



Guide de l'utilisateur

Migration Hub Strategy Recommendations



Migration Hub Strategy Recommendations: Guide de l'utilisateur

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

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

Table of Contents

Quelles sont les recommandations relatives à la stratégie de Migration Hub ?	1
Êtes-vous un client de Strategy Recommendations pour la première fois ?	2
Présentation	2
Services connexes	2
Configuration	4
Inscrivez-vous pour un Compte AWS	4
Création d'un utilisateur doté d'un accès administratif	5
Stratégies, recommandations, utilisateurs et rôles	6
Premiers pas	8
Prérequis	8
Étape 1 : Téléchargez le collecteur	10
Étape 2 : Déployer le collecteur	11
Déployer le collecteur dans vCenter	12
Déployer l'AMI du collecteur	13
Étape 3 : Connectez-vous au collecteur	14
Connectez-vous au collecteur déployé dans vCenter	14
Connectez-vous au collecteur déployé en tant qu' EC2 instance Amazon	15
Étape 4 : Configuration du collecteur	15
Configurations AWS	16
Configurations de vCenter	17
Configurations de serveurs distants	21
Configurations de contrôle de version	23
Préparez vos serveurs distants pour la collecte de données	24
Vérifier la configuration pour la collecte de données	28
Étape 5 : Obtenir des recommandations	30
Recommandations	33
Afficher les recommandations de stratégie	33
Recommandations relatives aux composants de l'application	34
Utilisation des composants de l'application	35
Analyse du code source	37
Analyse de base de données	38
Analyse binaire	40
Recommandations relatives aux serveurs	41
Préférences	42

Sources de données	43
Affichage des sources de données	43
Collecteur de données d'application	44
Données collectées par le collecteur	44
Mise à niveau du collecteur	47
Importation de données	48
Modèle d'importation	49
Supprimer des données	54
Sécurité	55
Protection des données	56
Chiffrement au repos	57
Chiffrement en transit	57
Gestion des identités et des accès	57
Public ciblé	58
Authentification par des identités	59
Gestion des accès à l'aide de politiques	63
Comment fonctionne Migration Hub Strategy Recommendations avec IAM	66
AWS politiques gérées	73
Exemples de politiques basées sur l'identité	80
Résolution des problèmes	84
Utilisation des rôles liés à un service	87
Points de terminaison d'un VPC (AWS PrivateLink)	90
Validation de conformité	92
Utilisation d'autres services	94
AWS CloudTrail	94
Informations sur les recommandations de stratégie dans CloudTrail	94
Comprendre les entrées du fichier journal des recommandations en matière de stratégie	96
Quotas	98
Notes de mise à jour	99
17 novembre 2023	99
12 octobre 2023	99
17 avril 2023	100
17 mars 2023	100
07 novembre 2022	100
27 septembre 2022	100
30 juin 2022	101

18 avril 2022	101
25 février 2022	101
10 février 2022	101
28 janvier 2022	102
14 janvier 2022	102
21 décembre 2021	102
15 décembre 2021	102
25 octobre 2021	103
Historique de la documentation	104
.....	cvii

Quelles sont les recommandations relatives à la stratégie de Migration Hub ?

Migration Hub Strategy Recommendations vous aide à planifier vos initiatives de migration et de modernisation en vous proposant des recommandations de stratégie de migration et de modernisation de chemins de transformation viables pour vos applications.

Strategy Recommendations peut analyser l'inventaire de vos serveurs, votre environnement d'exécution et les fichiers binaires des applications Microsoft IIS, Java Tomcat et Jboss afin de générer des rapports anti-modèles. En outre, vous pouvez configurer votre code source pour permettre à Strategy Recommendations d'effectuer une analyse du code source et de la base de données de toutes vos applications. Strategy Recommendations compare cette analyse à vos objectifs commerciaux et aux préférences de transformation des applications et des bases de données que vous avez fournies pour recommander :

- La stratégie de migration la plus efficace pour chacune de vos applications.
- Outils ou services de migration et de modernisation que vous pouvez utiliser.
- Incompatibilités d'application et anti-modèles à résoudre pour une option spécifique.

Migration Hub Strategy Recommendations recommande des stratégies de migration et de modernisation pour le réhébergement, la replateforme et le refactoring avec les destinations, outils et programmes de déploiement associés. Pour plus d'informations sur le réhébergement, la replateforme et le refactoring, voir Termes de [migration - 7 R dans le glossaire](#) des directives prescriptives.AWS

Les recommandations stratégiques peuvent recommander des options simples, telles que le réhébergement sur Amazon Elastic Compute Cloud (Amazon EC2) à l'aide du service de migration AWS d'applications (AWS MGN). Des recommandations plus optimisées peuvent inclure le replatforming vers des conteneurs à l'aide d' AWS App2Container ou le refactoring vers des technologies open source telles que .NET Core et PostgreSQL.

Êtes-vous un client de Strategy Recommendations pour la première fois ?

Si c'est la première fois que vous utilisez les recommandations de stratégie, nous vous recommandons de commencer par lire les sections suivantes :

- [Vue d'ensemble des recommandations stratégiques](#)
- [Configuration des recommandations de stratégie](#)
- [Commencer à utiliser les recommandations stratégiques](#)

Vue d'ensemble des recommandations stratégiques

Vous pouvez démarrer l'évaluation de votre portefeuille de serveurs et d'applications en utilisant les recommandations de stratégie de Migration Hub depuis la AWS Migration Hub console. Vous utilisez la console pour configurer et effectuer une évaluation. Après l'évaluation, vous pouvez utiliser la console pour consulter les données d'évaluation pour chaque serveur et application, ainsi que l'outil de transformation recommandé.

Pour recevoir des recommandations de refactorisation et une liste d'incompatibilités, vous pouvez utiliser les recommandations de stratégie pour évaluer le code source et les bases de données de votre application.

Vous pouvez également télécharger les données des recommandations dans un fichier Microsoft Excel.

Services connexes

- [AWS Migration Hub](#)— Vous utilisez la AWS Migration Hub console pour accéder à la console Migration Hub Strategy Recommendations. Il affiche également des informations sur les serveurs auprès desquels vous collectez les données.
- [AWS Application Discovery Service](#)— Vous utilisez Application Discovery Service pour collecter des données sur vos serveurs et applications dans la AWS Migration Hub console avant d'utiliser Strategy Recommendations.
- [AWS Service de migration](#) d' AWS applications — Le service de migration d'applications est le principal service de migration recommandé pour les lift-and-shift migrations vers AWS.

- [AWS Database Migration Service](#)— AWS Database Migration Service est un service Web que vous pouvez utiliser pour migrer les données de votre base de données sur site, sur une instance de base de données Amazon Relational Database Service (Amazon RDS) ou d'une base de données d'une instance Amazon Elastic Compute Cloud (EC2Amazon) vers une base de données sur un service. AWS
- [AWS App2Container](#) — AWS App2Container (A2C) est un outil de ligne de commande permettant de moderniser les applications .NET et Java en applications conteneurisées.
- [Assistant de portage pour .NET](#) — À utiliser pour l'analyse du code source .NET. L'assistant de portage pour .NET est un scanner de compatibilité qui réduit l'effort manuel requis pour porter des applications Microsoft .NET Framework vers .NET Core. L'assistant de portage pour .NET évalue le code source de l'application .NET et identifie les packages tiers APIs et incompatibles.
- [End-of-Support Programme de migration pour Windows Server](#) — Le programme de End-of-Support migration (EMP) pour Windows Server inclut des outils permettant de migrer vos anciennes applications de Windows Server 2003, 2008 et 2008 R2 vers des versions plus récentes prises en charge AWS, sans aucune refactorisation.
- [AWS Schema Conversion Tool](#) : vous pouvez utiliser le AWS Schema Conversion Tool (AWS SCT) pour convertir votre schéma de base de données existant d'un moteur de base de données à un autre.
- Assistant de [migration d'applications Web Windows](#) — [L'assistant](#) de migration d'applications Web Windows pour AWS Elastic Beanstalk est un PowerShell utilitaire interactif qui migre les applications ASP.NET et ASP.NET Core des serveurs Windows IIS locaux vers Elastic Beanstalk.
- [Babelfish pour Aurora PostgreSQL](#) — [Babelfish pour Aurora PostgreSQL](#) est une nouvelle fonctionnalité de l'édition compatible avec Amazon Aurora PostgreSQL qui permet à Aurora de comprendre les commandes des applications écrites pour le serveur Microsoft SQL.

Configuration des recommandations de stratégie

Avant d'utiliser les recommandations de stratégie de Migration Hub pour la première fois, effectuez les tâches suivantes :

Rubriques

- [Inscrivez-vous pour un Compte AWS](#)
- [Création d'un utilisateur doté d'un accès administratif](#)
- [Stratégies, recommandations, utilisateurs et rôles](#)

Inscrivez-vous pour un Compte AWS

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

Pour vous inscrire à un Compte AWS

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

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

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

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

Création d'un utilisateur doté d'un accès administratif

Une fois que vous vous êtes inscrit à un utilisateur administratif Compte AWS, que vous Utilisez l'utilisateur racine d'un compte AWS l'avez sécurisé AWS IAM Identity Center, que vous l'avez activé et que vous en avez créé un, afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en [AWS Management Console](#) tant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez [Connexion en tant qu'utilisateur racine](#) dans le Guide de l'utilisateur Connexion à AWS .

2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

Pour obtenir des instructions, consultez la section [Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root \(console\)](#) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

Pour obtenir des instructions, consultez [Activation d' AWS IAM Identity Center](#) dans le Guide de l'utilisateur AWS IAM Identity Center .

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

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

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

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

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

Attribution d'un accès à d'autres utilisateurs

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

Pour obtenir des instructions, consultez [Création d'un ensemble d'autorisations](#) dans le Guide de l'utilisateur AWS IAM Identity Center .

2. Attribuez des utilisateurs à un groupe, puis attribuez un accès par authentification unique au groupe.

Pour obtenir des instructions, consultez [Ajout de groupes](#) dans le Guide de l'utilisateur AWS IAM Identity Center .

Stratégies, recommandations, utilisateurs et rôles

Nous vous recommandons de créer deux rôles pour les recommandations de stratégie :

- Pour accéder à la console, créez un rôle auquel sont associées les politiques `AWSMigrationHubStrategyConsoleFullAccess` gérées `AWSMigrationHubFullAccess` et les politiques gérées.
- Pour accéder au collecteur de données de l'application Strategy Recommendations, créez un rôle auquel est attachée la politique `AWSMigrationHubStrategyCollector` gérée.

Les politiques gérées par IAM définissent le niveau d'accès des utilisateurs à un service. La politique AWS Migration Hub `AWSMigrationHubFullAccess` gérée donne accès à la console Migration Hub. Pour plus d'informations, consultez la section [Rôles et politiques du Migration Hub](#). Pour plus d'informations sur les politiques `AWSMigrationHubStrategyCollector` gérées `AWSMigrationHubStrategyConsoleFullAccess` et les politiques gérées, consultez [AWS politiques gérées pour les recommandations stratégiques du Migration Hub](#).

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

- Utilisateurs et groupes dans AWS IAM Identity Center :

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

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

Créez un rôle pour la fédération d'identité. Suivez les instructions de la rubrique [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) dans le Guide de l'utilisateur IAM.

- Utilisateurs IAM :

- Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique [Création d'un rôle pour un utilisateur IAM](#) dans le Guide de l'utilisateur IAM.

- (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique [Ajout d'autorisations à un utilisateur \(console\)](#) du Guide de l'utilisateur IAM.

Commencer à utiliser les recommandations stratégiques

Cette section décrit comment démarrer avec les recommandations de stratégie de Migration Hub.

Rubriques

- [Conditions préalables aux recommandations de stratégie](#)
- [Étape 1 : Téléchargez le collecteur de recommandations stratégiques](#)
- [Étape 2 : Déployer le collecteur de recommandations de stratégie](#)
- [Étape 3 : Connectez-vous au collecteur de recommandations stratégiques](#)
- [Étape 4 : Configuration du collecteur de recommandations de stratégie](#)
- [Étape 5 : utilisez les recommandations de stratégie dans la console Migration Hub pour obtenir des recommandations](#)

Conditions préalables aux recommandations de stratégie

Les conditions requises pour utiliser les recommandations de stratégie de Migration Hub sont les suivantes.

- Vous devez avoir un ou plusieurs AWS comptes, et les utilisateurs doivent être configurés pour ces comptes. Pour de plus amples informations, veuillez consulter [Configuration des recommandations de stratégie](#).
- Le client collecteur de données de l'application Strategy Recommendations doit être en mesure de collecter des données à distance depuis les serveurs. Cela nécessite que vous utilisiez un ensemble d'informations d'identification qui fonctionnent pour tous vos serveurs Windows et un ensemble d'informations d'identification qui fonctionnent pour tous vos serveurs Linux. Les informations d'identification doivent être autorisées à créer et à supprimer des répertoires sur vos serveurs.
- La version du collecteur déployée dans vCenter prend en charge VMware vCenter Server V6.0, V6.5, 6.7 ou 7.0.

Vous pouvez également déployer le collecteur dans une EC2 instance Amazon à l'aide de l'AMI du collecteur.

- Vérifiez que votre environnement de système d'exploitation (OS) est pris en charge :
 - Linux

- Amazon Linux 2012.03, 2015.03
- Amazon Linux 2 (mise à jour du 25/9/2018 et versions ultérieures)
- Ubuntu 12,04, 14,04, 16,04, 18,04, 20,04
- Red Hat Enterprise Linux 5.11, 6.10, 7.3, 7.7, 8.1
- CentOS 5.11, 6.9, 7.3
- SUSE 11 SP4, 12 SP5
- Windows
 - Windows Server 2008 R1 SP2, 2008 R2 SP1
 - Windows Server 2012 R1, 2012 R2
 - Windows Server 2016
 - Windows Server 2019
- Pour l'analyse du code source, vos référentiels GitHub et GitHub ceux de votre entreprise doivent disposer d'un jeton d'accès personnel avec l'étendue du dépôt qui peut être partagé avec le client collecteur Strategy Recommendations. Pour plus d'informations sur la création d'un jeton d'accès personnel avec l'étendue du dépôt, voir [Création d'un jeton d'accès personnel](#) dans la GitHubdocumentation.

Pour analyser les référentiels .NET afin de détecter les recommandations de l'assistant de portage pour .NET, vous devez fournir un ordinateur Windows configuré avec l'outil d'évaluation du portage de l'assistant de portage pour .NET. Pour plus d'informations, consultez la section [Prise en main de l'assistant de portage pour .NET](#) dans le guide de l'utilisateur de l'assistant de portage pour .NET.

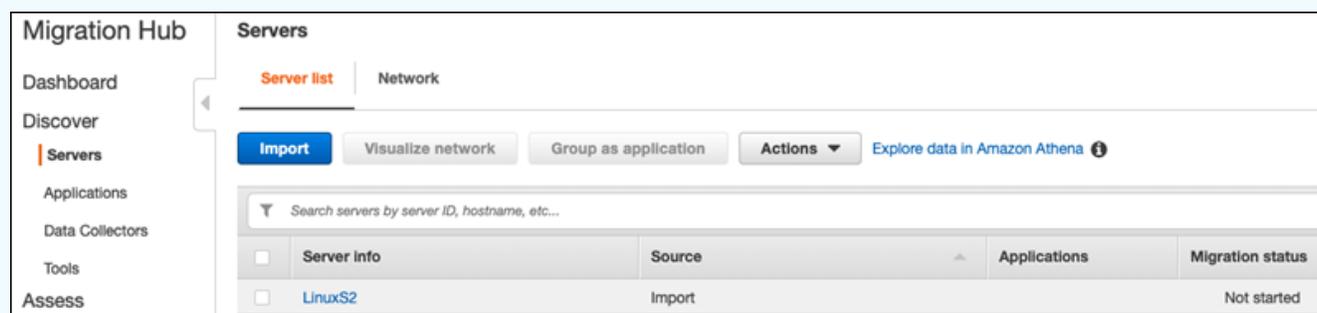
- Pour activer les recommandations de stratégie pour l'analyse de base de données, vous devez entrer des informations d'identification AWS Secrets Manager. Pour de plus amples informations, veuillez consulter [Analyse de la base de données de recommandations stratégiques](#).
- Vous devez utiliser AWS Application Discovery Service pour collecter des données sur vos serveurs et applications dans la AWS Migration Hub console avant d'utiliser les recommandations de stratégie. Vous pouvez utiliser l'une des méthodes suivantes pour collecter les données.
 - Importation du Migration Hub : grâce à l'importation du Migration Hub, vous pouvez importer des informations sur vos serveurs et applications locaux dans Migration Hub. Pour plus d'informations, consultez [Migration Hub Import](#) dans le guide de l'utilisateur d'Application Discovery Service.
 - AWS Application Discovery Service Collecteur sans agent : le collecteur sans agent est une VMware appliance qui collecte des informations sur les machines VMware virtuelles (VMs). Pour

plus d'informations, consultez [Agentless Collector](#) dans le guide de l'utilisateur d'Application Discovery Service.

