	
Je suis un rôle	rôle personnalisé ec2	Non	
location	Partagé	Oui	
r_type	Recréation de plateforme	Oui	
root_vol_size	50	Oui	
ami_id	ami-zzzzzzzzzzz	Oui	
zone de disponibilité	us-west-2a	Oui	
root_vol_type	gp2	Non	
ajouter_vols_size	40:100	Non	

Nom de la colonne	Exemple de données	Obligatoire	Remarques
ajouter_vols_type	gp2 : gp3	Non	
ebs_optimized	false	Non	
ebs_kmskey_id	1111-1111-1111-1111	Non	
surveillance_détaillée	true	Non	
nom_fichier_racine	Serveur1_Root_Volume	Non	
ajouter_vols_name	Serveur1_root_volumeS : Server1_Root_VolumeB	Non	

Pour importer le formulaire d'admission, suivez le même processus que pour toute autre importation de données dans la AWS solution Cloud Migration Factory on.

Actions de déploiement

Validation des entrées EC2

Après avoir défini les paramètres de l'instance, vous devez d'abord exécuter l'action Wave : Replatform > EC2 > EC2 Input Validation. Cette action vérifie que tous les paramètres corrects ont été fournis pour chaque serveur afin de créer un CloudFormation modèle valide.

Note

Cette validation ne vérifie pas actuellement que les paramètres d'entrée sont valides, mais seulement qu'ils sont présents dans chaque définition de serveur. Vous devez vérifier les valeurs correctes avant de créer le modèle, sinon le déploiement du modèle échouera.

Modèle de génération CloudFormation EC2

Une fois que les définitions de tous les serveurs inclus dans une vague ont été vérifiées, le CloudFormation modèle peut être généré. Pour ce faire, exécutez l'action Wave : Replatform >

EC2 > EC2 Generate CF Template. Cette action crée un CloudFormation modèle pour chaque application de la vague, dans lequel les serveurs de l'application ont une stratégie de migration ou de replateforme ; les serveurs ayant défini d'autres stratégies de migration ne seront pas inclus dans le modèle.

Une fois exécutés, les modèles de chaque application seront stockés dans le compartiment S3 : [préfixe spécifique à l'instance] -gfbuild-cftemplates, qui a été créé automatiquement lors du déploiement de la solution Cloud Migration Factory on. AWS La structure de dossiers de ce bucket est la suivante :

- [ID AWS du compte cible]
 - [Nom de la vague]
 - CFN_Template_ [ID de l'application] _ [Nom de l'application] .yaml

Chaque fois que l'action de génération est exécutée, une nouvelle version du modèle est stockée dans le compartiment S3. Les URI S3 pour les modèles seront fournis dans la notification, ces modèles peuvent être revus ou modifiés selon les besoins avant le déploiement.

Les CloudFormation modèles génèrent actuellement les types de CloudFormation ressources suivants :

- AWS: :EC2 : :Instance
- AWS: :EC2 : :Volume
- AWS: :EC2 : : VolumeAttachment

Déploiement d'EC2

Une fois que vous êtes prêt à déployer les nouvelles instances EC2, vous pouvez lancer l'action de déploiement EC2 qui peut être lancée via l'action Wave Replatform > EC2 > EC2 Deployment. Cette action utilisera la dernière version du CloudFormation modèle pour chaque application de la vague et déploiera ces modèles dans les comptes cibles sélectionnés, via AWS CloudFormation.

Gestion des scripts

La AWS solution Cloud Migration Factory on permet aux utilisateurs de gérer entièrement la bibliothèque de scripts ou de packages d'automatisation au sein de l'interface utilisateur. Vous pouvez télécharger de nouveaux scripts personnalisés ainsi que de nouvelles versions du script

à l'aide de l'interface de gestion des scripts. Lorsque plusieurs versions sont disponibles, un administrateur peut passer d'une version à l'autre, ce qui permet de tester les mises à jour avant de les définir par défaut. L'interface de gestion des scripts permet également aux administrateurs de télécharger des packages de scripts pour mettre à jour ou revoir le contenu.

Un package de script pris en charge est une archive zip compressée contenant les fichiers obligatoires suivants à la racine :

- `Package-structure.yml` — Utilisé pour définir les arguments du script et d'autres métadonnées, telles que la description et le nom par défaut. Reportez-vous à la section [Composer un nouveau package de script](#) pour plus de détails.
- `[script python personnalisé].py` — Il s'agit du script initial qui sera exécuté lors de la soumission d'une tâche. Ce script peut appeler d'autres scripts et modules et si c'est le cas, ceux-ci doivent être inclus dans l'archive. Le nom de ce script doit correspondre à la valeur spécifiée dans la `MasterFileName` clé du `Package-Structure.yml`.

Télécharger un nouveau package de script

Note

Un package de script doit être conforme au format pris en charge. Reportez-vous à la section [Composer un nouveau package de script](#) pour plus de détails.

1. Choisissez Ajouter dans le tableau des scripts d'automatisation.
2. Sélectionnez le fichier d'archive du package que vous souhaitez télécharger.
3. Entrez un nom unique pour le script. Les utilisateurs référenceront le script par ce nom pour lancer des tâches.

Télécharger des packages de scripts

Vous pouvez télécharger des packages de scripts depuis la console pour activer les mises à jour et la vérification du contenu.

1. Sélectionnez Automatisation, puis Scripts.
2. Sélectionnez le script que vous souhaitez télécharger dans le tableau, puis sélectionnez Actions et choisissez Télécharger la version par défaut ou Télécharger la dernière version.

Vous pouvez télécharger des versions spécifiques d'un script. Pour ce faire, sélectionnez le script, puis Actions et choisissez Modifier la version par défaut. Dans la liste des versions par défaut du script, choisissez Télécharger la version sélectionnée.

Ajouter une nouvelle version d'un package de script

Les mises à jour des packages de scripts AWS Cloud Migration Factory peuvent être téléchargées dans la section Automation > Scripts en suivant les étapes suivantes :

1. Sélectionnez Automatisation, puis Scripts.
2. Sélectionnez le script existant pour ajouter une nouvelle version, puis sélectionnez Actions et choisissez Ajouter une nouvelle version.
3. Sélectionnez le fichier d'archive du package mis à jour que vous souhaitez télécharger, puis choisissez Next. La nouvelle version du script conservera le nom existant par défaut. Entrez un nom de script unique. Tout changement de nom ne sera appliqué qu'à cette version du script.
4. Vous pouvez faire de la nouvelle version du script la version par défaut en sélectionnant Créer la version par défaut.
5. Sélectionnez Charger.

Suppression de packages et de versions de scripts

Vous ne pouvez pas supprimer de scripts ou de versions d'un script à des fins d'audit. Cela permet de vérifier le script exact qui a été exécuté sur un système à un moment donné. Chaque version de script possède une signature et un identifiant uniques lors du téléchargement, qui sont enregistrés par rapport à l'historique des tâches dans lesquelles le script et la version ont été utilisés.

Composer un nouveau package de script

Cloud Migration Factory sur les packages de AWS script prend en charge Python comme langage de script principal. Vous pouvez lancer d'autres langages de script shell selon les besoins à partir d'un programme principal ou d'un wrapper Python. Pour créer rapidement un nouveau package de scripts, nous vous recommandons de télécharger une copie de l'un des scripts préemballés et de le mettre à jour pour effectuer la tâche requise. Vous devez d'abord créer un script Python principal qui exécutera les fonctionnalités de base du script. Créez ensuite un `Package-Structure.yml` fichier pour définir les arguments et les autres métadonnées nécessaires au script. Reportez-vous aux `Package-Structure.yml` options pour plus de détails.

Script Python principal

Il s'agit du script principal initial qui s'exécute lorsqu'une tâche est initiée. Une fois l'exécution du script terminée, la tâche est terminée et le code de retour final détermine le statut de la tâche. Toutes les sorties de ce script sont capturées lorsqu'elles sont exécutées à distance et transmises au journal d'audit des sorties de la tâche à des fins de référence. Ce journal est également stocké sur Amazon CloudWatch.

Accès à Cloud Migration Factory sur les AWS données et les API à partir d'un script

Pour fournir un accès à Cloud Migration Factory sur les AWS API et les données, vous pouvez utiliser le module d'assistance python inclus. Le module fournit les fonctions communes suivantes :

Connexion en usine

Renvoie un jeton d'accès qui peut être utilisé pour appeler Cloud Migration Factory sur les AWS API. Cette fonction tentera de se connecter à CMF en utilisant un certain nombre de tentatives d'identification :

1. En essayant d'accéder au secret par défaut contenant l'identifiant et le mot de passe du compte de service s'il existe et si l'accès est autorisé. Ce nom secret MF ServiceAccount - [**userpool id**] sera vérifié.
2. Si l'étape 1 échoue et que l'utilisateur exécute le script depuis la ligne de commande, il sera invité à fournir un identifiant et un mot de passe AWS Cloud Migration Factory. Si elle est exécutée à partir d'une tâche d'automatisation distante, la tâche échouera.

getServerCredentials

Renvoie les informations de connexion d'un serveur stockées dans AWS Cloud Migration Factory, soit dans le Gestionnaire d'informations d'identification, soit via les entrées de l'utilisateur. Cette fonction vérifie un certain nombre de sources différentes afin de déterminer les informations d'identification d'un serveur spécifique. L'ordre des sources est le suivant :

1. Si `local_username` et `local_password` sont définis et valides, ils seront renvoyés.
2. Si `secret_override` est défini, cela sera utilisé pour récupérer le secret spécifié dans AWS Secret Manager, sinon, si l'enregistrement du serveur contient la clé `secret_name` et si elle n'est pas vide, c'est ce nom de secret qui sera utilisé.

3. En cas d'échec lors de la localisation ou de l'accès aux secrets spécifiés, la fonction recommencera à demander à l'utilisateur les informations d'identification, mais uniquement si le paramètre `no_user_prompts` est défini sur `False`, sinon elle renverra un échec.

Paramètres

`local_username` — S'il est passé, il sera renvoyé.

`local_password` — S'il est passé, il sera renvoyé.

`server` : nom du serveur, tel qu'il est enregistré dans l'attribut `server_name` dans AWS Cloud Migration Factory.

`Secret_override` — Une fois passé, cela définira le nom du secret à récupérer depuis le Secrets Manager pour ce serveur.

`No_User_Prompts` — Indique à la fonction de ne pas demander à un utilisateur de saisir un identifiant et un mot de passe s'ils ne sont pas stockés. Cela doit être vrai pour tout script d'automatisation à distance.

Obtenir des informations d'identification

Récupère les informations d'identification stockées à l'aide de AWS Cloud Migration Factory Credentials Manager à partir de Secrets Manager.

Paramètres

`secret_name` — nom du secret à récupérer.

`get_factory_servers`

Renvoie un tableau de serveurs à partir de la banque de données AWS Cloud Migration Factory en fonction du `waveid` fourni.

Paramètres

`Waveid` — ID d'enregistrement Wave des serveurs qui sera renvoyé.

`Jeton` : jeton d'authentification obtenu à partir de la `FactoryLogin` fonction Lambda.

