Guide de l’utilisateur

AWS Application Discovery Service

AWS Application Discovery Service: Guide de l’utilisateur

Table of Contents

Qu'est-ce que c'est AWS Application Discovery Service ?

AWS Application Discovery Service vous aide à planifier votre migration vers le AWS cloud en collectant des données d'utilisation et de configuration concernant vos serveurs et bases de données sur site. Application Discovery Service est intégré à AWS Migration Hub AWS Database Migration Service Fleet Advisor. Migration Hub simplifie le suivi de votre migration en regroupant les informations relatives à l'état de la migration dans une console unique. Vous pouvez afficher les serveurs découverts, les regrouper en applications, puis suivre l'état de migration de chaque application depuis la console Migration Hub de votre région d'origine. Vous pouvez utiliser DMS Fleet Advisor pour évaluer les options de migration pour les charges de travail des bases de données.

Toutes les données découvertes sont stockées dans votre région d' AWS Migration Hub origine. Par conséquent, vous devez définir votre région d'origine dans la console Migration Hub ou à l'aide des commandes de la CLI avant d'effectuer des activités de découverte et de migration. Vos données peuvent être exportées à des fins d'analyse dans Microsoft Excel ou dans des outils d' AWS analyse tels qu'Amazon Athena et Amazon Quick.

Application Discovery Service APIs vous permet d'exporter les données de performance et d'utilisation du système pour les serveurs découverts. Entrez ces données dans votre modèle de coûts pour calculer le coût d'exploitation de ces serveurs AWS. En outre, vous pouvez exporter des données sur les connexions réseau existant entre les serveurs. Ces informations vous aident à déterminer les dépendances réseau entre les serveurs et à les regrouper dans des applications pour planifier la migration.

> **Note**
>
> Votre région d'origine doit être définie AWS Migration Hub avant de commencer le processus de découverte, car vos données seront stockées dans votre région d'origine. Pour plus d'informations sur l'utilisation d'une région d'origine, consultez la section Région d'origine.

Application Discovery Service propose trois méthodes pour effectuer la découverte et collecter des données sur vos serveurs locaux :

- La découverte sans agent peut être effectuée en déployant le collecteur sans agent Application Discovery Service (collecteur sans agent) (fichier OVA) via votre vCenter. VMware Une fois

qu'Agentless Collector est configuré, il identifie les machines virtuelles (VMs) et les hôtes associés à vCenter. Agentless Collector collecte les données de configuration statiques suivantes : noms d'hôte du serveur, adresses IP, adresses MAC, allocations de ressources de disque, versions du moteur de base de données et schémas de base de données. En outre, il collecte les données d'utilisation pour chaque machine virtuelle et base de données, fournissant l'utilisation moyenne et maximale pour des indicateurs tels que le processeur, la RAM et les E/S de disque.

- La découverte basée sur un agent peut être effectuée en déployant l'agent de découverte d' AWS applications (agent de découverte) sur chacun de vos serveurs VMs physiques. Le programme d'installation de l'agent est disponible pour les systèmes d'exploitation Windows et Linux. Il collecte les données de configuration statiques, les informations relatives aux performances du système détaillées en séries chronologiques, les connexions réseau entrantes et sortantes, et les processus en cours d'exécution.
- L'importation basée sur des fichiers vous permet d'importer les détails de votre environnement sur site directement dans Migration Hub sans utiliser Agentless Collector ou Discovery Agent. Vous pouvez ainsi évaluer et planifier la migration directement à partir de vos données importées. Les données ingérées dépendent des données fournies.

Application Discovery Service s'intègre aux solutions de découverte d'applications des AWS partenaires du réseau de partenaires (APN). Ces solutions tierces peuvent vous aider à importer des informations relatives à votre environnement sur site directement dans Migration Hub, sans utiliser de collecteur ou d'agent de découverte sans agent. Les outils de découverte d'applications tiers peuvent interroger AWS Application Discovery Service et écrire dans la base de données Application Discovery Service à l'aide de l'API publique. De cette façon, vous pouvez importer et visualiser des données dans Migration Hub, de manière à pouvoir associer des applications à des serveurs et suivre les migrations.

VMware Découverte

Si vous avez des machines virtuelles (VMs) qui s'exécutent dans l'environnement VMware vCenter, vous pouvez utiliser le collecteur sans agent pour collecter des informations système sans avoir à installer d'agent sur chaque machine virtuelle. Au lieu de cela, vous chargez ce dispositif sur site dans vCenter et vous l'autorisez à découvrir tous ses hôtes et. VMs

Agentless Collector capture les informations relatives aux performances du système et à l'utilisation des ressources pour chaque machine virtuelle exécutée dans le vCenter, quel que soit le système d'exploitation utilisé. Cependant, il ne peut pas « examiner » chacune d'entre elles et ne peut donc

pas déterminer quels processus sont exécutés sur chaque machine virtuelle ni quelles connexions réseau existent. VMs Par conséquent, si vous avez besoin de ce niveau de détail et que vous souhaitez examiner de plus près certains de vos modèles existants VMs afin de planifier votre migration, vous pouvez installer le Discovery Agent selon vos besoins.

En outre, pour l' VMs hébergement sur VMware, vous pouvez utiliser à la fois le collecteur sans agent et l'agent de découverte pour effectuer la découverte simultanément. Pour plus de détails concernant les types exacts de données que chaque outil de découverte collectera, consultezUtilisation du module de collecte de VMware données vCenter Agentless Collector.

Découverte des bases de données

Si vous avez des serveurs de base de données et d'analyse dans votre environnement local, vous pouvez utiliser le collecteur sans agent pour découvrir et inventorier ces serveurs. Vous pouvez ensuite collecter des mesures de performance pour chaque serveur de base de données sans avoir à installer Agentless Collector sur chaque ordinateur de votre environnement.

Le module de collecte de données de base de données et d'analyse Agentless Collector capture les métadonnées et les indicateurs de performance qui fournissent un aperçu de votre infrastructure de données. Le module de collecte de données de base de données et d'analyse utilise le protocole LDAP dans Microsoft Active Directory pour recueillir des informations sur le système d'exploitation, la base de données et les serveurs d'analyse de votre réseau. Ensuite, le module de collecte de données exécute régulièrement des requêtes pour collecter les mesures d'utilisation réelles du processeur, de la mémoire et de la capacité du disque pour les bases de données et les serveurs d'analyse. Pour plus de détails concernant les mesures collectées, consultezDonnées collectées par la base de données et le module d'analyse.

Une fois qu'Agentless Collector a terminé la collecte des données de votre environnement, vous pouvez utiliser la AWS DMS console pour une analyse plus approfondie et pour planifier votre migration. Par exemple, pour choisir une cible de migration optimale dans le AWS Cloud, vous pouvez générer des recommandations de cibles pour vos bases de données sources. Pour de plus amples informations, veuillez consulter Utilisation du module de collecte de données de base de données et d'analyse.

Comparez Agentless Collector et Discovery Agent

Le tableau suivant fournit une comparaison rapide des méthodes de collecte de données prises en charge par Application Discovery Service.

	Collectionneur sans agent	Agent de découverte	Modèle de Hub de migration	RVTools exportation
Supported server types				
VMware machine virtuelle	Oui	Oui	Oui	Oui
Serveur physique	Non	Oui	Oui	Oui
Deployment				
Par serveur	Non	Oui	N/A	Non
Par vCenter	Oui	Non	N/A	Oui
Par centre de données sur le même réseau	Non	Non	N/A	Non
Collected data				
Données de profil de serveur (configuration statique)	Oui	Oui	Oui	Oui
Mesures d'utilisation du serveur fournies par l'hyperviseur (processeur, RAM, etc.)	Oui	Oui	Oui	Non
Mesures d'utilisation du serveur provenant du	Oui	Oui	Oui	Non

	Collectionneur sans agent	Agent de découverte	Modèle de Hub de migration	RVTools exportation
serveur (CPU, RAM, etc.)				
Connexions réseau au serveur (TCP uniquement)	Oui	Oui	Non	Non
Processus en cours d'exécution	Non	Oui	Non	Non
Intervalle de collecte	-60 minutes	-15 secondes	Instantané unique	Instantané unique
Server data use cases				
Afficher les données du serveur dans Migration Hub	Oui	Oui	Profil uniquement	Non
Génération de recommandations Amazon EC2 en fonction du profil du serveur	Oui	Oui	Oui	Oui
Génération de recommandations Amazon EC2 en fonction des données d'utilisation	Oui	Oui	Oui	Non

	Collectionneur sans agent	Agent de découverte	Modèle de Hub de migration	RVTools exportation
Exportation des dernières données instantanées d'utilisation	Oui	Oui	Oui	Non
Exportation des données d'utilisation des séries chronologiques	Non	Oui	Non	Non
Network data use cases				
Visualisation dans Migration Hub	Oui	Oui	Non	Non
Exportez vers Amazon Athena pour une exploration plus approfondie	Non	Oui	Non	Non
Exporter vers un fichier CSV	Non	Oui	Non	Non
Database use cases				
Données de profil du serveur de base de données (configuration statique)	Oui	Non	Non	Non

	Collectionneur sans agent	Agent de découverte	Modèle de Hub de migration	RVTools exportation
Moteurs de base de données pris en charge	Oracle, SQL Server, MySQL, PostgreSQL	Aucune	Aucun	Aucune
Complexité du schéma de base de données et doublons	Oui	Non	Non	Non
objets de schéma de base de données	Oui	Non	Non	Non
Platform support				
Systèmes d'exploitation pris en charge	Tout système d'exploitation fonctionnant dans VMware Center v5.5 ou versions plus récentes	N'importe quel serveur Linux ou Windows	N'importe quel serveur Linux ou Windows	Tout serveur Linux, serveur Windows ou VMware version 5.5 ou ultérieure

Hypothèses

Pour utiliser Application Discovery Service, les conditions suivantes sont supposées :

- Vous vous êtes inscrit à AWS. Pour de plus amples informations, veuillez consulter Configuration d'Application Discovery Service.
- Vous avez sélectionné une région d'origine du Migration Hub. Pour plus d'informations, consultez la documentation concernant les régions d'origine.

Ce à quoi vous pouvez vous attendre :

- La région d'origine du Migration Hub est la seule région dans laquelle Application Discovery Service stocke vos données de découverte et de planification.
- Les agents de découverte, les connecteurs et les importations ne peuvent être utilisés que dans la région d'origine du Migration Hub que vous avez sélectionnée.
- Pour obtenir la liste des AWS régions dans lesquelles vous pouvez utiliser Application Discovery Service, consultez le Référence générale d'Amazon Web Services.

AWS Application Discovery Service changement de disponibilité

Après mûre réflexion, nous avons décidé de fermer nos portes AWS Application Discovery Service à de nouveaux clients à compter du 7 novembre 2025. Si vous souhaitez utiliser le service, inscrivez-vous avant cette date. Les clients existants peuvent continuer à utiliser le service normalement.

Cette rubrique fournit des informations sur le changement de disponibilité et des conseils pour la transition vers AWS Transform.

Informations sur la disponibilité des services

Application Discovery Service cessera d'accepter de nouveaux clients à compter du 7 novembre 2025. AWS Transform est notre service d'intelligence artificielle agentique de nouvelle génération qui fournit des fonctionnalités similaires ainsi que des capacités améliorées de découverte et d'évaluation des machines virtuelles. Les clients existants de l'Application Discovery Service peuvent continuer à utiliser le service pour mener à bien leurs projets de découverte en cours, qui ont généralement un cycle de vie de 4 mois. Les fonctionnalités de base du service, qui permettent de découvrir et de collecter des données sur les serveurs et applications sur site, sont désormais disponibles AWS Transform avec des fonctionnalités améliorées, ce qui ne nécessite aucun effort du client pour effectuer la transition.

Jusqu'au 7 novembre 2025, nous continuerons de garantir la sécurité et la fiabilité d'Application Discovery Service. Bien que nous n'ajoutions pas de nouvelles fonctionnalités au service, nous restons déterminés à fournir des mises à jour de sécurité et à maintenir la disponibilité du service afin de garantir le bon déroulement de vos projets de migration en cours. Notre objectif est de garantir un environnement stable permettant aux clients existants de mener à bien leurs initiatives de migration en vol tout en se préparant aux capacités améliorées disponibles dans AWS Transform.

AWS Transform transition

AWS Transform est notre solution recommandée qui réunit toutes les fonctionnalités d'Application Discovery Service tout en introduisant de nouvelles fonctionnalités puissantes. Il fournit des fonctionnalités complètes de découverte et d'évaluation par le biais de collecteurs basés sur des agents et sans agent, avec une analyse améliorée VMware de l'environnement. Le service permet

d'automatiser le mappage des dépendances des applications et la planification des vagues, tout en offrant une logique de découverte améliorée avec des analyses hypothétiques et des estimations de coûts. Ses fonctionnalités avancées, notamment le stockage intégré et la découverte de bases de données, l'intégration consolidée des outils 3P et l'analyse complète de la configuration des machines virtuelles, AWS Transform sont conçues pour rendre le processus d'évaluation et de planification de la migration des clients plus efficace et plus efficace.

La transition vers AWS Transform est simple, aucune migration de données n'est requise. Les projets de découverte existants dans Application Discovery Service continueront de fonctionner normalement jusqu'à leur achèvement. Lorsque les clients sont prêts à démarrer de nouveaux projets de découverte, ils peuvent commencer à les utiliser AWS Transform directement : toutes les fonctionnalités de découverte et d'évaluation d'Application Discovery Service y sont disponibles avec des fonctionnalités améliorées. Pour commencer à utiliser, AWS Transform veuillez consulter le guide de démarrage. AWS L'équipe de support est disponible via la console de AWS support pour répondre aux questions AWS Transform d'accès ou aux questions concernant les projets de découverte en cours.

Questions fréquentes (FAQ)

Qu'est-ce que cela signifie pour le service (allez-vous le fermer) ?

Application Discovery Service cessera d'accepter de nouveaux clients à compter du 7 novembre 2025. Le service continuera de fonctionner pour les clients existants afin de mener à bien leurs projets de migration en cours.

Quel sera l'impact sur les clients existants ?

Les clients existants ne subiront aucune interruption de leurs projets de migration en cours. Ils peuvent continuer à utiliser Application Discovery Service normalement jusqu'à ce que leurs projets soient terminés. Tous les projets en cours resteront accessibles, et les mises à jour de sécurité continueront d'être déployées pour maintenir la fiabilité du service.

Le 7 novembre 2025, le client rencontre des problèmes, comment peuvent-ils s'aggraver ?

Les clients qui rencontrent des problèmes peuvent contacter le AWS Support via leur console de AWS support. L'équipe de AWS support est disponible pour répondre à toutes les questions ou préoccupations liées au service.

Quelles sont les alternatives que les clients peuvent explorer ?

AWS Transform est le service de remplacement recommandé. Lancé en 2025, AWS Transform inclut des fonctionnalités similaires d'Application Discovery Service. Offre des fonctionnalités améliorées avec une analyse améliorée de VMware l'environnement et un mappage automatique des dépendances. Fournit des fonctionnalités intégrées de stockage et de découverte de bases de données ainsi que des outils d'évaluation complets. Aucun outillage spécial n'est requis lors de la transition vers. AWS Transform

Comment les clients peuvent-ils migrer hors Application Discovery Service ?

Aucune procédure de migration officielle n'est requise. Les projets existants peuvent être poursuivis dans Application Discovery Service jusqu'à leur fin. Pour les nouveaux projets, les clients peuvent s'y lancer directement AWS Transform, ce qui leur permet de bénéficier de toutes les fonctionnalités habituelles d'Application Discovery Service, ainsi que de fonctionnalités améliorées. Aucune migration de données n'est nécessaire et le AWS Support est disponible pour vous aider dans cette transition.

Si vous avez d'autres questions, veuillez nous contacter via le AWS Support ou lire notre FAQs.

Configuration d'Application Discovery Service

Avant de l'utiliser AWS Application Discovery Service pour la première fois, effectuez les tâches suivantes :

- S'inscrire à Amazon Web Services
- Créez des utilisateurs IAM
- Connectez-vous à la console Migration Hub et choisissez une région d'origine

S'inscrire à Amazon Web Services

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

Pour vous inscrire à un Compte AWS

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

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

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

Créez des utilisateurs IAM

Lorsque vous créez un AWS compte, vous obtenez une identité de connexion unique qui donne un accès complet à tous les AWS services et ressources du compte. Cette identité est appelée utilisateur root du AWS compte. La connexion à l' AWS Management Console aide de l'adresse e-mail et du mot de passe que vous avez utilisés pour créer le compte vous donne un accès complet à toutes les AWS ressources de votre compte.

Il est vivement recommandé de ne pas employer l'utilisateur racine pour vos tâches quotidiennes, y compris pour les tâches administratives. Suivez plutôt les meilleures pratiques en matière de

sécurité : créez des utilisateurs IAM individuels et créez un utilisateur administrateur Gestion des identités et des accès AWS (IAM). Ensuite, mettez en sécurité les informations d'identification de l'utilisateur racine et utilisez-les uniquement pour effectuer certaines tâches de gestion des comptes et des services.

Outre la création d'un utilisateur administratif, vous devez également créer des utilisateurs IAM non administratifs. Les rubriques suivantes expliquent comment créer les deux types d'utilisateurs IAM.

Rubriques

Création d'un utilisateur administratif IAM

Par défaut, un compte administrateur hérite de toutes les politiques requises pour accéder à Application Discovery Service.

Pour créer un utilisateur administrateur

- Créez un utilisateur administrateur dans votre AWS compte. Pour obtenir des instructions, veuillez consulter Création de votre premier groupe d'utilisateurs et d'administrateurs IAM dans le Guide de l'utilisateur IAM.

Création d'un utilisateur non administratif IAM

Lorsque vous créez des utilisateurs IAM non administrateurs, suivez les bonnes pratiques de sécurité Accorder le moindre privilège, en accordant aux utilisateurs des autorisations minimales.

Utilisez les politiques gérées par IAM pour définir le niveau d'accès à Application Discovery Service pour les utilisateurs IAM non administrateurs. Pour plus d'informations sur les politiques gérées par Application Discovery Service, consultezAWS politiques gérées pour AWS Application Discovery Service.

Pour créer un utilisateur IAM non administrateur

1. Dans AWS Management Console, accédez à la console IAM.

2. Créez un utilisateur IAM non administrateur en suivant les instructions de création d'un utilisateur avec la console, comme décrit dans la section Création d'un utilisateur IAM dans votre AWS compte du guide de l'utilisateur IAM.

   En suivant les instructions du guide de l'utilisateur IAM :

   - À l'étape concernant la page Définir les autorisations, choisissez l'option Associer directement les politiques existantes à l'utilisateur. Sélectionnez ensuite une stratégie IAM gérée pour Application Discovery Service dans la liste des politiques. Pour plus d'informations sur les politiques gérées par Application Discovery Service, consultezAWS politiques gérées pour AWS Application Discovery Service.
   - Lorsque vous consultez les clés d'accès de l'utilisateur (clé d'accès IDs et clés d'accès secrètes), suivez les instructions de la note importante concernant l'enregistrement du nouvel identifiant de clé d'accès et de la nouvelle clé d'accès secrète de l'utilisateur dans un endroit sûr et sécurisé.
3. Après avoir créé l'utilisateur, accordez-lui un accès programmatique comme décrit dans la section Support de l'accès utilisateur programmatique.

Connectez-vous à la console Migration Hub et choisissez une région d'origine

Vous devez choisir une région d' AWS Migration Hub origine dans le AWS compte que vous utilisez pour le AWS Application Discovery Service.

Pour choisir une région d'origine

1. À l'aide de votre AWS compte, 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 Paramètres, puis choisissez une région d'accueil.

   Les données de votre Hub de migration sont stockées dans votre région d'origine à des fins de découverte, de planification et de suivi de la migration. Pour plus d'informations, consultez la région d'origine de The Migration Hub.

AWS Agent de découverte d'applications

L'agent de découverte AWS d'applications (agent de découverte) est un logiciel que vous installez sur des serveurs locaux et des machines virtuelles destinés à la découverte et à la migration. L'agent collecte des informations relatives à la configuration système, aux performances du système, aux processus en cours d'exécution, ainsi que des détails sur les connexions réseau entre les systèmes. Les agents prennent en charge la plupart des systèmes d'exploitation Linux et Windows, et vous pouvez les déployer sur des serveurs physiques sur site, des instances Amazon EC2 et des machines virtuelles.

> **Note**
>
> Avant de déployer le Discovery Agent, vous devez choisir une région d'origine du Migration Hub. Vous devez enregistrer votre agent dans votre région d'origine.

Le Discovery Agent s'exécute dans votre environnement local et nécessite des privilèges root. Lorsque vous démarrez le Discovery Agent, il se connecte en toute sécurité à votre région d'origine et s'enregistre auprès d'Application Discovery Service.