- AWS Agent de découverte d'applications — L'agent de découverte est AWS un logiciel que vous installez sur vos serveurs locaux et qui permet VMs de capturer les informations système et les détails des connexions réseau entre les systèmes. Pour plus d'informations, consultez la section [AWS Application Discovery Agent](#) dans le Guide de l'utilisateur d'Application Discovery Service.
- Collecteur de données Strategy Recommendations : si vos serveurs sont hébergés dans VMware vCenter et que vous leur donnez accès, Strategy Recommendations peut récupérer automatiquement votre inventaire de serveurs. La console Strategy Recommendations utilisera les informations collectées pour faciliter l'évaluation.

Note

Pour vérifier que l'importation du Migration Hub s'est correctement terminée, dans le volet de navigation de la console Migration Hub, sous Discover, sélectionnez Servers. Tous les serveurs importés doivent être répertoriés.



Étape 1 : Téléchargez le collecteur de recommandations stratégiques

Le collecteur de données de l'application Migration Hub Strategy Recommendations est un dispositif virtuel que vous pouvez installer dans votre VMware environnement local. Le collecteur de données de l'application Strategy Recommendations est également disponible sous forme d'Amazon Machine Image (AMI). Si vous souhaitez utiliser la version AMI du collecteur pour évaluer des AWS applications ou pour toute autre raison, il n'est pas nécessaire de télécharger le collecteur. Vous pouvez ignorer cette section et accéder à [Déployer le collecteur Strategy Recommendations dans une EC2 instance Amazon](#).

Cette section explique comment télécharger le fichier OVA (Open Virtualization Archive) du collecteur que vous utilisez pour déployer le collecteur en tant que machine virtuelle (VM) dans votre VMware environnement.

Pour télécharger le fichier OVA du collecteur

1. À l'aide du AWS compte que vous avez créé [Configuration des recommandations de stratégie](#), connectez-vous à la console Migration Hub AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/migrationhub/>.
2. Dans le volet de navigation de la console Migration Hub, sélectionnez Strategy.
3. Sur la page des recommandations de stratégie du Migration Hub, choisissez Télécharger le collecteur de données.
4. Vous pouvez éventuellement choisir Télécharger le modèle d'importation si vous souhaitez importer des données d'application. Pour plus d'informations sur l'importation de données, veuillez consulter [Importation de données dans les recommandations de stratégie](#).
5. Cliquez sur le bouton Obtenir des recommandations et choisissez Accepter pour autoriser Migration Hub à créer un rôle lié à un service (SLR) sur votre compte. Lorsque vous configurez des recommandations de stratégie pour la première fois, vous devez créer le SLR. Pour de plus amples informations, veuillez consulter [Utilisation de rôles liés à un service pour les recommandations de stratégie](#).

Étape 2 : Déployer le collecteur de recommandations de stratégie

Cette section décrit comment déployer le collecteur de données de l'application Strategy Recommendations. Un collecteur de données d'application est un collecteur de données sans agent qui identifie les applications en cours d'exécution sur vos serveurs, effectue une analyse du code source et analyse vos bases de données.

Il existe deux manières de déployer le collecteur :

- Déployez en tant que machine virtuelle (VM) dans votre VMware vCenter Server. Pour de plus amples informations, veuillez consulter [Déployer le collecteur de recommandations de stratégie dans vCenter](#).
- Si vous souhaitez évaluer AWS des applications, vous pouvez utiliser le collecteur de recommandations stratégiques Amazon Machine Image (AMI). Pour de plus amples informations, veuillez consulter [Déployer le collecteur Strategy Recommendations dans une EC2 instance Amazon](#).

Déployer le collecteur de recommandations de stratégie dans vCenter

Le collecteur de données de l'application Migration Hub Strategy Recommendations est un dispositif virtuel que vous pouvez installer dans votre VMware environnement local. Cette section décrit comment déployer le fichier Open Virtualization Archive (OVA) du collecteur en tant que machine virtuelle (VM) dans votre VMware environnement.

La procédure suivante décrit comment déployer le collecteur Strategy Recommendations dans votre VMware environnement vCenter Server.

Pour déployer le collecteur dans vCenter

1. Connectez-vous à vCenter en tant qu'administrateur. VMware
2. Déployez le fichier OVA que vous avez téléchargé à l'étape 1. Le fichier OVA inclut le collecteur et une CLI qui peuvent être utilisés pour accéder à l'API Strategy Recommendations.

Vous pouvez également télécharger le fichier OVA à partir du lien suivant :

<https://application-data-collector-release.s3.us-west-2.amazonaws.com/ova/latest/AWSMHubApplicationDataCollector.ova>

Nous recommandons les spécifications suivantes pour la machine virtuelle.

Recommandations stratégiques : spécifications de la machine virtuelle du collecteur

- RAM : au moins 8 Go
- CPUs— au moins 4

Note

Pour vous assurer que vous utilisez la dernière version du collecteur avec toutes les nouvelles fonctionnalités et corrections de bogues, mettez à niveau le collecteur après avoir déployé le fichier OVA du collecteur. Pour obtenir des instructions sur la procédure de mise à niveau, consultez [Mise à niveau du collecteur de recommandations stratégiques](#).

Déployer le collecteur Strategy Recommendations dans une EC2 instance Amazon

Si vous souhaitez évaluer AWS des applications, vous pouvez utiliser le collecteur de données d'applications Strategy Recommendations Amazon Machine Image (AMI).

La procédure suivante décrit comment lancer une EC2 instance Amazon à partir de l'AMI du collecteur.

Pour déployer l' EC2 instance Amazon du collecteur

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation en haut de l'écran, la région actuelle est affichée (par exemple, US East (Ohio)). Choisissez une région qui répond à vos besoins parmi les régions utilisées par Strategy Recommendations. Pour une liste de ces régions, voir les [points de terminaison des recommandations stratégiques](#) dans le Références générales AWS.
3. Dans le volet de navigation, sous Images, sélectionnez AMIs.
4. Choisissez Images publiques dans la liste déroulante Owned by me.
5. Choisissez la barre de recherche et sélectionnez le nom de l'AMI dans le menu.
6. Saisissez le nom AWSMHubApplicationDataCollector.
7. Pour vous assurer que l'AMI provient d'une source sécurisée, vérifiez que le propriétaire du compte est 703163444405.
8. Pour lancer une instance à partir de cette AMI, sélectionnez-la, puis choisissez Launch. Pour plus d'informations sur le lancement d'une instance à l'aide de la console, consultez la section [Lancement de votre instance depuis une AMI](#) dans le guide de EC2 l'utilisateur Amazon.

Nous recommandons les spécifications suivantes pour l' EC2 instance Amazon.

Spécifications des EC2 instances Amazon du collecteur Strategy Recommendations

- RAM : 8 Go minimum
- CPUs— Au moins 4

L'AMI Strategy Recommendations inclut le collecteur et une CLI qui peuvent être utilisés pour accéder à l'API Strategy Recommendations.

Note

Pour vous assurer que vous utilisez la dernière version du collecteur avec toutes les nouvelles fonctionnalités et corrections de bogues, mettez à niveau le collecteur après avoir déployé le collecteur Strategy Recommendations en tant qu' EC2 instance Amazon. Pour obtenir des instructions sur la procédure de mise à niveau, consultez [Mise à niveau du collecteur de recommandations stratégiques](#).

Étape 3 : Connectez-vous au collecteur de recommandations stratégiques

Cette section décrit comment se connecter au collecteur de données de l'application Migration Hub Strategy Recommendations déployée. La manière dont vous vous connectez au collecteur dépend de la manière dont vous l'avez déployé.

- [Connectez-vous au collecteur déployé dans l'environnement basé sur vCenter](#)
- [Connectez-vous au collecteur déployé en tant qu' EC2 instance Amazon](#)

Connectez-vous au collecteur déployé dans l'environnement basé sur vCenter

Pour vous connecter au collecteur Strategy Recommendations déployé dans l'environnement basé sur vCenter

1. Utilisez la commande suivante pour vous connecter au collecteur à l'aide d'un client SSH.

```
ssh ec2-user@CollectorIPAddress
```

2. Lorsque vous êtes invité à saisir un mot de passe, entrez le mot de passe par défaut aq1@WSde3. Vous devez modifier le mot de passe la première fois que vous vous connectez.

Connectez-vous au collecteur déployé en tant qu' EC2 instance Amazon

Pour vous connecter au collecteur Strategy Recommendations déployé en tant qu' EC2 instance Amazon

- Utilisez la commande suivante pour vous connecter au collecteur à l'aide d'un client SSH.

```
ssh -i "KeyName.pem" ec2-user@CollectorIPAddress
```

KeyName.pem est la clé privée qui a été générée lorsque vous avez lancé l' EC2 instance Amazon à partir de l'AMI du collecteur.

Étape 4 : Configuration du collecteur de recommandations de stratégie

Cette section décrit comment utiliser les `collector setup` commandes de ligne de commande pour configurer le collecteur de données de l'application Migration Hub Strategy Recommendations. Ces configurations sont stockées localement.

Avant de pouvoir utiliser des `collector setup` commandes, vous devez créer une session shell bash dans le conteneur Docker du collecteur à l'aide de la commande suivante `docker exec`.

```
docker exec -it application-data-collector bash
```

La `collector setup` commande exécute successivement toutes les commandes suivantes, mais vous pouvez les exécuter individuellement :

- `collector setup --aws-configurations`— Configurez AWS les configurations.
- `collector setup --vcenter-configurations`— Configurez les configurations de vCenter.

Note

La configuration de vCenter n'est disponible que si le collecteur est hébergé sur vCenter. Toutefois, vous pouvez forcer la configuration de vCenter à l'aide de la commande.

```
collector setup --vcenter-configurations
```

- `collector setup --remote-server-configurations`— Configurez les configurations de serveurs distants.
- `collector setup --version-control-configurations`— Configurez les configurations de contrôle de version.

Pour configurer toutes les configurations du collecteur en même temps

1. Entrez la commande suivante.

```
collector setup
```

2. Entrez les informations relatives aux AWS configurations comme décrit dans [Configuration des AWS configurations](#).
3. Entrez les informations relatives aux configurations de vCenter comme décrit dans. [Configuration des configurations de vCenter](#)
4. Entrez les informations relatives aux configurations de serveurs distants comme décrit dans [Configuration des configurations de serveurs distants](#).
5. Entrez les informations relatives aux configurations de contrôle de version comme décrit dans [Configuration des configurations de contrôle de version](#).
6. Préparez vos serveurs Windows et Linux pour la collecte des données du collecteur en suivant les instructions de [Préparez vos serveurs Windows et Linux distants pour la collecte de données](#).

Configuration des AWS configurations

Pour configurer des AWS configurations, lors de l'utilisation de la `collector setup` commande ou de la `collector setup --aws-configurations` commande.

1. Entrez Y pour Oui à la case Avez-vous configuré les autorisations IAM... question. Vous configurez ces autorisations lorsque vous avez créé un utilisateur pour accéder au collecteur à l'aide de la politique `AWSMigrationHubStrategyCollector` gérée en suivant les étapes décrites dans [Stratégies, recommandations, utilisateurs et rôles](#).
2. Entrez votre clé d'accès et votre clé secrète à partir du AWS compte sur lequel l'utilisateur que vous avez créé accède au collecteur en suivant les étapes décrites [Stratégies, recommandations, utilisateurs et rôles](#).

3. Entrez une région, par exemple `us-west-2`. Choisissez une région qui répond à vos besoins parmi les régions utilisées par Strategy Recommendations. Pour une liste de ces régions, voir les [points de terminaison des recommandations stratégiques](#) dans le Références générales AWS.
4. Entrez `Y` pour oui aux statistiques relatives au collecteur de téléchargement vers le service de stratégie du hub de migration ? question. Les informations relatives aux métriques vous aident à vous AWS fournir une assistance appropriée.
5. Entrez `Y` pour Oui au service de stratégie Upload Collector to Migration Hub ? question. Les informations issues des journaux permettent de vous AWS fournir une assistance appropriée.

L'exemple suivant montre ce qui est affiché, y compris des exemples d'entrées pour les AWS configurations.

```
Have you setup IAM permissions in you AWS account as per the user guide? [Y/N]: Y
Choose one of the following options for providing user credentials:
1. Long term AWS credentials
2. Temporary AWS credentials
Enter your options [1-2]: 2
AWS session token:
AWS access key ID [None]:
AWS secret access Key [None]:
AWS region name [us-west-2]:
AWS configurations are saved successfully
Upload collector related metrics to migration hub strategy service? By default
collector will upload metrics. [Y/N]: Y
Upload collector related logs to migration hub strategy service? By default collector
will upload logs. [Y/N]: Y
Application data collector configurations are saved successfully
Start registering application data collector
Application data collector is registered successfully.
```

Configuration des configurations de vCenter

Pour configurer les configurations de vCenter, lors de l'utilisation de la `collector setup` commande ou de la `collector setup --vcenter-configurations` commande :

1. Entrez Y pour répondre oui à la question Voulez-vous vous authentifier à l'aide des informations d'identification VMware vCenter, si vous souhaitez vous authentifier à l' VMware aide des informations d'identification vCenter ?

 Note

L'authentification à l'aide des informations d'identification VMware vCenter nécessite VMware l'installation des outils sur les serveurs cibles.

Entrez l'URL de l'hôte, qui peut être l'adresse IP ou l'URL du vCenter. Entrez ensuite le nom d'utilisateur et le mot de passe pour VMware vCenter.

2. Entrez Y pour répondre « oui » à la question Avez-vous des machines Windows gérées par VMware vCenter, si vous souhaitez configurer des serveurs Windows.

Entrez le nom d'utilisateur et le mot de passe pour Windows.

 Note

Si votre serveur distant Windows appartient à un domaine Active Directory, vous devez entrer le nom d'utilisateur sous la forme *domain-name \ username* lorsque vous utilisez la CLI pour fournir des configurations de serveur distant. Par exemple, si le nom de votre domaine est *exampledomain* et que votre nom d'utilisateur est *Administrator*, le nom d'utilisateur que vous entrez dans la CLI est *exampledomain \ Administrator*.

3. Entrez Y pour répondre « oui » à la question Configuration pour Linux à l'aide de VMware vCenter, si vous souhaitez configurer des serveurs Linux.

Entrez le nom d'utilisateur et le mot de passe pour Linux.

4. Entrez Y pour répondre à la question « Voulez-vous configurer les informations d'identification pour les serveurs extérieurs à vCenter à l'aide de NTLM pour Windows et basées sur SSH/Cert pour Linux », si vous souhaitez configurer des informations d'identification de serveur distant pour des serveurs extérieurs à vCenter.

5. Pour la question Voulez-vous utiliser les mêmes informations d'identification Windows utilisées lors de la configuration de vCenter, entrez Y pour oui si les informations d'identification pour les machines Windows gérées en dehors de vCenter sont les mêmes que celles fournies lors de la

configuration des informations d'identification pour les machines Windows vCenter. Sinon, entrez N pour non.

Si vous répondez « oui » à la réponse Y, les questions suivantes sont posées.

- a. Entrez Y pour oui à la case Êtes-vous d'accord avec le fait que le collecteur accepte et stocke localement les certificats de serveur en votre nom lors de la première interaction avec les serveurs Windows ? question.
- b. Entrez 1 pour la question Entrez vos options, si vous souhaitez configurer l'authentification SSH.

Si vous choisissez d'utiliser l'authentification SSH, vous devez copier les informations d'identification clés générées sur vos serveurs Linux. Pour de plus amples informations, veuillez consulter [Configurer l'authentification par clé sur les serveurs Linux](#).

L'exemple suivant montre ce qui est affiché, y compris des exemples d'entrées pour les configurations de VMware vCenter.

```
Your Linux remote server configurations are saved successfully.
collector setup -vcenter-configurations
Start setting up vCenter configurations for remote execution
Note: Authenticating using VMware vCenter credentials requires VMware tools to be
installed on the target servers
Would you like to authenticate using VMware vCenter credentials? [Y/N]: y

NOTE: Your vSphere user must have Guest Operations privileges enabled.

Host Url for VMware vCenter: domain-name
Username for VMware vCenter: username
Password for VMware vCenter: password
Reenter password for VMware vCenter: password
Successfully stored vCenter credentials...
Do you have Windows machines managed by VMware vCenter? [Y/N]: y

NOTE: For the best experience, we recommend that you create a new Active Directory user
in the Domain Admins group.

Username for Windows (Domain\User): username
Password for Windows: password
Reenter password for Windows: password
```

Successfully stored windows credentials...

You can verify your setup for vCenter windows machines is correct with "collector diag-check"

Do you have Linux machines managed by VMWare vCenter? [Y/N]: y

Username for Linux: *username*

Password for Linux: *password*

Reenter password for Linux: *password*

Successfully stored linux credentials...

You can verify your setup for vCenter linux machines is correct with "collector diag-check"

Would you like to setup credentials for servers not managed by vCenter using NTLM for windows and SSH/Cert based for Linux? [Y/N]: y

Setting up target server for remote execution:

Would you like to setup credentials for servers not managed by vCenter using NLTM for Windows [Y/N]: y

Would you like to use the same Windows credentials used during vCenter setup? [Y/N]: y

Are you okay with collector accepting and locally storing server certificates on your behalf during first interaction with windows servers? These certificates will be used by collector for secure communication with windows servers [Y/N]: y

Successfully stored windows server credentials...