`UserHost` — URL du point de terminaison de l'API utilisateur de AWS Cloud Migration Factory.

OSSplit — Si cette valeur est définie sur `true`, deux listes seront renvoyées, une pour les serveurs Linux et une pour les serveurs Windows, si elle est définie sur `False`, une seule liste combinée sera renvoyée.

Résumé du message final

Il est recommandé de fournir un message récapitulatif du résultat du script en tant que sortie finale à l'écran ou à la sortie système. Cela sera affiché sur la console dans la propriété `Last Message`, qui fournit un état rapide du résultat du script sans que l'utilisateur n'ait à lire le journal de sortie complet.

Code de retour

Le script python principal doit renvoyer un code de retour différent de zéro à la sortie si la fonction du script n'est pas complètement réussie. À la réception d'un code de retour différent de zéro, le statut de la tâche sera affiché comme `Échec` dans le journal des tâches, indiquant à l'utilisateur qu'il doit consulter le journal de sortie pour obtenir des détails sur l'échec.

Options de structure de package YAML .yaml

Exemple de fichier YAML

```
Name: "0-Check MGN Prerequisites"
Description: "This script will verify the source servers meet the basic requirements
  for AWS MGN agent installation."
MasterFileName: "0-Prerequisites-checks.py"
UpdateUrl: ""
Arguments:
-
  name: "ReplicationServerIP"
  description: "Replication Server IP."
  long_desc: "IP Address of an AWS MGN Replication EC2 Instance."
  type: "standard"
  required: true
-
  name: "SecretWindows"
  long_desc: "Windows Secret to use for credentials."
  description: "Windows Secret"
  type: "relationship"
  rel_display_attribute: "Name"
  rel_entity: "secret"
  rel_key: "Name"
-
  name: "SecretLinux"
```

```
long_desc: "Linux Secret to use for credentials."
description: "Linux Secret"
type: "relationship"
rel_display_attribute: "Name"
rel_entity: "secret"
rel_key: "Name"
-
name: "Waveid"
description: "Wave Name"
type: "relationship"
rel_display_attribute: "wave_name"
rel_entity: "wave"
rel_key: "wave_id"
validation_regex: "^(?!\\s*$).+"
validation_regex_msg: "Wave must be provided."
required: true
SchemaExtensions:
-
schema: "server"
name: "server_pre_reqs_output"
description: "Pre-Req Output"
type: "string"
```

Descriptions des clés YAML

Obligatoire

Nom : nom par défaut que le script utilisera lors de l'importation.

Description — Description de l'utilisation du script.

MasterFileName— C'est le point de départ de l'exécution du script. Il doit s'agir d'un nom de fichier python inclus dans l'archive du package du script.

Arguments — Liste des arguments acceptés par le script MasterFileName Python. Chaque argument à spécifier est au format de définition de l'attribut AWS Cloud Migration Factory. Les propriétés obligatoires pour chaque argument sont le nom et le type, toutes les autres propriétés sont facultatives.

Facultatif

UpdateUrl— Fournissez une URL où la source du package de script est disponible pour fournir des mises à jour. Pour le moment, c'est uniquement pour référence.

SchemaExtensions— Liste des attributs dont le script Python a besoin pour figurer dans le schéma pour stocker la sortie ou récupérer des données supplémentaires. Chaque attribut doit être spécifié dans le format de définition d'attribut AWS CMF. Les propriétés requises pour chaque attribut sont le schéma, le nom, la description et le type. Toutes les autres propriétés sont facultatives. Tous les nouveaux attributs seront automatiquement ajoutés au schéma lors du chargement initial du script, et les modifications apportées ne SchemaExtensions seront pas traitées pour les nouvelles versions du script. Si cela est nécessaire pour qu'un nouveau script soit ajouté, des mises à jour manuelles du schéma doivent être effectuées.

Gestion des schémas

La AWS solution Cloud Migration Factory on fournit un référentiel de métadonnées entièrement extensible, permettant de stocker les données pour l'automatisation, l'audit et le suivi du statut dans un seul outil. Le référentiel fournit un ensemble par défaut d'entités (Waves, applications, serveurs et bases de données) et d'attributs au moment du déploiement pour vous permettre de commencer à capturer et à utiliser les données les plus fréquemment utilisées. À partir de là, vous pouvez personnaliser le schéma selon vos besoins.

Seuls les utilisateurs du groupe d'administrateurs Cognito sont autorisés à gérer le schéma. Pour faire d'un utilisateur un membre de l'administrateur ou d'autres groupes, reportez-vous à la section [Gestion des utilisateurs](#).

Accédez à Administration, puis sélectionnez Attributs pour les onglets d'entités par défaut. Les onglets suivants sont disponibles pour faciliter la gestion de l'entité.

Attributs : permet d'ajouter, de modifier et de supprimer des attributs.

Panneau d'informations — Permet de modifier le contenu d'aide du panneau d'informations, qui est affiché à droite de l'écran des entités dans la section Gestion de la migration.

Paramètres du schéma — Actuellement, cet onglet permet uniquement de modifier le nom convivial de l'entité, c'est le nom affiché sur l'interface utilisateur. S'il n'est pas défini, l'interface utilisateur utilise le nom programmatique de l'entité.

Ajouter/modifier un attribut

Les attributs peuvent être modifiés dynamiquement via la section Administration des attributs de la solution Cloud Migration Factory sur AWS. Lorsque des attributs sont ajoutés, modifiés ou supprimés,

les mises à jour sont appliquées en temps réel pour l'administrateur effectuant les modifications. Tout autre utilisateur actuellement connecté à la même instance verra sa session automatiquement mise à jour dans la minute suivant l'enregistrement des modifications par l'administrateur.

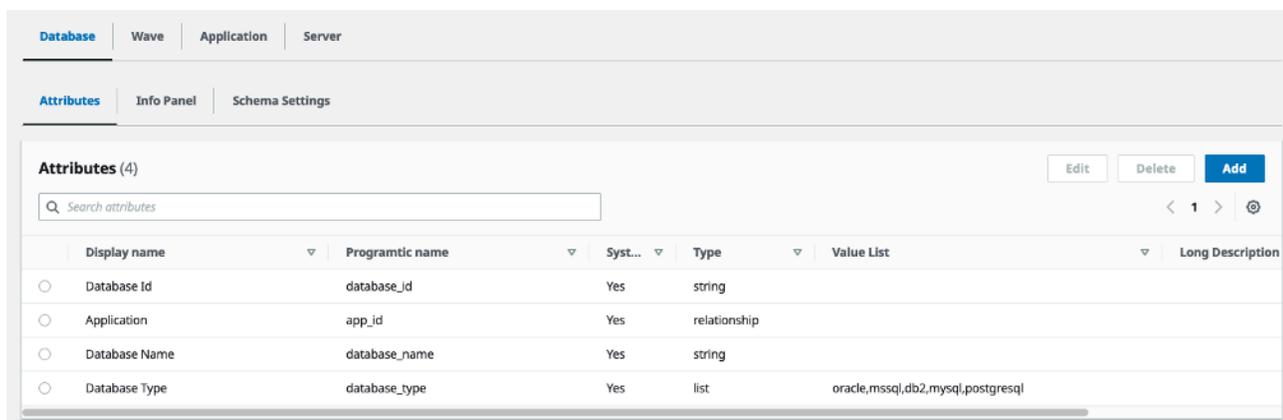
Certains attributs sont définis comme des attributs système, ce qui signifie qu'ils sont essentiels aux fonctionnalités de base de Cloud Migration Factory sur AWS. Par conséquent, seules certaines propriétés peuvent être modifiées par les administrateurs. Tout attribut qui est un attribut système sera affiché avec un avertissement en haut de l'écran Modifier l'attribut.

Pour les attributs définis par le système, seuls les éléments suivants peuvent être modifiés :

- Panneau d'information
- Options avancées
 - Regroupement et positionnement des attributs
 - Validation des entrées

Toutes les autres propriétés de l'attribut défini par le système sont en lecture seule.

Ajouter un attribut :



Vous pouvez ajouter de nouveaux attributs en cliquant sur le bouton Ajouter dans l'onglet attributs de l'entité à laquelle vous souhaitez ajouter l'attribut. Dans l'exemple ci-dessus, le choix de Ajouter ajoutera un nouvel attribut à l'entité de base de données.

Dans la boîte de dialogue Modifier l'attribut, vous devez fournir les propriétés requises suivantes :

Nom programmatique : il s'agit de la clé qui sera utilisée pour stocker les données de l'attribut par rapport aux éléments de la table DynamoDB. Il est également référencé lors de l'utilisation des API Migration Factory et dans les scripts d'automatisation.

Nom d'affichage — Il s'agit de l'étiquette qui sera affichée sur l'interface Web à côté du champ de saisie des données.

Type : cette sélection déroulante définit le type de données que l'utilisateur sera autorisé à stocker par rapport à l'attribut. Les options suivantes sont disponibles :

Type	Utilisation
Chaîne	Les utilisateurs peuvent saisir n'importe quelle ligne de texte. Les retours ne sont pas autorisés.
Chaîne à valeurs multiples	Semblable à une chaîne, la seule différence étant que l'utilisateur peut saisir plusieurs valeurs sur des lignes distinctes dans le champ, celles-ci sont ensuite stockées sous forme de tableau/de liste.
Mot de passe	Fournit à l'utilisateur un moyen de saisir en toute sécurité des données qui ne doivent pas être affichées à l'écran par défaut.

 **Note**

Les données ne sont pas stockées cryptées lors de l'utilisation de ce type d'attribut et sont affichées en texte clair lorsqu'elles sont consultées dans les charges utiles de l'API. Elles ne doivent donc pas être utilisées pour stocker des données sensibles. Tous les mots de passe ou secrets doivent être stockés dans le gestionnaire d'informations d'identification de Migration Factory (décrit dans ce document) qui utilise AWS Secrets Manager pour stocker et

Type	Utilisation
	fournir un accès sécurisé aux informations d'identification.
Date	Fournit un champ avec un sélecteur de date permettant à l'utilisateur de sélectionner une date ou de saisir manuellement la date requise.
Checkbox	Fournit une case à cocher standard. Lorsque cette case est cochée, la valeur de la clé sera « vrai ». Si elle n'est pas cochée, elle sera « faux » ou la clé n'existera pas dans l'enregistrement.
TextArea	Contrairement au type String qui TextAreas permet de stocker du texte sur plusieurs lignes, il ne prend en charge que les caractères de texte de base.
Tag	Permet aux utilisateurs de stocker une liste de paires clé/valeur.
Liste	Fournit à l'utilisateur une liste d'options prédéfinies parmi lesquelles sélectionner. Ces options sont définies dans la définition de l'attribut de schéma dans la propriété Value List de l'attribut.