- Par exemple, s'il s'`eu-central-1`agit de votre région d'origine, elle s'enregistre `arsenal-discovery.`*`eu-central-1`*`.amazonaws.com` auprès d'Application Discovery Service.
- Ou remplacez votre région d'origine par toutes les autres régions, à l'exception de us-west-2, selon les besoins.
- S'il s'`us-west-2`agit de votre région d'origine, elle s'enregistre `arsenal.us-west-2.amazonaws.com` auprès d'Application Discovery Service.

Comment ça marche

Après l'enregistrement, l'agent commence à collecter des données pour l'hôte ou la machine virtuelle où il réside. L'agent envoie un ping à l'Application Discovery Service à intervalles de 15 minutes pour obtenir des informations de configuration.

Les données collectées incluent les spécifications du système, l'utilisation des séries temporelles ou les données de performances, les connexions réseau et les données de traitement. Vous pouvez utiliser ces informations pour mapper vos ressources informatiques et leurs dépendances réseau.

Tous ces points de données peuvent vous aider à déterminer le coût d'exploitation de ces serveurs AWS et à planifier la migration.

Les données sont transmises en toute sécurité par les agents de découverte à Application Discovery Service à l'aide du cryptage TLS (Transport Layer Security). Les agents sont configurés pour être mis à niveau automatiquement lorsque de nouvelles versions deviennent disponibles. Si vous le souhaitez, vous pouvez modifier ce paramètre de configuration.

> **Tip**
>
> Avant de télécharger et de commencer l'installation de Discovery Agent, assurez-vous de lire tous les prérequis requis dans Conditions requises pour Discovery Agent

Données collectées par Discovery Agent

AWS L'agent de découverte d'applications (agent de découverte) est un logiciel que vous installez sur des serveurs locaux et VMs. Discovery Agent collecte la configuration du système, les données d'utilisation ou de performance des séries chronologiques, les données de processus et les connexions réseau TCP (Transmission Control Protocol). Cette section décrit les données collectées.

Légende du tableau pour les données collectées par Discovery Agent :

- Le terme « hôte » fait référence à un serveur physique ou à une machine virtuelle.
- Les données collectées sont mesurées en kilo-octets (Ko), sauf indication contraire.
- Les données équivalentes de la console Migration Hub sont indiquées en mégaoctets (Mo).
- La période de sondage se déroule à intervalles d'environ 15 secondes et est envoyée AWS toutes les 15 minutes.
- Les champs de données marqués d'un astérisque (*) ne sont disponibles que dans les `.csv` fichiers produits à partir de la fonction d'exportation de l'API de l'agent.

Champ de données	Description
agentAssignedProcessIdentifiant *	ID des processus détectés par l'agent
agentId	ID unique de l'agent

Champ de données	Description
agentProvidedTimeTampon *	Date et heure de l'observation de l'agent (mm/dd/yyyy hh:mm:ss am/pm)
cmdLine*	Processus entré dans la ligne de commande
cpuType	Type d'UC (unité de traitement centrale) utilisée dans l'hôte
destinationIp*	Adresse IP de l'appareil auquel le paquet est envoyé
destinationPort*	Numéro de port auquel data/request le doit être envoyé
family*	Protocole de famille de routage
freeRAM (MB)	RAM libre et RAM mise en cache qui peuvent être immédiatement disponibles pour les applications, calculées en MB
gateway*	Adresse du nœud du réseau
hostName	Nom de l'hôte sur lequel des données ont été collectées
hyperviseur	Type d'hyperviseur
ipAddress	Adresse IP de l'hôte
ipVersion*	Numéro de la version IP
isSystem*	Attribut booléen pour indiquer si un processus est détenu par le système d'exploitation
macAddress	Adresse MAC de l'hôte
name*	Nom de l'hôte, du réseau, des métriques, etc., pour lesquels les données sont collectées

Champ de données	Description
netMask*	Préfixe de l'adresse IP à laquelle l'hôte réseau appartient
osName	Nom du système d'exploitation sur l'hôte
osVersion	Version du système d'exploitation sur l'hôte
path	Chemin de la commande provenant de la ligne de commande
sourceIp*	Adresse IP de l'appareil qui envoie le paquet IP
sourcePort*	Numéro de port d'où data/request provient le
timestamp*	Date et heure de l'attribut signalé et enregistré par l'agent
totalCpuUsagePCT	Pourcentage d'utilisation de l'UC sur l'hôte pendant la période d'interrogation
totalDiskBytesReadPerSecond (Kbits/s)	Nombre total de kilobits lus par seconde sur tous les disques
totalDiskBytesWrittenPerSecond (Kbits/s)	Nombre total de kilobits écrits par seconde sur tous les disques
totalDiskFreeTaille (Go)	Espace disque libre exprimé en Go
totalDiskReadOpsPerSecond	Nombre total d' I/O opérations de lecture par seconde
totalDiskSize (Go)	Capacité totale du disque exprimée en Go
totalDiskWriteOpsPerSecond	Nombre total d' I/O opérations d'écriture par seconde
totalNetworkBytesReadPerSecond (Kbits/s)	Quantité totale de débit d'octets lus par seconde

Champ de données	Description
totalNetworkBytesWrittenPerSecond (Kbits/s)	Quantité totale de débit d'octets écrits par seconde
totalNumCores	Nombre total d'unités de traitement indépendant au sein de l'UC
totalNumCpus	Nombre total d'unités de traitement centrales
totalNumDisks	Nombre de disques durs physiques sur un hôte
totalNumLogicalProcesseurs*	Nombre total de cœurs physiques multiplié par le nombre de threads qui peuvent s'exécuter sur chaque cœur
totalNumNetworkCartes	Nombre total de cartes réseau sur le serveur
totalRAM (Mo)	Quantité totale de RAM disponible sur l'hôte
transportProtocol*	Type de protocole de transport utilisé

Conditions requises pour Discovery Agent

Vous trouverez ci-dessous les conditions préalables et les tâches que vous devez effectuer avant de pouvoir installer correctement l'agent de découverte AWS d'applications (agent de découverte).

- Vous devez définir une région d'AWS Migration Hub origine avant de commencer à installer Discovery Agent.
- Si la version de l'agent installée est 1.x, elle doit être supprimée avant que vous installiez la dernière version.
- Si l'hôte sur lequel l'agent est installé exécute Linux, vérifiez qu'il prend au moins en charge l'architecture du processeur Intel i686 (également appelée microarchitecture P6).
- Générez les clés d'accès nécessaires à l'installation de Discovery Agent.
- 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, 15 SP5

Windows

Windows Server 2003 R2 SP2

Windows Server 2008 R1 SP2, 2008 R2 SP1

Windows Server 2012 R1, 2012 R2

Windows Server 2016

Windows Server 2019

Windows Server 2022

- Si les connexions sortantes de votre réseau sont restreintes, vous devez mettre à jour vos paramètres de pare-feu. Les agents doivent pouvoir accéder à `arsenal` sur le port TCP 443. Ils n'ont pas besoin que les ports entrants soient ouverts.

  Par exemple, si votre région d'origine est`eu-central-1`, vous utiliseriez `https://arsenal-discovery.`*`eu-central-1`*`.amazonaws.com:443`
- L'accès à Amazon S3 dans votre région d'origine est nécessaire pour que la mise à niveau automatique fonctionne.
- Créez un utilisateur Gestion des identités et des accès AWS (IAM) dans la console et associez la politique gérée `AWSApplicationDiscoveryAgentAccess` IAM existante. Cette stratégie permet à l'utilisateur d'effectuer les actions d'agent nécessaires en votre nom. Pour en savoir plus sur les politiques gérées, consultez AWS politiques gérées pour AWS Application Discovery Service.
- Vérifiez le décalage horaire par rapport à vos serveurs NTP et corrigez-le, le cas échéant. Une synchronisation de l'heure incorrecte provoque l'échec de l'enregistrement de l'agent.

> **Note**
>
> Le Discovery Agent possède un agent exécutable 32 bits, qui fonctionne sur les systèmes d'exploitation 32 bits et 64 bits. Le nombre de packages d'installation nécessaires pour le déploiement est réduit si vous disposez d'un seul exécutable. Cet agent exécutable

fonctionne pour les systèmes d'exploitation Linux et Windows. Ce sujet est abordé dans leur section d'installation respective ci-après.

Installation de Discovery Agent

Cette page explique comment installer le Discovery Agent sous Linux et Microsoft Windows.

Installation de Discovery Agent sous Linux

Exécutez la procédure suivante sous Linux. Assurez-vous que la région d'origine de votre Migration Hub a été définie avant de commencer cette procédure.

> **Note**
>
> Si vous utilisez une version de Linux autre que la version actuelle, consultez Considérations relatives aux anciennes plateformes Linux.

Pour installer AWS l'agent Application Discovery dans votre centre de données

1. Connectez-vous à votre serveur ou à votre machine virtuelle Linux et créez un nouveau répertoire contenant les composants de votre agent.
2. Basculez vers le nouveau répertoire et téléchargez le script d'installation à partir de la ligne de commande ou de la console.

    a. Pour télécharger à partir de la ligne de commande, exécutez la commande suivante.

    ```
    curl -o ./aws-discovery-agent.tar.gz https://s3.region.amazonaws.com/aws-discovery-agent.region/linux/latest/aws-discovery-agent.tar.gz
    ```

    b. Pour effectuer le téléchargement depuis la console Migration Hub, procédez comme suit :

        i. Connectez-vous à la console Migration Hub AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/migrationhub/.

        ii. Dans la page de navigation de gauche, sous Découvrir, sélectionnez Outils.

        iii. Dans le champ AWS Discovery Agent, choisissez Download agents, puis Download for Linux. Votre téléchargement commence immédiatement.

3. Vérifiez la signature de chiffrement du package d'installation avec les trois commandes suivantes :

```
curl -o ./agent.sig https://s3.region.amazonaws.com/aws-discovery-agent.region/linux/latest/aws-discovery-agent.tar.gz.sig
```

```
curl -o ./discovery.gpg https://s3.region.amazonaws.com/aws-discovery-agent.region/linux/latest/discovery.gpg
```

```
gpg --no-default-keyring --keyring ./discovery.gpg --verify agent.sig aws-discovery-agent.tar.gz
```

L'empreinte de la clé publique de l'agent (`discovery.gpg`) est `7638 F24C 6717 F97C 4F1B 3BC0 5133 255E 4DF4 2DA2`.

4. Procédez à l'extraction du fichier tarball, comme illustré ci-après.

```
tar -xzf aws-discovery-agent.tar.gz
```

5. Pour installer l'agent, choisissez l'une des méthodes d'installation suivantes.

Pour…	Faites ceci...
Installation de Discovery Agent	Pour installer l'agent, exécutez la commande d'installation de l'agent comme indiqué dans l'exemple suivant. Dans l'exemple, remplacez -le *your-home-region* par le nom de votre région d'origine, *aws-access-key-id* par l'identifiant de votre clé d'accès et *aws-secret-access-key* par votre clé d'accès secrète. `sudo bash install -r your-home-region -k aws-access-key-id -s aws-secret-access-key`

Pour…	Faites ceci...
	Par défaut, les agents téléchargent et appliquent automatiquement les mises à jour dès qu'elles sont disponibles. Nous vous recommandons d'utiliser cette configuration par défaut. Toutefois, si vous ne souhaitez pas que les agents téléchargent et appliquent les mises à jour automatiquement, incluez le `-u false` paramètre lors de l'exécution de la commande d'installation de l'agent.

Pour…	Faites ceci...
(Facultatif) Installez Discovery Agent et configurez un proxy non transparent	Pour configurer un proxy non transparent, ajoutez les paramètres suivants à la commande d'installation de l'agent : • -e Le mot de passe du proxy. • -f Le numéro de port du proxy. • -g Le schéma de proxy. • -i Le nom d'utilisateur du proxy. Voici un exemple de commande d'installation de l'agent utilisant les paramètres de proxy non transparents. `sudo bash install -r your-home-region -k aws-access-key-id -s aws-secret-access-key -d myproxy.mycompany.com -e mypassword -f proxy-port-number -g https -i myusername` Si votre proxy ne nécessite pas d'authentification, omettez les `-i` paramètres `-e` et. L'exemple de commande d'installation utilise`https`, si votre proxy utilise le protocole HTTP, spécifiez `http` la valeur du `-g` paramètre.

6. Si les connexions sortantes de votre réseau sont restreintes, vous devez mettre à jour vos paramètres de pare-feu. Les agents doivent pouvoir accéder à `arsenal` sur le port TCP 443. Ils n'ont pas besoin que les ports entrants soient ouverts.

   Par exemple, si votre région d'origine est`eu-central-1`, vous utiliseriez `https://arsenal-discovery.eu-central-1.amazonaws.com:443`

Considérations relatives aux anciennes plateformes Linux

Certaines plateformes plus anciennes, telles que SUSE 10, CentOS 5 et RHEL 5 sont en fin de vie ou sont prises en charge de façon minimale. Ces plateformes peuvent être affectées par des suites de out-of-date chiffrement qui empêchent le script de mise à jour de l'agent de télécharger les packages d'installation.

Curl

L'agent Application Discovery nécessite `curl` des communications sécurisées avec le AWS serveur. Certaines anciennes versions de `curl` ne sont pas en mesure de communiquer de manière sécurisée avec un service web moderne.

Pour utiliser la version de `curl` incluse avec l'agent de détection d'applications pour toutes les opérations, exécutez le script d'installation avec le paramètre `-c true`.

Bundle d'autorité de certification

Les anciens systèmes Linux peuvent disposer d'un bundle d'autorités de out-of-date certification (CA), essentiel pour sécuriser les communications Internet.

Pour utiliser le bundle de CA inclus avec l'agent de détection d'applications pour toutes les opérations, exécutez le script d'installation avec le paramètre `-b true`.

Ces options de script d'installation peuvent être utilisées conjointement. Dans l'exemple de commande suivant, les deux paramètres du script sont transmis au script d'installation :

```
sudo bash install -r your-home_region -k aws-access-key-id -s aws-secret-access-key -c
 true -b true
```

Installation de Discovery Agent sous Microsoft Windows

Procédez comme suit pour installer un agent sous Microsoft Windows. Assurez-vous que la région d'origine de votre Migration Hub a été définie avant de commencer cette procédure.

Pour installer AWS l'agent Application Discovery dans votre centre de données

1. Téléchargez le programme d'installation de l'agent Windows, mais ne double-cliquez pas pour exécuter le programme d'installation sous Windows.

> **Important**
>
> Ne double-cliquez pas pour exécuter le programme d'installation sous Windows, car l'installation échouera. L'installation de l'agent fonctionne uniquement à partir de l'invite de commande. (Si vous avez déjà double-cliqué sur le programme d'installation, vous devez accéder à Ajout/Suppression de programmes et désinstaller l'agent avant de poursuivre les étapes d'installation restantes.)
> Si le programme d'installation de l'agent Windows ne détecte aucune version du moteur d'exécution Visual C++ x86 sur l'hôte, il installe automatiquement le moteur d'exécution Visual C++ x86 2015—2019 avant d'installer le logiciel agent.

2. Ouvrez une invite de commande en tant qu'administrateur et naviguez jusqu'à l'emplacement où vous avez enregistré le package d'installation.
3. Pour installer l'agent, choisissez l'une des méthodes d'installation suivantes.

Pour…	Faites ceci...
Installation de Discovery Agent	Pour installer l'agent, exécutez la commande d'installation de l'agent comme indiqué dans l'exemple suivant. Dans l'exemple, remplacez-le *your-home-region* par le nom de votre région d'origine, *aws-access-key-id* par l'ID de votre clé d'accès et *aws-secret-access-key* par votre clé d'accès secrète. Vous pouvez éventuellement définir l'emplacement d'installation de l'agent en spécifiant le chemin du dossier *C:\install-location* pour le paramètre INSTALLLOCATION. Par exemple, `INSTALLLOCATION="` *C:\install-location* `"`. La hiérarchie de dossiers résultante sera [INSTALLLOCATION path] \AWS Discovery. Par défaut, l'emplace

Pour…	Faites ceci...
	ment d'installation est le `Program Files` dossier. Vous pouvez éventuellement l'utiliser `LOGANDCONFIGLOCATION` pour remplacer le répertoire par défaut (ProgramData) pour le dossier des journaux de l'agent et le fichier de configuration. La hiérarchie de dossiers qui en résulte est`[`*`LOGANDCONFIGLOCATION path`*` ]\AWS Discovery .` `.\AWSDiscoveryAgentInstaller.exe REGION="`*`your-home-region`*`" KEY_ID="`*`aws-access-key-id`*`" KEY_SECRET="`*`aws-secret-access-key`*`" /quiet` Par défaut, les agents téléchargent et appliquent automatiquement les mises à jour dès qu'elles sont disponibles. Nous vous recommandons d'utiliser cette configuration par défaut. Toutefois, si vous ne souhaitez pas que les agents téléchargent et appliquent les mises à jour automatiquement, incluez le paramètre suivant lors de l'exécution de la commande d'installation de l'agent : `AUTO_UPDATE=false`

Pour…	Faites ceci...
	Warning La désactivation des mises à niveau automatiques empêche l'installation des derniers correctifs de sécurité.

Pour…	Faites ceci...
(Facultatif) Installez Discovery Agent et configurez un proxy non transparent	Pour configurer un proxy non transparent, ajoutez les propriétés publiques suivantes à la commande d'installation de l'agent : • PROXY_HOST — Le nom de l'hôte proxy • PROXY_SCHEME — Le schéma de proxy • PROXY_PORT — Le numéro de port du proxy • PROXY_USER — Le nom d'utilisateur du proxy • PROXY_PASSWORD — Le mot de passe de l'utilisateur proxy Voici un exemple de commande d'installation de l'agent utilisant les propriétés non transparentes du proxy. `.\AWSDiscoveryAgentInstaller.exe REGION=" your-home-region " KEY_ID="aws-access-key-id " KEY_SECRET=" aws-secret-access-key " PROXY_HOST=" myproxy.mycompany.com " PROXY_SCHEME="https" PROXY_PORT=" proxy-port-number " PROXY_USER=" myusername " PROXY_PASSWORD=" mypassword " /quiet` Si votre proxy ne nécessite pas d'authentification, omettez les PROXY_PASSWORD propriétés PROXY_USER et. L'exemple de commande d'installation utilise`https`. Si votre proxy utilise le protocole HTTP, spécifiez `http` la PROXY_SCHEME valeur.

4. Si les connexions sortantes de votre réseau sont limitées, vous devez mettre à jour les paramètres de votre pare-feu. Les agents doivent pouvoir accéder à `arsenal` sur le port TCP 443. Ils n'ont pas besoin que les ports entrants soient ouverts.

   Par exemple, si votre région d'origine est la suivante`eu-central-1`, vous devez utiliser ce qui suit : `https://arsenal-discovery.eu-central-1.amazonaws.com:443`

Signature du package et mises à niveau automatiques

Pour Windows Server 2008 et versions ultérieures, Amazon signe cryptographiquement le package d'installation de l'agent Application Discovery Service avec un SHA256 certificat. Pour les mises à jour automatiques SHA2 signées sous Windows Server 2008 SP2, assurez-vous qu'un correctif est installé sur les hôtes pour prendre en charge l'authentification par signature. SHA2 Le dernier correctif de support de Microsoft permet de prendre en charge SHA2 l'authentification sur Windows Server 2008. SP2

> **Note**
>
> Les correctifs pour le SHA256 support de Windows 2003 ne sont plus accessibles au public auprès de Microsoft. Si ces correctifs ne sont pas déjà installés sur votre hôte Windows 2003, des mises à niveau manuelles sont nécessaires.

Pour effectuer des mises à niveau manuellement

1. Téléchargez le programme de mise à jour de l'agent Windows.
2. Ouvrez l'invite de commande en tant qu'administrateur.
3. Accédez à l'emplacement où le programme de mise à jour a été enregistré.
4. Exécutez la commande suivante.

```
AWSDiscoveryAgentUpdater.exe /Q
```

Gestion du processus Discovery Agent

Cette page explique comment gérer le Discovery Agent sous Linux et Microsoft Windows.

Gestion du processus Discovery Agent sous Linux

Vous pouvez gérer le comportement du Discovery Agent au niveau du système à l'aide des `System V init` outils `systemd``Upstart`, ou. Les onglets suivants décrivent les commandes pour les tâches prises en charge dans chacun des outils respectifs.

systemd

Commandes de gestion pour l'agent de détection d'applications

Sous-tâche	Commande
Vérifier qu'un agent est en cours d'exécution	`sudo systemctl status aws-discovery-daemon.service`
Démarrer un agent	`sudo systemctl start aws-discovery-daemon.service`
Arrêter un agent	`sudo systemctl stop aws-discovery-daemon.service`
Redémarrer un agent	`sudo systemctl restart aws-discovery-daemon.service`

Upstart

Commandes de gestion pour l'agent de découverte d'applications

Sous-tâche	Commande
Vérifier qu'un agent est en cours d'exécution	`sudo initctl status aws-discovery-daemon`
Démarrer un agent	`sudo initctl start aws-discovery-daemon`
Arrêter un agent	`sudo initctl stop aws-discovery-daemon`
Redémarrer un agent	`sudo initctl restart aws-discovery-daemon`

System V init

Commandes de gestion pour l'agent de découverte d'applications

Sous-tâche	Commande
Vérifier qu'un agent est en cours d'exécution	`sudo /etc/init.d/aws-discovery-daemon status`
Démarrer un agent	`sudo /etc/init.d/aws-discovery-daemon start`
Arrêter un agent	`sudo /etc/init.d/aws-discovery-daemon stop`
Redémarrer un agent	`sudo /etc/init.d/aws-discovery-daemon restart`

Gestion du processus Discovery Agent sous Microsoft Windows

Vous pouvez gérer le comportement du Discovery Agent au niveau du système via la console Windows Server Manager Services. Le tableau suivant décrit la procédure.