Please note that all windows server certificates are stored in directory /opt/amazon/application-data-collector/remote-auth/windows/certs

Please note the IP address of the collector and run the script specified in the user documentation on all the windows servers in your inventory

You can verify your setup for remote windows machines is correct with "collector diag-check"

Would you like to setup credentials for servers not managed by vCenter using SSH/Cert based for Linux? [Y/N]: y

Choose one of the following options for remote authentication:

1. SSH based authentication
2. Certificate based authentication

Enter your options [1-2]: 1

Would you like to use the same Linux credentials used during vCenter setup? [Y/N]: y

Generating SSH key on this machine...

Successfully generated SSH key pair

SSH key pair path: /opt/amazon/application-data-collector/remote-auth/linux/keys/id_rsa_assessment

Please add the public key "id_rsa_assessment.pub" to the "\$HOME/.ssh/authorized_keys" file in your remote machines.

You can verify your setup for remote linux machines is correct with "collector diag-check"

Configuration des configurations de serveurs distants

Pour configurer des configurations de serveurs distants, lors de l'utilisation de la `collector setup` commande ou de la `collector setup --remote-server-configurations` commande :

1. Entrez Y pour répondre à la question Voulez-vous configurer les informations d'identification pour les serveurs non gérés par vCenter à l'aide de NLTM pour Windows, si vous souhaitez configurer des serveurs Windows ?

Entrez le nom d'utilisateur et le mot de passe de WinRM.

Note

Si votre serveur distant Windows appartient à un domaine Active Directory, vous devez entrer le nom d'utilisateur sous la forme `domain-name \ username` lorsque vous utilisez la CLI pour fournir des configurations de serveur distant. Par exemple, si le nom de votre domaine est `exampledomain` et que votre nom d'utilisateur est `Administrator`, le nom d'utilisateur que vous entrez dans la CLI est `exampledomain \ Administrator`.

Entrez Y pour oui à la case Êtes-vous d'accord avec le fait que le collecteur accepte et stocke localement les certificats de serveur en votre nom lors de la première interaction avec les serveurs Windows ? question. Les certificats Windows Server sont stockés dans le répertoire `opt/amazon/application-data-collector/remote-auth/windows/certs`.

Vous devez copier les informations d'identification du serveur générées sur vos serveurs Windows. Pour de plus amples informations, veuillez consulter [Configurer la configuration du serveur distant sur les serveurs Windows](#).

2. Entrez Y pour répondre « oui » à la question Configuration pour Linux à l'aide de SSH ou de Cert, si vous souhaitez configurer des serveurs Linux.
3. Entrez 1 pour la question Entrez vos options, si vous souhaitez configurer l'authentification par clé SSH.

Si vous choisissez d'utiliser l'authentification SSH, vous devez copier les informations d'identification clés générées sur vos serveurs Linux. Pour de plus amples informations, veuillez consulter [Configurer l'authentification par clé sur les serveurs Linux](#).

- Entrez 2 pour la question Entrez vos options, si vous souhaitez configurer l'authentification basée sur des certificats.

Pour plus d'informations sur la configuration de l'authentification basée sur des certificats, consultez. [Configurer l'authentification basée sur des certificats sur les serveurs Linux](#)

L'exemple suivant montre ce qui s'affiche, y compris des exemples d'entrées pour les configurations du serveur distant.

```
Setting up target server for remote execution
Would you like to setup credentials for servers not managed by vCenter using NLTM for
Windows [Y/N]: y

NOTE: For the best experience, we recommend that you create a new Active Directory user
in the Domain Admins group.

Username for WinRM (Domain\User): username
Password for WinRM: password
Reenter password for WinRM: password
Are you okay with collector accepting and locally storing server certificates on your
behalf during first interaction with windows servers? These certificates will be used
by collector for secure communication with windows servers [Y/N]: Y
Successfully stored windows server credentials...
Please note that all windows server certificates are stored in directory /opt/amazon/
application-data-collector/remote-auth/windows/certs

Please note the IP address of the collector and run the script specified in the user
documentation on all the windows servers in your inventory
Would you like to setup credentials for servers not managed by vCenter using SSH/Cert
based for Linux? [Y/N]: Y
Choose one of the following options for remote authentication:
1. SSH based authentication
2. Certificate based authentication
Enter your options [1-2]: 1
User name for remote server: username
Generating SSH key on this machine...
SSH key pair path: /opt/amazon/application-data-collector/remote-auth/linux/keys/
id_rsa_assessment
Please add the public key "id_rsa_assessment.pub" to the "$HOME/.ssh/authorized_keys"
file in your remote machines.
Your Linux remote server configurations are saved successfully.
```

Configuration des configurations de contrôle de version

Pour configurer les configurations de contrôle de version, lors de l'utilisation de la `collector setup` commande ou de la `collector setup --version-control-configurations` commande :

1. Entrez Y pour Oui à la case Configurer l'analyse du code source ? question.
2. Entrez 1 pour la question Entrez vos options, si vous souhaitez configurer le point de terminaison du serveur Git.

Entrez `github.com` pour le point de terminaison du serveur GIT :

3. Entrez 2 pour la question Entrez vos options, si vous souhaitez configurer un serveur GitHub d'entreprise.

Entrez le point de terminaison d'entreprise sans `https://`, comme suit : point de terminaison du serveur GIT : *git-enterprise-endpoint*

4. Entrez votre Git *username* et votre accès personnel *token*.
5. Entrez Y pour Oui à la case Avez-vous des référentiels csharp qui devraient être analysés sur une machine Windows ? question, si vous souhaitez analyser le code C#.

Note

Pour analyser les référentiels .NET afin de détecter les recommandations de l'assistant de portage pour .NET, vous devez fournir un ordinateur Windows configuré avec l'outil d'évaluation du portage de l'assistant de portage pour .NET. Pour plus d'informations, consultez la section [Prise en main de l'assistant de portage pour .NET](#) dans le guide de l'utilisateur de l'assistant de portage pour .NET.

6. Pour le Voulez-vous réutiliser les informations d'identification Windows existantes sur cette machine ? question. Entrez Y pour Oui, si la machine Windows pour l'analyse du code source C# utilise les mêmes informations d'identification que celles fournies précédemment dans le cadre de la configuration `--remote-server-configurations` ou `--vcenter-configurations`.

Entrez N pour non, si vous souhaitez saisir de nouvelles informations d'identification.

7. Pour utiliser les informations d'identification de VMWare vCenter Windows Machine, entrez 1 pour Choisissez l'une des options suivantes pour les informations d'identification Windows.
8. Entrez l'adresse IP de l'ordinateur Windows.

L'exemple suivant montre ce qui est affiché, y compris des exemples d'entrées pour les configurations de contrôle de version.

```
Set up for source code analysis [Y/N]: y
Choose one of the following options for version control type:
1. GIT
2. GIT Enterprise
3. Azure DevOps - Git
Enter your options [1-3]: 3
Your server endpoint: dev.azure.com (http://dev.azure.com/)
Your DevOps Organization name: <Your organization name>
Personal access token [None]:
Your version control credentials are saved successfully.
Do you have any csharp repositories that should be analyzed on a windows machine? [Y/N]: y
Would you like to reuse existing windows credentials on this machine? [Y/N]: y
Choose one of the following options for windows credentials:
1. VMWare vCenter Windows Machine
2. Standard Windows Machine
Enter your options [1-2]:
1
Windows machine IP Address: <Your windows machine IP address>
Using VMWare vCenter Windows Machine credentials
Successfully stored windows server credentials...
```

Préparez vos serveurs Windows et Linux distants pour la collecte de données

Note

Cette étape n'est pas nécessaire si vous configurez le collecteur de données des applications Strategy Recommendations à l'aide des informations d'identification vCenter.

Après avoir configuré les configurations de vos serveurs distants, si vous utilisez la commande `collector setup command` ou la `collector setup --remote-server-configurations` commande, vous devez préparer vos serveurs distants afin que le collecteur de données des applications Strategy Recommendations puisse collecter des données auprès de ceux-ci.

Note

Vous devez vous assurer que les serveurs sont accessibles à l'aide de leur adresse IP privée. Pour obtenir des instructions supplémentaires sur la configuration de l'environnement via un cloud privé virtuel (VPC) AWS pour une exécution à distance, consultez le guide de [l'utilisateur d'Amazon Virtual Private Cloud](#).

Pour préparer vos serveurs Linux distants, consultez [Préparation de serveurs Linux distants](#).

Pour préparer vos serveurs Windows distants, voir [Configurer la configuration du serveur distant sur les serveurs Windows](#).

Préparation de serveurs Linux distants

Configurer l'authentification par clé sur les serveurs Linux

Si vous choisissez de configurer l'authentification par clé SSH pour Linux lors de la configuration de serveurs distants, vous devez suivre les étapes suivantes pour configurer l'authentification par clé sur vos serveurs afin que les données puissent être collectées par le collecteur de données des applications Strategy Recommendations.

Pour configurer l'authentification par clé sur vos serveurs Linux

1. Copiez la clé publique générée sous le nom `id_rsa_assessment.pub` depuis le dossier suivant du conteneur :

```
/opt/amazon/application-data-collector/remote-auth/linux/keys.
```

2. Ajoutez la clé publique copiée dans le `$HOME/.ssh/authorized_keys` fichier pour toutes les machines distantes. Si aucun fichier n'est disponible, créez-le à l'aide de la `vim` commande `touch` ou.
3. Assurez-vous que le dossier de base du serveur distant possède un niveau d'autorisation inférieur 755 ou égal. Si c'est le cas777, cela ne marchera pas. Vous pouvez utiliser la `chmod` commande pour restreindre les autorisations.

Configurer l'authentification basée sur des certificats sur les serveurs Linux

Si vous choisissez de configurer l'authentification basée sur des certificats pour Linux lors de la configuration de serveurs distants, vous devez effectuer les étapes suivantes afin que les données puissent être collectées par le collecteur de données de l'application Strategy Recommendations.

Nous recommandons cette option si l'autorité de certification (CA) est déjà configurée pour vos serveurs d'applications.

Pour configurer l'authentification basée sur des certificats sur vos serveurs Linux

1. Copiez le nom d'utilisateur qui fonctionne avec tous vos serveurs distants.
2. Copiez la clé publique du collecteur sur l'autorité de certification.

La clé publique du collecteur se trouve à l'emplacement suivant :

```
/opt/amazon/application-data-collector/remote-auth/linux/keys/id_rsa_assessment.pub
```

Cette clé publique doit être ajoutée à votre autorité de certification pour générer le certificat.

3. Copiez le certificat généré à l'étape précédente à l'emplacement suivant dans le collecteur :

```
/opt/amazon/application-data-collector/remote-auth/linux/keys
```

Le nom du certificat doit être `id_rsa_assessment-cert.pub`.

4. Indiquez le nom du fichier de certificat lors de l'étape de configuration.

Configurer la configuration du serveur distant sur les serveurs Windows

Si vous choisissez de configurer Windows lors de la configuration de serveurs distants dans la configuration du collecteur, vous devez effectuer les étapes suivantes afin que les données puissent être collectées conformément aux recommandations de stratégie.

 Pour en savoir plus sur le PowerShell script exécuté sur le serveur distant, lisez cette note.

Le script active la PowerShell télécommande et désactive toutes les méthodes d'authentification autres que la négociation. Ceci est utilisé pour Windows NT LAN Manager (NTLM) et définit le WSMAN protocole « AllowUnencrypted » sur false pour garantir que le récepteur nouvellement créé accepte uniquement le trafic crypté. À l'aide du script fourni par `MicrosoftNew-SelfSignedCertificateEx.ps1`, il crée un certificat auto-signé.

Toute WSMAN instance dotée d'un écouteur HTTP est supprimée en même temps que les écouteurs HTTPS existants. Ensuite, il crée un nouvel écouteur HTTPS. Il crée également une règle de pare-feu entrant pour le port TCP 5986. Dans la dernière étape, le service WinRM est redémarré.

Pour configurer la collecte de données via une connexion à distance sur vos serveurs Windows 2008

1. Utilisez la commande suivante pour vérifier la version de PowerShell installée sur votre serveur.

```
$PSVersionTable
```

2. Si la PowerShell version n'est pas 5.1, téléchargez et installez WMF 5.1 en suivant les instructions de la section [Installer et configurer WMF 5.1](#) dans la documentation Microsoft.
3. Utilisez la commande suivante dans une nouvelle PowerShell fenêtre pour vous assurer que la PowerShell version 5.1 est installée.

```
$PSVersionTable
```

4. Suivez les étapes suivantes, qui décrivent comment configurer la collecte de données via une connexion à distance sous Windows 2012 et versions ultérieures.

Pour configurer la collecte de données par le biais d'une connexion à distance sur vos serveurs Windows 2012 et versions plus récentes

1. Téléchargez le script de configuration à partir de l'URL suivante :

<https://application-data-collector-release.s3.us-west-2.amazonaws.com/scripts/WinRMSetup.ps1>

2. Téléchargez-le `New-SelfSignedCertificateEx.ps1` à partir de l'URL suivante et collez-le dans le même dossier que celui dans lequel vous l'avez téléchargé `WinRMSetup.ps1` :

<https://github.com/Azure/azure-libraries-for-net/blob/master/Samples/Asset/New-SelfSignedCertificateEx.ps1>

3. Pour terminer la configuration, exécutez le PowerShell script téléchargé sur tous les serveurs d'applications.

```
.\WinRMSetup.ps1
```

Note

Si la gestion à distance Windows (WinRM) n'est pas correctement configurée sur le serveur Windows Remote Server, toute tentative de collecte de données à partir de ce serveur échouera. Dans ce cas, vous devez supprimer le certificat correspondant à ce serveur à l'emplacement suivant sur le conteneur :

```
/opt/amazon/application-data-collector/remote-auth/windows/certs/ads-server-id.cer
```

Après avoir supprimé le certificat, attendez que le processus de collecte de données soit réessayé.

Vérifiez que votre collecteur et vos serveurs sont configurés pour la collecte de données

Vérifiez que votre collecteur et vos serveurs sont correctement configurés pour la collecte de données à l'aide de la commande suivante.

```
collector diag-check
```

Cette commande effectue un ensemble de tests de diagnostic sur les configurations de votre serveur et fournit des informations sur les vérifications qui ont échoué.

Lorsque vous utilisez la commande en -a mode, vous obtenez le résultat dans un fichier DiagnosticCheckResult.txt une fois les vérifications terminées.

```
collector diag-check -a
```

Vous pouvez effectuer un diagnostic sur les configurations de serveur d'un seul serveur à l'aide de l'adresse IP de ce serveur.

Les exemples suivants montrent le résultat d'une installation réussie.

serveur Linux

```
Provide your test server IP address: IP address
```

```
-----  
Start checking connectivity & credentials...  
Connectivity and Credential Checks succeeded
```

```
-----  
Start checking permissions...  
Permission Check succeeded  
-----  
Start checking OS version...  
OS version check succeeded  
-----  
Start checking Linux Bash installation...  
Linux Bash installation check succeeded  
-----  
All diagnostic checks complete successfully.  
This server is correctly set up and ready for data collection.
```

serveur Windows

```
Windows PowerShell Version Check succeeded  
Provide your test server IP address: IP address  
-----  
Start checking connectivity & credentials...  
Connectivity and Credential Checks succeeded  
-----  
Start checking permissions...  
Permission Check succeeded  
-----  
Start checking OS version...  
OS version check succeeded  
-----  
Start checking Windows architecture type...  
Windows Architecture Type Check succeeded  
-----  
All diagnostic checks complete successfully.  
This server is correctly set up and ready for data collection.
```

L'exemple suivant montre un message d'erreur qui s'affiche lorsque les informations d'identification de votre serveur distant sont incorrectes.

```
Unable to authenticate the server credentials with IP address ${IPAddress}.  
Ensure that your credentials are accurate and the server is configured correctly.  
Use the following command to reset incorrect credentials.
```

```
collector setup --remote-server-configurations
```

Étape 5 : utilisez les recommandations de stratégie dans la console Migration Hub pour obtenir des recommandations

Cette section explique comment utiliser les recommandations de stratégie dans la console Migration Hub pour obtenir des recommandations de migration pour la première fois.