Type	Utilisation
Relation	<p>Ce type d'attribut permet de stocker des relations entre deux entités ou enregistrements quelconques. Lorsque vous définissez un attribut de relation, vous sélectionnez l'entité à laquelle la relation sera destinée, puis la valeur clé utilisée pour relier les éléments et sélectionner l'attribut dans l'élément associé que vous souhaitez afficher à l'utilisateur.</p> <p>Une liste déroulante basée sur l'entité et les valeurs d'affichage disponibles pour la relation est présentée à l'utilisateur.</p> <p>Sous chaque champ de relation, l'utilisateur dispose d'un lien rapide pour afficher le résumé de l'élément associé.</p>
JSON	<p>Fournit un champ d'éditeur JSON dans lequel les données JSON peuvent être stockées et modifiées. Cela peut être utilisé pour stocker les paramètres d'entrée/sortie du script ou d'autres données nécessaires à l'automatisation des tâches, ou à toute autre utilisation.</p>

Lorsque vous ajoutez un nouvel attribut, vous devez autoriser les utilisateurs à accéder au nouvel attribut par le biais d'une politique. Consultez la section [Gestion des autorisations](#) pour plus de détails sur la façon d'accorder l'accès aux attributs.

Panneau d'information

Permet de spécifier une aide contextuelle et des conseils pour l'utilisation de l'attribut. Une fois spécifié, l'étiquette de l'attribut sur l'interface utilisateur comportera un lien d'information affiché sur la droite. En cliquant sur ce lien, l'utilisateur accède au contenu d'aide et aux liens d'aide spécifiés dans cette section à droite de l'écran.

La section du panneau d'informations propose deux vues des données, la vue Modifier, dans laquelle vous pouvez définir le contenu, et la vue Aperçu, qui fournit un aperçu rapide de ce que l'utilisateur verra lorsque les mises à jour de l'attribut seront enregistrées.

Le titre de l'aide ne prend en charge que les valeurs en texte brut. Le contenu de l'aide prend en charge un sous-ensemble de balises HTML qui permettent le formatage du texte. Par exemple, si vous ajoutez des balises de ``début et `` de fin autour du texte, le texte inclus sera mis en gras (c'est-à-dire que `l'ID d'interface réseau` se traduira par un ID d'interface réseau). Les balises prises en charge sont les suivantes :

Tag	Utilisation	Exemple d'interface utilisateur
<code><p></p></code>	Définit un paragraphe.	<code><p>Mon premier paragraphe</p></code> <code><p>Mon deuxième paragraphe</p></code>
<code><a></code>	Définit un lien hypertexte.	<code>Visitez AWS !</code>
<code><h3></code> , <code><h4></code> et <code><h5></code>	Définit les titres h3 à h5	<code><h3>Ma rubrique 3</h3></code>
<code></code>	Définit une section de texte, permettant d'appliquer une mise en forme supplémentaire, telle que la couleur, la taille et la police du texte.	<code>bleu</code>
<code><div></code>	Définit un bloc du document, permettant d'appliquer une mise en forme supplémentaire, telle que la couleur, la taille et la police du texte.	<code><div style="color:blue"></code> <code><h3>Il s'agit d'un titre bleu</h3></code> <code><p>Il s'agit d'un texte bleu dans un div. </p></code> <code></div></code>

Tag	Utilisation	Exemple d'interface utilisateur
<code>+ </code>	Définit une liste à puces non ordonnée.	<pre> Réhéberger Replateforme Prendre sa retraite </pre>
<code>, </code>	Définit une liste ordonnée/numérotée.	<pre> Réhéberger Replateforme Prendre sa retraite </pre>
<code><code></code>	Définit un bloc ou une section de texte contenant du code.	<code><code>couleur d'arrière-plan</code></code>
<code><pre></code>	Définit un bloc de texte préformaté, tous les sauts de ligne, tabulations et espaces sont affichés.	<pre><pre> Mon texte préformaté. Ceci est affiché dans une police de largeur fixe et s'affichera tel que saisi << ces espaces seront affichés. </pre></pre>

Tag	Utilisation	Exemple d'interface utilisateur
<code><dl></code> , <code><dt></code> et <code><dd></code>	Définit une liste de descriptions.	<pre><dl> <dt>Réhéberger</dt> <dd>Migration par levage et changement de vitesse</dd> <dt>Prendre sa retraite</dt> <dd>Mettre hors service l'instance ou le service</dd> </dl></pre>
<code><hr></code>	Définit une règle horizontale sur toute la page pour afficher un changement de sujet ou de section.	<code><hr></code>
<code>
</code>	Définit un saut de ligne dans le texte. Ils sont pris en charge mais ne sont pas obligatoires, car tout retour de chariot dans l'éditeur sera remplacé par un retour une <code>
</code> fois enregistré.	<code>
</code>
<code><i></code> et <code></code>	Définit le texte inclus en italique ou dans un autre format localisé.	<code><i></code> Ceci est en italique <code></i></code> ou <code></code> c'est également <code></code> en italique
<code></code> et <code></code>	Définit le texte encadré en gras.	<code></code> Je suis en gras <code></code> ou <code></code> C'est différent <code></code>

Une autre option disponible pour fournir de l'aide consiste à créer des liens vers du contenu externe et des conseils. Pour ajouter un lien externe vers l'aide contextuelle de l'attribut, cliquez sur Ajouter

une nouvelle URL et saisissez une étiquette et une URL. Vous pouvez ajouter plusieurs liens vers le même type d'attribut selon les besoins.

Options avancées

Regroupement et positionnement des attributs

Cette section permet à l'administrateur de définir l'endroit où l'attribut sera positionné dans l'interface utilisateur d'ajout/modification et permet également de regrouper les attributs, fournissant à l'utilisateur un moyen simple de localiser les attributs associés.

Le groupe d'interface utilisateur est une valeur de texte qui définit le nom du groupe dans lequel l'attribut doit être affiché, tous les attributs ayant la même valeur de groupe d'interface utilisateur seront placés dans le même groupe, tout attribut pour lequel aucun groupe d'interface utilisateur n'est spécifié sera placé dans le groupe par défaut en haut du formulaire intitulé Détails. Lorsque le groupe d'interface utilisateur est spécifié, l'interface utilisateur affiche le texte affiché ici comme titre du groupe.

La deuxième propriété de cette section est Ordre en groupe. Elle peut être définie sur n'importe quel nombre positif ou négatif. Une fois spécifiée, les attributs seront listés en fonction de cette valeur, du plus bas au plus élevé. Tous les attributs pour lesquels aucun ordre dans un groupe n'est spécifié auront une priorité inférieure et seront triés par ordre alphabétique.

Validation des entrées

Cette section permet à l'administrateur de définir des critères de validation qui garantissent que l'utilisateur a saisi des données valides avant de pouvoir enregistrer un élément. La validation utilise une expression régulière ou une chaîne regex composée d'une série de caractères qui spécifient un modèle de recherche pour une valeur de texte. Par exemple, le modèle `^(subnet- ([a-z0-9]{17})*)$` recherchera le texte `subnet-` suivi de toute combinaison des caractères `a` à `z` (minuscules) et des chiffres `0` à `9` avec un nombre exact de caractères de `17`. S'il trouve autre chose, il renverra `false` indiquant que la validation a échoué. Dans ce guide, nous ne pouvons pas couvrir toutes les combinaisons et modèles possibles, mais il existe de nombreuses ressources sur Internet qui peuvent vous aider à créer la solution idéale pour votre cas d'utilisation. Voici quelques exemples courants pour vous aider à démarrer :

Motif Regex	Utilisation
<code>^(?!\\s*\$) . +</code>	Garantit que la valeur est définie.

Motif Regex	Utilisation
<code>^(sous-réseau- ([a-z0-9] {17}) *) \$</code>	Vérifie que la valeur est un ID de sous-réseau valide. [Commence par le sous-réseau de texte, suivi de 17 caractères composés uniquement de lettres et de chiffres]
<code>^(ami- ([a-z0-9] {8,17}) +) \$</code>	Vérifiez que la valeur est un ID AMI valide. [Commence par le texte ami- suivi de 8 à 17 caractères composés uniquement de lettres et de chiffres]
<code>^(sg- ([a-z0-9] {17}) *) \$</code>	Vérifie que la valeur est dans un format d'ID de groupe de sécurité valide. [Commence par le texte sg- suivi de 17 caractères composés uniquement de lettres et de chiffres]
<code>^([A-zA-Z0-9] [A-zA-Z0-9] [A-zA-Z0-9 \ -] * [A-zA-Z0-9]) \. * ([A-Za-Z0-9] [A-zA-Z0-9] [A-zA-Z0-9 \ -] * [A-zA-Z0-9]) \$</code>	Garantit que les noms de serveurs sont valides et ne contiennent que des caractères alphanumériques, des tirets et des points.
<code>^([1-9] [1-9] [0-9] [1-9] [0-9] [0-9] [1-9] [0-9] [0-9] [0-9] [1] [0-6] [0-3] [0-8] [0-4]) \$</code>	Garantit la saisie d'un nombre compris entre 1 et 1634.
<code>^(standard io1 io2 gp2 gp3) \$</code>	Garantit que la chaîne saisie correspond à la norme, io1, io2, gp2 ou gp3.

Une fois que vous avez créé votre modèle de recherche regex, vous pouvez spécifier le message d'erreur spécifique qui sera affiché à l'utilisateur sous le champ, saisissez-le dans la propriété du message d'aide à la validation.

Une fois ces deux propriétés définies, dans le même écran, vous verrez ci-dessous un simulateur de validation, où vous pourrez tester que votre modèle de recherche fonctionne comme prévu et que

le message d'erreur s'affiche correctement. Tapez simplement un texte de test dans le champ de validation du test pour vérifier que le modèle correspond correctement.

Exemple de données

La section des exemples de données permet à l'administrateur de montrer à l'utilisateur un exemple de format de données requis pour un attribut. Ce format peut être spécifié pour le format des données requis lorsqu'il est fourni lors du téléchargement d'un formulaire d'admission, via l'interface utilisateur et/ou directement via l'API.

Les données d'exemple affichées dans la propriété d'exemple de données du formulaire d'admission seront sorties dans tout modèle d'admission créé dans lequel l'attribut est inclus, lorsque vous utilisez la fonction Télécharger, un modèle de formulaire de réception, sous Gestion de la migration > Importer.

Les données d'exemple d'interface utilisateur et les données d'exemple d'API sont stockées dans l'attribut, mais ne sont actuellement pas exposées dans l'interface Web. Ils peuvent être utilisés dans les intégrations et les scripts.

Gestion des autorisations

La AWS solution Cloud Migration Factory on fournit un contrôle d'accès granulaire basé sur les rôles aux données et des fonctions d'automatisation disponibles dans la solution. Amazon Cognito, qui fournit l'annuaire des utilisateurs et le moteur d'authentification, est à la base de ce contrôle.

Le tableau suivant présente les différents éléments qui constituent le cadre de contrôle d'accès au sein de la solution Cloud Migration Factory sur AWS et indique à partir duquel chaque élément est géré.