Sous-tâche	Service Name	Statut du service/Action
Vérifier qu'un agent est en cours d'exécution	AWS Agent de découverte AWS Discovery Updater	Démarré(e)
Démarrer un agent	AWS Agent de découverte AWS Discovery Updater	Choisissez Démarrer
Arrêter un agent	AWS Agent de découverte AWS Discovery Updater	Choisissez Arrêt
Redémarrer un agent	AWS Agent de découverte AWS Discovery Updater	Choisissez Redémarrer

Désinstallation de Discovery Agent

Cette page explique comment désinstaller le Discovery Agent sous Linux et Microsoft Windows.

Désinstallez Discovery Agent sous Linux

Cette section explique comment désinstaller Discovery Agent sous Linux.

Pour désinstaller un agent si vous utilisez le gestionnaire de packages yum

- Utilisez la commande suivante pour désinstaller un agent si vous utilisez yum.

```
rpm -e --nodeps aws-discovery-agent
```

Pour désinstaller un agent si vous utilisez le gestionnaire de paquets apt-get

- Utilisez la commande suivante pour désinstaller un agent si vous utilisez apt-get.

```
apt-get remove aws-discovery-agent:i386
```

Pour désinstaller un agent si vous utilisez le gestionnaire de packages zypper

- Utilisez la commande suivante pour désinstaller un agent si vous utilisez zypper.

```
zypper remove aws-discovery-agent
```

Désinstallez Discovery Agent sous Microsoft Windows

Cette section explique comment désinstaller Discovery Agent sous Microsoft Windows.

Pour désinstaller un agent de détection sur Windows

1. Ouvrez le panneau de configuration sous Windows.
2. Choisissez Programmes.
3. Choisissez Programmes et fonctionnalités.
4. Sélectionnez AWS Discovery Agent.

5. Choisissez Désinstaller.

> **Note**
>
> Si vous choisissez de réinstaller l'agent après l'avoir désinstallé, exécutez la commande suivante avec les `/norestart` options `/repair` et.
>
> ```
> .\AWSDiscoveryAgentInstaller.exe REGION="your-home-region" KEY_ID="aws-access-key-id" KEY_SECRET="aws-secret-access-key" /quiet /repair /norestart
> ```

Pour désinstaller un agent de découverte sous Windows à l'aide de la ligne de commande

1. Cliquez avec le bouton droit sur Démarrer
2. Choisissez Command Prompt.
3. Utilisez la commande suivante pour désinstaller un agent de découverte sous Windows.

```
wmic product where name='AWS Discovery Agent' call uninstall
```

> **Note**
>
> Si le `.exe` fichier est présent sur le serveur, vous pouvez désinstaller complètement l'agent du serveur à l'aide de la commande suivante. Si vous utilisez cette commande pour désinstaller, vous n'avez pas besoin d'utiliser les `/norestart` options `/repair` et lorsque vous réinstallez l'agent.
>
> ```
> .\AWSDiscoveryAgentInstaller.exe /quiet /uninstall
> ```

Démarrage et arrêt de la collecte de données avec le Discovery Agent

Une fois le Discovery Agent déployé et configuré, si la collecte de données s'arrête, vous pouvez le redémarrer. Vous pouvez démarrer ou arrêter la collecte de données via la console en suivant les étapes décrites dans Démarrage et arrêt des collecteurs de données dans la AWS Migration Hub console ou en effectuant des appels d'API via le AWS CLI. Avant de commencer, veillez à générer les clés d'accès nécessaires à la gestion du Discovery Agent.

Pour installer AWS CLI et démarrer ou arrêter la collecte de données

1. Si ce n'est pas déjà fait, installez le système AWS CLI correspondant à votre type de système d'exploitation (Windows ou Mac/Linux). Consultez le guide de AWS Command Line Interface l'utilisateur pour obtenir des instructions.
2. Ouvrez l'invite de commande (Windows) ou Terminal (MAC/Linux).
   a. Tapez `aws configure` et appuyez sur Entrer.
   b. Entrez votre code AWS d'accès et votre clé d'accès AWS secrète.
   c. Entrez votre région d'origine pour le nom de région par défaut, par exemple*us-west-2*. (Dans cet exemple, nous supposons qu'`us-west-2`il s'agit de votre région d'origine.)
   d. Saisissez `text` pour Default output format (Format de sortie par défaut).
3. Pour trouver l'ID de l'agent pour lequel vous souhaitez arrêter ou démarrer la collecte de données, tapez la commande suivante :

```
aws discovery describe-agents
```

4. Pour démarrer la collecte de données par l'agent, tapez la commande suivante :

```
aws discovery start-data-collection-by-agent-ids --agent-ids <agent ID>
```

   Pour arrêter la collecte de données par l'agent, tapez la commande suivante :

```
aws discovery stop-data-collection-by-agent-ids --agent-ids <agent ID>
```

Résolution des problèmes avec Discovery Agent

Cette page traite de la résolution des problèmes liés au Discovery Agent sous Linux et Microsoft Windows.

Résolution des problèmes liés à Discovery Agent sous Linux

Si vous rencontrez des problèmes lors de l'installation ou de l'utilisation du Discovery Agent sous Linux, consultez les instructions suivantes concernant la journalisation et la configuration. Lorsqu'il aide à résoudre des problèmes potentiels liés à l'agent ou à sa connexion à Application Discovery Service, le AWS Support demande souvent ces fichiers.

- Les fichiers journaux

  Les fichiers journaux de Discovery Agent se trouvent dans le répertoire suivant.

  ```
  /var/log/aws/discovery/
  ```

  Les fichiers journaux sont nommés de manière à indiquer s'ils sont générés par le démon principal, le programme de mise à niveau automatique ou le programme d'installation.

- Fichiers de configuration

  Les fichiers de configuration de Discovery Agent version 2.0.1617.0 ou ultérieure se trouvent dans le répertoire suivant.

  ```
  /etc/opt/aws/discovery/
  ```

  Les fichiers de configuration des versions de Discovery Agent antérieures à la version 2.0.1617.0 se trouvent dans le répertoire suivant.

  ```
  /var/opt/aws/discovery/
  ```

- Pour obtenir des instructions sur la façon de supprimer les anciennes versions du Discovery Agent, consultezConditions requises pour Discovery Agent.

Résolution des problèmes liés à Discovery Agent sous Microsoft Windows

Si vous rencontrez des problèmes lors de l'installation ou de l'utilisation de l'agent de découverte d' AWS applications sous Microsoft Windows, consultez les instructions suivantes concernant la journalisation et la configuration. AWS Support demande souvent ces fichiers pour aider à résoudre des problèmes potentiels liés à l'agent ou à sa connexion à Application Discovery Service.

- Journalisation de l'installation

  Dans certains cas, la commande d'installation de l'agent semble échouer. Par exemple, un échec peut s'afficher dans le Gestionnaire des services Windows, indiquant que les services de détection n'ont pas été créés. Dans ce cas, ajoutez /log install.log à la commande pour générer un journal d'installation explicite.
- Journalisation opérationnelle

  Sous Windows Server 2008 et versions ultérieures, les fichiers journaux de l'agent sont disponibles dans le répertoire suivant.

  ```
  C:\ProgramData\AWS\AWS Discovery\Logs
  ```

  Sous Windows Server 2003, les fichiers journaux de l'agent sont disponibles dans le répertoire suivant.

  ```
  C:\Documents and Settings\All Users\Application Data\AWS\AWS Discovery\Logs
  ```

  Les fichiers journaux sont nommés de manière à indiquer s'ils ont été générés par le service principal, les mises à niveau automatiques ou le programme d'installation.

- Fichier de configuration

  Sous Windows Server 2008 et versions ultérieures, le fichier de configuration de l'agent est disponible à l'emplacement suivant.

  ```
  C:\ProgramData\AWS\AWS Discovery\config
  ```

  Sous Windows Server 2003, le fichier de configuration de l'agent est disponible à l'emplacement suivant.

```
C:\Documents and Settings\All Users\Application Data\AWS\AWS Discovery\config
```

- Pour obtenir des instructions sur la façon de supprimer des versions antérieures du Discovery Agent, consultezConditions requises pour Discovery Agent.

Collecteur sans agent du Service de découverte d'applications

Application Discovery Service Agentless Collector (Agentless Collector) est une application locale qui collecte des informations par le biais de méthodes sans agent concernant votre environnement local, notamment les informations de profil du serveur (par exemple, le système d'exploitation, le nombre de RAM) CPUs, les métadonnées de base de données, les mesures d'utilisation et les données sur le trafic réseau entre les serveurs locaux. Vous installez le collecteur sans agent en tant que machine virtuelle (VM) dans votre environnement VMware vCenter Server à l'aide d'un fichier Open Virtualization Archive (OVA).

Agentless Collector possède une architecture modulaire qui permet l'utilisation de plusieurs méthodes de collecte sans agent. Agentless Collector fournit des modules pour la collecte de données depuis VMware VMs et depuis des serveurs de base de données et d'analyse. Il fournit également un module permettant de collecter des données sur le trafic réseau entre vos serveurs locaux.

Agentless Collector prend en charge la collecte de données pour AWS Application Discovery Service (Application Discovery Service) en collectant des données d'utilisation et de configuration concernant vos serveurs et bases de données sur site, ainsi que des données sur le trafic réseau entre vos serveurs locaux.

Application Discovery Service est intégré à AWS Migration Hub un service qui simplifie le suivi de votre migration car il regroupe les informations relatives à l'état de la migration dans une console unique. Vous pouvez consulter les serveurs découverts, obtenir les recommandations d'Amazon EC2, visualiser les connexions réseau, regrouper les serveurs dans des applications, puis suivre l'état de migration de chaque application depuis la console Migration Hub de votre région d'origine.

La base de données Agentless Collector et le module de collecte de données analytiques sont intégrés à AWS Database Migration Service (AWS DMS). Cette intégration permet de planifier votre migration vers le AWS Cloud. Vous pouvez utiliser le module de collecte de données de base de données et d'analyse pour découvrir les serveurs de base de données et d'analyse de votre environnement et créer un inventaire des serveurs vers lesquels vous souhaitez migrer AWS Cloud. Ce module de collecte de données collecte les métadonnées de base de données et les mesures d'utilisation réelles du processeur, de la mémoire et de la capacité du disque. Après avoir collecté ces mesures, vous pouvez utiliser la AWS DMS console pour générer des recommandations cibles pour vos bases de données sources.

Conditions requises pour Agentless Collector

Les conditions requises pour utiliser Application Discovery Service Agentless Collector (Agentless Collector) sont les suivantes :

- Un ou plusieurs AWS comptes.
- Un AWS compte dont la région d' AWS Migration Hub origine est définie, voirConnectez-vous à la console Migration Hub et choisissez une région d'origine. Les données de votre Hub de migration sont stockées dans votre région d'origine à des fins de découverte, de planification et de suivi de la migration.
- Un utilisateur IAM du AWS compte configuré pour utiliser la politique AWS `AWSApplicationDiscoveryAgentlessCollectorAccess` gérée. Pour utiliser le module de collecte de données de base de données et d'analyse, cet utilisateur IAM doit également utiliser deux politiques `DMSCollectorPolicy` IAM gérées par le client et. `FleetAdvisorS3Policy` Pour de plus amples informations, veuillez consulter Déploiement d'Application Discovery Service Agentless Collector. L'utilisateur IAM doit être créé dans un AWS compte dont la région d'origine de Migration Hub est définie.
- VMware vCenter Server V5.5, V6, V6.5, 6.7 ou 7.0.

  > **Note**
  >
  > Le collecteur sans agent prend en charge toutes ces versions de VMware, mais nous effectuons actuellement des tests par rapport aux versions 6.7 et 7.0.

- Pour la configuration de VMware vCenter Server, assurez-vous de pouvoir fournir des informations d'identification vCenter avec les autorisations de lecture et d'affichage définies pour le groupe System.
- Agentless Collector nécessite un accès sortant via le port TCP 443 à plusieurs domaines. AWS Pour obtenir la liste de ces domaines, consultezConfiguration du pare-feu pour l'accès sortant aux domaines AWS.
- Pour utiliser le module de collecte de données de base de données et d'analyse, créez un compartiment Amazon S3 dans le compartiment Région AWS que vous avez défini comme région d'origine de votre Migration Hub. Les modules de collecte de données de base de données et d'analyse stockent les métadonnées d'inventaire dans ce compartiment Amazon S3. Pour plus d'informations, consultez Création d'un compartiment dans le Guide de l'utilisateur Amazon S3.
- La version 2 d'Agentless Collector nécessite la version ESXi 6.5 ou une version ultérieure.

Configuration du périmètre de données pour l'accès aux ressources appartenant aux services AWS

La fonction de mise à jour automatique d'Agentless Collector récupère les mises à jour sous forme d'images Docker à partir d'un référentiel ECR public appartenant au AWS service. Si vous utilisez des périmètres de données pour contrôler l'accès à Amazon ECR dans votre environnement, vous devrez peut-être autoriser explicitement l'accès aux éléments suivants pour utiliser la fonctionnalité de mise à jour automatique :

- Ressource ARNs nécessitant un accès : `arn:aws:ecr-public::446372222237:repository/6e5498e4-8c31-4f57-9991-13b4b992ff7b`
- Autorisations requises : `ecr-public:DescribeImages`

Configuration du pare-feu pour l'accès sortant aux domaines AWS

Si les connexions sortantes de votre réseau sont restreintes, vous devez mettre à jour les paramètres de votre pare-feu pour autoriser l'accès sortant aux AWS domaines requis par Agentless Collector. Les AWS domaines nécessitant un accès sortant varient selon que la région d'origine de votre Hub de migration est la région USA Ouest (Oregon), us-west-2 ou une autre région.

Les domaines suivants nécessitent un accès sortant si la région d'origine de votre AWS compte est us-west-2 :

- `arsenal-discovery.us-west-2.amazonaws.com`— Le collecteur utilise ce domaine pour vérifier qu'il est configuré avec les informations d'identification utilisateur IAM requises. Le collecteur l'utilise également pour envoyer et stocker les données collectées puisque la région d'origine est us-west-2.
- `migrationhub-config.us-west-2.amazonaws.com`— Le collecteur utilise ce domaine pour déterminer à quelle région d'origine le collecteur envoie les données en fonction des informations d'identification de l'utilisateur IAM fournies.
- `api.ecr-public.us-east-1.amazonaws.com`— Le collecteur utilise ce domaine pour découvrir les mises à jour disponibles.
- `public.ecr.aws`— Le collecteur utilise ce domaine pour télécharger les mises à jour.
- `dms.`*`your-migrationhub-home-region`*`.amazonaws.com`— Le collecteur utilise ce domaine pour se connecter au collecteur de AWS DMS données.

- `s3.amazonaws.com`— Le collecteur utilise ce domaine pour télécharger les données collectées par le module de collecte de données de base de données et d'analyse dans votre compartiment Amazon S3.
- `sts.amazonaws.com`— Le collecteur utilise ce domaine pour comprendre avec quel compte le collecteur a été configuré.

Les domaines suivants nécessitent un accès sortant si la région d'origine de votre AWS compte ne l'est pas **`us-west-2`** :

- `arsenal-discovery.us-west-2.amazonaws.com`— Le collecteur utilise ce domaine pour vérifier qu'il est configuré avec les informations d'identification utilisateur IAM requises.
- `arsenal-discovery.`*`your-migrationhub-home-region`*`.amazonaws.com`— Le collecteur utilise ce domaine pour envoyer et stocker les données collectées.
- `migrationhub-config.us-west-2.amazonaws.com`— Le collecteur utilise ce domaine pour déterminer à quelle région d'origine le collecteur doit envoyer les données en fonction des informations d'identification de l'utilisateur IAM fournies.
- `api.ecr-public.us-east-1.amazonaws.com`— Le collecteur utilise ce domaine pour découvrir les mises à jour disponibles.
- `public.ecr.aws`— Le collecteur utilise ce domaine pour télécharger les mises à jour.
- `dms.`*`your-migrationhub-home-region`*`.amazonaws.com`— Le collecteur utilise ce domaine pour se connecter au collecteur de AWS DMS données.
- `s3.amazonaws.com`— Le collecteur utilise ce domaine pour télécharger les données collectées par le module de collecte de données de base de données et d'analyse dans votre compartiment Amazon S3.
- `sts.amazonaws.com`— Le collecteur utilise ce domaine pour comprendre avec quel compte le collecteur a été configuré.

Lors de la configuration d'Agentless Collector, vous pouvez recevoir des messages d'erreur tels que l'échec de l'installation : vérifiez vos informations d'identification et réessayez ou vous êtes AWS introuvable. Vérifiez les paramètres réseau. Ces erreurs peuvent être causées par une tentative infructueuse du collecteur sans agent d'établir une connexion HTTPS avec l'un des AWS domaines auxquels il a besoin d'un accès sortant.

S'il n'est AWS pas possible d'établir une connexion, Agentless Collector ne peut pas collecter de données à partir de votre environnement sur site. Pour plus d'informations sur la façon de réparer la connexion à AWS, consultezFixation du collecteur sans agent impossible à atteindre AWS lors de l'installation.

Déploiement d'Application Discovery Service Agentless Collector

Pour déployer Application Discovery Service Agentless Collector, vous devez d'abord créer un utilisateur IAM et télécharger le collecteur. Cette page explique les étapes à suivre pour déployer un collecteur.

Création d'un utilisateur IAM pour Agentless Collector

Pour utiliser Agentless Collector, dans le AWS compte que vous avez utiliséConnectez-vous à la console Migration Hub et choisissez une région d'origine, vous devez créer un utilisateur Gestion des identités et des accès AWS (IAM). Configurez ensuite cet utilisateur IAM pour qu'il utilise la politique AWS AWSApplicationDiscoveryAgentlessCollectorAccessgérée suivante. Vous attachez cette politique IAM lorsque vous créez l'utilisateur IAM.

Pour utiliser le module de collecte de données de base de données et d'analyse, créez deux politiques IAM gérées par le client. Ces politiques permettent d'accéder à votre compartiment Amazon S3 et à l' AWS DMS API. Pour plus d'informations, voir Création d'une politique gérée par le client dans le guide de l'utilisateur IAM.

- Utilisez le code JSON suivant pour créer la **`DMSCollectorPolicy`** politique.

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "dms:DescribeFleetAdvisorCollectors",
            "dms:ModifyFleetAdvisorCollectorStatuses",
            "dms:UploadFileMetadataList"
        ],
        "Resource": "*"
    }]
}
```

- Utilisez le code JSON suivant pour créer la **`FleetAdvisorS3Policy`** politique.

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject*",
                "s3:GetBucket*",
                "s3:List*",
                "s3:DeleteObject*",
                "s3:PutObject*"
            ],
            "Resource": [
                "arn:aws:s3:::bucket_name",
                "arn:aws:s3:::bucket_name/*"
            ]
        }
    ]
}
```

  Dans l'exemple précédent, remplacez *`bucket_name`* par le nom du compartiment Amazon S3 que vous avez créé à l'étape des prérequis.

Nous vous recommandons de créer un utilisateur IAM non administratif à utiliser avec Agentless Collector. Lorsque vous créez des utilisateurs IAM non administrateurs, suivez les bonnes pratiques de sécurité Accorder le moindre privilège, en accordant aux utilisateurs des autorisations minimales.

Pour créer un utilisateur IAM non administrateur à utiliser avec Agentless Collector

1. Dans AWS Management Console, accédez à la console IAM à l'aide du AWS compte que vous avez utilisé pour définir la région d'origine. Connectez-vous à la console Migration Hub et choisissez une région d'origine
2. Créez un utilisateur IAM non administrateur en suivant les instructions de création d'un utilisateur avec la console, comme décrit dans la section Création d'un utilisateur IAM dans votre AWS compte du guide de l'utilisateur IAM.

   En suivant les instructions du guide de l'utilisateur IAM :

- À l'étape de sélection du type d'accès, sélectionnez Accès programmatique. Remarque : bien que cela ne soit pas recommandé, sélectionnez l'accès à la console de AWS gestion uniquement si vous prévoyez d'utiliser les mêmes informations d'identification utilisateur IAM pour accéder à la AWS console.
- À l'étape concernant la page Définir les autorisations, choisissez l'option Associer directement les politiques existantes à l'utilisateur. Sélectionnez ensuite la stratégie `AWSApplicationDiscoveryAgentlessCollectorAccess` AWS gérée dans la liste des politiques.