Obtention de recommandations

1. À l'aide du AWS compte que vous avez créé [Configuration des recommandations de stratégie](#), connectez-vous à la console Migration Hub AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/migrationhub/>.
2. Dans le volet de navigation de la console Migration Hub, sélectionnez Strategy.
3. Sur la page Recommandations relatives à la stratégie du Migration Hub, sélectionnez Obtenir des recommandations.
4. Choisissez Accepter si vous acceptez d'autoriser Migration Hub à créer un rôle lié à un service (SLR) sur votre compte. Pour plus d'informations sur le réflex, consultez [Utilisation de rôles liés à un service pour les recommandations de stratégie](#).
5. Configuration des sources de données
 - a. Sur la page Configurer les sources de données, vous devez choisir la source de vos serveurs à analyser parmi les options suivantes :
 - i. Collecteur de données d'application Strategy Recommendations : vous pouvez utiliser le collecteur Strategy Recommendations pour récupérer automatiquement les informations VMs relatives à l'hébergement dans VMware vCenter. Avec cette option, vous n'avez pas besoin d'effectuer de configuration supplémentaire.
 - ii. Importation manuelle : si vous souhaitez importer des données relatives à vos serveurs et applications de manière indépendante, vous pouvez utiliser le modèle d'importation Strategy Recommendations. Le modèle d'importation est un fichier JSON dans lequel vous pouvez renseigner les informations disponibles pour votre VMs.
 - iii. Application Discovery Service : vous pouvez utiliser Application Discovery Service pour recueillir des informations sur vos applications et serveurs locaux. Dans la console Migration Hub, dans la section Outils, vous pouvez choisir parmi plusieurs options sous

Outils de découverte. Par exemple, vous pouvez choisir Application Discovery Service Agentless Collector, AWS Discovery Agent ou Import (pour les fichiers CSV).

- b. Le tableau Servers répertorie tous les serveurs disponibles en fonction de votre sélection dans la section des sources de données.
- c. Sous Collecteurs de données d'applications enregistrés, les collecteurs de données d'applications que vous avez configurés sont répertoriés. Si vous n'avez configuré aucun collecteur de données, vous pouvez télécharger le collecteur de données, puis le déployer. Pour plus d'informations, consultez [Étape 1 : Téléchargez le collecteur de recommandations stratégiques](#) et [Étape 2 : Déployer le collecteur de recommandations de stratégie](#).

 Note

Pour obtenir des recommandations stratégiques, vous devez configurer au moins un collecteur de données d'application ou effectuer une importation de données d'application. Si vous souhaitez ajouter vos données au niveau de l'application sans configurer de collecteur, vous pouvez utiliser le modèle d'importation des données de l'application. Vous pourrez ajouter des sources de données supplémentaires ultérieurement.

- d. Si vous avez sélectionné Importation manuelle, sous Détails de l'importation, choisissez Ajouter une nouvelle importation.
- e. Dans Nom de l'importation, entrez un nom pour votre importation.
- f. Pour l'URI du compartiment S3, entrez l'URI du compartiment S3 vers lequel le fichier JSON d'importation doit être téléchargé.

 Important

Le nom du compartiment S3 doit commencer par le préfixe **demigrationhub-strategy**.

- g. Choisissez Suivant.
6. Spécifier les préférences
- a. Sur la page Spécifier les préférences, définissez vos objectifs commerciaux et vos préférences de migration. Strategy Recommendations recommande la stratégie optimale pour migrer et moderniser vos applications et bases de données en fonction des préférences que vous spécifiez. Vous pourrez modifier ces préférences ultérieurement.

- b. Choisissez Suivant.
7. Vérifiez et soumettez.
 - a. Passez en revue vos sources de données configurées et vos préférences de migration.
 - b. Si tout semble correct, choisissez Démarrer l'analyse des données. Cela permettra d'effectuer une analyse de l'inventaire de votre serveur et de votre environnement d'exécution, ainsi que des fichiers binaires des applications Microsoft IIS et Java.

 Note

L'état de l'analyse binaire n'est pas affiché dans la console. Lorsque l'analyse est terminée, vous verrez soit un lien vers le rapport anti-modèle, soit un message indiquant que l'analyse a échoué.

Recommandations en matière de stratégie

Cette section explique comment consulter les recommandations stratégiques en matière de migration et de modernisation pour les serveurs et les applications de votre portefeuille de migration.

Rubriques

- [Afficher les recommandations de stratégie dans les recommandations de stratégie](#)
- [Recommandations de stratégie, recommandations relatives aux composants de l'application](#)
- [Recommandations stratégiques : recommandations relatives au serveur](#)
- [Stratégies, recommandations et préférences](#)

Afficher les recommandations de stratégie dans les recommandations de stratégie

Cette section explique comment utiliser les recommandations de stratégie dans la AWS Migration Hub console pour consulter les recommandations de stratégie de migration.

Pour consulter les recommandations de stratégie

1. À l'aide du AWS compte que vous avez créé [Configuration des recommandations de stratégie](#), connectez-vous à la console Migration Hub AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/migrationhub/>.
2. Dans le volet de navigation de la console Migration Hub, choisissez Strategy puis Recommendations.
3. Sur la page Recommendations, vous pouvez consulter et exporter les recommandations récapitulatives de votre portefeuille ainsi que les recommandations détaillées relatives à la stratégie « R » de migration. Vous pouvez également consulter les outils et les destinations de migration et de modernisation, ainsi que les anti-modèles pour vos serveurs et composants d'application.

Les anti-modèles sont une liste de problèmes connus découverts dans votre portefeuille, classés par gravité. Les anti-modèles de sévérité élevée représentent des incompatibilités qui doivent être résolues, les anti-modèles de sévérité moyenne représentent des avertissements, et les anti-modèles de gravité faible représentent des problèmes d'information. Pour plus d'informations

sur la stratégie « R », voir [Termes de migration - 7 R](#) dans le glossaire des directives AWS prescriptives.

- Si un changement survient dans votre centre de données ou si vous mettez à jour vos préférences, nous vous recommandons de réanalyser vos données. Pour réanalyser vos données afin d'obtenir de nouvelles recommandations, choisissez Réanalyser les données.

Jusqu'à ce que le processus de réanalyse soit terminé, les résultats de vos recommandations peuvent être un mélange de données antérieures et de nouvelles données.

Pour télécharger un fichier de rapport contenant les recommandations, choisissez Exporter les recommandations.

4. Dans l'onglet Composants d'application, vous pouvez consulter les recommandations relatives aux composants d'application de votre portefeuille de migration. Pour de plus amples informations, veuillez consulter [Recommandations de stratégie, recommandations relatives aux composants de l'application](#).
5. Dans l'onglet Serveurs, vous pouvez consulter les recommandations relatives aux serveurs de votre portefeuille de migration. Pour de plus amples informations, veuillez consulter [Recommandations stratégiques : recommandations relatives au serveur](#).
6. Dans l'onglet Préférences, vous pouvez modifier les préférences que vous avez spécifiées dans [Étape 5 : Obtenir des recommandations](#). Pour plus d'informations sur la modification de vos préférences, consultez [Stratégies, recommandations et préférences](#).

Recommandations de stratégie, recommandations relatives aux composants de l'application

Cette section explique comment utiliser les recommandations de stratégie dans la console Migration Hub pour afficher et analyser les recommandations de stratégie de migration pour les composants de l'application.

Rubriques

- [Utilisation des composants de l'application dans les recommandations de stratégie](#)
- [Analyse du code source des recommandations stratégiques](#)
- [Analyse de la base de données de recommandations stratégiques](#)
- [Analyse binaire des recommandations de stratégie](#)

Utilisation des composants de l'application dans les recommandations de stratégie

Cette section explique comment utiliser les recommandations de stratégie de Migration Hub dans la console Migration Hub pour afficher et configurer les recommandations de stratégie de migration et de modernisation.

Rubriques

- [Affichage des recommandations relatives aux composants de l'application](#)
- [Configuration de l'analyse du code source pour un composant d'application](#)
- [Configuration de l'analyse de base de données pour un composant d'application](#)

Affichage des recommandations relatives aux composants de l'application

Cette section explique comment utiliser les recommandations de stratégie dans la console Migration Hub pour consulter les recommandations de stratégie de migration pour les composants de l'application.

Pour afficher le détail des recommandations relatives aux composants de l'application

1. À l'aide du AWS compte que vous avez créé [Configuration des recommandations de stratégie](#), connectez-vous à la console Migration Hub AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/migrationhub/>.
2. Dans le volet de navigation de la console Migration Hub, choisissez Strategy puis Recommendations.
3. Sur la page Recommendations, choisissez l'onglet Composants de l'application.
 - a. Sous Résumé des composants de l'application, vous trouverez un aperçu des différents types de composants d'application que vous exécutez dans votre portefeuille de serveurs.
 - b. Sous Composants de l'application, vous pouvez consulter le nom du composant, le type de composant et les recommandations de stratégie « R » de migration. Vous pouvez également consulter la destination de la migration ainsi que les outils de migration et de modernisation à utiliser pour les différents composants d'application exécutés dans votre portefeuille de serveurs. Pour plus d'informations sur la stratégie « R », voir [Termes de migration - 7 R](#) dans le glossaire des directives AWS prescriptives.

4. Pour afficher les détails d'un composant d'application, sélectionnez un composant d'application, puis choisissez Afficher les détails.
5. Sur la page de détails du composant d'application (la page dont le titre est le nom du composant), sous Résumé des recommandations, vous pouvez consulter les recommandations relatives au composant d'application. Vous pouvez également voir les anti-patterns identifiés. Les anti-modèles sont une liste de problèmes connus découverts dans votre portefeuille, classés par gravité.
6. Choisissez l'onglet Options de stratégie pour afficher les recommandations de migration pour le composant de l'application. Vous pouvez annuler la stratégie recommandée en sélectionnant une autre stratégie, puis en choisissant Définir les préférences.
7. Selon le type de composant d'application que vous consultez, il existe un onglet Configuration source ou Configuration de base de données. Pour plus d'informations sur la configuration de la source, consultez [Configuration de l'analyse du code source pour un composant d'application](#). Pour plus d'informations sur la configuration de la base de données, consultez [Configuration de l'analyse de base de données pour un composant d'application](#).

Configuration de l'analyse du code source pour un composant d'application

Cette section décrit comment utiliser les recommandations de stratégie dans la console Migration Hub pour configurer l'analyse du code source pour un composant d'application.

Pour configurer l'analyse du code source pour un composant d'application

1. Dans le volet de navigation de la console Migration Hub, choisissez Strategy puis Recommendations.
2. Sur la page Recommendations, choisissez l'onglet Composants de l'application.
3. Dans la liste des composants sous Composants de l'application, sélectionnez un composant d'application avec un type de composant Java, Dotnetframework ou IIS, puis choisissez Afficher les détails.
4. Sur la page de détails du composant de l'application (page avec le nom du composant comme titre), choisissez l'onglet Configuration du code source.
5. Sous Détails de configuration du code source, choisissez Analyser le code source.
6. Sur la page Analyser le code source, indiquez le nom du référentiel, le nom de la branche et le nom du projet (le cas échéant) qui stocke le code source du composant d'application. Sélectionnez le type de contrôle de version du code GitHub source que vous souhaitez utiliser, puis choisissez Analyser.

Une fois l'analyse terminée, vous pouvez consulter les recommandations mises à jour sur la page de détails des composants de l'application.

Pour plus d'informations sur l'analyse du code source, consultez [Analyse du code source des recommandations stratégiques](#).

Configuration de l'analyse de base de données pour un composant d'application

Cette section décrit comment utiliser les recommandations de stratégie dans la console Migration Hub pour configurer l'analyse de base de données pour un composant d'application.

Pour configurer l'analyse de base de données pour un composant d'application

1. Dans le volet de navigation de la console Migration Hub, choisissez Strategy puis Recommendations.
2. Sur la page Recommendations, choisissez l'onglet Composants de l'application.
3. Dans la liste des composants sous Composants de l'application, sélectionnez un composant d'application avec le type de composant, SQLServer puis choisissez Afficher les détails.
4. Sur la page de détails du composant de l'application (page avec le nom du composant comme titre), choisissez l'onglet Configuration de la base de données.
5. Sous Détails de configuration de la base de données, sélectionnez Analyser les détails de la base de données.
6. Choisissez un nom secret dans le menu déroulant que vous avez créé dans AWS Secrets Manager à utiliser pour les informations d'identification de base de données, puis choisissez Analyser.

Une fois l'analyse terminée, vous pouvez consulter les recommandations mises à jour sur la page de détails des composants de l'application.

Pour plus d'informations sur l'analyse de base de données et la configuration d'un nom secret, consultez [Analyse de la base de données de recommandations stratégiques](#).

Analyse du code source des recommandations stratégiques

Migration Hub Strategy Recommendations identifie automatiquement les applications de votre portefeuille et crée des composants d'application pour celles-ci. Par exemple, si votre portefeuille

contient une application Java, elle est identifiée comme un composant d'application avec un type de composant Java.

Strategy Recommendations analyse le code source des composants de l'application si vous le configurez à cette fin. Pour plus d'informations sur la configuration d'un composant d'application pour l'analyse du code source, consultez [Configuration de l'analyse du code source pour un composant d'application](#).

Strategy Recommendations analyse le code source pour les langages de programmation Java et C#.

Pour plus d'informations sur les conditions préalables à l'utilisation de l'analyse du code source Strategy Recommendations, consultez [Conditions préalables aux recommandations de stratégie](#).

Analyse de la base de données de recommandations stratégiques

Strategy Recommendations identifie automatiquement les serveurs de base de données de votre portefeuille et crée des composants d'application pour ceux-ci. Par exemple, si votre portefeuille contient une base de données SQL Server, elle est identifiée comme le composant d'application sqlservr.exe.

Strategy Recommendations analyse les bases de données individuelles dans le composant d'application SQL Server identifié, sqlservr.exe, à l'aide de l'outil AWS Schema Conversion Tool. Strategy Recommendations identifie également les incompatibilités liées à la migration des bases de données vers des AWS bases de données telles qu'Amazon Aurora MySQL Compatible Edition, Amazon Aurora PostgreSQL Compatible Edition, Amazon RDS for MySQL et Amazon RDS for PostgreSQL.

Actuellement, l'analyse de la base de données Strategy Recommendations n'est disponible que pour SQL Server.

Pour configurer Strategy Recommendations afin d'analyser vos bases de données, vous devez fournir les informations d'identification permettant au collecteur de données de l'application Strategy Recommendations de se connecter à vos bases de données. Pour ce faire, créez un secret dans AWS Secrets Manager de votre AWS compte.

Pour plus d'informations sur les autorisations et les privilèges associés aux informations d'identification que vous fournissez, consultez [Privilèges nécessaires pour les informations d'identification de AWS Schema Conversion Tool](#). Pour plus d'informations sur la création d'un secret à l'aide des informations d'identification, consultez [Création d'un secret dans Secrets Manager pour les informations d'identification de base de données](#).

Après avoir défini les informations d'identification et le secret, vous pouvez configurer l'analyse AWS Schema Conversion Tool sur le serveur de base de données. Pour de plus amples informations, veuillez consulter [Configuration de l'analyse de base de données pour un composant d'application](#).

Après avoir configuré l'analyse de base de données pour le composant d'application, une tâche d'inventaire de AWS Schema Conversion Tool est planifiée. Une fois cette tâche terminée, vous verrez les nouveaux composants d'application créés pour chaque base de données individuelle sur ce serveur de base de données. Par exemple, si votre serveur SQL possède deux bases de données (exampleddb1 et exampleddb2), un composant d'application est créé pour chacune des bases de données avec les noms exampleddb1 et exampleddb2.

Si vous souhaitez voir des anti-modèles lors de la migration de chaque base de données identifiée vers des AWS bases de données, configurez l'analyse pour chaque base de données en suivant les étapes décrites dans [Configuration de l'analyse de base de données pour un composant d'application](#).

Privilèges nécessaires pour les informations d'identification de AWS Schema Conversion Tool

Les identifiants de connexion que vous fournissez à AWS Secrets Manager ne nécessitent que VIEW SERVER STATE des VIEW ANY DEFINITION privilèges.

Vous pouvez fournir le nom de connexion et le mot de passe de votre choix lors de la création de l'identifiant SQL Server.

Création d'un secret dans Secrets Manager pour les informations d'identification de base de données

Une fois que les informations d'identification sont prêtes pour que le collecteur de données de l'application Strategy Recommendations puisse se connecter à une base de données, créez un secret dans AWS Secrets Manager de votre AWS compte, comme décrit dans la procédure suivante.

Pour créer un secret avec AWS Secrets Manager dans votre AWS compte

1. À l'aide du AWS compte que vous avez créé [Configuration des recommandations de stratégie](#), connectez-vous à la console AWS Secrets Manager AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/secretsmanager/>.
2. Choisissez Store a new secret (Stocker un nouveau secret).
3. Sélectionnez le type de secret comme Autre type de secret.

4. Sous Paires clé/valeur, entrez les informations suivantes.

nom d'utilisateur - *your-username*

Choisissez ensuite + Ajouter une ligne et entrez les informations suivantes.

mot de passe - *your-password*

5. Choisissez Suivant.
6. Entrez le nom secret sous la forme d'une chaîne avec le préfixe migrationhub-strategy -. Par exemple, migrationhub-strategy-one.

 Note

Conservez votre nom secret dans un endroit sûr pour une utilisation ultérieure.

7. Choisissez Next, puis de nouveau Next.
8. Choisissez Stocker.

Vous pouvez utiliser le secret que vous avez créé pour les informations d'identification de base de données lors de la configuration de l'analyse de base de données dans Strategy Recommendations.