Élément de contrôle d'accès	Interface de gestion	Description
Utilisateur	Amazon Cognito et Cloud Migration Factory sur AWS	Les utilisateurs sont créés, supprimés et mis à jour dans Amazon Cognito, où le profil des utilisateurs peut être établi ainsi que l'authentification multifactorielle (MFA) si nécessaire. Dans l'interface

Élément de contrôle d'accès	Interface de gestion	Description
		utilisateur d'AWS CMF, vous pouvez uniquement ajouter et supprimer des utilisateurs dans des groupes.
Groupe	Cloud Migration Factory sur AWS	Vous pouvez créer ou supprimer des groupes depuis l'interface utilisateur AWS CMF.
Rôle	Cloud Migration Factory sur AWS	<p>Un rôle est mappé à un ou plusieurs groupes. La modification des groupes auxquels un rôle est attribué est effectuée dans la section d'administration du AWS CMF. Tout utilisateur membre d'un groupe assigné à un rôle se verra attribuer toutes les politiques associées au rôle.</p> <p>Une ou plusieurs politiques peuvent être attribuées à un rôle.</p>

Élément de contrôle d'accès	Interface de gestion	Description
Politique	Cloud Migration Factory sur AWS	Une politique contient les droits détaillés qui sont attribués à tout utilisateur auquel la politique s'applique (via l'appartenance à un groupe). Une politique unique peut inclure des droits d'accès aux données pour plusieurs entités ou pour une seule entité, ainsi que des droits d'accès pour exécuter des tâches d'automatisation et d'autres actions au sein de l'interface utilisateur AWS CMF. Ces politiques s'appliquent également lorsqu'un utilisateur interagit avec les API AWS CMF.

Politiques

Une politique fournit les autorisations les plus détaillées possibles dans Cloud Migration Factory. Elle contient la définition au niveau des tâches des droits accordés à un utilisateur. AWS Dans le cadre d'une politique, deux principaux types d'autorisations peuvent être accordés à un groupe d'utilisateurs : les autorisations relatives aux métadonnées et les autorisations relatives aux actions d'automatisation. Les autorisations de métadonnées permettent à un administrateur de contrôler le niveau d'accès d'un groupe aux schémas individuels et à leurs attributs, en spécifiant les droits de création, de lecture, de mise à jour et/ou de suppression selon les besoins. Les autorisations d'action d'automatisation permettent aux utilisateurs d'exécuter des actions d'automatisation spécifiques, telles que l'action d'intégration AWS MGN.

Autorisations relatives aux métadonnées

Pour chaque schéma ou entité au sein de AWS CMF, un administrateur peut définir une politique qui permet aux utilisateurs d'accéder à des attributs spécifiques et également définir le niveau d'accès

dont ils disposent à ces attributs. Lors de la création d'une nouvelle politique, les droits par défaut pour tous les schémas sont l'absence d'accès. La première chose à définir est le niveau d'accès requis pour cette politique au niveau de l'article/de l'enregistrement. Le tableau ci-dessous décrit les autorisations d'accès disponibles au niveau des enregistrements.

Niveau d'accès	Description
Création	Lorsque cette option est sélectionnée, un utilisateur auquel cette politique s'applique aura la possibilité d'ajouter de nouveaux enregistrements/éléments de ce type au magasin de métadonnées. Lorsque l'option Créer est sélectionnée mais qu'aucun autre droit n'est autorisé, l'utilisateur a la possibilité de créer des enregistrements et de définir uniquement une valeur pour les attributs requis, quels que soient les attributs sélectionnés.
Lecture	Pas encore implémenté Lorsque cette option est sélectionnée, l'utilisateur aura des droits de lecture sur tous les enregistrements/éléments de ce type d'entité. Lorsqu'elle n'est pas sélectionnée, les éléments de données ne seront pas visibles dans l'interface utilisateur ou dans l'API.
Mettre à jour	Lorsque cette option est sélectionnée, un utilisateur auquel cette politique s'applique pourra mettre à jour les enregistrements/éléments de ce type dans le magasin de métadonnées, mais uniquement pour les attributs spécifiés dans la liste d'accès au niveau des attributs. Lorsque la mise à jour est sélectionnée, au moins un attribut doit être sélectionné, sinon une erreur s'affichera lors de l'enregistrement.

Niveau d'accès	Description
Suppression	Lorsque cette option est sélectionnée, un utilisateur auquel cette politique s'applique aura la possibilité de supprimer des enregistrements/éléments de ce type du magasin de métadonnées.

Rôles

Les rôles permettent d'attribuer une ou plusieurs politiques à un ou plusieurs groupes. La combinaison de toutes les politiques attribuées à un rôle fournit des autorisations d'accès. Les rôles peuvent être créés en fonction des rôles ou des fonctions du projet ou de l'organisation.

Manuel du développeur

Code source

Vous pouvez consulter notre [GitHub référentiel](#) pour télécharger les modèles et les scripts de cette solution et partager vos personnalisations avec d'autres personnes. Si vous avez besoin d'une version antérieure du CloudFormation modèle ou si vous avez un problème technique à signaler, vous pouvez le faire depuis la page [GitHub des problèmes](#). Signalez les problèmes techniques liés à la solution sur la [page Problèmes](#) du GitHub référentiel.

Sujets supplémentaires

Liste des activités de migration automatisées à l'aide de la console Web Migration Factory

La AWS solution Cloud Migration Factory on déploie des activités de migration automatisées que vous pouvez exploiter pour vos projets de migration. Vous pouvez suivre les activités de migration répertoriées ci-dessous et les personnaliser en fonction des besoins de votre entreprise.

Avant de commencer toute activité, assurez-vous de lire le [Guide de l'utilisateur — Exécuter l'automatisation depuis la console](#) pour comprendre comment cela fonctionne. Vous devez également [créer un serveur d'automatisation](#) et [créer des utilisateurs Windows et Linux](#) pour exécuter l'automatisation à partir de la console.

Suivez les procédures suivantes dans le même ordre pour effectuer un test complet de la solution à l'aide des exemples de script et d'activités d'automatisation.

Vérifiez les prérequis

Connectez-vous aux serveurs source concernés pour vérifier les prérequis nécessaires tels que TCP 1500, TCP 443, l'espace libre sur le volume racine, la version du framework .Net et d'autres paramètres. Ces conditions préalables sont requises pour la réplication.

Avant de procéder à la vérification des prérequis, vous devez installer le premier manuellement sur un serveur source afin de créer un serveur de réplication dans EC2. Nous allons nous connecter à ce serveur pour tester le port 1500. Après l'installation, AWS Application Migration Service (AWSMGN) crée le serveur de réplication dans Amazon Elastic Compute Cloud (Amazon EC2). Dans le cadre de cette activité, vous devez vérifier le port TCP 1500 entre le serveur source et le serveur de réplication. Pour plus d'informations sur l'installation de l'agent AWS MGN sur vos serveurs sources, reportez-vous aux [instructions d'installation](#) du guide de l'utilisateur d'AWS Application Migration Service.

Utilisez la procédure suivante lorsque vous êtes connecté à la console Web de Migration Factory.

1. Sur la console Migration Factory, sélectionnez Jobs dans le menu de gauche, sélectionnez Actions, puis Run Automation sur le côté droit.

- Entrez le nom du job, sélectionnez le script 0-Check MGN Prerequisites et votre serveur d'automatisation pour exécuter le script. Si le serveur d'automatisation n'existe pas, assurez-vous de terminer la [création d'un serveur d'automatisation de la migration](#).
- La sélection de Linux Secrets et/ou Windows Secrets dépend du système d'exploitation que vous utilisez pour cette vague. Entrez l'adresse IP du serveur de réplication MGN, choisissez la vague sur laquelle vous souhaitez exécuter l'automatisation et choisissez Submit Automation Job.
- Vous serez redirigé vers la page de liste des tâches, le statut de la tâche devrait être EN COURS d'exécution. Choisissez Actualiser pour voir le statut. Il devrait devenir Complet au bout de quelques minutes.
- Le script mettra également à jour l'état de migration de la solution dans l'interface Web de Migration Factory, comme indiqué dans la capture d'écran suivante d'un exemple de projet.

The screenshot shows the AWS Migration Factory console. On the left, there is a navigation menu with 'Server' highlighted. The main area displays a table of servers with the following columns: Server Name, Server OS Family, Server OS Version, Server FQDN, and Migration Status. The Migration Status column is highlighted with a red box, showing 'Pre-requisites check : Passed' for all listed servers.

Server Name	Server OS Family	Server OS Version	Server FQDN	Migration Status
ofbiz-db.onpremsim...	linux	CentOS7	ofbiz-db.onpremsim...	Pre-requisites check : Passed
ofbiz-web.onpremsi...	linux	CentOS7	ofbiz-web.onpremsi...	Pre-requisites check : Passed
wordpress-db.onpr...	linux	CentOS7	wordpress-db.onpr...	Pre-requisites check : Passed
wordpress-web.onp...	linux	CentOS7	wordpress-web.onp...	Pre-requisites check : Passed
windows.onpremsi...	windows	Windows 2019	windows.onpremsi...	

Installation des agents de réplication

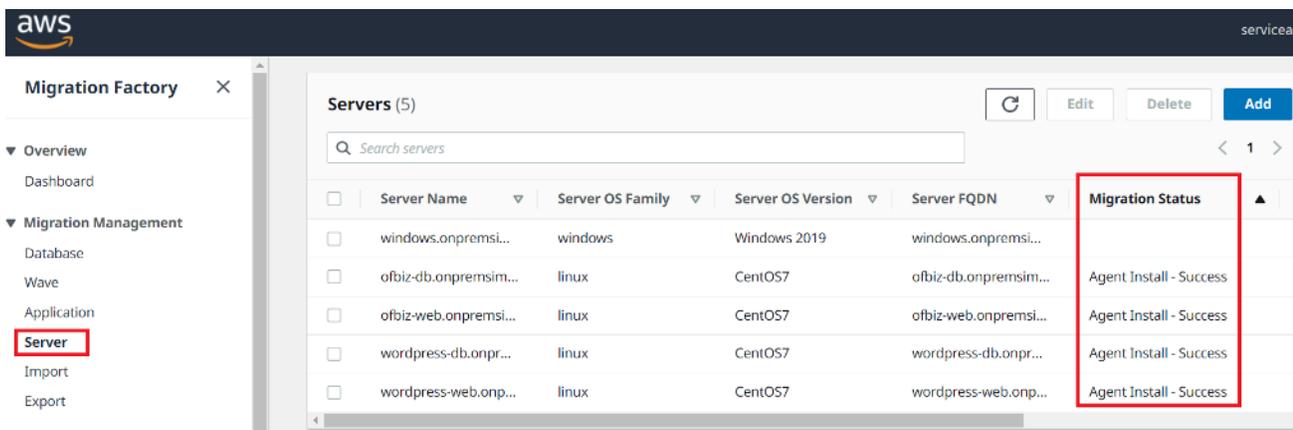
Note

Avant d'installer l'agent, assurez-vous que [AWSMGN est initialisé dans chaque compte et région cibles](#).

Utilisez la procédure suivante pour installer automatiquement les agents de réplication sur les serveurs sources concernés.

- Sur la console Migration Factory, sélectionnez Jobs dans le menu de gauche, sélectionnez Actions, puis Run Automation sur le côté droit.