  Ensuite, sélectionnez les politiques IAM gérées par le `FleetAdvisorS3Policy` client `DMSCollectorPolicy` et celles gérées par le client.
- Lorsque vous consultez les clés d'accès de l'utilisateur (clé d'accès IDs et clés d'accès secrètes), suivez les instructions de la note importante concernant l'enregistrement du nouvel identifiant de clé d'accès et de la nouvelle clé d'accès secrète de l'utilisateur dans un endroit sûr et sécurisé. Vous aurez besoin de ces clés d'accèsConfiguration du collecteur sans agent.

  La rotation des clés d'accès constitue une bonne pratique en matière de AWS sécurité. Pour plus d'informations sur la rotation des clés, voir Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification à long terme dans le guide de l'utilisateur IAM.

Téléchargez le collecteur sans agent

Pour configurer l'Application Discovery Service Agentless Collector (Agentless Collector), vous devez télécharger et déployer le fichier Agentless Collector Open Virtualization Archive (OVA). Le collecteur sans agent est un dispositif virtuel que vous installez dans votre environnement local VMware . Cette étape décrit comment télécharger le fichier OVA du collecteur et l'étape suivante décrit comment le déployer.

Pour télécharger le fichier OVA du collecteur et vérifier sa somme de contrôle

1. Connectez-vous à vCenter en tant qu' VMware administrateur et accédez au répertoire dans lequel vous souhaitez télécharger le fichier OVA Agentless Collector.
2. Téléchargez le fichier OVA à l'adresse suivante :

   Collecteur OVA sans agent

3. Selon l'algorithme de hachage que vous utilisez dans votre environnement système, téléchargez le MD5ou SHA256pour obtenir le fichier contenant la valeur de la somme de contrôle. Utilisez la valeur téléchargée pour vérifier le `ApplicationDiscoveryServiceAgentlessCollector` fichier téléchargé à l'étape précédente.
4. Selon votre variante de Linux, exécutez la MD5 commande ou SHA256 la commande appropriée à la version pour vérifier que la signature cryptographique du `ApplicationDiscoveryServiceAgentlessCollector.ova` fichier correspond à la valeur du SHA256 fichier MD5/correspondant que vous avez téléchargé.

```
$ md5sum ApplicationDiscoveryServiceAgentlessCollector.ova
```

```
$ sha256sum ApplicationDiscoveryServiceAgentlessCollector.ova
```

Déployer un collecteur sans agent

Application Discovery Service Agentless Collector (Agentless Collector) est un dispositif virtuel que vous installez dans votre environnement local VMware . Cette section décrit comment déployer le fichier Open Virtualization Archive (OVA) que vous avez téléchargé dans votre VMware environnement.

Spécifications de la machine virtuelle Agentless Collector

Agentless Collector version 2

- Système d'exploitation — Amazon Linux 2023
- RAM — 16 Go
- Processeur : 4 cœurs
- VMware exigences — Voir les exigences de VMware l'hôte pour l'exécution AL2023 sur VMware

Agentless Collector version 1

- Système d'exploitation — Amazon Linux 2
- RAM — 16 Go
- Processeur : 4 cœurs

La procédure suivante vous explique comment déployer le fichier OVA Agentless Collector dans votre VMware environnement.

Pour déployer Agentless Collector

1. Connectez-vous à vCenter en tant qu'administrateur. VMware
2. Utilisez l'une des méthodes suivantes pour installer le fichier OVA :
   - Utilisez l'interface utilisateur : choisissez Fichier, choisissez Déployer le modèle OVF, sélectionnez le fichier OVA du collecteur que vous avez téléchargé dans la section précédente, puis exécutez l'assistant. Assurez-vous que les paramètres du proxy dans le tableau de bord de gestion du serveur sont correctement configurés.
   - Utilisez la ligne de commande : pour installer le fichier OVA du collecteur à partir de la ligne de commande, téléchargez et utilisez l'outil VMware Open Virtualization Format (ovftool). Pour télécharger ovftool, sélectionnez une version sur la page de documentation de l'outil OVF.

     Voici un exemple d'utilisation de l'outil de ligne de commande ovftool pour installer le fichier OVA du collecteur.

     ```
     ovftool --acceptAllEulas --name=AgentlessCollector --datastore=datastore1
      -dm=thin ApplicationDiscoveryServiceAgentlessCollector.ova
      'vi://username:password@vcenterurl/Datacenter/host/esxi/'
     ```

     Les ***replaceable*** valeurs indiquées dans l'exemple sont décrites ci-dessous :

     - Le nom est le nom que vous souhaitez utiliser pour votre machine virtuelle Agentless Collector.
     - La banque de données est le nom de la banque de données de votre vCenter.
     - Le nom du fichier OVA est le nom du fichier OVA collecteur téléchargé.
     - username/password Il s'agit de vos informations d'identification vCenter.
     - Le vcenterurl est l'URL de votre vCenter.
     - Le chemin vi est le chemin d'accès à votre VMware ESXi hôte.
3. Localisez le collecteur sans agent déployé dans votre vCenter. Cliquez avec le bouton droit sur la machine virtuelle, puis choisissez Power, Power On.
4. Après quelques minutes, l'adresse IP du collecteur s'affiche dans vCenter. Vous utilisez cette adresse IP pour vous connecter au collecteur.

Accès à la console Agentless Collector

La procédure suivante décrit comment accéder à la console Application Discovery Service Agentless Collector (Agentless Collector).

Pour accéder à la console Agentless Collector

1. Ouvrez un navigateur Web, puis tapez l'URL suivante dans la barre d'adresse : **`https://`***`<ip_address>`***`/`**, d'où *`<ip_address>`* provient l'adresse IP du collecteur Déployer un collecteur sans agent ?
2. Choisissez Get Started la première fois que vous accédez à Agentless Collector. Par la suite, il vous sera demandé de vous connecter.

Si vous accédez à la console Agentless Collector pour la première fois, c'est la prochaine étape. Configuration du collecteur sans agent Sinon, vous verrez ensuiteLe tableau de bord Agentless Collector.

Configuration du collecteur sans agent

Application Discovery Service Agentless Collector (Agentless Collector) est une machine virtuelle (VM) basée sur Amazon Linux 2. La section suivante décrit comment configurer une machine virtuelle de collecteur sur la page Configurer le collecteur sans agent de la console Agentless Collector.

Pour configurer une machine virtuelle de collecteur sur la page Configurer un collecteur sans agent

1. Dans Nom du collecteur, entrez un nom pour le collecteur afin de l'identifier. Le nom peut contenir des espaces, mais il ne peut pas contenir de caractères spéciaux.
2. Sous Synchronisation des données, entrez la clé d' AWS accès et la AWS clé secrète que l'utilisateur IAM doit spécifier comme compte de destination pour recevoir les données découvertes par le collecteur. Pour plus d'informations sur les exigences relatives à l'utilisateur IAM, consultezDéploiement d'Application Discovery Service Agentless Collector.
    a. Pour la AWS clé d'accès, entrez la clé d'accès du AWS compte utilisateur IAM que vous spécifiez comme compte de destination.
    b. Pour AWS clé secrète, entrez la clé secrète du AWS compte utilisateur IAM que vous spécifiez comme compte de destination.

c. (Facultatif) Si votre réseau nécessite l'utilisation d'un proxy pour y accéder AWS, entrez l'hôte du proxy, le port du proxy et, éventuellement, les informations d'identification nécessaires pour vous authentifier auprès de votre serveur proxy existant.

3. Sous Mot de passe Agentless Collector, configurez un mot de passe à utiliser pour authentifier l'accès à Agentless Collector.

   - Les mots de passe distinguent les majuscules
   - Les mots de passe doivent comporter entre 8 et 64 caractères
   - Les mots de passe doivent contenir au moins un caractère appartenant à chacune des quatre catégories suivantes :
     - Lettres minuscules (a-z)
     - Lettres majuscules (A-Z)
     - Chiffres (0-9)
     - Caractères non alphanumériques (@$! #%* ? &)
   - Les mots de passe ne peuvent pas contenir de caractères spéciaux autres que les suivants : @$! #%* ? &

   a. Pour le mot de passe du collecteur sans agent, entrez un mot de passe à utiliser pour authentifier l'accès au collecteur.

   b. Pour saisir à nouveau le mot de passe Agentless Collector, pour vérification, saisissez-le à nouveau.

4. Sous Autres paramètres, lisez le contrat de licence. Si vous acceptez de l'accepter, cochez la case.

5. Pour activer les mises à jour automatiques pour Agentless Collector, sous Autres paramètres, sélectionnez Mettre à jour automatiquement Agentless Collector. Si vous ne cochez pas cette case, vous devrez mettre à jour manuellement Agentless Collector comme décrit dans. Mise à jour manuelle d'Application Discovery Service Agentless Collector

6. Choisissez Enregistrer les configurations.

Les rubriques suivantes décrivent les tâches de configuration facultatives du collecteur.

Tâches de configuration facultatives

- (Facultatif) Configurer une adresse IP statique pour la machine virtuelle Agentless Collector

- (Facultatif) Réinitialisez la machine virtuelle du collecteur sans agent pour qu'elle utilise à nouveau le protocole DHCP
- (Facultatif) Configurer le protocole d'authentification Kerberos

(Facultatif) Configurer une adresse IP statique pour la machine virtuelle Agentless Collector

Les étapes suivantes décrivent comment configurer une adresse IP statique pour la machine virtuelle Application Discovery Service Agentless Collector (Agentless Collector). Lors de la première installation, la machine virtuelle du collecteur est configurée pour utiliser le protocole DHCP (Dynamic Host Configuration Protocol).

> **Note**
>
> L'Agentless Collector prend en charge IPv4. Il ne prend pas en charge IPv6.

Agentless Collector version 2

Pour configurer une adresse IP statique pour la machine virtuelle du collecteur

1. Collectez les informations réseau suivantes à partir de VMware vCenter :
   - Adresse IP statique : adresse IP non signée dans le sous-réseau. Par exemple, 192.168.1.138.
   - Masque de réseau CIDR : pour obtenir le masque de réseau CIDR, vérifiez le paramètre d'adresse IP de l'hôte VMware vCenter qui héberge la machine virtuelle du collecteur. Par exemple, /24.
   - Passerelle par défaut : pour obtenir la passerelle par défaut, vérifiez le paramètre d'adresse IP de l'hôte VMware vCenter qui héberge la machine virtuelle du collecteur. Par exemple, 192.168.1.1.
   - DNS principal : pour obtenir le DNS principal, vérifiez le paramètre d'adresse IP de l'hôte VMware vCenter qui héberge la machine virtuelle du collecteur. Par exemple, 192.168.1.1.
   - DNS secondaire (facultatif)
   - (Facultatif) Nom de domaine local : cela permet au collecteur d'accéder à l'URL de l'hôte vCenter sans le nom de domaine.

2. Ouvrez la console de machine virtuelle du collecteur et connectez-vous en **`ec2-user`** utilisant le mot de passe**`collector`**, comme indiqué dans l'exemple suivant.

```
username: ec2-user
password: collector
```

3. Désactivez l'interface réseau en saisissant la commande suivante dans le terminal distant.

```
sudo ip link set ens192 down
```

4. Mettez à jour la configuration de l'interface en procédant comme suit.

   a. Ouvrez 10- cloud-init-ens 192.network dans l'éditeur vi à l'aide de la commande suivante.

```
sudo vi /etc/systemd/network/10-cloud-init-ens192.network
```

   b. Mettez à jour les valeurs, comme indiqué dans l'exemple suivant, avec les informations que vous avez collectées à l'étape Collecter les informations du réseau.

```
[Match]
Name=ens192

[Network]
DHCP=no
Address=static-ip-value/CIDR-netmask
Gateway=gateway-value
DNS=dnsserver-value
```

5. Mettez à jour le système de noms de domaine (DNS) en procédant comme suit.

   a. Ouvrez le `resolv.conf` fichier dans vi à l'aide de la commande suivante.

```
sudo vi /etc/resolv.conf
```

   b. Mettez à jour le `resolv.conf` fichier dans vi à l'aide de la commande suivante.

```
search localdomain-name
options timeout:2 attempts:5
nameserver dnsserver-value
```

   L'exemple suivant montre un `resolv.conf` fichier modifié.

```
search vsphere.local
options timeout:2 attempts:5
nameserver 192.168.1.1
```

6. Activez l'interface réseau en saisissant la commande suivante.

```
sudo ip link set ens192 up
```

7. Redémarrez la machine virtuelle comme indiqué dans l'exemple suivant.

```
sudo reboot
```

8. Vérifiez vos paramètres réseau en procédant comme suit.

   a. Vérifiez si l'adresse IP est correctement configurée en saisissant les commandes suivantes.

   ```
   ifconfig
   ip addr show
   ```

   b. Vérifiez que la passerelle a été correctement ajoutée en saisissant la commande suivante.

   ```
   route -n
   ```

   Le résultat doit être similaire à celui de l'exemple suivant.

   ```
   Kernel IP routing table
   Destination     Gateway         Genmask         Flags Metric Ref    Use
    Iface
   0.0.0.0         192.168.1.1     0.0.0.0         UG    0      0        0 eth0
   172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0
    docker0
   192.168.1.0     0.0.0.0         255.255.255.0   U     0      0
   ```

   c. Vérifiez que vous pouvez envoyer un ping à une URL publique en saisissant la commande suivante.

   ```
   ping www.google.com
   ```

d. Vérifiez que vous pouvez envoyer un ping à l'adresse IP ou au nom d'hôte du vCenter, comme indiqué dans l'exemple suivant.

```
ping vcenter-host-url
```

Agentless Collector version 1

Pour configurer une adresse IP statique pour la machine virtuelle du collecteur

1. Collectez les informations réseau suivantes à partir de VMware vCenter :
   - Adresse IP statique : adresse IP non signée dans le sous-réseau. Par exemple, 192.168.1.138.
   - Masque réseau : pour obtenir le masque réseau, vérifiez le paramètre d'adresse IP de l'hôte VMware vCenter qui héberge la machine virtuelle du collecteur. Par exemple, 255.255.255.0.
   - Passerelle par défaut : pour obtenir la passerelle par défaut, vérifiez le paramètre d'adresse IP de l'hôte VMware vCenter qui héberge la machine virtuelle du collecteur. Par exemple, 192.168.1.1.
   - DNS principal : pour obtenir le DNS principal, vérifiez le paramètre d'adresse IP de l'hôte VMware vCenter qui héberge la machine virtuelle du collecteur. Par exemple, 192.168.1.1.
   - DNS secondaire (facultatif)
   - (Facultatif) Nom de domaine local : cela permet au collecteur d'accéder à l'URL de l'hôte vCenter sans le nom de domaine.
2. Ouvrez la console de machine virtuelle du collecteur et connectez-vous en **`ec2-user`** utilisant le mot de passe**`collector`**, comme indiqué dans l'exemple suivant.

```
username: ec2-user
password: collector
```

3. Désactivez l'interface réseau en saisissant la commande suivante dans le terminal distant.

```
sudo /sbin/ifdown eth0
```

4. Mettez à jour la configuration de l'interface eth0 en procédant comme suit.

a. Ouvrez ifcfg-eth0 dans l'éditeur vi à l'aide de la commande suivante.

```
sudo vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

b. Mettez à jour les valeurs de l'interface, comme indiqué dans l'exemple suivant, avec les informations que vous collectez à l'étape Collecter les informations du réseau.

```
DEVICE=eth0
BOOTPROTO=static
ONBOOT=yes
IPADDR=static-ip-value
NETMASK=netmask-value
GATEWAY=gateway-value
TYPE=Ethernet
USERCTL=yes
PEERDNS=no
RES_OPTIONS="timeout:2 attempts:5"
```

5. Mettez à jour le système de noms de domaine (DNS) en procédant comme suit.

a. Ouvrez le `resolv.conf` fichier dans vi à l'aide de la commande suivante.

```
sudo vi /etc/resolv.conf
```

b. Mettez à jour le `resolv.conf` fichier dans vi à l'aide de la commande suivante.

```
search localdomain-name
options timeout:2 attempts:5
nameserver dnsserver-value
```

L'exemple suivant montre un `resolv.conf` fichier modifié.

```
search vsphere.local
options timeout:2 attempts:5
nameserver 192.168.1.1
```

6. Activez l'interface réseau en saisissant la commande suivante.

```
sudo /sbin/ifup eth0
```

7. Redémarrez la machine virtuelle comme indiqué dans l'exemple suivant.

```
sudo reboot
```

8. Vérifiez vos paramètres réseau en procédant comme suit.

   a. Vérifiez si l'adresse IP est correctement configurée en saisissant les commandes suivantes.

   ```
   ifconfig
   ip addr show
   ```

   b. Vérifiez que la passerelle a été correctement ajoutée en saisissant la commande suivante.

   ```
   route -n
   ```

   Le résultat doit être similaire à celui de l'exemple suivant.

   ```
   Kernel IP routing table
   Destination     Gateway         Genmask         Flags Metric Ref    Use
    Iface
   0.0.0.0         192.168.1.1     0.0.0.0         UG    0      0        0 eth0
   172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0
    docker0
   192.168.1.0     0.0.0.0         255.255.255.0   U     0      0
   ```

   c. Vérifiez que vous pouvez envoyer un ping à une URL publique en saisissant la commande suivante.

   ```
   ping www.google.com
   ```

   d. Vérifiez que vous pouvez envoyer un ping à l'adresse IP ou au nom d'hôte du vCenter, comme indiqué dans l'exemple suivant.

   ```
   ping vcenter-host-url
   ```

(Facultatif) Réinitialisez la machine virtuelle du collecteur sans agent pour qu'elle utilise à nouveau le protocole DHCP

Les étapes suivantes décrivent comment reconfigurer la machine virtuelle Agentless Collector pour utiliser le protocole DHCP.

Agentless Collector version 2

Pour configurer la machine virtuelle du collecteur afin qu'elle utilise le protocole DHCP

1. Désactivez l'interface réseau en exécutant la commande suivante sur le terminal distant.

```
sudo ip link set ens192 down
```

2. Mettez à jour la configuration de l'interface en procédant comme suit.

   a. Ouvrez le `10-cloud-init-ens192.network` fichier dans l'éditeur vi à l'aide de la commande suivante.

```
sudo vi /etc/systemd/network/10-cloud-init-ens192.network
```

   b. Mettez à jour les valeurs comme indiqué dans l'exemple suivant.

```
[Match]
Name=ens192

[Network]
DHCP=yes

[DHCP]
ClientIdentifier=mac
```

3. Réinitialisez le paramètre DNS en saisissant la commande suivante.

```
echo "" | sudo tee /etc/resolv.conf
```

4. Activez l'interface réseau en saisissant la commande suivante.

```
sudo ip link set ens192 up
```

5. Redémarrez la machine virtuelle du collecteur comme indiqué dans l'exemple suivant.

```
sudo reboot
```

Agentless Collector version 1

Pour configurer la machine virtuelle du collecteur afin qu'elle utilise le protocole DHCP

1. Désactivez l'interface réseau en exécutant la commande suivante sur le terminal distant.

```
sudo /sbin/ifdown eth0
```

2. Mettez à jour la configuration réseau en procédant comme suit.

   a. Ouvrez le `ifcfg-eth0` fichier dans l'éditeur vi à l'aide de la commande suivante.

   ```
   sudo /sbin/ifdown eth0
   ```

   b. Mettez à jour les valeurs du `ifcfg-eth0` fichier comme indiqué dans l'exemple suivant.

   ```
   DEVICE=eth0
   BOOTPROTO=dhcp
   ONBOOT=yes
   TYPE=Ethernet
   USERCTL=yes
   PEERDNS=yes
   DHCPV6C=yes
   DHCPV6C_OPTIONS=-nw
   PERSISTENT_DHCLIENT=yes
   RES_OPTIONS="timeout:2 attempts:5"
   ```

3. Réinitialisez le paramètre DNS en saisissant la commande suivante.

```
echo "" | sudo tee /etc/resolv.conf
```

4. Activez l'interface réseau en saisissant la commande suivante.

```
sudo /sbin/ifup eth0
```

5. Redémarrez la machine virtuelle du collecteur comme indiqué dans l'exemple suivant.