Analyse binaire des recommandations de stratégie

Les recommandations de stratégie de Migration Hub identifient automatiquement les applications de votre portefeuille et les composants d'application qui leur appartiennent. Par exemple, si votre portefeuille contient une application Java, Strategy Recommendations l'identifie comme un composant d'application avec un type de composant java. Sans que vous configuriez l'accès au code source, Strategy Recommendations peut effectuer une analyse binaire en inspectant l'application DLLs IIS sous Windows ou les fichiers JAR de l'application sous Linux et en fournissant des rapports anti-modèles ou des rapports d'incompatibilité. Un rapport anti-modèle est une liste des problèmes connus que Strategy Recommendations détecte dans votre portefeuille, classés par gravité. Un rapport d'incompatibilité contient un sous-ensemble des anti-modèles, à savoir la compatibilité des API, le Nuget Package et l'action de portage.

Strategy Recommendations effectue des analyses pour les applications Windows IIS et Java Tomcat et Jboss. Si vous possédez une application IIS, Strategy Recommendations génère un rapport d'incompatibilité par défaut ; vous devez configurer l'accès au code source pour recevoir le rapport

anti-modèle complet. Si vous avez une application Java, Strategy Recommendations génère le rapport anti-pattern complet par défaut.

Le rapport incompatible ou anti-modèle s'affiche une fois l'analyse terminée. Si l'analyse échoue, vous pouvez essayer d'exécuter une analyse du code source en fournissant un accès au code source comme décrit dans [Configuration des configurations de contrôle de version](#).

Recommandations stratégiques : recommandations relatives au serveur

Cette section explique comment utiliser les recommandations de stratégie de Migration Hub dans la console Migration Hub pour consulter les recommandations de stratégie de migration pour les serveurs de votre portefeuille de migration.

Pour consulter les recommandations relatives aux serveurs

1. À l'aide du AWS compte que vous avez créé [Configuration des recommandations de stratégie](#), connectez-vous à la console Migration Hub AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/migrationhub/>.
2. Dans le volet de navigation de la console Migration Hub, choisissez Strategy puis Recommendations.
3. Sur la page Recommendations, choisissez l'onglet Serveurs.
 - a. Sous Résumé des serveurs, vous pouvez consulter un aperçu des différents types de serveurs que vous utilisez dans votre portefeuille.
 - b. Sous Serveurs, vous pouvez consulter les détails du serveur et du système d'exploitation ainsi que les recommandations relatives à la stratégie « R » de migration. Vous pouvez également consulter la destination de la migration et le nombre d'anti-modèles identifiés sur vos serveurs, en fonction des recommandations. Pour plus d'informations sur la stratégie « R », voir [Termes de migration - 7 R](#) dans le glossaire des directives AWS prescriptives.
4. Pour afficher les détails détaillés des recommandations pour un serveur, sélectionnez le serveur dans la liste, puis choisissez Afficher les détails. Vous pouvez consulter les métadonnées collectées pour le serveur, ainsi que les analyses approfondies et les recommandations correspondantes, basées sur les composants de l'application trouvés en cours d'exécution sur le serveur.
5. Sur la page des détails du serveur (la page avec le nom du serveur comme titre), sous Résumé des recommandations, vous pouvez voir un aperçu des recommandations de stratégie pour le

serveur. Vous pouvez également voir les anti-patterns identifiés. Les anti-modèles sont une liste de problèmes connus découverts dans votre portefeuille, classés par gravité.

6. Choisissez l'onglet Options de stratégie pour afficher les recommandations de migration pour le serveur. Vous pouvez annuler la stratégie recommandée en sélectionnant une autre stratégie, puis en choisissant Définir les préférences.
7. Choisissez l'onglet Composants de l'application pour afficher la liste des composants de l'application associés au serveur.
8. Pour afficher les détails du composant d'application, sélectionnez-le dans la liste, puis choisissez Afficher les détails. Pour plus d'informations sur les composants de l'application, consultez [Utilisation des composants de l'application](#).

Stratégies, recommandations et préférences

Cette section explique comment afficher et modifier les préférences des recommandations de stratégie de Migration Hub dans la console Migration Hub.

Vous choisissez vos préférences de recommandation lorsque vous configurez les recommandations de stratégie pour la première fois, comme décrit dans [Étape 5 : Obtenir des recommandations](#). Vous pouvez modifier ces préférences.

Pour modifier les préférences de recommandation

1. À l'aide du AWS compte que vous avez créé [Configuration des recommandations de stratégie](#), connectez-vous à la console Migration Hub AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/migrationhub/>.
2. Dans le volet de navigation de la console Migration Hub, choisissez Strategy puis Recommendations.
3. Sur la page Recommendations, choisissez l'onglet Préférences.
4. Sous Objectifs commerciaux priorités, vous pouvez glisser-déposer les objectifs commerciaux pour les réorganiser.
5. Choisissez les préférences d'application et les préférences de base de données souhaitées, puis sélectionnez Enregistrer les modifications.

Si vous modifiez vos préférences, une bannière s'affiche pour vous rappeler de choisir Réanalyser les données.

Sources de données relatives aux recommandations de stratégie

Cette section décrit les sources de données utilisées par Strategy Recommendations.

Rubriques

- [Afficher les sources de données des recommandations de stratégie](#)
- [Collecte de données d'application Strategy Recommendations](#)
- [Importation de données dans les recommandations de stratégie](#)
- [Supprimer vos données des recommandations stratégiques](#)

Afficher les sources de données des recommandations de stratégie

Cette section décrit comment afficher les sources de données Strategy Recommendations dans le AWS Management Console.

Pour afficher les sources de données

1. À l'aide du AWS compte que vous avez créé [Configuration des recommandations de stratégie](#), connectez-vous à la console Migration Hub AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/migrationhub/>.
2. Dans le volet de navigation de la console Migration Hub, choisissez Strategy, puis Data sources.
3. Dans l'onglet Collecteurs, vous pouvez consulter les collecteurs de données de l'application Strategy Recommendations que vous avez configurés. Pour plus d'informations sur le collecteur, consultez [Collecte de données d'application Strategy Recommendations](#).
4. Dans l'onglet Importations, vous pouvez importer des données et consulter vos importations de données. Pour de plus amples informations, veuillez consulter [Importation de données dans les recommandations de stratégie](#).
5. Dans l'onglet Outils, vous pouvez télécharger le collecteur et le modèle de données d'importation de l'application.

Collecte de données d'application Strategy Recommendations

Cette section décrit comment utiliser le collecteur de données de l'application Strategy Recommendations.

Pour plus d'informations sur le téléchargement et la configuration d'un collecteur de données d'application, consultez [Étape 1 : Téléchargez le collecteur de recommandations stratégiques](#).

Rubriques

- [Données collectées par le collecteur de recommandations stratégiques](#)
- [Mise à niveau du collecteur de recommandations stratégiques](#)

Données collectées par le collecteur de recommandations stratégiques

Cette section décrit le type de données que le collecteur de données de l'application Migration Hub Strategy Recommendations collecte. Un collecteur de données d'application est un collecteur de données sans agent qui identifie les applications en cours d'exécution sur vos serveurs, effectue une analyse du code source et analyse vos bases de données.

Champ de données	Description
Type de système d'exploitation	Windows ou Linux
Version du système d'exploitation	Version spécifique du système d'exploitation. Par exemple, Windows Server 2003, RHEL 5.2.
Architecture du système d'exploitation	Système d'exploitation 32 bits ou 64 bits
Est une machine virtuelle du serveur	Le serveur est une machine virtuelle ou une machine physique.
Logiciel de virtualisation	Par exemple, vCenter, Hyper-V.
Emplacement	Par exemple, la console Amazon Elastic Compute Cloud (Amazon EC2) ou sur site.
Est-ce que DualBoot	Permet de démarrer en plusieurs OSs
Type de microprogramme	BIOS, UEFI

Champ de données	Description
Chargeur de démarrage	GRUB, GRUB 2
Type de table de partition	MBR, GPT
Vitesse du processeur	Vitesse du processeur en GHz. Par exemple, 2.4 GHz.
Windows OS data	
Édition Windows	Standard, centre de données, entreprise
Version du framework .NET	Version du framework .NET installée.
Version .NET Core	Version de .NET Core installée.
Linux data	
Distribution du système d'exploitation Linux	RHEL, CentOS, SUSE, etc.
Version de noyau	sortie <code>uname -r</code> , telle que <code>4.9.217-0.1.ac.205.84.332.meta11.x86_64</code>
For each disk volume	
Type de système de fichiers	FAT32, NTFS, ReFS, ext4, jfs, etc.
Taille du volume du disque	Taille totale du disque
Espace libre sur le volume du disque	Espace disque libre
Format d'image de disque virtuel	vmdk, vhd, vhdx
Type de disque (Windows)	Basique, dynamique
Application level data	
Nom de l'application	Nom du processus en cours d'exécution. Par exemple, <code>SQLSrvr MSdtsservr .exe</code> , <code>.exe</code> , etc.
Type d'application	IIS JBoss, Tomcat, etc.

Champ de données	Description
Langage de programmation et version	C#, Java
Version du JDK	Version du JDK installée.
Le code source est-il disponible	Si vous fournissez un référentiel de code source, cela indique que le code source est disponible.
Taille en bits de l'application	16 bits, 32 bits, 64 bits
Windows	
Version du framework .NET utilisée par l'application	Version de la DLL .NET Framework chargée lors de l'exécution de l'application.
Version .NET Core	Version .NET Core DLL chargée lors de l'exécution de l'application.
Utilise le framework WPF ?	Détermine si l'application .NET est un type d'application WPF ou non.
Utilise le framework WCF ?	Détermine si l'application .NET est un type d'application WCF ou non.
Version d'ASP.NET	Version d'ASP.NET.
Version d'IIS	Version du serveur IIS installée sur l'ordinateur Windows.
Taille en bits des pilotes du système d'exploitation des applications	32 bits, 64 bits
Utilisation du registre Windows	Interroge les clés de registre de la machine pour trouver des informations telles que la version de la base de données, la version Java, la version .NET, etc.

Champ de données	Description
Tous DLLs utilisés par l'application	Récupère la liste de tous les fichiers DLLs chargés au moment de l'exécution par un processus Windows.
PowerShell version	Vérifie la PowerShell version installée sur la machine, qui doit être 5.1 ou ultérieure.
Linux	
Type de cadre d'application	Tomcat, Spring Boot,, JBoss, WebLogic WebSphere
Version du framework d'application	Version du framework d'application.
Database	
Type de base de données	MS SQL, Oracle, MySQL, etc.
Version de base de données	Version de la base de données.

Supprimer vos données des recommandations stratégiques

Pour que toutes vos données soient supprimées des recommandations stratégiques, contactez [AWS Support](#) et demandez la suppression complète des données.

Mise à niveau du collecteur de recommandations stratégiques

Le collecteur de données de l'application Migration Hub Strategy Recommendations est automatiquement mis à niveau. Vous pouvez utiliser la procédure suivante pour mettre à niveau manuellement le collecteur, si nécessaire.

Pour mettre à niveau le collecteur de recommandations stratégiques

1. Utilisez la commande suivante pour vous connecter à la machine virtuelle du collecteur à l'aide d'un client SSH.

```
ssh ec2-user@CollectorIPAddress
```

2. Accédez au répertoire de mise à niveau dans la machine virtuelle du collecteur, comme indiqué dans l'exemple suivant.

```
cd /home/ec2-user/collector/upgrades
```

3. Utilisez la commande suivante pour exécuter le script de mise à niveau.

```
sudo bash application-data-collector-upgrade
```

Importation de données dans les recommandations de stratégie

Au lieu d'utiliser le collecteur de données d'application, vous pouvez importer des informations sur les applications et les serveurs pour lesquels vous souhaitez des recommandations de migration et de modernisation.

Lorsque vous importez des données, les recommandations ne sont pas aussi détaillées que lorsque vous utilisez le collecteur de données. Par exemple, vous ne pouvez pas utiliser l'analyse du code source sur des données importées.

Cette section décrit comment utiliser le modèle d'importation d'applications pour importer des données dans Strategy Recommendations dans la console Migration Hub.

Pour importer des données

1. À l'aide du AWS compte que vous avez créé [Configuration des recommandations de stratégie](#), connectez-vous à la console Migration Hub AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/migrationhub/>.
2. Dans le volet de navigation de la console Migration Hub, choisissez Strategy, puis Data sources.
3. Choisissez l'onglet Importations.
4. Choisissez Télécharger le modèle d'importation pour télécharger le modèle d'importation de l'application.
5. Remplissez le modèle et chargez-le dans un compartiment Amazon S3. Assurez-vous que le nom du bucket commence par le préfixe `migrationhub-strategy`.
6. Retournez à l'onglet Importations, puis choisissez Importer.
7. Entrez un nom pour votre importation, entrez l'URI de l'objet Amazon S3 pour votre modèle de données rempli, puis choisissez Démarrer l'importation.

Le modèle d'importation des recommandations de stratégie

Le modèle d'importation que vous téléchargez est un .json fichier, comme illustré dans l'exemple suivant.

```
{
  "ImportFormatVersion": 1,
  "Resources": [
    {
      "ResourceType": "SERVER",
      "ResourceName": "",
      "ResourceId": "",
      "IpAddress": "",
      "OSDistribution": "",
      "OSType": "",
      "HostName": "",
      "OSVersion": "",
      "CPUArchitecture": ""
    },
    {
      "ResourceType": "PROCESS",
      "ResourceName": "",
      "ResourceId": "",
      "ApplicationType": "",
      "DotNetFrameworkVersion": "",
      "ApplicationVersion": "",
      "DotNetCoreVersion": "",
      "JdkVersion": "",
      "ProgrammingLanguage": "",
      "DatabaseType": "",
      "DatabaseVersion": "",
      "DatabaseEdition": "",
      "AssociatedServerIds": []
    }
  ]
}
```

Pour vous aider à remplir le modèle d'importation, les valeurs valides des champs de données sont répertoriées dans les tableaux suivants.

Les champs obligatoires pour les serveurs sont répertoriés dans le tableau suivant.

Name (Nom)	Description	Type	Obligatoire	Valeurs valides
ResourceId	Un identifiant unique pour la ressource	Chaîne	Oui	Toute chaîne unique
ResourceName	Le nom de la ressource	Chaîne	Oui	Toute chaîne
ResourceType	Type de ressource à importer	Chaîne	Oui	« Serveur », « Processus »
OSDistribution	Windows, Windows Server, Ubuntu	Chaîne	Oui	Windows : « PC Windows », « Serveur Windows » Linux : « Ubuntu », « RHEL », « Amazon Linux », « DEBIAN », « SLES », « CENT_OS », « ORACLE_LINUX », « FEDORA », « KALI »
OSType	Le type de système d'exploitation	Chaîne	Oui	« Windows », « Linux »
OSVersion	La version du noyau	Chaîne	Oui	Consultez la version HTML de la documentation.
CPUArchitecture	L'architecture du processeur	Chaîne	Non	« 32 bits », « 64 bits »
IpAddress	L'adresse IP du serveur	Tableau	Non	Au format xxx.xxx.xxx.xxx
MacAddresses	Les adresses Mac	Tableau	Non	Au format xx:xx:xx:xx:xx:xx

Name (Nom)	Description	Type	Obligatoire	Valeurs valides
	associées au serveur			
Hostname	Le nom de l'hôte	Chaîne	Non	Toute chaîne

Les champs obligatoires pour les processus sont répertoriés dans le tableau suivant.