2. Entrez le nom du job, sélectionnez le script 1-Install MGN Agents et votre serveur d'automatisation pour exécuter le script. Si le serveur d'automatisation n'existe pas, assurez-vous de terminer la [création d'un serveur d'automatisation de la migration](#).
3. La sélection de Linux Secrets et/ou Windows Secrets dépend du système d'exploitation que vous utilisez pour cette vague. Choisissez la vague pour laquelle vous souhaitez exécuter l'automatisation, puis choisissez Submit Automation Job.
4. Vous serez redirigé vers la page de liste des tâches, le statut de la tâche devrait être en cours d'exécution. Choisissez Actualiser pour voir le statut. Il devrait devenir Complet au bout de quelques minutes.
5. Le script fournit également l'état de la migration dans l'interface Web de Migration Factory, comme illustré dans l'exemple de capture d'écran suivant.



Envoyez les scripts de post-lancement

AWS Application Migration Service (MGN) prend en charge les scripts de post-lancement pour vous aider à automatiser les activités au niveau du système d'exploitation, telles que l'installation/la désinstallation du logiciel après le lancement des instances cibles. Cette activité envoie les scripts de post-lancement vers des machines Windows et/ou Linux, en fonction des serveurs identifiés pour la migration.

Note

Avant de lancer les scripts de post-lancement, vous devez copier les fichiers dans un dossier du serveur d'automatisation de la migration.

Suivez la procédure ci-dessous pour envoyer les scripts de post-lancement aux machines Windows.

1. Sur la console Migration Factory, sélectionnez Jobs dans le menu de gauche, sélectionnez Actions, puis Run Automation sur le côté droit.
2. Entrez le nom du job, sélectionnez le script 1-Copy Post Launch Scripts et votre serveur d'automatisation pour exécuter le script. Si le serveur d'automatisation n'existe pas, assurez-vous de terminer la [création d'un serveur d'automatisation de la migration](#).
3. La sélection de Linux Secrets et/ou Windows Secrets dépend du système d'exploitation que vous utilisez pour cette vague. Indiquez un emplacement source Linux et/ou un emplacement source Windows.
4. Choisissez la vague sur laquelle vous souhaitez exécuter l'automate, puis choisissez Submit Automation Job.
5. Vous serez redirigé vers la page de liste des tâches, le statut de la tâche doit être en cours d'exécution et vous pouvez choisir Actualiser pour voir le statut. Il devrait devenir Complet au bout de quelques minutes.

Vérifiez l'état de la réplication

Cette activité vérifie automatiquement l'état de réplication des serveurs sources concernés. Le script se répète toutes les cinq minutes jusqu'à ce que l'état de tous les serveurs sources de la vague donnée passe à l'état Sain.

Utilisez la procédure suivante pour vérifier l'état de la réplication.

1. Sur la console Migration Factory, sélectionnez Jobs dans le menu de gauche, sélectionnez Actions, puis Run Automation sur le côté droit.
2. Entrez le nom du job, sélectionnez 2-Verify Replication Status script et votre serveur d'automatisation pour exécuter le script. Si le serveur d'automatisation n'existe pas, assurez-vous de terminer la [création d'un serveur d'automatisation de la migration](#).
3. Choisissez la vague sur laquelle vous souhaitez exécuter l'automate, puis choisissez Submit Automation Job.
4. Vous serez redirigé vers la page de liste des tâches, le statut de la tâche devrait être en cours d'exécution et vous pouvez cliquer sur le bouton Actualiser pour voir le statut. Il devrait devenir Complet au bout de quelques minutes.

The screenshot shows the AWS Management Console for the Application Migration Service (MGN). The page title is 'Source servers'. There are 4 active source servers listed in the table below:

Source server name	Alerts	Replication type	Migration lifecycle	Data replication status
ofbiz-db.onpremsim.env	-	Agent based	Ready for testing	Healthy
ofbiz-web.onpremsim.env	-	Agent based	Ready for testing	Healthy
wordpress-db.onpremsim.env	-	Agent based	Ready for testing	Healthy
wordpress-web.onpremsim.env	-	Agent based	Ready for testing	Healthy

Note

La réplication peut prendre un certain temps. Il se peut que vous ne voyiez pas la mise à jour de statut depuis la console d'usine pendant quelques minutes. En option, vous pouvez également vérifier l'état dans le service MGN.

Valider le modèle de lancement

Cette activité valide les métadonnées du serveur dans l'usine de migration et garantit qu'elles fonctionnent avec le modèle EC2 et qu'elles sont exemptes de fautes de frappe. Il validera à la fois les métadonnées de test et de transition.

Utilisez la procédure suivante pour valider le modèle de lancement EC2.

1. Accédez à la console Migration Factory, puis sélectionnez Wave dans le volet de menu.
2. Sélectionnez la vague cible, puis sélectionnez Actions. Sélectionnez Rehost, puis MGN.
3. Sélectionnez Valider le modèle de lancement pour l'action, puis sélectionnez Toutes les applications.
4. Choisissez Soumettre pour lancer la validation.

Après un certain temps, la validation renverra un résultat positif.

Note

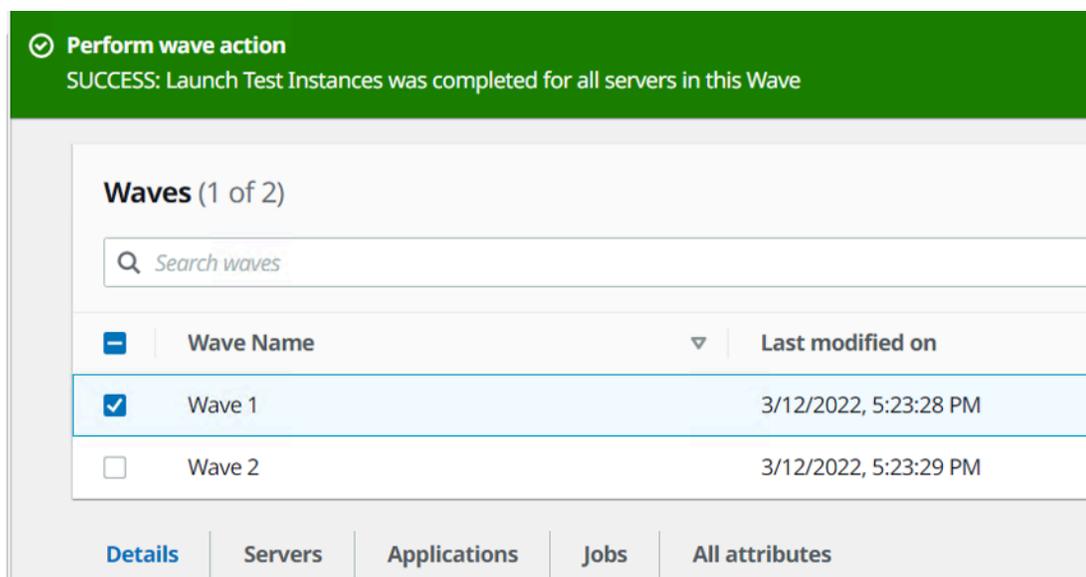
Si la validation échoue, vous recevrez un message d'erreur spécifique :
Les erreurs peuvent être dues à des données non valides dans l'attribut du serveur, telles qu'un Subnet_IDS, SecurityGroup_IDS ou InstanceType non valide.
Vous pouvez accéder à la page Pipeline depuis l'interface Web de Migration Factory et sélectionner le serveur problématique pour corriger les erreurs.

Lancer des instances à des fins de test

Cette activité lance toutes les machines cibles pour une vague donnée dans AWS Application Migration Service (MGN) en mode test.

Utilisez la procédure suivante pour lancer des instances de test.

1. Sur la console Migration Factory, sélectionnez Wave dans le menu de navigation.
2. Sélectionnez la vague cible, puis sélectionnez Actions. Sélectionnez Rehost, puis MGN.
3. Sélectionnez l'action Launch Test Instances, puis sélectionnez Toutes les applications.
4. Choisissez Soumettre pour lancer les instances de test.
5. Après un certain temps, la validation renverra un résultat positif.



Perform wave action
SUCCESS: Launch Test Instances was completed for all servers in this Wave

Waves (1 of 2)

Search waves

	Wave Name	Last modified on
<input checked="" type="checkbox"/>	Wave 1	3/12/2022, 5:23:28 PM
<input type="checkbox"/>	Wave 2	3/12/2022, 5:23:29 PM

Details Servers Applications Jobs All attributes

Note

Cette action mettra également à jour l'état de migration du serveur lancé.

Vérifier l'état de l'instance cible

Cette activité vérifie l'état de l'instance cible en vérifiant le processus de démarrage de tous les serveurs sources concernés au cours de la même vague. Le démarrage des instances cibles peut prendre jusqu'à 30 minutes. Vous pouvez vérifier le statut manuellement en vous connectant à la console Amazon EC2, en recherchant le nom du serveur source et en vérifiant le statut. Vous recevrez un message de vérification de santé indiquant que deux vérifications ont été effectuées avec succès, ce qui indique que l'instance est saine du point de vue de l'infrastructure.

Cependant, dans le cas d'une migration à grande échelle, la vérification de l'état de chaque instance prend du temps. Vous pouvez donc exécuter ce script automatique pour vérifier que les vérifications 2/2 ont réussi le statut de tous les serveurs source au cours d'une vague donnée.

Utilisez la procédure suivante pour vérifier l'état de l'instance cible.

1. Accédez à la console Migration Factory, puis sélectionnez Jobs dans le menu de gauche.
2. Sélectionnez Actions, puis Exécuter l'automatisation sur le côté droit.
3. Entrez le nom du job, sélectionnez le script 3-Verify Instance Status et votre serveur d'automatisation pour exécuter le script. Si le serveur d'automatisation n'existe pas, assurez-vous de terminer la [création d'un serveur d'automatisation de la migration](#).
4. Choisissez la vague sur laquelle vous souhaitez exécuter l'automate, puis choisissez Submit Automation Job.
5. Vous serez redirigé vers la page de liste des tâches, le statut de la tâche doit être en cours d'exécution et vous pouvez choisir Actualiser pour voir le statut. Il devrait devenir Complet au bout de quelques minutes.



Note

Le démarrage de l'instance peut prendre un certain temps et il est possible que vous ne voyiez pas la mise à jour de statut depuis la console d'usine pendant quelques minutes. Migration Factory reçoit également une mise à jour de statut de la part du script. Rafraîchissez l'écran si nécessaire.

Note

Si vos instances cibles échouent aux vérifications de santé 2/2 la première fois, cela peut être dû au fait que le processus de démarrage prend plus de temps. Nous recommandons d'effectuer les bilans de santé une seconde fois environ une heure après le premier bilan de santé. Cela garantit la fin du processus de démarrage. Si les bilans de santé échouent pour la deuxième fois, rendez-vous au [centre de AWS support](#) pour enregistrer un dossier d'assistance.