```
sudo reboot
```

(Facultatif) Configurer le protocole d'authentification Kerberos

Si votre serveur de système d'exploitation prend en charge le protocole d'authentification Kerberos, vous pouvez utiliser ce protocole pour vous connecter à votre serveur. Pour ce faire, vous devez configurer la machine virtuelle Application Discovery Service Agentless Collector.

Les étapes suivantes décrivent comment configurer le protocole d'authentification Kerberos sur votre machine virtuelle Application Discovery Service Agentless Collector.

Pour configurer le protocole d'authentification Kerberos sur votre machine virtuelle de collecte

1. Ouvrez la console de machine virtuelle du collecteur et connectez-vous en **`ec2-user`** utilisant le mot de passe**`collector`**, comme indiqué dans l'exemple suivant.

   ```
   username: ec2-user
   password: collector
   ```

2. Ouvrez le fichier `krb5.conf` de configuration dans le `/etc` dossier. Pour ce faire, vous pouvez utiliser l'exemple de code suivant.

   ```
   cd /etc
   sudo nano krb5.conf
   ```

3. Mettez à jour le fichier de `krb5.conf` configuration avec les informations suivantes.

   ```
   [libdefaults]
       forwardable = true
       dns_lookup_realm = true
       dns_lookup_kdc = true
       ticket_lifetime = 24h
       renew_lifetime = 7d
       default_realm = default_Kerberos_realm

   [realms]
    default_Kerberos_realm = {
        kdc = KDC_hostname
        server_name = server_hostname
        default_domain = domain_to_expand_hostnames
   ```

```
 }

[domain_realm]
 .domain_name = default_Kerberos_realm
 domain_name = default_Kerberos_realm
```

Enregistrez le fichier et quittez l'éditeur de texte.

4. Redémarrez la machine virtuelle du collecteur comme indiqué dans l'exemple suivant.

```
sudo reboot
```

Utilisation du module de collecte de données réseau Agentless Collector

Le module de collecte de données réseau vous permet de découvrir les dépendances entre les serveurs de votre centre de données sur site. Ces données réseau accélèrent la planification de votre migration en fournissant une visibilité sur la manière dont les applications communiquent entre les serveurs.

Le module de collecte de données réseau se connecte aux serveurs identifiés par le module VMware vCenter et analyse l'adresse IP source par rapport au IP/port trafic de destination de ces serveurs.

Rubriques

- Configuration du module de collecte de données réseau
- Tentatives de collecte de données réseau
- État du serveur dans le module de collecte de données réseau

Configuration du module de collecte de données réseau

Le module de collecte de données réseau collecte des données réseau pour l'inventaire des serveurs provenant du module VMware vCenter. Par conséquent, pour utiliser le module Network Data Collection, configurez d'abord le module VMware vCenter. Pour obtenir des instructions, suivez les instructions des rubriques suivantes :

1. the section called “Déploiement d'un collecteur”
2. the section called “Accès à la console du collecteur”

3. the section called "Configuration du collecteur"
4. the section called "Utilisation du module VMware de collecte de données"

Pour configurer le module de collecte de données réseau

1. Sur le tableau de bord Agentless Collector, dans la section Collecte de données réseau, choisissez Afficher les connexions réseau.
2. Sur la page Connexions réseau, choisissez Modifier le collecteur.
3. Dans la section des informations d'identification, entrez au moins un ensemble d'informations d'identification. Vous pouvez saisir jusqu'à 10 ensembles d'informations d'identification. La première fois que le module tente de collecter des données pour un serveur, il essaie toutes les informations d'identification jusqu'à ce qu'il trouve un ensemble d'informations d'identification qui fonctionne ; il enregistre ensuite cet ensemble et l'utilise à nouveau lors de tentatives ultérieures. Pour plus d'informations sur la configuration des informations d'identification, consultezthe section called "Définition des informations d'identification".
4. Dans la section Préférences de collecte de données, pour démarrer automatiquement la collecte de données lorsqu'un serveur redémarre, sélectionnez Démarrer la collecte de données automatiquement.
5. Si vous n'avez pas configuré de certificats WinRM, sélectionnez Désactiver les vérifications de certificats WinRM.
6. Choisissez Enregistrer.
7. La collecte a lieu sur les serveurs toutes les 15 secondes. Pour voir le détail des tentatives de collecte pour un serveur donné, cochez la case située à gauche du serveur dans le tableau Serveurs.

Définition des informations d'identification

Le module de collecte de données réseau utilise WinRM pour collecter des données à partir de serveurs Windows. Il utilise SNMPv2 et collecte des données SNMPv3 à partir de serveurs Linux.

Informations d'identification WinRM :

- Spécifiez le nom d'utilisateur et le mot de passe d'un compte Windows présentant les caractéristiques suivantes :
  - Accès en lecture à l'espace de `\root\standardcimv2` noms

  - Permissions de lecture pour le `MSFT_NetTCPConnection` cours
  - Accès WMI à distance
- Nous vous recommandons de créer un compte de service dédié avec les autorisations minimales requises.
- Évitez d'utiliser des comptes d'administrateur de domaine ou d'administrateur local.
- Le port 5986 (HTTPS) doit être ouvert entre le collecteur et les serveurs cibles.
- Évitez de désactiver la vérification des certificats WinRM. Pour plus d'informations sur la configuration des certificats WinRM, consultez. the section called "Résolution des problèmes de certification auto-signée lors de la configuration des certificats WinRM"

SNMPv2 informations d'identification :

- Fournissez une chaîne communautaire en lecture seule qui peut accéder à l'OID 1.3.6.1.2.1.6.13.*
- SNMPv3 est préférable en SNMPv2 raison de l'amélioration de la sécurité dans SNMPv3
- Le port 161/UDP doit être ouvert entre le collecteur et les serveurs cibles
- Utiliser des chaînes communautaires complexes autres que celles par défaut
- Évitez les chaînes communes telles que « public » ou « privé »
- Traitez les chaînes communautaires comme des mots de passe

SNMPv3 credentials

- Fournissez un identifiant username/password et des auth/privacy détails avec une autorisation en lecture seule qui peut accéder à l'OID 1.3.6.1.2.1.6.13.*.
- Le port 161/UDP doit être ouvert entre le collecteur et les serveurs cibles
- Activez à la fois l'authentification et la confidentialité
- Utiliser des protocoles d'authentification forts (SHA préféré MD5)
- Utilisez des protocoles de chiffrement puissants (AES préféré au DES)
- Utilisez des mots de passe complexes pour l'authentification et la confidentialité
- Utilisez des noms d'utilisateur uniques (évitez les noms communs)

Bonnes pratiques générales pour la gestion des accréditations

- Stockez vos identifiants en toute sécurité

- Alternez régulièrement toutes les informations d'identification
- Utilisez des gestionnaires de mots de passe ou des coffres-forts sécurisés
- Surveiller l'utilisation des informations d'identification
- Respectez le principe du moindre privilège et n'accordez que les autorisations minimales nécessaires

Tentatives de collecte de données réseau

Lorsqu'un nouveau serveur est découvert, le collecteur essaie chaque identifiant configuré pour chaque adresse IP. Une fois que le collecteur a trouvé un identifiant valide, il utilise uniquement cet identifiant. Après deux échecs consécutifs, le collecteur tente de collecter des données réseau pour un serveur après 30 minutes, 2 heures, 8 heures, puis 24 heures. Après 6 tentatives infructueuses, le collecteur continue de tester toutes les informations d'identification configurées une fois par jour. Pour résoudre le problème, modifiez les informations d'identification actuelles ou ajoutez-en d'autres en choisissant Modifier le collecteur, ou apportez des modifications au serveur cible surveillé.

État du serveur dans le module de collecte de données réseau

Le tableau suivant explique les valeurs du statut de la collection.

Statut	Signification
Collecte ou collecte	La dernière tentative de collecte des connexion s réseau a réussi.
Erreur ou erreur	La dernière tentative de collecte pour les connexions réseau a échoué en raison d'un problème de réseau ou d'autorisations. Pour plus d'informations, cochez la case située à gauche du serveur présentant l'erreur.
Ignoré	Serveurs pour lesquels aucune information d'identification valide n'a été fournie. Mettez à jour ou configurez les informations d'identif ication supplémentaires du serveur.

Statut	Signification
Aucune donnée	La collecte de données pour le serveur n'a pas démarré. Pour commencer à collecter des données, choisissez Start collector.
En attente	La collecte a été lancée mais aucune tentative de collecte n'a été effectuée. Patientez quelques minutes, puis actualisez la liste.

Utilisation du module de collecte de VMware données vCenter Agentless Collector

Cette section décrit le module de collecte de données VMware vCenter Application Discovery Service Agentless Collector (Agentless Collector), qui est utilisé pour collecter les données d'inventaire, de profil et d'utilisation des serveurs auprès de votre. VMware VMs

Rubriques

Configuration du module de collecte de données Agentless Collector pour vCenter VMware

Cette section décrit comment configurer le module de collecte de données Agentless Collector VMware vCenter pour collecter les données d'inventaire, de profil et d'utilisation des serveurs auprès de votre. VMware VMs

> **Note**
>
> Avant de démarrer la configuration de vCenter, assurez-vous de pouvoir fournir des informations d'identification vCenter avec les autorisations de lecture et de visualisation définies pour le groupe System.

Pour configurer le module de VMware collecte de données vCenter

1. Sur la page du tableau de bord d'Agentless Collector, sous Collecte de données, choisissez Configurer dans la section VMware vCenter.
2. Sur la page Configurer la collecte de données VMware vCenter, effectuez les opérations suivantes :

    a. Sous les informations d'identification vCenter :

        i. Pour l'URL/IP de vCenter, entrez l'adresse IP de votre hôte VMware vCenter Server.

        ii. Pour le nom d'utilisateur de vCenter, entrez le nom d'un utilisateur local ou de domaine que le collecteur utilise pour communiquer avec vCenter. Pour les utilisateurs de domaine, utilisez le format domaine\nom d'utilisateur ou nom d'utilisateur@domaine.

        iii. Pour vCenter Password (Mot de passe vCenter), entrez le mot de passe de l'utilisateur local ou du domaine.

    b. Sous Préférences de collecte de données :

        - Pour démarrer automatiquement la collecte de données immédiatement après une configuration réussie, sélectionnez Démarrer la collecte de données automatiquement.

    c. Choisissez Set up (Configurer).

Vous verrez ensuite la page des détails de la collecte de VMware données, décrite dans la rubrique suivante.

Afficher les détails VMware de la collecte de données

La page des détails de la collecte de VMware données contient des informations sur le vCenter que vous avez configuré. Configuration du module de collecte de données Agentless Collector pour vCenter VMware

Sous Serveurs vCenter découverts, le vCenter que vous avez configuré est répertorié avec les informations suivantes sur le vCenter :

- Adresse IP du serveur vCenter.
- Le nombre de serveurs dans le vCenter.
- État de la collecte de données.
- Combien de temps s'est écoulé depuis la dernière mise à jour.

Choisissez Supprimer le serveur vCenter pour supprimer le serveur vCenter affiché et revenir à la page Configurer la collecte de données vCenter VMware .

Si vous n'avez pas choisi de démarrer la collecte de données automatiquement, vous pouvez démarrer la collecte de données en utilisant le bouton Démarrer la collecte de données sur cette page. Une fois la collecte de données lancée, le bouton de démarrage devient Arrêter la collecte de données.

Si la colonne État de la collecte indique Collecte, la collecte des données a commencé.

Vous pouvez consulter les données collectées dans la AWS Migration Hub console. Si vous collectez des données pour un inventaire de VMware vCenter Server, vous pouvez accéder aux données qui apparaissent dans la console environ 15 minutes après avoir activé la collecte de données.

Vous pouvez choisir Afficher les serveurs dans Migration Hub sur cette page pour ouvrir la console Migration Hub, si votre accès à Internet n'est pas bloqué. Que vous choisissiez ce bouton ou non, pour savoir comment accéder à la console Migration Hub, consultezAfficher les données que vous avez collectées.

Voici les directives relatives à la durée recommandée pour la collecte des données en fonction des activités de planification de la migration :

- TCO (coût total de possession) : 2 à 4 semaines
- Planification de la migration : 2 à 6 semaines

Contrôle de l'étendue de la collecte de données vCenter

L'utilisateur de vCenter a besoin d'autorisations en lecture seule sur chaque hôte ou machine virtuelle ESX pour effectuer un inventaire à l'aide d'Application Discovery Service. À l'aide des paramètres

d'autorisation, vous pouvez contrôler quels hôtes VMs sont inclus dans la collecte de données. Vous pouvez soit autoriser l'inventaire de tous les hôtes situés VMs sous le vCenter actuel, soit accorder des autorisations sur une base déterminée. case-by-case

> **Note**
>
> Pour des raisons de sécurité, nous vous recommandons de ne pas accorder d'autorisations supplémentaires inutiles à l'utilisateur vCenter de l'Application Discovery Service.

Les procédures suivantes décrivent les scénarios de configuration classés du moins granulaire au plus granulaire. Ces procédures concernent vSphere Client v6.7.0.2. Les procédures applicables aux autres versions du client peuvent être différentes en fonction de la version du client vSphere que vous utilisez.

Pour découvrir les données relatives à tous les hôtes ESX et VMs sous le vCenter actuel

1. Dans votre client VMware vSphere, choisissez vCenter, puis choisissez Hosts and Clusters ou and Templates. VMs
2. Choisissez une ressource de centre de données, puis sélectionnez Autorisations.
3. Choisissez l'utilisateur vCenter, puis le symbole pour ajouter, modifier ou supprimer un rôle d'utilisateur.
4. Choisissez Lecture seule dans le menu Rôle.
5. Choisissez Propager aux enfants, puis cliquez sur OK.

Pour détecter les données sur un hôte ESX spécifique et tous ses objets enfants

1. Dans votre client VMware vSphere, choisissez vCenter, puis choisissez Hosts and Clusters ou and Templates. VMs
2. Choisissez Objets associés, Hôtes.
3. Ouvrez le menu contextuel (cliquez avec le bouton droit de la souris) et choisissez Toutes les actions vCenter, Ajouter une autorisation.
4. Sous Ajouter l'autorisation, ajoutez l'utilisateur vCenter à l'hôte. Pour Rôle assigné, choisissez En lecture seule.
5. Sélectionnez Propager aux enfants, puis choisissez OK.

Pour découvrir les données relatives à un hôte ESX spécifique ou à une machine virtuelle enfant

1. Dans votre client VMware vSphere, choisissez vCenter, puis choisissez Hosts and Clusters ou and Templates. VMs
2. Choisissez Objets associés.
3. Choisissez Hosts (affichant la liste des hôtes ESX connus de vCenter) ou Virtual Machines (affichant une liste VMs de tous les hôtes ESX).
4. Ouvrez le menu contextuel pour le nom de l'hôte ou de la machine virtuelle (cliquez avec le bouton droit de la souris) et choisissez Toutes les actions vCenter, Ajouter une autorisation.
5. Sous Ajouter une autorisation, ajoutez l'utilisateur vCenter à l'hôte ou à la machine virtuelle. Pour Rôle assigné, choisissez En lecture seule, .
6. Choisissez OK.

> **Note**
>
> Si vous avez choisi Propagate to children, vous pouvez toujours supprimer l'autorisation de lecture seule sur les hôtes ESX et VMs sur une base. case-by-case Cette option n'a aucun effet sur les autorisations héritées s'appliquant aux autres hôtes ESX et VMs.

Données collectées par le module de collecte de données Agentless Collector VMware vCenter

Les informations suivantes décrivent les données collectées par le module de collecte de données VMware vCenter Application Discovery Service Agentless Collector (Agentless Collector). Pour plus d'informations sur la configuration de la collecte de données, consultezConfiguration du module de collecte de données Agentless Collector pour vCenter VMware.

Légende du tableau pour les données collectées par Agentless Collector VMware vCenter :

- Les données collectées sont mesurées en kilo-octets (Ko), sauf indication contraire.
- Les données équivalentes de la console Migration Hub sont indiquées en mégaoctets (Mo).
- Les champs de données marqués d'un astérisque (*) ne sont disponibles que dans les fichiers .csv produits à partir de la fonction d'exportation de l'API Application Discovery Service.

Le collecteur sans agent prend en charge l'exportation de données à l'aide de la AWS CLI. Pour exporter les données collectées à l'aide de la AWS CLI, suivez les instructions décrites dans la section Exporter les données de performance du système pour tous les serveurs sur la page Exporter les données collectées du guide de l'utilisateur d'Application Discovery Service.

- L'intervalle entre les périodes d'interrogation est d'environ 60 minutes.
- Les champs de données signalés par deux astérisques (**) renvoient actuellement une valeur null.

Champ de données	Description
applicationConfigurationId*	ID de l'application de migration sous laquelle la machine virtuelle est regroupée.
avgCpuUsagePCT	Pourcentage moyen d'utilisation du processeur au cours de la période d'enquête.
avgDiskBytesReadPerSecond	Nombre moyen d'octets lus sur le disque au cours de la période d'interrogation.
avgDiskBytesWrittenPerSecond	Nombre moyen d'octets écrits sur le disque au cours de la période d'interrogation.
avgDiskReadOpsPerSecond**	Nombre moyen d' I/O opérations de lecture par seconde nul.
avgDiskWriteOpsPerSecond**	Nombre moyen d' I/O opérations d'écriture par seconde.
avgFreeRAM	Mémoire vive libre moyenne exprimée en Mo.
avgNetworkBytesReadPerSecond	Débit moyen d'octets lus par seconde.
avgNetworkBytesWrittenPerSecond	Débit moyen d'octets écrits par seconde.
Fabricant d'ordinateurs	Fournisseur indiqué par l' ESXi hôte.
Modèle d'ordinateur	Modèle d'ordinateur indiqué par l' ESXi hôte.

Champ de données	Description
configId	ID attribué par Application Discovery Service à la machine virtuelle découverte.
configType	Type de ressource découverte.
connectorId	ID de l'appliance virtuelle.
cpuType	vCPU pour une machine virtuelle, modèle réel pour un hôte.
datacenterId	ID du vCenter.
hostId*	ID de l'hôte de la machine virtuelle.
hostName	Nom de l'hôte exécutant le logiciel de virtualis ation.
hyperviseur	Type d'hyperviseur.
id	ID du serveur.
lastModifiedTimeTampon *	Date et heure de collecte des données les plus récentes avant l'exportation des données.
macAddress	Adresse MAC de la machine virtuelle.
manufacturer	Créateur du logiciel de virtualisation.
maxCpuUsagePCT	Pourcentage maximal d'utilisation du processeu r pendant la période de sondage.
maxDiskBytesReadPerSecond	Nombre maximal d'octets lus sur le disque pendant la période d'interrogation.
maxDiskBytesWrittenPerSecond	Nombre maximal d'octets écrits sur le disque pendant la période d'interrogation.
maxDiskReadOpsPerSecond**	Nombre maximal d' I/O opérations de lecture par seconde.

Champ de données	Description
maxDiskWriteOpsPerSecond**	Nombre maximal d' I/O opérations d'écriture par seconde.
maxNetworkBytesReadPerSecond	Débit maximal d'octets lus par seconde.
maxNetworkBytesWrittenPerSecond	Débit maximal d'octets écrits par seconde.
memoryReservation*	Limite pour éviter un surengagement de la mémoire sur la machine virtuelle.
moRefId	ID de référence unique de l'objet géré par vCenter.
name*	Nom de la machine virtuelle ou du réseau (spécifié par l'utilisateur).
numCores	Nombre de cœurs de processeur affectés à la machine virtuelle.
numCpus	Nombre de sockets du processeur sur l' ESXi hôte.
numDisks**	Nombre de disques sur la machine virtuelle.
numNetworkCards**	Nombre de cartes réseau sur la machine virtuelle.
osName	Nom du système d'exploitation sur la machine virtuelle.
osVersion	Version du système d'exploitation sur la machine virtuelle.
portGroupId*	ID du groupe de ports membres du VLAN.
portGroupName*	Nom du groupe de ports membres du VLAN.
powerState*	État du pouvoir.

Champ de données	Description
serverId	Application Discovery Service a attribué un ID à la machine virtuelle découverte.
smBiosId*	ID/version du BIOS de gestion du système.
state*	État de l'appliance virtuelle.
toolsStatus	État de fonctionnement des VMware outils
totalDiskFreeTaille	L'espace disque libre est exprimé en Mo. Disponible pour vCenter Server 7.0 et versions ultérieures.
totalDiskSize	Capacité totale du disque exprimée en Mo.
totalRAM	Quantité totale de RAM disponible sur la machine virtuelle en Mo.
type	Type d'hôte
vCenterId	Numéro d'identification unique d'une machine virtuelle.
vCenterName*	Nom de l'hôte vCenter.
virtualSwitchName*	Nom du commutateur virtuel.
vmFolderPath	Chemin du répertoire des fichiers de machine virtuelle.
vmName	Nom de la machine virtuelle.

Utilisation du module de collecte de données de base de données et d'analyse

Cette section décrit comment configurer, configurer et utiliser une base de données et un module de collecte de données analytiques. Vous pouvez utiliser ce module de collecte de données pour

vous connecter à votre environnement de données et collecter des métadonnées et des indicateurs de performance à partir de vos bases de données et de vos serveurs d'analyse sur site. Pour plus d'informations sur les métriques que vous pouvez collecter avec ce module, consultezDonnées collectées par la base de données Agentless Collector et le module de collecte de données analytiques.

> **Important**
>
> Avis de fin de support : le 20 mai 2026, le support de AWS Database Migration Service Fleet Advisor AWS prendra fin. Après le 20 mai 2026, vous ne pourrez plus accéder à la console AWS DMS Fleet Advisor ni aux ressources de AWS DMS Fleet Advisor. Pour plus d'informations, consultez la section de fin du support de AWS DMS Fleet Advisor.

À un niveau élevé, lorsque vous utilisez le module de collecte de données de base de données et d'analyse, vous devez suivre les étapes suivantes.

1. Effectuez les étapes préalables, configurez votre utilisateur IAM et créez le collecteur de AWS DMS données.
2. Configurez le transfert de données pour vous assurer que votre module de collecte de données peut envoyer les métadonnées collectées et les indicateurs de performance à AWS.
3. Ajoutez vos serveurs LDAP et utilisez-les pour découvrir les serveurs du système d'exploitation dans votre environnement de données. Vous pouvez également ajouter vos serveurs de système d'exploitation manuellement ou utiliser leUtilisation du module VMware de collecte de données.
4. Configurez les informations d'identification de connexion à vos serveurs de système d'exploitation, puis utilisez-les pour découvrir les serveurs de base de données.
5. Configurez les informations d'identification de connexion à votre base de données et à vos serveurs d'analyse, puis exécutez la collecte de données. Pour de plus amples informations, veuillez consulter Collecte de données de base de données et d'analyse.
6. Affichez les données collectées dans la AWS DMS console et utilisez-les pour générer des recommandations cibles pour une migration vers le AWS Cloud. Pour de plus amples informations, veuillez consulter Collecte de données de base de données et d'analyse.

Rubriques

- Systèmes d'exploitation, bases de données et serveurs d'analyse pris en charge
- Création du collecteur AWS DMS de données

- Configuration du transfert de données
- Ajouter vos serveurs LDAP et OS
- Découverte de vos serveurs de base de données
- Données collectées par la base de données Agentless Collector et le module de collecte de données analytiques

Systèmes d'exploitation, bases de données et serveurs d'analyse pris en charge

Le module de collecte de données de base de données et d'analyse de l'Agentless Collector prend en charge les serveurs LDAP Microsoft Active Directory.

Ce module de collecte de données prend en charge les serveurs de systèmes d'exploitation suivants.

- Amazon Linux 2
- CentOS Linux version 6 et supérieure
- Debian version 10 et supérieure
- Red Hat Enterprise Linux version 7 et supérieure
- SUSE Linux Enterprise Server version 12 et supérieure
- Ubuntu version 16.01 et supérieure
- Windows Server 2012 et versions ultérieures
- Windows XP et supérieur

En outre, le module de collecte de données de base de données et d'analyse prend en charge les serveurs de base de données suivants.

- Microsoft SQL Server versions 2012 et jusqu'à 2019
- MySQL versions 5.6 et jusqu'à 8
- Oracle versions 11g Release 2 et jusqu'à 12c, 19c et 21c
- PostgreSQL versions 9.6 et jusqu'à 13

Création du collecteur AWS DMS de données

Votre module de collecte de données de base de données et d'analyse utilise un collecteur de AWS DMS données pour interagir avec la AWS DMS console. Vous pouvez consulter les données collectées dans la AWS DMS console ou les utiliser pour déterminer le moteur AWS cible de la bonne taille. Pour plus d'informations, consultez la section Utilisation de la fonctionnalité AWS DMS Fleet Advisor Target Recommendations.

Avant de créer un collecteur de AWS DMS données, créez un rôle IAM que votre collecteur de AWS DMS données utilise pour accéder à votre compartiment Amazon S3. Vous avez créé ce compartiment Amazon S3 lorsque vous avez rempli les conditions requises dansConditions requises pour Agentless Collector.

Pour créer un rôle IAM permettant à votre collecteur de AWS DMS données d'accéder à Amazon S3

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.
2. Dans le volet de navigation, choisissez Rôles, puis Create role.
3. Sur la page Sélectionner une entité de confiance, pour Type d'entité approuvée, choisissez Service AWS . Pour les cas d'utilisation d'autres AWS services, choisissez DMS.
4. Cochez la case DMS et choisissez Suivant.
5. Sur la page Ajouter des autorisations, choisissez FleetAdvisorS3Policy que vous avez créé auparavant. Choisissez Suivant.
6. Sur la page Nommer, vérifier et créer, entrez **`FleetAdvisorS3Role`** pour Nom du rôle, puis choisissez Créer un rôle.
7. Ouvrez le rôle que vous avez créé, puis choisissez l'onglet Relations de confiance. Choisissez Modifier la politique d'approbation.
8. Sur la page Modifier la politique de confiance, collez le code JSON suivant dans l'éditeur en remplaçant le code existant.

   JSON

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