Name (Nom)	Description	Type	Obligatoire	Valeurs valides
ResourceId	Un identifiant unique pour la ressource	Chaîne	Oui	Toute chaîne unique
ResourceName	Le nom de la ressource	Chaîne	Oui	Toute chaîne
ResourceType	Type de ressource à importer	Chaîne	Oui	« Serveur », « Processus »
AssociateServerIds	Liste des serveurs IDs sur lesquels le processus est exécuté.	Chaîne	Oui	Le ResourceId depuis le "ResourceType" : « SERVEUR » que vous avez défini.
ApplicationType	Le type de candidature	Chaîne	Oui	« Tomcat », JBoss « Spring », « IIS », « Mongo DB », « Maria DB », DB2 « MySQL », « Oracle », « Sybase », SQLServer « Postgre », « Cassandra », SQLServer « IBM »,

Name (Nom)	Description	Type	Obligatoire	Valeurs valides
				« Oracle », WebSphere « Java Generic WebLogic »
ApplicationVersion	La version de l'application	Chaîne	Oui	« IIS 1.0 », « IIS 2.0 », « IIS 3.0 », « IIS 4.0 », « IIS 5.0 », « IIS 5.1 », « IIS 6.0 », « IIS 7.0 », « IIS 7,5 », « IIS 8.0 », « IIS 8.5 », « IIS 10.0 »
ProgrammingLanguage	Le langage de programmation de l'application	Chaîne	Non	« Java », "CSharp»

Name (Nom)	Description	Type	Obligatoire	Valeurs valides
DotNetFrameworkVersion	Version de .NET Framework si l'application est basée sur .NET Framework	Chaîne	Non	« DotnetFramework 1,0 », SP1 « DotnetFramework 1,0 », « DotnetFramework 1,0 », SP2 « DotnetFramework 1,0 », SP3 « 1,1 »DotnetFramework , « DotnetFramework 1,1 », « 2,0 », SP1 « DotnetFramework 2,0 », « DotnetFramework 2,0 », SP1 « 3,0 »DotnetFramework , SP2 « 3,0 », « DotnetFramework DotnetFramework 3,0 », SP1 « DotnetFramework 3,5 », SP2 « DotnetFramework DotnetFramework 4,0 », « DotnetFramework 4,5", SP1 « DotnetFramework DotnetFramework 4,5,2 », « 4,6 », « DotnetFramework 4.6.1 », « 4.6.2 », « 4,7", » 7,1 pouces, « DotnetFramework 4,7,2 pouces »DotnetFramework , DotnetFramework DotnetFramework DotnetFramework « DotnetFramework 4,8 »

Name (Nom)	Description	Type	Obligatoire	Valeurs valides
DotNetCoreVersion	Version de .NET Core si l'application est basée sur .NET Core	Chaîne	Non	« .NET Core 1.0 », « .NET Core 1.1 », « .NET Core 2.0 », « .NET Core 2.1 », « .NET Core 2.2 », « .NET Core 3.0 », « .NET Core 3.1 »
JdkVersion	Version du JDK, si l'application utilise le JDK	Chaîne	Non	« JDK1 .0", « .0", « JDK2 .0",..., « JDK3 .0" JDK11
DatabaseType	La base de données de types	Chaîne	Non	SQLServer« », « Oracle », « Sybase », « Mongo DB », « Maria DB », « Apache Cassandra », « MySQL », « IBM », DB2 « Postgre » SQLServer
DatabaseEdition	L'édition de la base de données	Chaîne	Non	
DatabaseVersion	Version de la base de données	Chaîne	Non	Consultez la version HTML de la documentation.

Supprimer vos données des recommandations stratégiques

Pour que toutes vos données soient supprimées des recommandations de stratégie de Migration Hub, contactez [AWS Support](#).

Recommandations stratégiques relatives à la sécurité dans le Hub de Migration

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le [modèle de responsabilité partagée](#) décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de [AWS conformité Programmes](#) de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent aux recommandations stratégiques de Migration Hub, voir [AWS Services concernés par programme de conformitéAWS](#) .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation des recommandations de stratégie. Les rubriques suivantes expliquent comment configurer les recommandations de stratégie pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources de recommandations de stratégie.

Rubriques

- [Recommandations stratégiques relatives à la protection des données dans le Migration Hub](#)
- [Recommandations stratégiques relatives à la gestion des identités et des accès pour Migration Hub](#)
- [Validation de conformité pour les recommandations stratégiques du Migration Hub](#)

Recommandations stratégiques relatives à la protection des données dans le Migration Hub

Le modèle de [responsabilité AWS partagée Le modèle](#) s'applique à la protection des données dans les recommandations stratégiques du Migration Hub. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez [Questions fréquentes \(FAQ\) sur la confidentialité des données](#). Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée [AWS et RGPD \(Règlement général sur la protection des données\)](#) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section [Utilisation des CloudTrail sentiers](#) dans le guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez [Norme FIPS \(Federal Information Processing Standard\) 140-3](#).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec des recommandations de stratégie ou autre Services AWS à l'aide de la console AWS CLI, de l'API ou AWS SDKs. Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Chiffrement au repos

Toutes les données stockées dans la base de données de Strategy Recommendations sont cryptées.

Chiffrement en transit

Recommandations stratégiques Les communications interréseaux prennent en charge le chiffrement TLS 1.2 entre tous les composants et les clients.

Recommandations stratégiques relatives à la gestion des identités et des accès pour Migration Hub

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources Strategy Recommendations. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- [Public ciblé](#)
- [Authentification par des identités](#)
- [Gestion des accès à l'aide de politiques](#)
- [Comment fonctionne Migration Hub Strategy Recommendations avec IAM](#)

- [AWS politiques gérées pour les recommandations stratégiques du Migration Hub](#)
- [Exemples de politiques basées sur l'identité pour les recommandations stratégiques du Migration Hub](#)
- [Résolution des problèmes : Migration Hub : stratégie, recommandations, identité et accès](#)
- [Utilisation de rôles liés à un service pour les recommandations de stratégie](#)
- [Recommandations relatives à la stratégie du Hub de migration et points de terminaison VPC d'interface \(\)AWS PrivateLink](#)

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Strategy Recommendations.

Utilisateur du service : si vous utilisez le service Strategy Recommendations pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités de recommandations de stratégie pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans les recommandations de stratégie, consultez [Résolution des problèmes : Migration Hub : stratégie, recommandations, identité et accès](#).

Administrateur du service — Si vous êtes responsable des ressources de recommandations stratégiques au sein de votre entreprise, vous avez probablement un accès complet aux recommandations de stratégie. C'est à vous de déterminer à quelles fonctionnalités et ressources de Strategy Recommendations doivent accéder aux utilisateurs de vos services. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser l'IAM avec des recommandations stratégiques, consultez [Comment fonctionne Migration Hub Strategy Recommendations avec IAM](#).

Administrateur IAM : si vous êtes administrateur IAM, vous souhaitez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès aux recommandations de stratégie. Pour consulter des exemples de stratégies basées sur les politiques basées sur l'identité que vous pouvez utiliser dans IAM, consultez. [Exemples de politiques basées sur l'identité pour les recommandations stratégiques du Migration Hub](#)

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez [Comment vous connecter à votre compte Compte AWS dans](#) le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer des demandes vous-même, consultez [AWS Signature Version 4 pour les demandes d'API](#) dans le Guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour plus d'informations, consultez [Authentification multifactorielle](#) dans le Guide de l'utilisateur AWS IAM Identity Center et [Authentification multifactorielle AWS dans IAM](#) dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas

utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur racine, consultez [Tâches nécessitant des informations d'identification d'utilisateur racine](#) dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez [Qu'est-ce que IAM Identity Center ?](#) dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un [utilisateur IAM](#) est une identité au sein de votre Compte AWS qui possède des autorisations spécifiques pour une seule personne ou application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme telles que des mots de passe et des clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons d'effectuer une rotation des clés d'accès. Pour plus d'informations, consultez [Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification](#) dans le Guide de l'utilisateur IAM.

Un [groupe IAM](#) est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations

pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer les ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour plus d'informations, consultez [Cas d'utilisation pour les utilisateurs IAM](#) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un [rôle IAM](#) est une identité au sein de votre Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Pour assumer temporairement un rôle IAM dans le AWS Management Console, vous pouvez [passer d'un rôle d'utilisateur à un rôle IAM \(console\)](#). Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez [Méthodes pour endosser un rôle](#) dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- **Accès utilisateur fédéré** : pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez [Jeux d'autorisations](#) dans le Guide de l'utilisateur AWS IAM Identity Center .
- **Autorisations d'utilisateur IAM temporaires** : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- **Accès intercompte** : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les

ressources pour l'accès intercompte, consultez [Accès intercompte aux ressources dans IAM](#) dans le Guide de l'utilisateur IAM.

- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
- Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez [Transmission des sessions d'accès](#).
- Rôle de service : il s'agit d'un [rôle IAM](#) attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez [Création d'un rôle pour la délégation d'autorisations à un Service AWS](#) dans le Guide de l'utilisateur IAM.
- Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés au service apparaissent dans votre Compte AWS fichier et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui envoient des demandes AWS CLI d' AWS API. Cela est préférable au stockage des clés d'accès dans l' EC2 instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l' EC2 instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez [Utiliser un rôle IAM pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon](#) dans le guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez [Vue d'ensemble des politiques JSON](#) dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez [Définition d'autorisations IAM personnalisées avec des politiques gérées par le client](#) dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre

une politique gérée et une politique en ligne, consultez [Choix entre les politiques gérées et les politiques en ligne](#) dans le Guide de l'utilisateur IAM.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez [spécifier un principal](#) dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACLs)

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et AWS WAF Amazon VPC sont des exemples de services compatibles. ACLs Pour en savoir plus ACLs, consultez la [présentation de la liste de contrôle d'accès \(ACL\)](#) dans le guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- **Limite d'autorisations** : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur

l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez [Limites d'autorisations pour des entités IAM](#) dans le Guide de l'utilisateur IAM.

- **Politiques de contrôle des services (SCPs) :** SCPs politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer des politiques de contrôle des services (SCPs) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les Organizations et consultez SCPs les [politiques de contrôle des services](#) dans le Guide de AWS Organizations l'utilisateur.
- **Politiques de contrôle des ressources (RCPs) :** RCPs politiques JSON que vous pouvez utiliser pour définir le maximum d'autorisations disponibles pour les ressources de vos comptes sans mettre à jour les politiques IAM associées à chaque ressource que vous possédez. Le RCP limite les autorisations pour les ressources des comptes membres et peut avoir un impact sur les autorisations effectives pour les identités, y compris Utilisateur racine d'un compte AWS, qu'elles appartiennent ou non à votre organisation. Pour plus d'informations sur les Organizations RCPs, y compris une liste de ces Services AWS supports RCPs, consultez la section [Resource control policies \(RCPs\)](#) dans le guide de AWS Organizations l'utilisateur.
- **Politiques de séance :** les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez [Politiques de session](#) dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section [Logique d'évaluation des politiques](#) dans le guide de l'utilisateur IAM.

Comment fonctionne Migration Hub Strategy Recommendations avec IAM

Avant d'utiliser IAM pour gérer l'accès aux recommandations de stratégie, découvrez quelles fonctionnalités IAM peuvent être utilisées avec les recommandations de stratégie.

Fonctionnalités IAM que vous pouvez utiliser avec les recommandations de stratégie de Migration Hub

Fonctionnalité IAM	Soutien aux recommandations stratégiques
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Non
Clés de condition d'une politique	Non
ACLs	Non
ABAC (étiquettes dans les politiques)	Non
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Fonctions du service	Non
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble de la façon dont les recommandations stratégiques et les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section [AWS Services compatibles avec IAM](#) dans le guide de l'utilisateur IAM.

Politiques basées sur l'identité pour les recommandations stratégiques

Prend en charge les politiques basées sur l'identité : oui

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez [Définition d'autorisations IAM personnalisées avec des politiques gérées par le client](#) dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité, car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez [Références des éléments de politique JSON IAM](#) dans le Guide de l'utilisateur IAM.

Exemples de politiques basées sur l'identité pour les recommandations stratégiques

Pour consulter des exemples de recommandations stratégiques et de politiques basées sur l'identité, voir [Exemples de politiques basées sur l'identité pour les recommandations stratégiques du Migration Hub](#)

Politiques basées sur les ressources dans le cadre des recommandations stratégiques

Prend en charge les politiques basées sur les ressources : non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez [spécifier un principal](#) dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal intercompte à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents

Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez [Accès intercompte aux ressources dans IAM](#) dans le Guide de l'utilisateur IAM.

Actions politiques pour les recommandations stratégiques

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions recommandées en matière de stratégie, consultez la section [Actions définies par les recommandations de stratégie de Migration Hub](#) dans la référence d'autorisation de service.

Dans les recommandations de stratégie, les actions stratégiques utilisent le préfixe suivant avant l'action :

```
migrationhub-strategy
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [  
    "migrationhub-strategy:action1",
```

```
"migrationhub-strategy:action2"  
]
```

Pour consulter des exemples de recommandations stratégiques et de politiques basées sur l'identité, voir. [Exemples de politiques basées sur l'identité pour les recommandations stratégiques du Migration Hub](#)

Ressources politiques pour les recommandations stratégiques

Prend en charge les ressources politiques : Non

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son [Amazon Resource Name \(ARN\)](#). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des types de ressources Strategy Recommendations et leurs caractéristiques ARNs, consultez la section [Ressources définies par Migration Hub Strategy Recommendations](#) dans la référence d'autorisation de service. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez la section [Actions définies par les recommandations stratégiques de Migration Hub](#).

Pour consulter des exemples de recommandations stratégiques et de politiques basées sur l'identité, voir. [Exemples de politiques basées sur l'identité pour les recommandations stratégiques du Migration Hub](#)

Clés de conditions de politique pour les recommandations de stratégie

Prend en charge les clés de condition de politique spécifiques au service : Non

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des [opérateurs de condition](#), tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération AND logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une OR opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez [Éléments d'une politique IAM : variables et identifications](#) dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de [contexte de condition AWS globales](#) dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de condition relatives aux recommandations de stratégie, consultez la section [Clés de condition pour les recommandations de stratégie de Migration Hub](#) dans la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez la section [Actions définies par les recommandations stratégiques de Migration Hub](#).

Pour consulter des exemples de recommandations stratégiques et de politiques basées sur l'identité, voir. [Exemples de politiques basées sur l'identité pour les recommandations stratégiques du Migration Hub](#)

Listes de contrôle d'accès (ACLs) dans les recommandations stratégiques

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Contrôle d'accès basé sur les attributs (ABAC) avec recommandations stratégiques

Supporte l'ABAC (balises dans les politiques) : Non

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'[élément de condition](#) d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur ABAC, consultez [Définition d'autorisations avec l'autorisation ABAC](#) dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez [Utilisation du contrôle d'accès par attributs \(ABAC\)](#) dans le Guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec des recommandations de stratégie

Prend en charge les informations d'identification temporaires : oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation [d'IAM](#) dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez [Passage d'un rôle utilisateur à un rôle IAM \(console\)](#) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez [Informations d'identification de sécurité temporaires dans IAM](#).

Autorisations principales interservices pour les recommandations de stratégie

Prend en charge les sessions d'accès direct (FAS) : oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez [Transmission des sessions d'accès](#).

Rôles de service pour les recommandations stratégiques

Prend en charge les rôles de service : Non

Un rôle de service est un [rôle IAM](#) qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez [Création d'un rôle pour la délégation d'autorisations à un Service AWS](#) dans le Guide de l'utilisateur IAM.

⚠ Warning

La modification des autorisations associées à un rôle de service peut perturber la fonctionnalité des recommandations de stratégie. Modifiez les rôles de service uniquement lorsque Strategy Recommendations fournit des conseils à cet effet.

Rôles liés aux services pour les recommandations de stratégie

Prend en charge les rôles liés aux services : Oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés au service apparaissent dans votre Compte AWS fichier et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus de détails sur la création ou la gestion des rôles liés au service Strategy Recommendations, consultez. [Utilisation de rôles liés à un service pour les recommandations de stratégie](#)

AWS politiques gérées pour les recommandations stratégiques du Migration Hub

Pour ajouter des autorisations aux utilisateurs, aux groupes et aux rôles, il est plus facile d'utiliser des politiques AWS gérées que de les rédiger vous-même. Il faut du temps et de l'expertise pour [créer des politiques gérées par le client IAM](#) qui ne fournissent à votre équipe que les autorisations dont elle a besoin. Pour démarrer rapidement, vous pouvez utiliser nos politiques AWS gérées. Ces politiques couvrent des cas d'utilisation courants et sont disponibles dans votre Compte AWS. Pour plus d'informations sur les politiques AWS gérées, voir les [politiques AWS gérées](#) dans le guide de l'utilisateur IAM.

AWS les services maintiennent et mettent à jour les politiques AWS gérées. Vous ne pouvez pas modifier les autorisations dans les politiques AWS gérées. Les services ajoutent parfois des autorisations supplémentaires à une politique AWS gérée pour prendre en charge de nouvelles fonctionnalités. Ce type de mise à jour affecte toutes les identités (utilisateurs, groupes et rôles) auxquelles la politique est attachée. Les services sont plus susceptibles de mettre à jour une politique

AWS gère lorsqu'une nouvelle fonctionnalité est lancée ou lorsque de nouvelles opérations sont disponibles. Les services ne suppriment pas les autorisations d'une politique AWS gérée. Les mises à jour des politiques n'endommageront donc pas vos autorisations existantes.

En outre, AWS prend en charge les politiques gérées pour les fonctions professionnelles qui couvrent plusieurs services. Par exemple, la politique `ReadOnlyAccess` AWS gérée fournit un accès en lecture seule à tous les AWS services et ressources. Lorsqu'un service lance une nouvelle fonctionnalité, il AWS ajoute des autorisations en lecture seule pour les nouvelles opérations et ressources. Pour obtenir la liste des politiques de fonctions professionnelles et leurs descriptions, consultez la page [politiques gérées par AWS pour les fonctions de tâche](#) dans le Guide de l'utilisateur IAM.

AWS politique gérée : `AWSMigrationHubStrategyConsoleFullAccess`

Vous pouvez associer la politique `AWSMigrationHubStrategyConsoleFullAccess` à vos identités IAM.