Marquer comme prêt pour le découpage

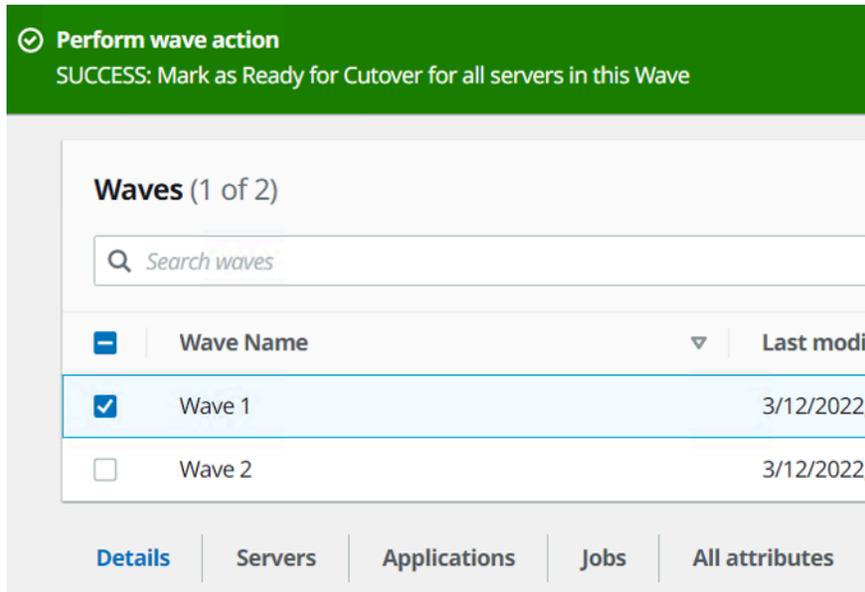
Une fois le test terminé, cette activité modifie l'état du serveur source pour le marquer comme étant prêt pour le passage, afin que l'utilisateur puisse lancer une instance de transfert.

Utilisez la procédure suivante pour valider le modèle de lancement EC2.

1. Sur la console Migration Factory, sélectionnez Wave sur le côté gauche.
2. Sélectionnez la vague cible, puis cliquez sur le bouton Actions. Sélectionnez Rehost, puis MGN.

3. Sélectionnez Marquer comme prêt pour l'action de transfert, puis sélectionnez Toutes les applications.
4. Choisissez Soumettre pour lancer des instances en direct.

Après un certain temps, la validation renverra un résultat positif.



Arrêtez les serveurs sources concernés

Cette activité arrête les serveurs sources concernés par la migration. Après avoir vérifié l'état de réplication des serveurs sources, vous êtes prêt à arrêter les serveurs sources pour arrêter les transactions entre les applications clientes et les serveurs. Vous pouvez arrêter les serveurs sources dans la fenêtre de transition. L'arrêt manuel des serveurs sources peut prendre cinq minutes par serveur et, pour les grandes vagues, cela peut prendre quelques heures au total. Au lieu de cela, vous pouvez exécuter ce script d'automatisation pour arrêter tous vos serveurs au cours de la vague donnée.

Utilisez la procédure suivante pour arrêter tous les serveurs sources concernés par la migration.

1. Sur la console Migration Factory, sélectionnez Jobs dans le menu de gauche, sélectionnez Actions, puis Run Automation sur le côté droit.
2. Entrez le nom du job, sélectionnez le script 3-Shutdown All Servers et votre serveur d'automatisation pour exécuter le script. Si le serveur d'automatisation n'existe pas, assurez-vous de terminer la [création d'un serveur d'automatisation de la migration](#).

3. La sélection de Linux Secrets et/ou Windows Secrets dépend du système d'exploitation que vous utilisez pour cette vague.
4. Choisissez la vague sur laquelle vous souhaitez exécuter l'automate, puis choisissez Submit Automation Job.
5. Vous serez redirigé vers la page de liste des tâches, le statut de la tâche devrait être en cours d'exécution et vous pouvez cliquer sur le bouton Actualiser pour voir le statut. Il devrait devenir Complet au bout de quelques minutes.

Lancer des instances pour Cutover

Cette activité lance toutes les machines cibles pour une vague donnée dans AWS Application Migration Service (MGN) en mode Cutover.

Utilisez la procédure suivante pour lancer des instances de test.

1. Sur la console Migration Factory, sélectionnez Wave sur le côté gauche.
2. Sélectionnez la vague cible, puis sélectionnez Actions. Sélectionnez Rehost, puis MGN.
3. Sélectionnez Launch Cutover Instances Action, sélectionnez Toutes les applications.
4. Choisissez Soumettre pour lancer les instances de test.

Après un certain temps, la validation renverra un résultat positif.

Note

Cette action mettra également à jour l'état de migration du serveur lancé.

Liste des activités de migration automatisées à l'aide d'une invite de commande

Note

Nous vous recommandons d'exécuter l'automatisation depuis Cloud Migration Factory sur la console AWS. Vous pouvez utiliser les étapes suivantes pour exécuter des scripts d'automatisation. Assurez-vous de télécharger les scripts d'automatisation depuis le GitHub dépôt et de configurer le serveur d'automatisation en suivant les étapes décrites dans

[Exécuter les automatisations à partir de l'invite de commande](#), et en suivant les instructions pour configurer les autorisations dans [Configurer les AWS autorisations pour le serveur d'automatisation de la migration](#).

La AWS solution Cloud Migration Factory on déploie des activités de migration automatisées que vous pouvez exploiter pour vos projets de migration. Vous pouvez suivre les activités de migration répertoriées ci-dessous et les personnaliser en fonction des besoins de votre entreprise.

Avant de commencer toute activité, vérifiez que vous êtes connecté à votre serveur d'automatisation de la migration en tant qu'utilisateur de domaine avec une autorisation d'administrateur local sur les serveurs source concernés.

 Important

Vous devez vous connecter en tant qu'utilisateur administrateur pour effectuer les activités répertoriées dans cette section.

Suivez les procédures suivantes dans le même ordre pour effectuer un test complet de la solution à l'aide des exemples de script et d'activités d'automatisation.

Vérifiez les prérequis

Connectez-vous aux serveurs source concernés pour vérifier les prérequis nécessaires tels que TCP 1500, TCP 443, l'espace libre sur le volume racine, la version du framework .Net et d'autres paramètres. Ces conditions préalables sont requises pour la réplication.

Avant de procéder à la vérification des conditions préalables, vous devez installer le premier agent manuellement sur un serveur source. Cela créera un serveur de réplication dans EC2. Nous nous connecterons à ce serveur pour tester le port 1500. Après l'installation, AWS Application Migration Service (AWSMGN) crée le serveur de réplication dans Amazon Elastic Compute Cloud (Amazon EC2). Dans le cadre de cette activité, vous devrez vérifier le port TCP 1500 entre le serveur source et le serveur de réplication. Pour plus d'informations sur l'installation de l'agent AWS MGN sur vos serveurs sources, reportez-vous aux [instructions d'installation](#) du Guide de l'utilisateur du service de migration d'applications.

Utilisez la procédure suivante lorsque vous êtes connecté au serveur d'automatisation de la migration pour vérifier les conditions préalables.

1. Connectez-vous en tant qu'administrateur, ouvrez une invite de commande (CMD . exe).
2. Accédez au `c:\migrations\scripts\script_mgn_0-Prerequisites-checks` dossier et exécutez la commande Python suivante :

```
python 0-Prerequisites-checks.py --Waveid <wave-id> --ReplicationServerIP <rep-server-ip>
```

Remplacez `<wave-id>` et `< rep-server-ip >` par les valeurs appropriées :

- WaveidIl s'agit d'une valeur entière unique permettant d'identifier vos vagues de migration.
- La ReplicationServerIP valeur identifie l'adresse IP du serveur de réplication. Remplacez cette valeur par l'adresse IP Amazon EC2. Pour localiser cette adresse, connectez-vous au AWS Management Console, recherchez Replication, sélectionnez l'un des serveurs de réplication et copiez l'adresse IP privée. Si la réplication a lieu sur Internet public, utilisez plutôt l'adresse IP publique.

3. Le script récupère automatiquement une liste de serveurs pour la vague spécifiée.

Le script vérifie ensuite les conditions requises pour les serveurs Windows et renvoie l'état correspondant à l'une ou l'autre des vérifications `pass` ou `fail` à chaque vérification.

Note

Vous pouvez recevoir un avertissement de sécurité comme celui-ci lorsque le PowerShell script n'est pas fiable. Exécutez la commande suivante PowerShell pour résoudre le problème :

```
Unblock-File C:\migrations\scripts\script_mgn_0-Prerequisites-checks\0-Prerequisites-Windows.ps1
```

Ensuite, le script vérifie les serveurs Linux.

Une fois les vérifications terminées, le script renverra un résultat final pour chaque serveur.

```
*****
**** Final results for all servers ****
*****

-----
-- Windows server passed all Pre-requisites checks --
-----

Server-T1.mydomain.local
server1.mydomain.local
Server-T15.mydomain.local
server2.mydomain.local

-----
-- Linux server passed all Pre-requisites checks --
-----

MF-RHEL.mydomain.local
MF-Ubuntu.mydomain.local
```

Si le serveur échoue à une ou plusieurs vérifications préalables, vous pouvez identifier le serveur défaillant en consultant le message d'erreur détaillé fourni à la fin de la vérification ou en faisant défiler les détails du journal.

Le script mettra également à jour l'état de migration de la solution dans l'interface Web de Migration Factory, comme indiqué dans la capture d'écran suivante d'un exemple de projet.

Installation des agents de réplication

Note

Avant d'installer l'agent, assurez-vous que [AWSMGN est initialisé dans chaque compte cible](#).

Utilisez la procédure suivante pour installer automatiquement les agents de réplication sur les serveurs sources concernés.

1. Sur le serveur d'automatisation de la migration, si vous êtes connecté en tant qu'administrateur, ouvrez une invite de commande (CMD.exe).
2. Accédez au `c:\migrations\scripts\script_mgn_1-AgentInstall` dossier et exécutez la commande Python suivante :

```
python 1-AgentInstall.py --Waveid <wave-id>
```

Remplacez < wave-id > par la valeur Wave ID appropriée pour installer l'agent de réplication sur tous les serveurs de la vague identifiée. Le script installera l'agent sur tous les serveurs sources au cours de la même vague, un par un.

Note

Pour réinstaller l'agent, vous pouvez ajouter un `--force` argument.

3. Le script génère une liste identifiant les serveurs sources inclus pour la vague spécifiée. En outre, des serveurs identifiés dans plusieurs comptes et pour différentes versions de système d'exploitation peuvent également être fournis.

Si des machines Linux sont incluses dans cette vague, vous devez saisir vos informations de connexion Linux sudo pour vous connecter à ces serveurs sources.