```
  "Principal": {
   "Service": [
    "dms.amazonaws.com",
    "dms-fleet-advisor.amazonaws.com"
   ]
  },
  "Action": "sts:AssumeRole"
 }]
}
```

9. Choisissez Mettre à jour une politique.

Créez maintenant un collecteur de données dans la AWS DMS console.

Pour créer un collecteur AWS DMS de données

1. Connectez-vous à la AWS DMS console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/dms/v2/.
2. Choisissez celle Région AWS que vous avez définie comme région d'origine de votre Migration Hub. Pour de plus amples informations, veuillez consulter Connectez-vous au Migration Hub et choisissez une région d'origine.
3. Dans le volet de navigation, choisissez Collecteurs de données sous Découvrir. La page Collecteurs de données s'ouvre.
4. Choisissez Créer un collecteur de données. La page Créer un collecteur de données s'ouvre.
5. Pour Nom dans la section Configuration générale, entrez le nom de votre collecteur de données.
6. Dans la section Connectivité, choisissez Parcourir S3. Choisissez le compartiment Amazon S3 que vous avez créé auparavant dans la liste.
7. Pour le rôle IAM, choisissez `FleetAdvisorS3Role` celui que vous avez créé auparavant.
8. Choisissez Créer un collecteur de données.

Configuration du transfert de données

Après avoir créé les AWS ressources requises, configurez le transfert de données depuis le module de collecte de données de base de données et d'analyse vers votre AWS DMS collecteur.

Pour configurer le transfert de données

1. Ouvrez la console Agentless Collector. Pour de plus amples informations, veuillez consulter Accès à la console du collecteur.
2. Choisissez Afficher la base de données et le collecteur d'analyses.
3. Sur la page Tableau de bord, choisissez Configurer le transfert de données dans la section Transfert de données.
4. Pour l'Région AWSID de clé d'accès IAM et la clé d'accès secrète IAM, votre collecteur sans agent utilise les valeurs que vous avez configurées auparavant. Pour plus d'informations, consultez Connectez-vous au Migration Hub et choisissez une région d'origine et Déploiement d'un collecteur.
5. Pour le collecteur de données Connected DMS, choisissez le collecteur de données que vous avez créé dans la AWS DMS console.
6. Choisissez Enregistrer.

Après avoir configuré le transfert de données, consultez la section Transfert de données sur la page du tableau de bord. Assurez-vous que votre module de collecte de données de base de données et d'analyse affiche

Conne

for Access to DMS et Access to S3.

Ajouter vos serveurs LDAP et OS

Le module de collecte de données de base de données et d'analyse utilise le protocole LDAP dans Microsoft Active Directory pour recueillir des informations sur le système d'exploitation, la base de données et les serveurs d'analyse de votre réseau. Le protocole LDAP (Lightweight Directory Protocol) est un protocole d'application standard ouvert. Vous pouvez utiliser ce protocole pour accéder aux services d'information d'annuaire distribués et les gérer sur votre réseau IP.

Vous pouvez ajouter un serveur LDAP existant à votre base de données et à votre module de collecte de données analytiques pour découvrir automatiquement les serveurs du système d'exploitation de votre réseau. Si vous n'utilisez pas LDAP, vous pouvez ajouter des serveurs de système d'exploitation manuellement.

Pour ajouter un serveur LDAP à votre base de données et à votre module de collecte de données analytiques

1. Ouvrez la console Agentless Collector. Pour de plus amples informations, veuillez consulter Accès à la console du collecteur.
2. Choisissez Afficher la base de données et le collecteur d'analyses, puis choisissez les serveurs LDAP sous Discovery dans le volet de navigation.
3. Choisissez Ajouter un serveur LDAP. La page Ajouter un serveur LDAP s'ouvre.
4. Dans Nom d'hôte, entrez le nom d'hôte de votre serveur LDAP.
5. Pour Port, entrez le numéro de port utilisé pour les demandes LDAP.
6. Dans Nom d'utilisateur, entrez le nom d'utilisateur que vous utilisez pour vous connecter à votre serveur LDAP.
7. Dans Mot de passe, entrez le mot de passe que vous utilisez pour vous connecter à votre serveur LDAP.
8. (Facultatif) Choisissez Vérifier la connexion pour vous assurer que vous avez correctement ajouté les informations d'identification de votre serveur LDAP. Vous pouvez également vérifier vos informations de connexion au serveur LDAP ultérieurement, à partir de la liste figurant sur la page des serveurs LDAP.
9. Choisissez Ajouter un serveur LDAP.
10. Sur la page des serveurs LDAP, sélectionnez votre serveur LDAP dans la liste et choisissez Discover OS servers.

> **⚠ Important**
>
> Pour la découverte du système d'exploitation, le module de collecte de données a besoin d'informations d'identification pour que le serveur de domaine puisse exécuter les demandes à l'aide du protocole LDAP.

Le module de collecte de données de base de données et d'analyse se connecte à votre serveur LDAP et découvre vos serveurs de système d'exploitation. Une fois que le module de collecte de données a terminé la découverte des serveurs de système d'exploitation, vous pouvez voir la liste des serveurs de système d'exploitation découverts en choisissant Afficher les serveurs de système d'exploitation.

Vous pouvez également ajouter vos serveurs de système d'exploitation manuellement ou importer la liste des serveurs à partir d'un fichier CSV (valeurs séparées par des virgules). Vous pouvez également utiliser le module de collecte de données VMware vCenter Agentless Collector pour découvrir vos serveurs de système d'exploitation. Pour de plus amples informations, veuillez consulter Utilisation du module VMware de collecte de données.

Pour ajouter un serveur OS à votre base de données et à votre module de collecte de données analytiques

1. Sur la page Base de données et collecteur d'analyses, sélectionnez les serveurs du système d'exploitation sous Discovery dans le volet de navigation.
2. Choisissez Ajouter un serveur OS. La page Ajouter un serveur OS s'ouvre.
3. Entrez les informations d'identification de votre serveur de système d'exploitation.
   a. Pour le type de système d'exploitation, choisissez le système d'exploitation de votre serveur.
   b. Pour Nom d'hôte/IP, entrez le nom d'hôte ou l'adresse IP de votre serveur OS.
   c. Pour Port, entrez le numéro de port utilisé pour les requêtes distantes.
   d. Pour Type d'authentification, choisissez le type d'authentification utilisé par votre serveur de système d'exploitation.
   e. Dans Nom d'utilisateur, entrez le nom d'utilisateur que vous utilisez pour vous connecter à votre serveur de système d'exploitation.
   f. Dans Mot de passe, entrez le mot de passe que vous utilisez pour vous connecter à votre serveur de système d'exploitation.
   g. Choisissez Vérifier pour vous assurer que vous avez correctement ajouté les informations d'identification de votre serveur de système d'exploitation.
4. (Facultatif) Ajoutez plusieurs serveurs de système d'exploitation à partir d'un fichier CSV.
   a. Choisissez Importer en bloc les serveurs du système d'exploitation à partir du format CSV.
   b. Choisissez Télécharger le modèle pour enregistrer un fichier CSV contenant un modèle que vous pouvez personnaliser.
   c. Entrez les informations de connexion pour vos serveurs de système d'exploitation dans le fichier conformément au modèle. L'exemple suivant montre comment vous pouvez fournir des informations d'identification de connexion au serveur du système d'exploitation dans un fichier CSV.

```
OS type,Hostname/IP,Port,Authentication type,Username,Password
```

```
Linux,192.0.2.0,22,Key-based authentication,USER-EXAMPLE,ANPAJ2UCCR6DPCEXAMPLE
Windows,203.0.113.0,,NTLM,USER2-EXAMPLE,AKIAIOSFODNN7EXAMPLE
```

Enregistrez votre fichier CSV après avoir ajouté les informations d'identification pour tous vos serveurs de système d'exploitation.

d. Choisissez Parcourir, puis choisissez votre fichier CSV.

5. Choisissez Ajouter un serveur OS.
6. Après avoir ajouté les informations d'identification pour tous les serveurs de système d'exploitation, sélectionnez vos serveurs de système d'exploitation et choisissez Découvrir les serveurs de base de données.

Découverte de vos serveurs de base de données

Cette section explique les étapes à suivre pour configurer votre système d'exploitation et vos serveurs de base de données. Ensuite, vous découvrirez vos serveurs et aurez la possibilité d'ajouter manuellement une base de données ou un serveur d'analyse.

Pour la découverte de bases de données, vous devez créer des utilisateurs pour vos bases de données source avec les autorisations minimales requises pour le module de collecte de données. Pour plus d'informations, consultez la section Création d'utilisateurs de base de données pour AWS DMS Fleet Advisor dans le guide de AWS DMS l'utilisateur.

Configuration de la configuration

Pour découvrir les bases de données exécutées sur les serveurs OS précédemment ajoutés, le module de collecte de données doit accéder au système d'exploitation et aux serveurs de base de données. Cette page décrit les étapes à suivre pour vous assurer que votre base de données est accessible sur le port que vous avez spécifié dans les paramètres de connexion. Vous allez également activer l'authentification à distance sur votre serveur de base de données et fournir des autorisations à votre module de collecte de données.

Configuration de la configuration sous Linux

Procédez comme suit pour configurer la configuration des serveurs de base de données pour détecter les serveurs de base de données sous Linux.

Pour configurer Linux afin de découvrir les serveurs de base de données

1. Fournissez un accès sudo aux `netstat` commandes `ss` et.

L'exemple de code suivant accorde à sudo l'accès aux `netstat` commandes `ss` et.

```
sudo bash -c "cat << EOF >> /etc/sudoers.d/username
username ALL=(ALL) NOPASSWD: /usr/bin/ss
username ALL=(ALL) NOPASSWD: /usr/bin/netstat
EOF"
```

Dans l'exemple précédent, remplacez par le nom *username* de l'utilisateur Linux que vous avez spécifié dans les informations d'identification de connexion au serveur du système d'exploitation.

L'exemple précédent utilise le `/usr/bin/` chemin d'accès aux `netstat` commandes `ss` et. Ce chemin peut être différent dans votre environnement. Pour déterminer le chemin d'accès aux `netstat` commandes `ss` et, exécutez les `which netstat` commandes `which ss` et.

2. Configurez vos serveurs Linux pour autoriser l'exécution de scripts SSH distants et autoriser le trafic ICMP (Internet Control Message Protocol).

Configuration de l'installation sous Microsoft Windows

Procédez comme suit pour configurer la configuration des serveurs de base de données pour détecter les serveurs de base de données sous Microsoft Windows.

Pour configurer Microsoft Windows afin de détecter les serveurs de base de données

1. Fournissez des informations d'identification avec des autorisations pour exécuter des requêtes Windows Management Instrumentation (WMI) et WMI Query Language (WQL) et lire le registre.
2. Ajoutez l'utilisateur Windows que vous avez spécifié dans les informations d'identification de connexion au serveur du système d'exploitation aux groupes suivants : utilisateurs COM distribués, utilisateurs du journal des performances, utilisateurs du moniteur de performances et lecteurs du journal des événements. Pour ce faire, utilisez l'exemple de code suivant.

```
net localgroup "Distributed COM Users" username /ADD
net localgroup "Performance Log Users" username /ADD
net localgroup "Performance Monitor Users" username /ADD
net localgroup "Event Log Readers" username /ADD
```

Dans l'exemple précédent, remplacez par le nom *username* de l'utilisateur Windows que vous avez spécifié dans les informations d'identification de connexion au serveur du système d'exploitation.

3. Accordez les autorisations requises à l'utilisateur Windows que vous avez spécifié dans les informations d'identification de connexion au serveur du système d'exploitation.

   - Pour les propriétés de gestion et d'instrumentation de Windows, choisissez Lancement local et activation à distance.
   - Pour WMI Control, choisissez les autorisations Execute Methods, Enable Account, Remote Enable et Read Security pour les `CIMV2` espaces de `WMI` noms `DEFAULTStandartCimv2`,, et.
   - Pour le plug-in WMI, exécutez puis choisissez Read **`winrm configsddl default`** and Execute.

4. Configurez votre hôte Windows à l'aide de l'exemple de code suivant.

```
netsh advfirewall firewall add rule name="Open Ports for WinRM incoming traffic"
 dir=in action=allow protocol=TCP localport=5985, 5986 # Opens ports for WinRM
netsh advfirewall firewall add rule name="All ICMP V4" protocol=icmpv4:any,any
 dir=in action=allow # Allows ICPM traffic

Enable-PSRemoting -Force # Enables WinRM
Set-Service WinRM -StartMode Automatic # Allows WinRM service to run on host
 startup
Set-Item WSMan:\localhost\Client\TrustedHosts -Value {IP} -Force # Sets the
 specific IP from which the access to WinRM is allowed

winrm set winrm/config/service '@{Negotiation="true"}' # Allow Negosiate auth usage
winrm set winrm/config/service '@{AllowUnencrypted="true"}' # Allow unencrypted
 connection
```

Découverte d'un serveur de base de données

Effectuez les tâches suivantes pour découvrir et ajouter des serveurs de base de données sur la console.

Pour démarrer la découverte de vos serveurs de base de données

1. Sur la page Base de données et collecteur d'analyses, sélectionnez les serveurs du système d'exploitation sous Discovery dans le volet de navigation.
2. Sélectionnez les serveurs du système d'exploitation qui incluent votre base de données et vos serveurs d'analyse, puis choisissez Vérifier la connexion dans le menu Actions.

3. Pour les serveurs dont le statut de connectivité est Echec, modifiez les informations d'identification de connexion.

   a. Sélectionnez un ou plusieurs serveurs dont les informations d'identification sont identiques, puis choisissez Modifier dans le menu Actions. La page Modifier le serveur du système d'exploitation s'ouvre.

   b. Pour Port, entrez le numéro de port utilisé pour les requêtes distantes.

   c. Pour Type d'authentification, choisissez le type d'authentification utilisé par votre serveur de système d'exploitation.

   d. Dans Nom d'utilisateur, entrez le nom d'utilisateur que vous utilisez pour vous connecter à votre serveur de système d'exploitation.

   e. Dans Mot de passe, entrez le mot de passe que vous utilisez pour vous connecter à votre serveur de système d'exploitation.

   f. Choisissez Vérifier la connexion pour vous assurer que vous avez correctement mis à jour les informations d'identification de votre serveur de système d'exploitation. Ensuite, choisissez Enregistrer.

4. Après avoir mis à jour les informations d'identification pour tous les serveurs de système d'exploitation, sélectionnez vos serveurs de système d'exploitation et choisissez Découvrir les serveurs de base de données.

Le module de collecte de données de base de données et d'analyse se connecte aux serveurs de votre système d'exploitation et découvre les serveurs de base de données et d'analyse pris en charge. Une fois que le module de collecte de données a terminé la découverte, vous pouvez voir la liste des serveurs de base de données et d'analyse découverts en choisissant Afficher les serveurs de base de données.

Vous pouvez également ajouter votre base de données et vos serveurs d'analyse à l'inventaire manuellement. Vous pouvez également importer la liste des serveurs à partir d'un fichier CSV. Vous pouvez ignorer cette étape si vous avez déjà ajouté tous vos serveurs de base de données et d'analyse à l'inventaire.

Pour ajouter manuellement une base de données ou un serveur d'analyse

1. Sur la page Base de données et collecteur d'analyses, sélectionnez Collecte de données dans le volet de navigation.

2. Choisissez Ajouter un serveur de base de données. La page Ajouter un serveur de base de données s'ouvre.
3. Entrez les informations d'identification de votre serveur de base de données.

   a. Pour Moteur de base de données, choisissez le moteur de base de données de votre serveur. Pour de plus amples informations, veuillez consulter Systèmes d'exploitation, bases de données et serveurs d'analyse pris en charge.

   b. Pour Nom d'hôte/IP, entrez le nom d'hôte ou l'adresse IP de votre base de données ou de votre serveur d'analyse.

   c. Dans le champ Port, entrez le port sur lequel votre serveur s'exécute.

   d. Pour Type d'authentification, choisissez le type d'authentification utilisé par votre base de données ou votre serveur d'analyse.

   e. Dans Nom d'utilisateur, entrez le nom d'utilisateur que vous utilisez pour vous connecter à votre serveur.

   f. Dans Mot de passe, entrez le mot de passe que vous utilisez pour vous connecter à votre serveur.

   g. Choisissez Vérifier pour vous assurer que vous avez correctement ajouté les informations d'identification de votre base de données ou de votre serveur d'analyse.
4. (Facultatif) Ajoutez plusieurs serveurs à partir d'un fichier CSV.

   a. Choisissez Importer en bloc des serveurs de base de données depuis CSV.

   b. Choisissez Télécharger le modèle pour enregistrer un fichier CSV contenant un modèle que vous pouvez personnaliser.

   c. Entrez les informations de connexion pour votre base de données et vos serveurs d'analyse dans le fichier conformément au modèle. L'exemple suivant montre comment vous pouvez fournir des informations d'identification de connexion à une base de données ou à un serveur d'analyse dans un fichier CSV.