La `AWSMigrationHubStrategyConsoleFullAccess` politique accorde à l'utilisateur un accès complet au service Strategy Recommendations via le AWS Management Console.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `discovery`— Accorde à l'utilisateur l'accès pour obtenir le résumé des découvertes dans Application Discovery Service.
- `iam`— Permet de créer un rôle lié à un service pour l'utilisateur, ce qui est obligatoire pour utiliser les recommandations de stratégie.
- `migrationhub-strategy`— Accorde à l'utilisateur un accès complet aux recommandations de stratégie.
- `s3`— Permet à l'utilisateur de créer et de lire à partir des compartiments S3 utilisés par Strategy Recommendations.
- `secretsmanager`— Permet à l'utilisateur de répertorier les accès aux secrets dans le Secrets Manager.

Pour consulter les autorisations associées à cette politique, voir [AWSMigrationHubStrategyConsoleFullAccess](#) dans le Guide de référence des politiques AWS gérées.

AWS politique gérée : AWSMigration HubStrategyCollector

Vous pouvez associer la politique `AWSMigrationHubStrategyCollector` à vos identités IAM.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `application-transformation`— Permet de télécharger des données de journal et de métrique pour les opérations de transformation des applications et de travailler sur les évaluations et recommandations de compatibilité du portage.
- `execute-api`— Permet à l'utilisateur d'accéder à Amazon API Gateway pour y télécharger des journaux et des métriques AWS.
- `migrationhub-strategy`— Permet à l'utilisateur d'enregistrer des messages, d'envoyer des messages, de télécharger des données de journal et de télécharger des données métriques dans les recommandations de stratégie.
- `s3`— Accorde à l'utilisateur l'accès aux compartiments de liste et à leur emplacement. Les utilisateurs sont également autorisés à écrire, à récupérer des objets, à y ajouter des objets, à renvoyer la liste de contrôle d'accès (ACL), à créer, à accéder, à configurer le chiffrement, à modifier la `PublicAccessBlock` configuration pour, à définir l'état de version pour, et à créer ou remplacer une configuration de cycle de vie pour les compartiments S3 utilisés par Strategy Recommendations.
- `secretsmanager`— Permet à l'utilisateur d'accéder aux secrets du Gestionnaire de secrets utilisés par Strategy Recommendations.

Pour consulter les autorisations associées à cette politique, voir [AWSMigrationHubStrategyCollector](#) dans le Guide de référence des politiques AWS gérées.

Recommandations stratégiques : mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées pour Strategy Recommendations depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au fil RSS sur la page d'historique du document de recommandations stratégiques.

Modification	Description	Date
AWSMigrationHubStrategyCollector – Mise à jour d'une stratégie existante	<p>Cette politique est mise à jour pour inclure les actions <code>PutLogData</code>, <code>StartPortingCompatibilityAssessment</code>, <code>GetPortingCompatibilityAssessment</code>, <code>StartPortingRecommendationAssessment</code> et de transformation des <code>GetPortingRecommendationAssessment</code> applications afin de permettre au service de transformation des applications d'envoyer des journaux et des métriques au service. Les <code>ListBucket</code> et <code>GetBucketLocation</code> ont été ajoutés pour Amazon Simple Storage Service (Amazon S3) afin de prendre en charge les téléchargements de journaux et de métriques. Les <code>PutLogData</code> et <code>PutMetricData</code> ont également été ajoutés pour permettre au collecteur de recommandations stratégiques d'envoyer des journaux et des métriques</p>	1er avril 2024

Modification	Description	Date
	au point de terminaison du service.	
AWSMigrationHubStrategyCollector – Mise à jour d'une politique existante	Cette politique est mise à jour avec les PutLogData actions PutMetricData et. Ces actions autorisent le téléchargement de données de journal et de métrique pour les opérations de transformation des applications. Cette mise à jour ajoute également des conditions garantissant <code>aws:ResourceAccount</code> que l'autorisation d'utiliser le service et <code>aws:PrincipalAccount</code> les AWS Secrets Manager actions Amazon Simple Storage inclus est égale à celle requise.	5 février 2024
AWSMigrationHubStrategyCollector – Mise à jour d'une politique existante	Cette politique est mise à jour avec les Amazon S3 suivants APIs : CreateBucket PutEncryptionConfiguration ,PutBucketPublicAccessBlock ,PutBucketPolicy ,PutBucketVersioning , etPutLifecycleConfiguration .	15 septembre 2023

Modification	Description	Date
AWSMigrationHubStrategyCollector – Mise à jour d'une politique existante	Cette mise à jour de la politique accorde des autorisations permettant l'analyse du code source.	8 mars 2023
AWSMigrationHubStrategyConsoleFullAccess – Mise à jour d'une politique existante	Cette politique est mise à jour avec trois AWS Application Discovery Service APIs — DescribeConfigurations, DescribeTags, et ListConfigurations.	10 novembre 2022
AWSMigrationHubStrategyCollector – Mise à jour d'une politique existante	Cette politique est mise à jour en fonction de l'UpdateCollectorConfiguration action. Cette action enregistre la configuration de votre collecteur pour en faciliter la récupération.	07 septembre 2022
AWSMigrationHubStrategyConsoleFullAccess — Nouvelle politique rendue disponible au lancement	AWSMigrationHubStrategyConsoleFullAccess accorde à l'utilisateur un accès complet au service Strategy Recommendations via le AWS Management Console.	25 octobre 2021

Modification	Description	Date
<p>AWSMigrationHubStrategyCollector— Nouvelle politique rendue disponible au lancement</p>	<p>AWSMigrationHubStrategyCollector accorde à un utilisateur l'accès au service Strategy Recommendations et un accès en lecture/écriture aux compartiments S3 associés au service. Il accorde également à Amazon API Gateway l'accès pour télécharger des journaux et des métriques AWS, ainsi que l'accès à AWS Secrets Manager pour récupérer les informations d'identification.</p>	<p>25 octobre 2021</p>
<p>AWSMigrationHubStrategyServiceRolePolicy— Nouvelle politique rendue disponible au lancement</p>	<p>La politique des rôles AWSMigrationHubStrategyServiceRolePolicy liés au service donne accès à AWS Migration Hub et. AWS Application Discovery Service Cette politique accorde également des autorisations pour le stockage de rapports dans Amazon Simple Storage Service (Amazon S3).</p>	<p>25 octobre 2021</p>
<p>Les recommandations stratégiques ont commencé à suivre les changements</p>	<p>Strategy Recommendations a commencé à suivre les modifications apportées AWS à ses politiques gérées.</p>	<p>25 octobre 2021</p>

Exemples de politiques basées sur l'identité pour les recommandations stratégiques du Migration Hub

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources de recommandations de stratégie. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez [Création de politiques IAM \(console\)](#) dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par Strategy Recommendations, y compris le ARNs format de chaque type de ressource, voir [Actions, ressources et clés de condition pour les recommandations de stratégie du Migration Hub](#) dans la référence d'autorisation de service.

Rubriques

- [Bonnes pratiques en matière de politiques](#)
- [Utilisation de la console Strategy Recommendations](#)
- [Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations](#)
- [Accès à un compartiment Amazon S3](#)

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources de recommandations de stratégie dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à

vos cas d'utilisation. Pour plus d'informations, consultez [politiques gérées par AWS](#) ou [politiques gérées par AWS pour les activités professionnelles](#) dans le Guide de l'utilisateur IAM.

- Accordez les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation d'IAM pour appliquer des autorisations, consultez [politiques et autorisations dans IAM](#) dans le Guide de l'utilisateur IAM.
- Utilisez des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez [Conditions pour éléments de politique JSON IAM](#) dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez [Validation de politiques avec IAM Access Analyzer](#) dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez [Sécurisation de l'accès aux API avec MFA](#) dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez [Bonnes pratiques de sécurité dans IAM](#) dans le Guide de l'utilisateur IAM.

Utilisation de la console Strategy Recommendations

Pour accéder à la console Migration Hub Strategy Recommendations, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les détails des ressources de recommandations de stratégie de votre Compte AWS. Si vous

créez une politique basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette politique.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent toujours utiliser la console Strategy Recommendations, attachez également les recommandations de stratégie ConsoleAccess ou la politique ReadOnly AWS gérée aux entités. Pour plus d'informations, consultez [Ajout d'autorisations à un utilisateur](#) dans le Guide de l'utilisateur IAM.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
```

```
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
```

Accès à un compartiment Amazon S3

Dans cet exemple, vous souhaitez accorder à un utilisateur IAM l' Compte AWS accès à l'un de vos compartiments Amazon S3. amzn-s3-demo-bucket Vous souhaitez également autoriser l'utilisateur à ajouter, mettre à jour et supprimer des objets.

En plus de l'octroi des autorisations `s3:PutObject`, `s3:GetObject` et `s3:DeleteObject` à l'utilisateur, la stratégie octroie aussi les autorisations `s3:ListAllMyBuckets`, `s3:GetBucketLocation` et `s3:ListBucket`. Ces conditions supplémentaires sont requises par la console. De la même manière, les actions `s3:PutObjectAcl` et `s3:GetObjectAcl` sont nécessaires pour que les objets puissent être copiés, coupés et collés dans la console. Pour un exemple de procédure pas à pas qui accorde des autorisations aux utilisateurs et les teste à l'aide de la console, consultez [Un exemple de procédure pas à pas : utilisation de politiques utilisateur pour contrôler l'accès à votre compartiment](#).

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"ListBucketsInConsole",
      "Effect":"Allow",
      "Action":[
        "s3:ListAllMyBuckets"
      ],
      "Resource":"arn:aws:s3:::*"
    },
    {
      "Sid":"ViewSpecificBucketInfo",
      "Effect":"Allow",
```

```
    "Action":[
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource":"arn:aws:s3:::amzn-s3-demo-bucket"
  },
  {
    "Sid":"ManageBucketContents",
    "Effect":"Allow",
    "Action":[
      "s3:PutObject",
      "s3:PutObjectAcl",
      "s3:GetObject",
      "s3:GetObjectAcl",
      "s3:DeleteObject"
    ],
    "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*"
  }
]
```

Résolution des problèmes : Migration Hub : stratégie, recommandations, identité et accès

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lors de l'utilisation de Strategy Recommendations et d'IAM.

Rubriques

- [Je ne suis pas autorisé à effectuer une action dans Strategy Recommendations](#)
- [Je ne suis pas autorisé à effectuer iam : PassRole](#)
- [Je veux afficher mes clés d'accès](#)
- [Je suis administrateur et je souhaite autoriser d'autres personnes à accéder aux recommandations de stratégie](#)
- [Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes ressources de recommandations stratégiques](#)

Je ne suis pas autorisé à effectuer une action dans Strategy Recommendations

S'il vous AWS Management Console indique que vous n'êtes pas autorisé à effectuer une action, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni votre nom d'utilisateur et votre mot de passe.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource `my-example-widget` fictive, mais ne dispose pas des autorisations `migrationhub-strategy:GetWidget` fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: migrationhub-strategy:GetWidget on resource: my-example-widget
```

Dans ce cas, Mateo demande à son administrateur de mettre à jour ses politiques pour lui permettre d'accéder à la ressource `my-example-widget` à l'aide de l'action `migrationhub-strategy:GetWidget`.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'action `iam:PassRole`, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à Strategy Recommendations.

Certains services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans Strategy Recommendations. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations de connexion.

Je veux afficher mes clés d'accès

Une fois les clés d'accès utilisateur IAM créées, vous pouvez afficher votre ID de clé d'accès à tout moment. Toutefois, vous ne pouvez pas revoir votre clé d'accès secrète. Si vous perdez votre clé d'accès secrète, vous devez créer une nouvelle paire de clés.

Les clés d'accès se composent de deux parties : un ID de clé d'accès (par exemple, AKIAIOSFODNN7EXAMPLE) et une clé d'accès secrète (par exemple, wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY). À l'instar d'un nom d'utilisateur et un mot de passe, vous devez utiliser à la fois l'ID de clé d'accès et la clé d'accès secrète pour authentifier vos demandes. Gérez vos clés d'accès de manière aussi sécurisée que votre nom d'utilisateur et votre mot de passe.

Important

Ne communiquez pas vos clés d'accès à un tiers, même pour qu'il vous aide à [trouver votre ID utilisateur canonique](#). Ce faisant, vous pourriez donner à quelqu'un un accès permanent à votre Compte AWS.

Lorsque vous créez une paire de clé d'accès, enregistrez l'ID de clé d'accès et la clé d'accès secrète dans un emplacement sécurisé. La clé d'accès secrète est accessible uniquement au moment de sa création. Si vous perdez votre clé d'accès secrète, vous devez ajouter de nouvelles clés d'accès pour votre utilisateur IAM. Vous pouvez avoir un maximum de deux clés d'accès. Si vous en avez déjà deux, vous devez supprimer une paire de clés avant d'en créer une nouvelle. Pour afficher les instructions, consultez [Gestion des clés d'accès](#) dans le Guide de l'utilisateur IAM.

Je suis administrateur et je souhaite autoriser d'autres personnes à accéder aux recommandations de stratégie

Pour permettre à d'autres personnes d'accéder aux recommandations de stratégie, vous devez accorder l'autorisation aux personnes ou aux applications qui ont besoin d'y accéder. Si vous utilisez AWS IAM Identity Center pour gérer des personnes et des applications, vous attribuez des ensembles d'autorisations aux utilisateurs ou aux groupes afin de définir leur niveau d'accès. Les ensembles d'autorisations créent et attribuent automatiquement des politiques IAM aux rôles IAM associés à la personne ou à l'application. Pour plus d'informations, consultez la section [Ensembles d'autorisations](#) dans le guide de AWS IAM Identity Center l'utilisateur.

Si vous n'utilisez pas IAM Identity Center, vous devez créer des entités IAM (utilisateurs ou rôles) pour les personnes ou les applications qui ont besoin d'un accès. Vous devez ensuite associer

une politique à l'entité qui lui accorde les autorisations appropriées dans les recommandations de stratégie. Une fois les autorisations accordées, fournissez les informations d'identification à l'utilisateur ou au développeur de l'application. Ils utiliseront ces informations d'identification pour accéder à AWS. Pour en savoir plus sur la création d'utilisateurs, de groupes, de politiques et d'autorisations [IAM](#), consultez la section [Identités, politiques et autorisations IAM dans le guide de l'utilisateur IAM](#).

Je souhaite permettre à des personnes extérieures à mon compte AWS d'accéder à mes ressources de recommandations stratégiques

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si Strategy Recommendations prend en charge ces fonctionnalités, consultez [Comment fonctionne Migration Hub Strategy Recommendations avec IAM](#).
- Pour savoir comment fournir l'accès à vos ressources sur celles de votre compte AWS que vous possédez, consultez la section [Fournir l'accès à un utilisateur IAM dans un autre utilisateur de votre compte AWS que vous possédez](#) dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers de votre compte AWS, consultez la section [Fournir un accès à des ressources de votre compte AWS détenues par des tiers](#) dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez [Fournir un accès à des utilisateurs authentifiés en externe \(fédération d'identité\)](#) dans le Guide de l'utilisateur IAM.
- Pour en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez [Accès intercompte aux ressources dans IAM](#) dans le Guide de l'utilisateur IAM.

Utilisation de rôles liés à un service pour les recommandations de stratégie

Les recommandations de stratégie du Migration Hub utilisent des AWS Identity and Access Management rôles liés à un [service](#) (IAM). Un rôle lié à un service est un type unique de rôle IAM

directement lié aux recommandations de stratégie. Les rôles liés au service sont prédéfinis par les recommandations de stratégie et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration des recommandations de stratégie, car vous n'avez pas à ajouter manuellement les autorisations nécessaires. Strategy Recommendations définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seules les recommandations de stratégie peuvent assumer ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez la section [AWS Services qui fonctionnent avec IAM](#) et recherchez les services dont la valeur est Oui dans la colonne Rôle lié au service. Choisissez un Yes (oui) ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle liées au service pour les recommandations de stratégie

Strategy Recommendations utilise le rôle lié au service nommé `AWSServiceRoleForMigrationHubStrategy` et l'associe à la politique `AWSMigrationHubStrategyServiceRolePolicyIAM` : donne accès à et. AWS Migration Hub AWS Application Discovery Service Cette politique accorde également des autorisations pour le stockage de rapports dans Amazon Simple Storage Service (Amazon S3).

Le rôle lié à un service `AWSServiceRoleForMigrationHubStrategy` approuve les services suivants pour endosser le rôle :

- `migrationhub-strategy.amazonaws.com`

La politique d'autorisation des rôles permet à Strategy Recommendations d'effectuer les actions suivantes.

AWS Application Discovery Service actions

`discovery:ListConfigurations`

`discovery:DescribeConfigurations`

AWS Migration Hub actions

`mgh:GetHomeRegion`

Actions Amazon S3

s3:GetBucketAcl

s3:GetBucketLocation

s3:GetObject

s3:ListAllMyBuckets

s3:ListBucket

s3:PutObject

s3:PutObjectAcl

Pour consulter les autorisations associées à cette politique, voir

[AWSMigrationHubStrategyServiceRolePolicy](#) dans le Guide de référence des politiques AWS gérées.

Pour consulter l'historique des mises à jour de cette politique, consultez [Recommandations stratégiques : mises à jour des politiques AWS gérées](#).

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez [Service-Linked Role Permissions \(autorisations du rôle lié à un service\)](#) dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour les recommandations de stratégie

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous acceptez d'autoriser Migration Hub à créer un rôle lié à un service (SLR) sur votre compte dans le AWS Management Console, Strategy Recommendations crée le rôle lié au service pour vous.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous acceptez d'autoriser Migration Hub à créer un rôle lié à un service (SLR) dans votre compte, Strategy Recommendations crée à nouveau le rôle lié au service pour vous.

Modification d'un rôle lié à un service pour les recommandations de stratégie

Les recommandations de stratégie ne vous permettent pas de modifier le rôle `AWSServiceRoleForMigrationHubStrategy` lié au service. Une fois que vous avez créé un rôle lié à

un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Toutefois, vous pouvez modifier la description du rôle à l'aide de la console Strategy Recommendations, de la CLI ou de l'API.

Supprimer un rôle lié à un service pour les recommandations de stratégie

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au `AWSServiceRoleForMigrationHubStrategyService`. Pour plus d'informations, consultez [Suppression d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Lorsque vous supprimez des ressources de recommandations de stratégie utilisées par le `AWSServiceRoleForMigrationHubStrategySLR`, vous ne pouvez pas exécuter d'évaluations (tâches de génération de recommandations). Aucune évaluation des antécédents ne peut non plus être en cours. Si des évaluations sont en cours, la suppression du SLR échoue dans la console IAM. Si la suppression du réflex échoue, vous pouvez réessayer une fois toutes les tâches en arrière-plan terminées. Il n'est pas nécessaire de nettoyer les ressources créées avant de supprimer le réflex.

Régions prises en charge pour les rôles liés au service Strategy Recommendations

Strategy Recommendations soutient l'utilisation de rôles liés au service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez [Régions et Points de terminaison AWS](#).

Recommandations relatives à la stratégie du Hub de migration et points de terminaison VPC d'interface ()AWS PrivateLink

Vous pouvez établir une connexion privée entre votre VPC et les recommandations de stratégie du Migration Hub en créant un point de terminaison VPC d'interface. Les points de terminaison d'interface sont alimentés par AWS PrivateLink. Avec AWS PrivateLink, vous pouvez accéder en privé aux opérations de l'API Strategy Recommendations sans passerelle Internet, appareil NAT, connexion VPN ou AWS Direct Connect connexion. Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour communiquer avec les opérations de l'API Strategy Recommendations. Le trafic entre votre VPC et Strategy Recommendations reste au sein du réseau Amazon.

Chaque point de terminaison d'interface est représenté par une ou plusieurs [interfaces réseau Elastic](#) dans vos sous-réseaux.

Pour de plus amples informations, consultez [Points de terminaison VPC \(AWS PrivateLink\)](#) dans le Guide de l'utilisateur Amazon VPC.

Considérations relatives aux recommandations de stratégie (points de terminaison VPC)

Avant de configurer un point de terminaison VPC d'interface pour les recommandations de stratégie, assurez-vous de consulter les [propriétés, les limites et les AWS PrivateLink quotas du point de terminaison d'interface](#) dans le guide de l'utilisateur Amazon VPC.

Strategy Recommendations permet d'appeler toutes ses actions d'API depuis votre VPC. Pour utiliser toutes les recommandations de stratégie, vous devez créer un point de terminaison VPC.

Création d'un point de terminaison VPC d'interface pour les recommandations de stratégie

Vous pouvez créer un point de terminaison VPC pour les recommandations de stratégie à l'aide de la console Amazon VPC ou du (). AWS Command Line Interface AWS CLI Pour plus d'informations, consultez [Création d'un point de terminaison d'interface](#) dans le Guide de l'utilisateur Amazon VPC.

Créez un point de terminaison VPC pour les recommandations de stratégie en utilisant le nom de service suivant :

- `com.amazonaws.region.migrationhub-strategy`

Si vous utilisez un DNS privé pour le point de terminaison, vous pouvez envoyer des demandes d'API à Strategy Recommendations en utilisant son nom DNS par défaut pour la région. Par exemple, vous pouvez utiliser le nom `migrationhub-strategy.us-east-1.amazonaws.com`.

Pour plus d'informations, consultez [Accès à un service via un point de terminaison d'interface](#) dans le Guide de l'utilisateur Amazon VPC.

Création d'une politique de point de terminaison VPC pour les recommandations de stratégie

Vous pouvez associer une politique de point de terminaison à votre point de terminaison VPC qui contrôle l'accès aux recommandations de stratégie. La politique spécifie les informations suivantes :

- Le principal qui peut exécuter des actions.
- Les actions qui peuvent être effectuées.
- Les ressources sur lesquelles ces actions peuvent être effectuées.

Pour plus d'informations, consultez [Contrôle de l'accès aux services avec points de terminaison d'un VPC](#) dans le Guide de l'utilisateur Amazon VPC.

Exemple : politique de point de terminaison VPC pour les actions de recommandation de stratégie

Voici un exemple de politique de point de terminaison pour les recommandations de stratégie. Lorsqu'elle est attachée à un point de terminaison, cette politique donne accès aux actions de recommandations de stratégie répertoriées pour tous les principaux sur toutes les ressources.

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "migrationhub-strategy:ListContacts",
      ],
      "Resource": "*"
    }
  ]
}
```