L'installation démarre sous Windows, puis passe à Linux pour chacun d'entre eux. Compte AWS.

```
*****
**** Installing Agents ****
*****

#####
### In Account: 515801112200 , region: us-east-1 ###
#####

-----
- Installing Application Migration Service Agent for: Server-T1.mydomain.local -
-----

** Successfully downloaded Agent installer for: Server-T1.mydomain.local **
Verifying that the source server has enough free disk space to install the AWS Replication Agent.
(a minimum of 2 GB of free disk space is required)
Identifying volumes for replication.
Disk to replicate identified: c:\0 of size 30 GiB
All volumes for replication were successfully identified.
Downloading the AWS Replication Agent onto the source server... Finished.
Installing the AWS Replication Agent onto the source server... Finished.
Syncing the source server with the Application Migration Service Console... Finished.
The following is the source server ID: s-3fe3e5342c624e6a0.
The AWS Replication Agent was successfully installed.
The installation of the AWS Replication Agent has started.

** Installation finished for : Server-T1.mydomain.local **
```

Note

Vous pouvez recevoir un avertissement de sécurité comme celui-ci lorsque le PowerShell script n'est pas fiable. Exécutez la commande suivante PowerShell pour résoudre le problème :

```
Unblock-File C:\migrations\scripts\script_mgn_1-AgentInstall\1-Install-  
Windows.ps1
```

Les résultats sont affichés une fois que le script a terminé d'installer les agents de réplication. Consultez les résultats pour détecter les messages d'erreur afin d'identifier les serveurs qui n'ont pas pu installer les agents. Vous devrez installer manuellement les agents sur les serveurs défectueux. Si l'installation manuelle échoue, rendez-vous au [centre de AWS support](#) et enregistrez un dossier de support.

```
*****  
*Checking Agent install results*  
*****  
  
-- SUCCESS: Agent installed on server: Server-T1.mydomain.local  
-- SUCCESS: Agent installed on server: server1.mydomain.local  
-- FAILED: Agent install failed on server: MF-RHEL.mydomain.local  
-- SUCCESS: Agent installed on server: Server-T15.mydomain.local  
-- SUCCESS: Agent installed on server: server2.mydomain.local  
-- SUCCESS: Agent installed on server: MF-Ubuntu.mydomain.local
```

Le script fournit également l'état de la migration dans l'interface Web de Migration Factory, comme illustré dans la capture d'écran suivante d'un exemple de projet.

Envoyez les scripts de post-lancement

AWS Application Migration Service prend en charge les scripts de post-lancement pour vous aider à automatiser les activités au niveau du système d'exploitation, telles que l'installation/la désinstallation de logiciels après le lancement d'instances cibles. Cette activité envoie les scripts de post-lancement vers des machines Windows et/ou Linux, en fonction des serveurs identifiés pour la migration.

Utilisez la procédure suivante depuis le serveur d'automatisation de la migration pour transférer les scripts de post-lancement vers les machines Windows.

1. Connectez-vous en tant qu'administrateur, ouvrez une invite de commande (CMD.exe).
2. Accédez au `c:\migrations\scripts\script_mgn_1-FileCopy` dossier et exécutez la commande Python suivante :

```
python 1-FileCopy.py --Waveid <wave-id> --WindowsSource <file-path> --  
LinuxSource <file-path>
```

<wave-id> Remplacez-le par la valeur Wave ID appropriée et <file-path> par le chemin complet du fichier Source, où se trouve le script. Par exemple, c:\migrations\scripts\script_mgn_1-FileCopy. Cette commande copie tous les fichiers du dossier source vers le dossier de destination.

Note

Au moins l'un de ces deux arguments doit être fourni : WindowsSource, LinuxSource. Si vous fournissez un WindowsSource chemin, ce script ne transmettra les fichiers qu'aux serveurs Windows de cette vague, de la même manière qu' LinuxSource ne transmet des fichiers qu'aux serveurs Linux de cette vague. Si vous fournissez les deux, les fichiers seront envoyés aux serveurs Windows et Linux.

3. Le script génère une liste identifiant les serveurs sources inclus pour la vague spécifiée. En outre, des serveurs identifiés dans plusieurs comptes et pour différentes versions de système d'exploitation peuvent également être fournis.

Si des machines Linux sont incluses dans cette vague, vous devez saisir vos informations de connexion Linux sudo pour vous connecter à ces serveurs sources.

4. Le script copie les fichiers dans le dossier de destination. Si le dossier de destination n'existe pas, la solution crée un répertoire et vous informe de cette action.

Vérifiez l'état de la réplication

Cette activité vérifie automatiquement l'état de réplication des serveurs sources concernés. Le script se répète toutes les cinq minutes jusqu'à ce que l'état de tous les serveurs sources de la vague donnée passe à l'état Sain.

Utilisez la procédure suivante depuis le serveur d'automatisation de la migration pour vérifier l'état de la réplication.

1. Connectez-vous en tant qu'administrateur, ouvrez une invite de commande (CMD.exe).
2. Accédez au \migrations\scripts\script_mgn_2-Verify-replication dossier et exécutez la commande Python suivante :

```
python 2-Verify-replication.py --Waveid <wave-id>
```

<wave-id> Remplacez-le par la valeur Wave ID appropriée pour vérifier l'état de la réplication. Le script vérifie les détails de réplication pour tous les serveurs de la vague spécifique et met à jour l'attribut d'état de réplication pour le serveur source identifié dans la solution.

3. Le script génère une liste identifiant les serveurs inclus pour la vague spécifiée.

L'état attendu des serveurs source concernés prêts à être lancés est « Sain ». Si vous recevez un statut différent pour un serveur, cela signifie qu'il n'est pas encore prêt à être lancé.

La capture d'écran suivante d'un exemple de vague montre que tous les serveurs de la vague en cours ont terminé la réplication et sont prêts à être testés ou transférés.

```
*****
* Verify replication status *
*****
Migration Factory : You have successfully logged in

#####
### Replication Status for Account: 515800000000 , region: us-east-1 ###
#####
Server Server-T1 replication status: Healthy
Server Server1 replication status: Healthy

#####
### Replication Status for Account: 114707000000 , region: us-east-2 ###
#####
Server MF-Ubuntu replication status: Healthy
Server Server-T15 replication status: Healthy
Server Server2 replication status: Healthy
```

Vous pouvez éventuellement vérifier le statut dans l'interface Web de Migration Factory.

Vérifier l'état de l'instance cible

Cette activité vérifie l'état de l'instance cible en vérifiant le processus de démarrage de tous les serveurs sources concernés au cours de la même vague. Le démarrage des instances cibles peut prendre jusqu'à 30 minutes. Vous pouvez vérifier le statut manuellement en vous connectant à

la console Amazon EC2, en recherchant le nom du serveur source et en vérifiant le statut. Vous recevrez un message de vérification de santé indiquant que deux vérifications ont été effectuées avec succès, ce qui indique que l'instance est saine du point de vue de l'infrastructure.

Toutefois, pour une migration à grande échelle, la vérification de l'état de chaque instance prend du temps. Vous pouvez donc exécuter ce script automatique pour vérifier que les vérifications 2/2 ont réussi le statut de tous les serveurs source au cours d'une vague donnée.

Utilisez la procédure suivante depuis le serveur d'automatisation de la migration pour vérifier l'état de l'instance cible.

1. Connectez-vous en tant qu'administrateur, ouvrez une invite de commande (CMD.exe).
2. Accédez au `c:\migrations\scripts\script_mgn_3-Verify-instance-status` dossier et exécutez la commande Python suivante :

```
python 3-Verify-instance-status.py --Waveid <wave-id>
```

<wave-id> Remplacez-le par la valeur Wave ID appropriée pour vérifier l'état de l'instance. Ce script vérifie le processus de démarrage de l'instance pour tous les serveurs sources de cette vague.

3. Le script renvoie une liste de serveurs et des identifiants d'instance pour la vague spécifiée.
4. Le script renverra ensuite une liste d'identifiants d'instances cibles.

Note

Si vous recevez un message d'erreur indiquant que l'ID de l'instance cible n'existe pas, la tâche de lancement est peut-être toujours en cours d'exécution. Patientez quelques minutes avant de continuer.

5. Vous recevrez des vérifications de l'état des instances qui indiqueront si vos instances cibles ont passé avec succès les tests de santé 2/2.

Note

Si vos instances cibles échouent aux vérifications de santé 2/2 la première fois, cela peut être dû au fait que le processus de démarrage prend plus de temps. Nous recommandons d'effectuer les bilans de santé une seconde fois environ une heure après le premier bilan.

de santé. Cela garantit la fin du processus de démarrage. Si les bilans de santé échouent pour la deuxième fois, rendez-vous au [centre de AWS support](#) pour enregistrer un dossier d'assistance.

Arrêtez les serveurs sources concernés

Cette activité arrête les serveurs sources concernés par la migration. Après avoir vérifié l'état de réplication des serveurs sources, vous êtes prêt à arrêter les serveurs sources pour arrêter les transactions entre les applications clientes et les serveurs. Vous pouvez arrêter les serveurs sources dans la fenêtre de transition. L'arrêt manuel des serveurs sources peut prendre cinq minutes par serveur et, pour les grandes vagues, cela peut prendre quelques heures au total. Au lieu de cela, vous pouvez exécuter ce script d'automatisation pour arrêter tous vos serveurs au cours de la vague donnée.

Utilisez la procédure suivante depuis le serveur d'automatisation de la migration pour arrêter tous les serveurs sources impliqués dans la migration.

1. Connectez-vous en tant qu'administrateur, ouvrez une invite de commande (CMD .exe).
2. Accédez au `c:\migrations\scripts\script_mgn_3-Shutdown-all-servers` dossier et exécutez la commande Python suivante :

```
Python 3-Shutdown-all-servers.py -Waveid <wave-id>
```

3. <wave-id>Remplacez-le par la valeur Wave ID appropriée pour arrêter les serveurs sources.
3. Le script renvoie une liste de serveurs et des identifiants d'instance pour la vague spécifiée.
4. Le script arrête d'abord les serveurs Windows au cours de la vague spécifiée. Une fois les serveurs Windows arrêtés, le script passe dans l'environnement Linux et demande les informations de connexion. Une fois la connexion établie, le script arrête les serveurs Linux.

Récupérez l'adresse IP de l'instance cible

Cette activité permet de récupérer l'adresse IP de l'instance cible. Si la mise à jour du DNS est un processus manuel dans votre environnement, vous devez obtenir les nouvelles adresses IP pour toutes les instances cibles. Cependant, vous pouvez utiliser le script d'automatisation pour exporter les nouvelles adresses IP de toutes les instances de la vague donnée vers un fichier CSV.

Utilisez la procédure suivante à partir du serveur d'automatisation de la migration pour récupérer les adresses IP de l'instance cible.

1. Connectez-vous en tant qu'administrateur, ouvrez une invite de commande (CMD . exe).
2. Accédez au `c:\migrations\scripts\script_mgn_4-Get-instance-IP` dossier et exécutez la commande Python suivante :

```
Python 4-Get-instance-IP.py --Waveid <wave-id>
```

<wave-id>Remplacez-la par la valeur Wave ID appropriée pour obtenir les nouvelles adresses IP des instances cibles.

3. Le script renvoie une liste de serveurs et les informations d'ID de l'instance cible.
4. Le script renverra ensuite l'adresse IP du serveur cible.

Le script exporte les informations relatives au nom du serveur et aux adresses IP vers un fichier CSV (<wave-id>- <project-name>-lps.csv) et le place dans le même répertoire que votre script de migration (`c:\migrations\scripts\script_mgn_4-Get-instance-IP`).

Le fichier CSV fournit les détails de `instance_name` et `instance_IPS`. Si l'instance contient plusieurs cartes réseau ou adresses IP, elles seront toutes répertoriées et séparées par des virgules.