```
Database engine,Hostname/IP,Port,Authentication type,Username,Password,Oracle
 service name,Database,Allow public key retrieval,Use SSL,Trust server
 certificate
Oracle,192.0.2.1,1521,Login/Password authentication,USER-
EXAMPLE,AKIAI44QH8DHBEXAMPLE,orcl,,,,
PostgreSQL,198.51.100.1,1533,Login/Password authentication,USER2-
EXAMPLE,bPxRfiCYEXAMPLE,,postgre,,TRUE,
MSSQL,203.0.113.1,1433,Login/Password authentication,USER3-
EXAMPLE,h3yCo8nvbEXAMPLE,,,,,TRUE
```

```
MySQL,2001:db8:4006:812:ffff:200e,8080,Login/Password authentication,USER4-
EXAMPLE,APKAEIVFHP46CEXAMPLE,,mysql,TRUE,TRUE,
```

Enregistrez votre fichier CSV après avoir ajouté les informations d'identification pour tous vos serveurs de base de données et d'analyse.

d. Choisissez Parcourir, puis choisissez votre fichier CSV.

5. Choisissez Ajouter un serveur de base de données.
6. Après avoir ajouté les informations d'identification pour tous les serveurs de système d'exploitation, sélectionnez vos serveurs de système d'exploitation et choisissez Découvrir les serveurs de base de données.

Après avoir ajouté tous vos serveurs de base de données et d'analyse dans le module de collecte de données, ajoutez-les à l'inventaire. Le module de collecte de données de base de données et d'analyse peut se connecter aux serveurs à partir de l'inventaire et collecter des métadonnées et des mesures de performance.

Pour ajouter votre base de données et vos serveurs d'analyse à l'inventaire

1. Sur la page Base de données et collecteur d'analyses, sélectionnez Serveurs de base de données sous Discovery dans le volet de navigation.
2. Sélectionnez les serveurs de base de données et d'analyse pour lesquels vous souhaitez collecter des métadonnées et des indicateurs de performance.
3. Choisissez Ajouter à l'inventaire.

Après avoir ajouté tous les serveurs de base de données et d'analyse à votre inventaire, vous pouvez commencer à collecter des métadonnées et des indicateurs de performance. Pour de plus amples informations, veuillez consulter Collecte de données de base de données et d'analyse.

Données collectées par la base de données Agentless Collector et le module de collecte de données analytiques

Le module de base de données et de collecte de données analytiques Application Discovery Service Agentless Collector (Agentless Collector) collecte les métriques suivantes à partir de votre environnement de données. Pour plus d'informations sur la configuration de la collecte de données, consultezUtilisation du module de collecte de données de base de données et d'analyse.

Lorsque vous utilisez le module de collecte de données de base de données et d'analyse pour collecter les métadonnées et la capacité de la base de données, il capture les mesures suivantes.

- Mémoire disponible sur vos serveurs OS
- Stockage disponible sur vos serveurs OS
- Version et édition de base de données
- Nombre de serveurs CPUs sur votre système d'exploitation
- Nombre de schémas
- Nombre de procédures stockées
- Nombre de tables
- Nombre de déclencheurs
- Nombre de vues
- Structure des schémas

Après avoir lancé l'analyse du schéma dans la AWS DMS console, votre module de collecte de données analyse et affiche les mesures suivantes.

- Dates de prise en charge de base de données
- Nombre de lignes de code
- Complexité de schéma
- Similarité des schémas

Lorsque vous utilisez le module de collecte de données de base de données et d'analyse pour collecter des métadonnées, la capacité de la base de données et l'utilisation des ressources, il capture les métriques suivantes.

- Débit d’E/S sur vos serveurs de base de données
- Opérations d’entrée/sortie par seconde (IOPS) sur vos serveurs de base de données
- Nombre CPUs utilisé par vos serveurs de système d'exploitation
- Utilisation de la mémoire sur vos serveurs OS
- Utilisation du stockage sur vos serveurs OS

Vous pouvez utiliser le module de collecte de données de base de données et d'analyse pour collecter des métadonnées, des mesures de capacité et d'utilisation à partir de vos bases de données Oracle et SQL Server. Dans le même temps, pour les bases de données PostgreSQL et MySQL, le module de collecte de données ne peut collecter que des métadonnées.

Afficher les données que vous avez collectées

> **Important**
>
> Avis de fin de support : le 20 mai 2026, le support de AWS Database Migration Service Fleet Advisor AWS prendra fin. Après le 20 mai 2026, vous ne pourrez plus accéder à la console AWS DMS Fleet Advisor ni aux ressources de AWS DMS Fleet Advisor. Pour plus d'informations, consultez la section Fin du support de AWS DMS Fleet Advisor.

Vous pouvez consulter les données collectées par votre Application Discovery Service Agentless Collector (Agentless Collector) dans la console Migration Hub en suivant les étapes décrites dans. Affichage des serveurs dans la AWS Migration Hub console

Vous pouvez également consulter les métriques collectées pour les serveurs de base de données et d'analyse dans la AWS DMS console en procédant comme suit.

Pour afficher les données découvertes par la base de données et le module de collecte de données analytiques dans la AWS DMS console

1. Connectez-vous à la AWS DMS console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/dms/v2/.
2. Choisissez Inventaire sous Découvrir. La page Inventaire s'ouvre.
3. Choisissez Analyser les inventaires pour déterminer les propriétés du schéma de base de données, telles que la similarité et la complexité.
4. Cliquez sur l'onglet Schémas pour voir les résultats de l'analyse.

Vous pouvez utiliser la AWS DMS console pour identifier les schémas dupliqués, déterminer la complexité de la migration et exporter les informations d'inventaire pour une analyse future. Pour plus d'informations, consultez la section Utilisation des stocks pour l'analyse dans AWS DMS Fleet Advisor.

Accès au collecteur sans agent

Cette section décrit comment utiliser le collecteur sans agent Application Discovery Service (collecteur sans agent).

Rubriques

Le tableau de bord Agentless Collector

Sur la page du tableau de bord Application Discovery Service Agentless Collector (Agentless Collector), vous pouvez voir l'état du collecteur et choisir une méthode de collecte de données, comme décrit dans les rubriques suivantes.

Rubriques

Statut du collectionneur

Le statut du collecteur vous donne des informations sur le statut du collecteur. Le nom du collecteur, l'état de la connexion du collecteur à AWS, la région d'origine du Migration Hub et la version.

Si vous rencontrez des problèmes de AWS connexion, vous devrez peut-être modifier les paramètres de configuration d'Agentless Collector.

Pour modifier les paramètres de configuration du collecteur, choisissez Modifier les paramètres du collecteur et suivez les instructions décrites dansModification des paramètres du collecteur sans agent.

Collecte des données

Sous Collecte de données, vous pouvez choisir une méthode de collecte de données. Application Discovery Service Agentless Collector (Agentless Collector) prend actuellement en charge la collecte de données depuis VMware VMs et depuis des serveurs de base de données et d'analyse. Les futurs

modules prendront en charge la collecte à partir de plateformes de virtualisation supplémentaires et la collecte au niveau du système d'exploitation.

Rubriques

- VMware Collecte de données vCenter
- Collecte de données de base de données et d'analyse

VMware Collecte de données vCenter

Pour collecter des données d'inventaire, de profil et d'utilisation des serveurs auprès de vous VMware VMs, configurez des connexions à vos serveurs vCenter. Pour configurer les connexions, choisissez Set up dans la section VMware vCenter et suivez les instructions décrites dans. Utilisation du module de collecte de VMware données vCenter Agentless Collector

Après avoir configuré la collecte de données vCenter, vous pouvez effectuer les opérations suivantes à partir du tableau de bord :

- Afficher l'état de la collecte de données
- Démarrer la collecte des données
- Arrêter la collecte des données

> **Note**
>
> Sur la page du tableau de bord, une fois que vous avez configuré la collecte de données vCenter, le bouton Configurer de la section VMwarevCenter est remplacé par des informations sur l'état de la collecte de données, un bouton Arrêter la collecte de données et un bouton Afficher et modifier.

Collecte de données de base de données et d'analyse

Vous pouvez exécuter votre module de collecte de données de base de données et d'analyse dans les deux modes suivants.

Métadonnées et capacité de base de données

Le module de collecte de données collecte des informations telles que les schémas, les versions, les éditions, le processeur, la mémoire et la capacité du disque à partir de votre base de données

et de vos serveurs d'analyse. Vous pouvez utiliser ces informations collectées pour calculer les recommandations cibles dans la AWS DMS console. Si votre base de données source est surapprovisionnée ou sous-approvisionnée, les recommandations cibles seront également surapprovisionnées ou sous-approvisionnées.

C'est le mode par défaut.

Métadonnées, capacité de base de données et utilisation des ressources

Outre les métadonnées et les informations sur la capacité des bases de données, le module de collecte de données collecte des mesures d'utilisation réelles du processeur, de la mémoire et de la capacité du disque pour les bases de données et les serveurs d'analyse. Ce mode fournit des recommandations cibles plus précises que le mode par défaut, car les recommandations sont basées sur les charges de travail réelles de la base de données. Dans ce mode, le module de collecte de données collecte des mesures de performance toutes les minutes.

Pour commencer à collecter des métadonnées et des indicateurs de performance à partir de votre base de données et de vos serveurs d'analyse

1. Sur la page Base de données et collecteur d'analyses, sélectionnez Collecte de données dans le volet de navigation.
2. Dans la liste d'inventaire des bases de données, sélectionnez les serveurs de base de données et d'analyse pour lesquels vous souhaitez collecter des métadonnées et des indicateurs de performance.
3. Choisissez Exécuter la collecte de données. La boîte de dialogue Type de collecte de données s'ouvre.
4. Choisissez le mode de collecte des données à des fins d'analyse.

   Si vous choisissez l'option Métadonnées, capacité de base de données et utilisation des ressources, définissez la période de collecte des données. Vous pouvez collecter des données au cours des 7 prochains jours ou définir la plage personnalisée de 1 à 60 jours.
5. Choisissez Exécuter la collecte de données. La page de collecte de données s'ouvre.
6. Cliquez sur l'onglet État de la collection pour voir l'état de la collecte de données.

Une fois la collecte de données terminée, votre module de collecte de données télécharge les données collectées dans votre compartiment Amazon S3. Vous pouvez ensuite consulter ces données collectées comme décrit dansAfficher les données que vous avez collectées.

Modification des paramètres du collecteur sans agent

Vous avez configuré le collecteur lorsque vous avez configuré pour la première fois Application Discovery Service Agentless Collector (Agentless Collector), comme décrit dans. Configuration du collecteur sans agent La procédure suivante décrit comment modifier les paramètres de configuration du collecteur sans agent.

Pour modifier les paramètres de configuration du collecteur

- Cliquez sur le bouton Modifier les paramètres du collecteur sur le tableau de bord Agentless Collector.

  Sur la page Modifier les paramètres du collecteur, effectuez les opérations suivantes :

  a. Dans Nom du collecteur, entrez un nom pour identifier le collecteur. Le nom peut contenir des espaces, mais il ne peut pas contenir de caractères spéciaux.

  b. Sous AWS Compte de destination pour les données de découverte, entrez la clé d' AWS accès et la clé secrète du AWS compte à spécifier comme compte de destination pour recevoir les données découvertes par le collecteur. Pour plus d'informations sur les exigences relatives à l'utilisateur IAM, consultezDéploiement d'Application Discovery Service Agentless Collector.

     i. Pour la AWS clé d'accès, entrez la clé d'accès du AWS compte utilisateur IAM que vous spécifiez comme compte de destination.

     ii. Pour AWS clé secrète, entrez la clé secrète du AWS compte utilisateur IAM que vous spécifiez comme compte de destination.

  c. Sous Mot de passe du collecteur sans agent, modifiez le mot de passe à utiliser pour authentifier l'accès au collecteur sans agent.

     i. Pour le mot de passe du collecteur sans agent, entrez un mot de passe à utiliser pour authentifier l'accès au collecteur sans agent.

     ii. Pour saisir à nouveau le mot de passe Agentless Collector, pour vérification, saisissez-le à nouveau.

  d. Choisissez Enregistrer les configurations.

Ensuite, tu verrasLe tableau de bord Agentless Collector.

Modification des informations d' VMware identification de vCenter

Pour collecter des données d'inventaire, de profil et d'utilisation des serveurs auprès de vous VMware VMs, configurez des connexions à vos serveurs vCenter. Pour plus d'informations sur la configuration des connexions VMware vCenter, consultez. Utilisation du module de collecte de VMware données vCenter Agentless Collector

Cette section décrit comment modifier les informations d'identification du vCenter.

> **Note**
>
> Avant de modifier les informations d'identification de vCenter, assurez-vous de pouvoir fournir des informations d'identification vCenter avec les autorisations de lecture et d'affichage définies pour le groupe System.

Pour modifier les informations d'identification du VMware vCenter

Sur la Afficher les détails VMware de la collecte de données page, choisissez Modifier les serveurs vCenter.

- Sur la page Modifier le vCenter, effectuez les opérations suivantes :
  a. Sous les informations d'identification vCenter :
     i. Pour l'URL/IP de vCenter, entrez l'adresse IP de votre hôte VMware vCenter Server.
     ii. Pour vCenter Username (Nom d'utilisateur vCenter), entrez le nom d'un utilisateur local ou de domaine que le connecteur utilise pour communiquer avec vCenter. Pour les utilisateurs de domaine, utilisez le format domaine\nom d'utilisateur ou nom d'utilisateur@domaine.
     iii. Pour vCenter Password (Mot de passe vCenter), entrez le mot de passe de l'utilisateur local ou du domaine.
  b. Choisissez Enregistrer.

Mise à jour manuelle d'Application Discovery Service Agentless Collector

Lorsque vous configurez Application Discovery Service Agentless Collector (Agentless Collector), vous pouvez choisir d'activer les mises à jour automatiques comme décrit dans. Configuration du collecteur sans agent Si vous n'activez pas les mises à jour automatiques, vous devez mettre à jour manuellement Agentless Collector.

La procédure suivante décrit comment mettre à jour manuellement Agentless Collector.

Pour mettre à jour manuellement Agentless Collector

1. Procurez-vous le dernier fichier Agentless Collector Open Virtualization Archive (OVA).
2. (Facultatif) Nous vous recommandons de supprimer le précédent fichier OVA Agentless Collector avant de déployer le dernier.
3. Suivez les étapes ci-dessousDéployer un collecteur sans agent.

La procédure précédente met uniquement à jour le collecteur sans agent. Il est de votre responsabilité de maintenir le système d'exploitation à jour.

Pour mettre à jour votre instance Amazon EC2

1. Obtenez l'adresse IP du collecteur sans agent auprès de VMware vCenter.
2. Ouvrez la console de machine virtuelle du collecteur et connectez-vous en **`ec2-user`** utilisant le mot de passe**`collector`**, comme indiqué dans l'exemple suivant.

   ```
   username: ec2-user
   password: collector
   ```

3. Suivez les instructions de la section Mettre à jour le logiciel de votre AL2 instance dans le guide de l'utilisateur Amazon Linux 2.

Correctif Kernel Live

Agentless Collector version 2

   La machine virtuelle Agentless Collector version 2 utilise Amazon Linux 2023 comme décrit dansDéployer un collecteur sans agent.

Pour activer et utiliser Live Patching pour Amazon Linux 2023, consultez Kernel Live Patching on AL2023 dans le guide de l'utilisateur Amazon EC2.

Agentless Collector version 1

La machine virtuelle Agentless Collector version 1 utilise Amazon Linux 2 comme décrit dansDéployer un collecteur sans agent.

Pour activer et utiliser Live Patching pour Amazon Linux 2, consultez Kernel Live Patching on AL2 dans le guide de l'utilisateur Amazon EC2.

Pour passer de la version 1 d'Agentless Collector à la version 2

1. Installez un nouveau collecteur OVA sans agent en utilisant la dernière image.
2. Configurez les informations d'identification.
3. Supprimez l'ancien dispositif virtuel.

Résolution des problèmes liés au collecteur sans agent

Cette section contient des rubriques qui peuvent vous aider à résoudre les problèmes connus liés à Application Discovery Service Agentless Collector (Agentless Collector).

Rubriques

- Fixation Unable to retrieve manifest or certificate file error
- Résolution des problèmes de certification auto-signée lors de la configuration des certificats WinRM
- Fixation du collecteur sans agent impossible à atteindre AWS lors de l'installation
- Résolution des problèmes de certification auto-signée lors de la connexion à l'hôte proxy
- Trouver des collectionneurs malsains
- Résoudre les problèmes d'adresse IP
- Résolution des problèmes liés aux informations d'identification de vCenter
- Résolution des problèmes de transfert de données dans le module de collecte de données de base de données et d'analyse
- Résolution des problèmes de connexion dans le module de collecte de données de base de données et d'analyse
- Support pour les hôtes ESX autonomes

- Contacter le AWS support pour des problèmes liés à Agentless Collector

Fixation **`Unable to retrieve manifest or certificate file error`**

Si vous recevez cette erreur lorsque vous essayez de déployer l'OVA à partir de l'URL Amazon S3 dans l'interface utilisateur de VMware vCenter, assurez-vous que votre serveur vCenter répond aux exigences suivantes :

- VMware vCenter Server version 8.0 mise à jour 1 ou ultérieure
- VMware vCenter Server 7.0 Update 3q (version ISO 23788036) ou version ultérieure

Résolution des problèmes de certification auto-signée lors de la configuration des certificats WinRM

Si vous activez les vérifications de certificats WinRM, vous devrez peut-être importer une autorité de certification autosignée dans le collecteur sans agent.

Pour importer une autorité de certification autosignée

1. Ouvrez la console Web de la machine virtuelle du collecteur dans VMware vCenter et connectez-vous `ec2-user` avec le mot de passe, `collector` comme indiqué dans l'exemple suivant.

   ```
   username: ec2-user
   password: collector
   ```

2. Assurez-vous que tous les certificats CA autosignés utilisés pour signer les certificats WinRM se trouvent dans le répertoire. `/etc/pki/ca-trust/source/anchors` Par exemple :

   ```
   /etc/pki/ca-trust/source/anchors/https-winrm-ca-1.pem
   ```

3. Pour installer les nouveaux certificats, exécutez la commande suivante.

   ```
   sudo update-ca-trust
   ```

4. Redémarrez le collecteur sans agent en exécutant la commande suivante

   ```
   sudo shutdown -r now
   ```

5. (Facultatif) Pour vérifier que les certificats ont bien été importés, vous pouvez exécuter la commande suivante.