Validation de conformité pour les recommandations stratégiques du Migration Hub

Pour savoir si un [programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité](#) spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de [AWS conformité Programmes AWS](#) de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir [Téléchargement de rapports dans AWS Artifact](#) .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- [Conformité et gouvernance de la sécurité](#) : ces guides de mise en œuvre de solutions traitent des considérations architecturales et fournissent les étapes à suivre afin de déployer des fonctionnalités de sécurité et de conformité.
- [Référence des services éligibles HIPAA](#) : liste les services éligibles HIPAA. Tous ne Services AWS sont pas éligibles à la loi HIPAA.
- AWS Ressources de <https://aws.amazon.com/compliance/resources/> de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- [AWS Guides de conformité destinés aux clients](#) — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- [Évaluation des ressources à l'aide des règles](#) du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- [AWS Security Hub](#)— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez [Référence des contrôles Security Hub](#).
- [Amazon GuardDuty](#) — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- [AWS Audit Manager](#)— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Utilisation d'autres services

Cette section décrit les autres AWS services qui interagissent avec les recommandations de stratégie de Migration Hub.

Rubriques

- [Appels d'API de recommandations de stratégie de journalisation avec AWS CloudTrail](#)

Appels d'API de recommandations de stratégie de journalisation avec AWS CloudTrail

Migration Hub Strategy Recommendations est intégré à un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Strategy Recommendations. AWS CloudTrail capture les appels d'API pour les recommandations de stratégie sous forme d'événements. Les appels capturés incluent des appels provenant de la console Strategy Recommendations et des appels de code vers les opérations de l'API Strategy Recommendations.

Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour les recommandations de stratégie. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à Strategy Recommendations, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires.

Pour en savoir plus CloudTrail, consultez le [guide de AWS CloudTrail l'utilisateur](#).

Informations sur les recommandations de stratégie dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans les recommandations de stratégie, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section [Affichage des événements à l'aide de l'historique des CloudTrail événements](#).

Pour un enregistrement continu des événements de votre entreprise Compte AWS, y compris des événements pour les recommandations stratégiques, créez un parcours. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- [Présentation de la création d'un journal de suivi](#)
- [CloudTrail services et intégrations pris en charge](#)
- [Configuration des notifications Amazon SNS pour CloudTrail](#)
- [Réception de fichiers CloudTrail journaux de plusieurs régions](#) et [réception de fichiers CloudTrail journaux de plusieurs comptes](#)

Strategy Recommendations prend en charge l'enregistrement des actions suivantes sous forme d'événements dans des fichiers CloudTrail journaux :

- [GetApplicationComponentStrategies](#)
- [GetApplicationComponentDetails](#)
- [GetAssesment](#)
- [GetImportFileTask](#)
- [GetPortfolioPreferences](#)
- [GetPortfolioSummary](#)
- [GetServerDetails](#)
- [GetServerStrategies](#)
- [ListApplicationComponents](#)
- [ListCollectors](#)
- [ListImportFileTask](#)
- [ListServers](#)
- [PutPortfolioPreferences](#)
- [StartAssessment](#)
- [StartImportFileTask](#)

- [StopAssessment](#)
- [UpdateApplicationComponentConfig](#)
- [UpdateServerConfig](#)

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec les informations d'identification de l'utilisateur root ou AWS Identity and Access Management (IAM)
- Si la demande a été effectuée avec des informations d'identification de sécurité temporaires pour un rôle ou un utilisateur fédéré
- Si la demande a été faite par un autre AWS service

Pour de plus amples informations, veuillez consulter l'[élément userIdentity CloudTrail](#).

Comprendre les entrées du fichier journal des recommandations en matière de stratégie

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'[GetServerDetails](#) action.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "777777777777",
    "arn": "arn:aws:sts::111122223333:assumed-role/myUserName/...",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
```

```
        "type": "Role",
        "principalId": "777777777777",
        "arn": "arn:aws:iam::111122223333:role/myUserName",
        "accountId": "111122223333",
        "userName": "myUserName"
    },
    "webIdFederationData": {},
    "attributes": {
        "creationDate": "2021-09-20T01:07:16Z",
        "mfaAuthenticated": "false"
    }
}
},
"eventTime": "2021-09-20T01:07:43Z",
"eventSource": "migrationhub-strategy.amazonaws.com",
"eventName": "GetServerDetails",
"awsRegion": "us-west-2",
"sourceIPAddress": "",
"userAgent": "",
"requestParameters": {
    "serverId": "ads-server-006"
},
"responseElements": null,
"requestID": "07D681279BD94AED",
"eventID": "cdc4b7ed-e171-4cef-975a-ad829d4123e8",
"readOnly": true,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111122223333",
"eventCategory": "Management"
}
```

Recommandations stratégiques relatives aux quotas pour le Migration Hub

Votre AWS compte dispose de quotas par défaut, anciennement appelés limites, pour chaque AWS service. Sauf indication contraire, chaque quota est spécifique à la région. Vous pouvez demander des augmentations pour certains quotas, et d'autres quotas ne peuvent pas être augmentés.

Pour consulter la liste des quotas pour les recommandations de stratégie de Migration Hub, consultez la section [Quotas de service Strategy Recommendations](#).

Vous pouvez également consulter les quotas pour les recommandations de stratégie en ouvrant la [console Service Quotas](#). Dans le volet de navigation, choisissez les AWS services, puis sélectionnez Migration Hub Strategy Recommendations.

Pour demander une augmentation de quota, consultez [Demander une augmentation de quota](#) dans le Guide de l'utilisateur de Service Quotas. Si le quota n'est pas encore disponible dans Service Quotas, utilisez le [Formulaire d'augmentation de limite de service](#).

Notes de mise à jour

Rubriques

- [17 novembre 2023](#)
- [12 octobre 2023](#)
- [17 avril 2023](#)
- [17 mars 2023](#)
- [07 novembre 2022](#)
- [27 septembre 2022](#)
- [30 juin 2022](#)
- [18 avril 2022](#)
- [25 février 2022](#)
- [10 février 2022](#)
- [28 janvier 2022](#)
- [14 janvier 2022](#)
- [21 décembre 2021](#)
- [15 décembre 2021](#)
- [25 octobre 2021](#)

17 novembre 2023

Nouvelles fonctionnalités

- Collector v1.1.47
- Support pour les applications .NET 8.

12 octobre 2023

Nouvelles fonctionnalités

- Collector v1.1.45
- Support pour les sources de données multiples.

17 avril 2023

Nouvelles fonctionnalités

- Collector v1.1.22
- Améliorations des scripts de mise à niveau Cela nécessite la dernière version du Collector.

17 mars 2023

Nouvelle fonction

Ajout d'une analyse binaire, qui permet de détecter les anti-modèles et les incompatibilités sans code source.

07 novembre 2022

Nouvelle fonction

- Filtrage des applications
- Filtrage du serveur par AWS Application Discovery Service balises

27 septembre 2022

Nouvelle fonction

- Collector v1.1.12
 - Version SCT 667
 - EMPAnalyzer 2,2,0,368
- `diag checkCommandes` ajoutées pour obtenir des informations sur le serveur.
- Ajout de la prise en charge des recommandations potentielles.
- Interface utilisateur améliorée pour vérifier l'état de la configuration et de l'évaluation.

Corrections de bugs

- Portage de l'assistant traducteur et autres corrections.

30 juin 2022

Nouvelle fonction

- Collector v1.1.11
 - Support VMware d'API ajouté.
 - A2C a demandé des modifications pour ajouter un en-tête utilisateur lors du téléchargement du fichier binaire.
 - Ajout du chemin d'accès Linux, du shell par défaut et de la terminaison à distance de tous les shells.
- Binaire public A2C v1.17
 - Ajout de la prise en charge d'Azure DevOps en tant que cible de déploiement du pipeline.

18 avril 2022

Nouvelle fonction

- Collector v1.1.7
- Ajout de la possibilité de télécharger dynamiquement le binaire A2C à partir de l'URL publique.

Corrections de bugs

- A2C v1.1.5

25 février 2022

Corrections de bugs

- SCT v5.6.9
- A2C v1.1.2
- Collector v1.1.4

10 février 2022

Corrections de bugs

- SCT v5.6.8
- A2C v1.1.1
 - Ajout d'une vérification de la tar commande sous Linux.
 - Le problème de vérification des images des applications dans Amazon ECR a été résolu.
 - Le problème nécessitant le retrait du conteneur pour la pré-validation a été résolu.
- Collector v1.1.3
 - Correction de l'erreur 4xx pour une machine distante 32 bits.
 - Les codes d'erreur A2C ont été mis à jour.
 - L'adresse IP a été validée C# pour l'analyse du code source de la machine distante.

28 janvier 2022

Nouvelle fonction

- Collecteur v1.1.2
- Ajout de la prise en charge du référentiel Azure DevOps Git pour l'analyse du code source.

14 janvier 2022

Nouvelle fonction

- Collecteur v1.1.1
- Ajout de recommandations Babelfish pour les bases de données SQL.

21 décembre 2021

Problème résolu

- Collector v1.1.0
- L'analyse de la base de données a été rétablie.

15 décembre 2021

Problème connu

- Collector v1.0.4
- L'analyse de base de données n'est actuellement pas prise en charge (CVE-2021-44228).

25 octobre 2021

Nouvelle fonction

- Collector v1.0.0
- Première publication du guide d'utilisation des recommandations de stratégie de Migration Hub.

Historique des documents et des versions

Le tableau suivant décrit les publications de documentation relatives aux recommandations de stratégie. Pour de plus amples informations, veuillez consulter [Notes de mise à jour](#).

Modification	Description	Date
AWS mises à jour des politiques gérées - mise à jour vers AWSMigration HubStrategyCollector	La AWSMigrationHubStrategyCollector politique a été mise à jour pour inclure de nouvelles migration hub-strategy actions s3application-transformation , et.	1er avril 2024
AWS mises à jour des politiques gérées - mise à jour vers AWSMigration HubStrategyCollector	La AWSMigrationHubStrategyCollector politique a été mise à jour pour inclure de nouvelles application-transformation actions. Cette mise à jour ajoute également des conditions pour restreindre diverses actions dont la valeur <code>aws:ResourceAccount</code> doit être égale à <code>aws:PrincipalAccount</code> .	5 février 2024
Nouvelle fonctionnalité	Le client de collecte de données d'application Strategy Recommendations v1.1.47 est disponible avec le support des applications .NET 8.	17 novembre 2023
Nouvelle fonctionnalité	Le client de collecte de données de l'application Strategy Recommendations	12 octobre 2023

	v1.1.45 est disponible avec le support de plusieurs sources de données .	
AWS mises à jour des politiques gérées - mise à jour vers AWSMigration HubStrategyCollector	Mise à jour AWSMigrationHubStrategyCollector de la politique pour inclure le nouvel Amazon S3 APIs.	15 septembre 2023
AWS mises à jour des politiques gérées - mise à jour vers AWSMigration HubStrategyCollector	Mise à jour de la AWSMigrationHubStrategyCollector politique afin d'inclure de nouveaux analyseurs pour le code source.	8 mars 2023
Mises à jour des bonnes pratiques IAM	Pour plus d'informations, consultez Bonnes pratiques de sécurité dans IAM .	25 février 2023
AWS mises à jour de politiques gérées : mise à jour d'une politique existante	Les recommandations relatives à la stratégie du Hub de migration en AWS Application Discovery Service APIs ont ajouté trois à une politique existante.	10 novembre 2022
Mises à jour de sécurité	Établissez une connexion privée avec le point de terminaison VPC de l'interface .	07 mars 2022
Nouvelle fonctionnalité	Ajout de la prise en charge du référentiel Azure DevOps Git pour l'analyse du code source .	28 janvier 2022
Nouvelle fonctionnalité	Ajout de recommandations Babelfish pour les bases de données SQL .	14 janvier 2022

Première version	Première publication du guide d'utilisation des recommandations de stratégie de Migration Hub.	25 octobre 2021
------------------	--	-----------------

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.