Vérifiez les connexions au serveur cible

Cette activité vérifie les connexions pour le serveur cible. Après avoir mis à jour les enregistrements DNS, vous pouvez vous connecter aux instances cibles avec le nom d'hôte. Au cours de cette activité, vous devez vérifier si vous pouvez vous connecter au système d'exploitation à l'aide du protocole RDP (Remote Desktop Protocol) ou via un accès Secure Shell (SSH). Vous pouvez vous connecter manuellement à chaque serveur individuellement, mais il est plus efficace de tester la connexion au serveur à l'aide du script d'automatisation.

Utilisez la procédure suivante depuis le serveur d'automatisation de la migration pour vérifier les connexions au serveur cible.

1. Connectez-vous en tant qu'administrateur, ouvrez une invite de commande (CMD . exe).

2. Accédez au `c:\migrations\scripts\script_mgn_4-Verify-server-connection` dossier et exécutez la commande Python suivante :

```
Python 4-Verify-server-connection.py --Waveid <wave-id>
```

<wave-id>Remplacez-la par la valeur Wave ID appropriée pour obtenir les nouvelles adresses IP des instances cibles.

Note

Ce script utilise le port RDP 3389 et le port SSH 22 par défaut. <rdp-port><ssh-port>Si nécessaire, vous pouvez ajouter les arguments suivants pour rétablir les ports par défaut : --RDPport --SSHport.

3. Le script renvoie une liste de serveurs.
4. Le script renvoie les résultats des tests pour l'accès RDP et SSH.

Référence

Cette section fournit des références pour le déploiement de la solution Cloud Migration Factory sur AWS.

Collecte de données anonymisée

Cette solution inclut une option permettant d'envoyer des métriques opérationnelles anonymisées à AWS. Nous utilisons ces données pour mieux comprendre la façon dont les clients utilisent cette solution et les services et produits associés. Une fois activé, les informations suivantes sont collectées et envoyées à AWS :

- ID de solution : identifiant de AWS solution
- ID unique (UUID) : identifiant unique généré aléatoirement pour chaque Cloud Migration Factory lors du déploiement de la AWS solution
- Horodatage : horodatage de la collecte de données
- État : le statut est migré une fois qu'un serveur est lancé dans AWS MGN avec cette solution
- Région : AWS région dans laquelle la solution est déployée

Note

AWS sera propriétaire des données recueillies dans le cadre de cette enquête. La collecte de données sera soumise à la politique de [confidentialité d'AWS](#). Pour désactiver cette fonctionnalité, suivez les étapes ci-dessous avant de lancer le AWS CloudFormation modèle.

1. Téléchargez le [AWS CloudFormation modèle](#) sur votre disque dur local.
2. Ouvrez le AWS CloudFormation modèle dans un éditeur de texte.
3. Modifiez la section de mappage du AWS CloudFormation modèle à partir de :

```
Send:  
  AnonymousUsage:  
    Data: 'Yes'
```

par :

```
Send:  
  AnonymousUsage:  
    Data: 'No'
```

4. Connectez-vous à la [console AWS CloudFormation](#).
5. Sélectionnez Créer une pile.
6. Sur la page Créer une pile, section Spécifier le modèle, sélectionnez Télécharger un fichier modèle.
7. Sous Télécharger un fichier modèle, choisissez Choisir un fichier et sélectionnez le modèle modifié sur votre disque local.
8. Choisissez Next et suivez les étapes décrites dans [Lancer la pile](#) dans la section Déploiement automatisé de ce guide.

Ressources connexes

Formation AWS

- [Utilisation des solutions AWS : cours Cloud Migration Factory Skill Builder](#) : vous découvrirez les fonctionnalités, les avantages et la mise en œuvre technique de la solution.
- [Réservé aux partenaires AWS : migration avancée vers AWS \(technique, en classe\)](#) : vous apprendrez à migrer des charges de travail à grande échelle et aborderez les modèles de migration courants, y compris un atelier pratique sur Cloud Migration Factory sur AWS.

Services AWS

- [AWS CloudFormation](#)
- [AWS Lambda](#)
- [Amazon API Gateway](#)
- [Amazon CloudFront](#)
- [Amazon Cognito](#)
- [Amazon DynamoDB](#)
- [Amazon Simple Storage Service](#)
- [AWS Systems Manager](#)
- [AWS Secrets Manager](#)

Ressources AWS

- [CloudEndure Guide Migration Factory](#)

Collaborateurs

Les personnes suivantes ont contribué à ce document :

- Aijun Peng
- Chris Baker
- Dev Kar
- Dilshad Hussein
- Gnanasekaran Kailasam
- Jijo James
- Lakshmi Sudhakar Nekkanti
- Lyka Segura
- Phi Nguyen
- Shyam Kumar
- Sapeksh Madan
- Simon Champion
- Thiemo Belméga
- Vijesh Vijayakumaran Nair
- Wally Lu

Révisions

Date	Modification
Juin 2020	Première version
février 2021	Version v1.1.0 : ajout d'un composant optionnel de suivi des migrations ; pour plus d'informations sur les nouvelles fonctionnalités, reportez-vous au fichier ChangeLog.md dans le référentiel. GitHub
mai 2021	Version v1.1.1 : fonctions AWS Lambda mises à jour pour prendre en charge Python v3.7 ; pour plus d'informations, consultez le fichier ChangeLog.md dans le référentiel. GitHub
août 2021	Version v2.0.0 : nouvelle fonctionnalité d'intégration à AWS Application Migration Service (AWS MGN) ; pour plus d'informations, consultez le fichier ChangeLog.md dans le référentiel. GitHub
septembre 2021	Version v2.0.1 : corrections de bogues ; pour plus d'informations, consultez le fichier ChangeLog.md dans le référentiel. GitHub
octobre 2021	Version v2.0.2 : corrections de bogues ; pour plus d'informations, consultez le fichier ChangeLog.md dans le référentiel. GitHub
juin 2022	Version v3.0.0 : nouvelle interface utilisateur Web et nouvelles fonctionnalités permettant d'exécuter toutes les tâches d'automatisation directement depuis l'interface utilisateur à l'aide de la nouvelle fonctionnalité d'automatisation à distance. Cette version élimine la nécessité de basculer entre les lignes de commande du serveur d'automatisation et l'interface utilisateur Web, offrant ainsi une vue unique de l'automatisation de la migration. Introduction de Replatform to EC2, qui permet à la migration d'effectuer des déploiements de nouvelles instances

Date	Modification	
	<p>EC2 en fonction des configurations chargées dans la banque de données Cloud Migration Factory, offrant ainsi aux vagues de migration la possibilité de combiner plusieurs stratégies de migration, avec Replatform vers EC2 et Rehost à l'aide de MGN gérés via une console Cloud Migration unique. Pour plus d'informations sur les nouvelles fonctionnalités, reportez-vous au fichier ChangeLog.md du référentiel. GitHub</p>	
Octobre 2022	<p>Version v3.1.0 : Ajout de la prise en charge des types de déploiement public AWS WAF, public avec et privé disponibles en option lors du déploiement de la CloudFormation pile. Cette version inclut également des mises à jour mineures basées sur les commentaires de la communauté des utilisateurs. Pour plus d'informations sur les nouvelles fonctionnalités, reportez-vous au fichier ChangeLog.md du référentiel. GitHub</p>	
Décembre 2022	<p>Version v3.2.0 : Ajout du support optionnel pour les fournisseurs d'identité externes et de la gestion des groupes dans la console CMF. Pour plus d'informations sur les nouvelles fonctionnalités, reportez-vous au fichier ChangeLog.md du référentiel. GitHub</p>	
Décembre 2022	<p>Version v3.2.0 : Ajout du support optionnel pour les fournisseurs d'identité externes et de la gestion des groupes dans la console CMF. Mises à jour mineures d'autres composants. Pour plus d'informations sur les mises à jour, reportez-vous au fichier ChangeLog.md du référentiel. GitHub</p>	
janvier 2023	<p>Version v3.2.1 : Mise à jour du package de requêtes python vers la version 4.1.0 afin de limiter les avertissements de sécurité concernant le package python certifi dépendant. Reportez-vous au fichier ChangeLog.md dans le référentiel pour plus de détails. GitHub</p>	

Date	Modification
Avril 2023	Version v3.2.2 : impact atténué causé par les nouveaux paramètres par défaut pour la propriété des objets S3 (ACL désactivées) pour tous les nouveaux compartiments S3. Pour plus d'informations, reportez-vous au fichier ChangeLog.md dans le référentiel. GitHub
Juin 2023	Version v3.3.0 : l'automatisation de l'ingestion de la charge de travail AWS Managed Services (AMS) a été supprimée ; une importante refactorisation du code source pour améliorer la maintenabilité afin de prendre en charge les futures versions ; et des mises à jour mineures et des corrections de bogues apportées à d'autres composants. Pour plus d'informations, reportez-vous au fichier ChangeLog.md dans le référentiel. GitHub
Octobre 2023	Version v3.3.1 : refactorisation importante du code source pour améliorer la maintenabilité afin de prendre en charge les futures versions ; mises à jour mineures et corrections de bogues pour d'autres composants. Pour plus d'informations, reportez-vous au fichier ChangeLog.md dans le référentiel. GitHub
Novembre 2023	Mise à jour de la documentation : ajout des balises de coût de confirmation associées à la solution dans la AppRegistry section Surveillance de la solution avec AWS Service Catalog.
Décembre 2023	Version v3.3.2 : refactorisation importante du code source pour améliorer la maintenabilité afin de prendre en charge les futures versions ; mises à jour mineures et corrections de bogues pour d'autres composants. Pour plus d'informations, reportez-vous au fichier ChangeLog.md dans le référentiel. GitHub
Janvier 2024	Version v3.3.3 : mises à jour mineures des autorisations IAM dans les comptes cibles et autres corrections de bogues, ainsi que la refactorisation du code source pour améliorer la maintenabilité. Pour plus d'informations, reportez-vous au fichier ChangeLog.md dans le référentiel. GitHub

Date	Modification	
Avril 2024	<p>Version v3.3.4 : correction d'un bogue qui provoquait des erreurs lors de l'affichage des attributs JSON dans l'interface utilisateur ; résolution également des erreurs lors de l'exportation vers Excel lorsque les champs contiennent de grandes quantités de données. Pendant les CloudFormation mises à jour, les scripts d'automatisation sont désormais mis à jour. Une nouvelle refactorisation du code a également été réalisée pour améliorer la maintenabilité. Pour plus d'informations, reportez-vous au fichier ChangeLog.md dans le référentiel. GitHub</p>	

Avis

Vous êtes tenu de réaliser votre propre évaluation indépendante des informations contenues dans ce document. Ce document : (a) est fourni à titre informatif uniquement, (b) représente les offres de AWS produits et les pratiques actuelles, qui sont susceptibles d'être modifiées sans préavis, et (c) ne crée aucun engagement ou assurance de la part de AWS ses filiales, fournisseurs ou concédants de licence. AWS les produits ou services sont fournis « tels quels » sans garantie, représentation ou condition d'aucune sorte, qu'elle soit expresse ou implicite. Les responsabilités et obligations AWS de ses clients sont régies par des accords, et ce document ne fait partie d'aucun accord entre AWS et ses clients et ne les modifie pas.

La solution Cloud Migration Factory on AWS est concédée sous licence selon les termes du [MIT No Attribution](#).

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.