```
sudo trust list --filter=ca-anchors | less
```

Fixation du collecteur sans agent impossible à atteindre AWS lors de l'installation

Agentless Collector nécessite un accès sortant via le port TCP 443 à plusieurs domaines. AWS Lorsque vous configurez Agentless Collector dans la console, le message d'erreur suivant peut s'afficher.

> Impossible d'atteindre AWS
>
> AWS ne peut pas être joint. Vérifiez les paramètres réseau.

Cette erreur se produit en raison d'une tentative infructueuse d'Agentless Collector d'établir une connexion HTTPS avec un AWS domaine avec lequel le collecteur doit communiquer pendant le processus de configuration. La configuration du collecteur sans agent échoue si aucune connexion ne peut être établie.

Pour réparer la connexion à AWS

1. Vérifiez auprès de votre administrateur informatique si le pare-feu de votre entreprise bloque le trafic sortant sur le port 443 vers l'un des AWS domaines nécessitant un accès sortant. Les AWS domaines nécessitant un accès sortant varient selon que votre région d'origine est la région USA Ouest (Oregon), us-west-2 ou une autre région.

   Les domaines suivants nécessitent un accès sortant si la région d'origine de votre AWS compte est us-west-2 :

   - `arsenal-discovery.us-west-2.amazonaws.com`
   - `migrationhub-config.us-west-2.amazonaws.com`
   - `api.ecr-public.us-east-1.amazonaws.com`
   - `public.ecr.aws`

Les domaines suivants nécessitent un accès sortant si la région d'origine de votre AWS compte ne l'est pas **`us-west-2`** :

- `arsenal-discovery.us-west-2.amazonaws.com`
- `arsenal-discovery.`*`your-home-region`*`.amazonaws.com`
- `migrationhub-config.us-west-2.amazonaws.com`
- `api.ecr-public.us-east-1.amazonaws.com`
- `public.ecr.aws`

Si votre pare-feu bloque l'accès sortant aux AWS domaines avec lesquels Agentless Collector doit communiquer, configurez un hôte proxy dans la section Synchronisation des données sous Configuration du collecteur.

2. Si la mise à jour du pare-feu ne résout pas le problème de connexion, suivez les étapes ci-dessous pour vous assurer que la machine virtuelle du collecteur dispose d'une connectivité réseau sortante vers les domaines répertoriés à l'étape précédente.

   a. Obtenez l'adresse IP du collecteur sans agent auprès de VMware vCenter.

   b. Ouvrez la console Web de la machine virtuelle du collecteur et connectez-vous en **`ec2-user`** utilisant le mot de passe, **`collector`** comme indiqué dans l'exemple suivant.

   ```
   username: ec2-user
   password: collector
   ```

   c. Testez la connexion aux domaines répertoriés en exécutant Telnet sur les ports 443, comme indiqué dans l'exemple suivant.

   ```
   telnet migrationhub-config.us-west-2.amazonaws.com 443
   ```

3. Si Telnet ne parvient pas à résoudre le domaine, essayez de configurer un serveur DNS statique en suivant les instructions d'Amazon Linux 2.

4. Si l'erreur persiste, pour obtenir de l'aide supplémentaire, consultezContacter le AWS support pour des problèmes liés à Agentless Collector.

Résolution des problèmes de certification auto-signée lors de la connexion à l'hôte proxy

Si la communication avec le proxy fourni en option se fait via HTTPS et que le proxy possède un certificat auto-signé, vous devrez peut-être fournir un certificat.

1. Obtenez l'adresse IP du collecteur sans agent auprès de VMware vCenter.
2. Ouvrez la console Web de la machine virtuelle du collecteur et connectez-vous `ec2-user` avec le mot de passe`collector`, comme indiqué dans l'exemple suivant.

   ```
   username: ec2-user
   password: collector
   ```

3. Collez le corps du certificat associé au proxy sécurisé, y compris les deux `-----BEGIN CERTIFICATE-----` et`-----END CERTIFICATE-----`, dans le fichier suivant :

   ```
   /etc/pki/ca-trust/source/anchors/https-proxy-ca.pem
   ```

4. Pour installer le nouveau certificat, exécutez les commandes suivantes :

   ```
   sudo update-ca-trust
   ```

5. Redémarrez le collecteur sans agent en exécutant la commande suivante :

   ```
   sudo shutdown -r now
   ```

Trouver des collectionneurs malsains

Les informations d'état de chaque collecteur se trouvent sur la page des collecteurs de données de la console AWS Migration Hub (Migration Hub). Vous pouvez identifier les collectionneurs qui rencontrent des problèmes en recherchant tous les collecteurs dont le statut nécessite une attention particulière.

La procédure suivante décrit comment accéder à la console Agentless Collector pour identifier les problèmes de santé.

Pour accéder à la console Agentless Collector

1. À l'aide de votre AWS compte, 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, sous Discover, sélectionnez Data collectors.
3. Dans l'onglet Collecteurs sans agent, notez l'adresse IP de chaque connecteur dont le statut est Requiert attention.
4. Pour ouvrir la console Agentless Collector, ouvrez un navigateur Web. Tapez ensuite l'URL suivante dans la barre d'adresse : **`https://`** *`<ip_address>`***`/`**, où ip_address est l'adresse IP d'un collecteur défectueux.
5. Choisissez Se connecter, puis entrez le mot de passe du collecteur sans agent, qui a été défini lors de la configuration du collecteur. Configuration du collecteur sans agent
6. Sur la page du tableau de bord d'Agentless Collector, sous Collecte de données, choisissez Afficher et modifier dans la section VMware vCenter.
7. Suivez les instructions Modification des informations d' VMware identification de vCenter pour corriger l'URL et les informations d'identification.

Une fois les problèmes de santé corrigés, le collecteur rétablira la connectivité avec le serveur vCenter, et l'état du collecteur passera à l'état Collecting. Si les problèmes persistent, consultezContacter le AWS support pour des problèmes liés à Agentless Collector.

Les problèmes d'adresse IP et d'informations d'identification sont les causes les plus courantes de dysfonctionnements des collecteurs. Résoudre les problèmes d'adresse IPet Résolution des problèmes liés aux informations d'identification de vCenter peut vous aider à résoudre ces problèmes et à rétablir le bon état d'un collecteur.

Résoudre les problèmes d'adresse IP

Un collecteur peut se retrouver dans un état défectueux si le point de terminaison vCenter fourni lors de la configuration du collecteur est mal formé, non valide ou si le serveur vCenter est actuellement en panne et inaccessible. Dans ce cas, vous recevrez un message d'erreur de connexion.

La procédure suivante peut vous aider à résoudre les problèmes d'adresse IP.

Pour résoudre les problèmes d'adresse IP du collecteur

1. Obtenez l'adresse IP du collecteur sans agent auprès de VMware vCenter.
2. Ouvrez la console Agentless Collector en ouvrant un navigateur Web, puis tapez l'URL suivante dans la barre d'adresse : **`https://`** *`<ip_address>`***`/`**, où ip_address est l'adresse IP du collecteur d'origine. Déployer un collecteur sans agent
3. Choisissez Se connecter, puis entrez le mot de passe du collecteur sans agent, qui a été défini lors de la configuration du collecteur. Configuration du collecteur sans agent
4. Sur la page du tableau de bord d'Agentless Collector, sous Collecte de données, choisissez Afficher et modifier dans la section VMware vCenter.
5. Sur la page des détails de la collecte de VMware données, sous Serveurs vCenter découverts, notez l'adresse IP dans la colonne vCenter.
6. À l'aide d'un outil de ligne de commande distinct tel que `ping` `outraceroute`, vérifiez que le serveur vCenter associé est actif et que l'adresse IP est accessible depuis la machine virtuelle du collecteur.

   - Si l'adresse IP est incorrecte et que le service vCenter est actif, mettez-la à jour dans la console du collecteur et choisissez Next.
   - Si l'adresse IP est correcte mais que le serveur vCenter est inactif, activez-le.
   - Si l'adresse IP est correcte et que le serveur vCenter est actif, vérifiez s'il bloque les connexions réseau en entrée en raison de problèmes de pare-feu. Dans l'affirmative, mettez à jour les paramètres de votre pare-feu pour autoriser les connexions entrantes depuis la machine virtuelle du collecteur.

Résolution des problèmes liés aux informations d'identification de vCenter

Les collecteurs peuvent se retrouver dans un état défectueux si les informations d'identification utilisateur de vCenter fournies lors de la configuration d'un collecteur ne sont pas valides ou s'ils ne disposent pas des privilèges de compte vCenter Read and View.

Si vous rencontrez des problèmes liés aux informations d'identification de vCenter, assurez-vous que les autorisations de lecture et d'affichage de vCenter sont définies pour le groupe System.

Pour plus d'informations sur la modification des informations d'identification de vCenter, consultez. Modification des informations d' VMware identification de vCenter

Résolution des problèmes de transfert de données dans le module de collecte de données de base de données et d'analyse

La page d'accueil du module de collecte de données de base de données et d'analyse dans Agentless Collector affiche l'état de connexion pour Access to DMS et Access to S3. Si aucun accès pour l'accès au DMS et l'accès à S3 s'affichent, configurez le transfert de données. Pour de plus amples informations, veuillez consulter Configuration du transfert de données.

Si vous rencontrez ce problème après avoir configuré le transfert de données, assurez-vous que votre module de collecte de données peut accéder à Internet. Assurez-vous ensuite d'avoir ajouté les DMSCollectorpolitiques Policy et FleetAdvisorS3Policy à votre utilisateur IAM. Pour de plus amples informations, veuillez consulter Déploiement d'Application Discovery Service Agentless Collector.

Si votre module de collecte de données ne parvient pas à se connecter AWS, fournissez un accès sortant aux domaines suivants.

- `dms.`*`your-home-region`*`.amazonaws.com`
- `s3.amazonaws.com`

Résolution des problèmes de connexion dans le module de collecte de données de base de données et d'analyse

Le module de collecte de données de base de données et d'analyse d'Agentless Collector se connecte à vos serveurs LDAP pour découvrir les serveurs du système d'exploitation dans votre environnement de données. Le module de collecte de données se connecte ensuite aux serveurs de votre système d'exploitation pour découvrir les serveurs de base de données et d'analyse. À partir de ces serveurs de base de données, le module de collecte de données collecte des mesures de capacité et de performance. Si votre module de collecte de données ne parvient pas à se connecter à ces serveurs, vérifiez que vous pouvez vous connecter à vos serveurs.

Dans les exemples suivants, remplacez *`replaceable`* les valeurs par les vôtres.

- Pour vérifier que vous pouvez vous connecter à votre serveur LDAP, installez le `ldap-util` package. Pour ce faire, exécutez la commande suivante.

  ```
  sudo apt-get install ldap-util
  ```

  Exécutez ensuite la commande ci-après.

```
ldapsearch -x -D "CN=user,CN=Users,DC=example,DC=com" -w "password" -b
 "dc=example,dc=com" -h
```

- Pour vérifier que vous pouvez vous connecter à un serveur du système d'exploitation Linux, utilisez les commandes suivantes.

  ```
  ssh -i C:\Users\user\private_key.pem -p 22 username@my-linux-host.domain.com
  ```

  Exécutez l'exemple précédent en tant qu'administrateur sous Windows.

  ```
  ssh username@my-linux-host.domain.com
  ```

  Exécutez l'exemple précédent sous Linux.

- Pour vérifier que vous pouvez vous connecter à un serveur du système d'exploitation Windows, utilisez les commandes suivantes.

  ```
  winrs -r:[hostname or ip] -u:username -p:password cmd
  ```

  Exécutez l'exemple précédent en tant qu'administrateur sous Windows.

  ```
  sudo apt install -y winrm
  winrm --user=username --password=password [http or https]://[hostname or ip]:[port]
   "[cmd.exe or any other CLI command]"
  ```

  Exécutez l'exemple précédent sous Linux.

- Pour vérifier que vous pouvez vous connecter à une base de données SQL Server, utilisez les commandes suivantes.

  ```
  sqlcmd -S [hostname or IP] -U username -P 'password'
  SELECT GETDATE() AS sysdate
  ```

- Pour vérifier que vous pouvez vous connecter à une base de données MySQL, utilisez les commandes suivantes.

  ```
  mysql -u username -p 'password' -h [hostname or IP] -P [port]
  SELECT NOW() FROM DUAL
  ```

- Pour vérifier que vous pouvez vous connecter à une base de données Oracle, utilisez les commandes suivantes.

```
sqlplus username/password@[hostname or IP]:port/servicename
SELECT SYSDATE FROM DUAL
```

- Pour vérifier que vous pouvez vous connecter à une base de données PostgreSQL, utilisez les commandes suivantes.

```
psql -U username -h [hostname or IP] -p port -d database
SELECT CURRENT_TIMESTAMP AS sysdate
```

Si vous ne parvenez pas à vous connecter à votre base de données et à vos serveurs d'analyse, assurez-vous de fournir les autorisations requises. Pour de plus amples informations, veuillez consulter Découverte de vos serveurs de base de données.

Support pour les hôtes ESX autonomes

Le collecteur sans agent ne prend pas en charge un hôte ESX autonome. L'hôte ESX doit faire partie de l'instance vCenter Server.

Contacter le AWS support pour des problèmes liés à Agentless Collector

Si vous rencontrez des problèmes avec Application Discovery Service Agentless Collector (Agentless Collector) et que vous avez besoin d'aide, contactez le AWS Support. Vous serez contacté et vous serez peut-être invité à envoyer les journaux du collecteur.

Pour obtenir les journaux de Agentless Collector

1. Obtenez l'adresse IP du collecteur sans agent auprès de VMware vCenter.
2. Ouvrez la console Web de la machine virtuelle du collecteur et connectez-vous en **`ec2-user`** utilisant le mot de passe, **`collector`** comme indiqué dans l'exemple suivant.

```
username: ec2-user
password: collector
```

3. Utilisez la commande suivante pour accéder au dossier journal.

```
cd /var/log/aws/collector
```

4. Compressez les fichiers journaux à l'aide des commandes suivantes.

```
sudo cp /local/agentless_collector/compose.log .
docker inspect $(docker ps --format {{.Names}}) | sudo tee docker_inspect.log >/
dev/null
sudo tar czf logs_$(date '+%d-%m-%Y_%H.%M.%S').tar.gz --exclude='db.mv*' *
```

5. Copiez le fichier journal depuis la machine virtuelle Agentless Collector.

```
scp logs*.tar.gz targetuser@targetaddress
```

6. Transmettez le `tar.gz` fichier au Support aux AWS entreprises.

Importation de données dans Migration Hub

AWS Migration Hub L'importation (Migration Hub) vous permet d'importer les détails de votre environnement sur site directement dans Migration Hub sans utiliser le collecteur sans agent Application Discovery Service (Agentless Collector) ou l'agent de découverte d' AWS applications (Discovery Agent). Vous pouvez ainsi évaluer et planifier la migration directement à partir de vos données importées. Vous pouvez également regrouper vos appareils en tant qu'applications et suivre leur statut de migration.

Cette page décrit les étapes à suivre pour effectuer une demande d'importation. Tout d'abord, vous devez utiliser l'une des deux options suivantes pour préparer les données de votre serveur sur site.

- Utilisez des outils tiers courants pour générer un fichier contenant les données de votre serveur local.
- Téléchargez notre modèle d'importation de valeurs séparées par des virgules (CSV) et remplissez-le avec les données de votre serveur sur site.

Après avoir utilisé l'une des deux méthodes décrites précédemment pour créer votre fichier de données sur site, vous téléchargez le fichier sur Migration Hub à l'aide de la console Migration Hub AWS CLI, ou de l' AWS SDKsune des. Pour plus d'informations sur les deux options, consultezthe section called “Formats d'importation pris en charge”.

Vous pouvez soumettre plusieurs demandes d'importation. Chaque demande est traitée de manière séquentielle. Vous pouvez vérifier le statut de vos demandes d'importation à tout moment, par le biais de la console ou de l'import APIs.

Une fois une requête d'importation terminée, vous pouvez afficher les détails d'enregistrements individuels importés. Affichez les données d'utilisation, les balises et les mappages d'applications directement depuis la console Migration Hub. Si des erreurs se sont produites lors de l'importation, vous pouvez consulter le nombre d'enregistrements réussis ou ayant échoué, ainsi que le détail des erreurs pour chaque enregistrement ayant échoué.

Gestion des erreurs : Un lien est fourni pour télécharger le journal d'erreurs et les fichiers d'enregistrements ayant échoué sous forme de fichiers CSV dans une archive compressée. Utilisez ces fichiers pour soumettre à nouveau votre requête d'importation après correction des erreurs.

Des limites s'appliquent au nombre d'enregistrements importés, de serveurs importés et d'enregistrements supprimés que vous pouvez conserver. Pour de plus amples informations, veuillez consulter AWS Application Discovery Service Quotas.

Formats d'importation pris en charge

Migration Hub prend en charge les formats d'importation suivants.

- RVTools
- Modèle d'importation de Migration Hub

RVTools

Migration Hub prend en charge l'importation d'exportations de VMware vSphere via. RVTools Lorsque vous enregistrez des données depuis RVTools, choisissez d'abord l'option Exporter tout au format csv ou l'option Tout exporter vers Excel, puis compressez le dossier et importez le fichier ZIP dans Migration Hub. Les fichiers suivants sont requis dans le fichier ZIP : vInfo, vNetwork, vCPU, vMemory, vDisk, vPartition, vSource, vTools, vHost, vNIC, VSC_vmk.

Modèle d'importation de Migration Hub

L'importation du Migration Hub vous permet d'importer des données depuis n'importe quelle source. Les données fournies doivent être à un format pris en charge pour un fichier CSV et contenir uniquement les champs pris en charge avec les plages prises en charge par ces champs.

Un astérisque (*) à côté du nom d'un champ d'importation dans le tableau suivant indique qu'il s'agit d'un champ obligatoire. Chaque enregistrement du fichier d'importation doit avoir au moins un ou plusieurs de ces champs obligatoires renseignés pour identifier de manière unique un serveur ou une application. Dans le cas contraire, l'importation d'un enregistrement sans l'un des champs obligatoires échoue.

Un curseur (^) à côté du nom d'un fichier d'importation dans le tableau suivant indique qu'il s'agit d'un fichier en lecture seule si un ServerID est fourni.

> **Note**
>
> Si vous utilisez l'un ou l'autre VMware. MoRefId ou VMWare. VCenterPar exemple, pour identifier un enregistrement, vous devez avoir les deux champs dans le même enregistrement.

Nom de champ d'importation	Description	Exemples
ExternalId*^	Un identifiant personnalisé qui vous permet de marquer chaque enregistrement comme uniques. Par exemple, il ExternalIdpeut s'agir de l'ID d'inventaire du serveur de votre centre de données.	ID d'inventaire 1 Serveur 2 ID CMBD 3
SMBiosIdentifiant^	ID du BIOS du système de gestion (SMBIOS).	
IPAddress*^	Une liste d'adresses IP du serveur séparées par des virgules, entre guillemets.	192.0.0.2 « 10.12.31.233, 10.12.32.11 »
MACAddress*^	Une liste d'adresses MAC du serveur séparées par des virgules, entre guillemets.	00:1B:44:11:3A:B7 « 00-15-E9-2B-99-3C, 00-14-22-01-23-45 »
HostName*^	Le nom d'hôte du serveur. Nous vous recommandons d'utiliser le nom de domaine complet (FQDN) pour cette valeur.	ip-1-2-3-4 localhost.domain
VMware.MoRefId*^	L'ID de référence d'objet géré. Doit être fourni avec un VMware. VCenterIdentifiant.	

Nom de champ d'importation	Description	Exemples
VMware. VCenterIdentifiant*^	Identifiant unique de la machine virtuelle. Doit être fourni avec un VMware. MoRefId.	
CPU. NumberOfProcessors^	Le nombre de CPUs.	4
CPU. NumberOfCores^	Nombre total de cœurs physiques.	8
CPU. NumberOfLogicalCores^	Le nombre total de threads qui peuvent être exécutés simultanément sur tous CPUs les serveurs. Certains CPUs prennent en charge l'exécuti on simultanée de plusieurs threads sur un seul cœur de processeur. Dans ce cas, ce nombre est supérieur au nombre de cœurs (physiques ou virtuels).	16
Nom du système d'exploit ation^	Le nom du système d'exploit ation.	Linux Windows.Hat
Version du système d'exploit ation^	La version du système d'exploitation.	16.04.3 NT 6.2.8
VMware.VMName^	Le nom de la machine virtuelle .	Corp1
BÉLIER. TotalSizeInMB ^	Quantité totale de mémoire RAM disponible sur le serveur, en Mo.	64 128

Nom de champ d'importation	Description	Exemples
BÉLIER. UsedSizeInMB.AVG^	Quantité moyenne de mémoire RAM utilisée sur le serveur, en MO.	64 128
BÉLIER. UsedSizeInMb. Max^	Quantité maximale de mémoire RAM utilisée disponible sur le serveur, en Mo.	64 128
CPU. UsagePct.Moyen^	L'utilisation moyenne de l'UC lorsque l'outil de détection collecte des données.	45 23.9
CPU. UsagePct.Max^	L'utilisation maximale de l'UC lorsque l'outil de détection collecte des données.	55.34 24
DiskReadsPerSecondInKb. moyen^	Le nombre moyen de lectures sur disque par seconde, en Ko.	1159 84506
DiskWritesPerSecondInKb. moyen^	Le nombre moyen d'écritures sur disque par seconde, en Ko.	199 6197
DiskReadsPerSecondInKb. Max^	Le nombre maximal de lectures sur disque par seconde, en Ko.	37892 869962
DiskWritesPerSecondInKb. Max^	Le nombre maximal d'écritur es sur disque par seconde, en Ko.	18436 1808
DiskReadsOpsPerSec ond.Moyen^	Nombre moyen d'opérati ons de lecture de disque par seconde.	45 28

Nom de champ d'importation	Description	Exemples
DiskWritesOpsPerSecond.Moyen^	Nombre moyen d'opérations d'écriture de disque par seconde.	8 3
DiskReadsOpsPerSecond.Max^	Le nombre maximal d'opérations de lecture sur disque par seconde.	1083 176
DiskWritesOpsPerSecond.Max^	Le nombre maximal d'opérations d'écriture sur disque par seconde.	535 71
NetworkReadsPerSecondInKb. moyen^	Le nombre moyen d'opérations de lecture du réseau par seconde, en Ko.	45 28
NetworkWritesPerSecondInKb. moyen^	Le nombre moyen d'opérations d'écriture du réseau par seconde, en Ko.	8 3
NetworkReadsPerSecondInKb. Max^	Le nombre maximal d'opérations de lecture du réseau par seconde, en Ko.	1083 176
NetworkWritesPerSecondInKb. Max^	Le nombre maximal d'opérations d'écriture du réseau par seconde, en Ko.	535 71
Applications	Une liste d'applications séparées par des virgules qui incluent ce serveur, entre guillemets. Cette valeur peut inclure les applications existantes, les and/or nouvelles applications créées lors de l'importation.	Application1 « Application2, Application3 »

Nom de champ d'importation	Description	Exemples
ApplicationWave	La vague de migration pour ce serveur.	
Balises^	Une liste de balises au format nom:valeur séparées par des virgules. **Important** Ne stockez pas d'informations sensibles (comme les données personnelles) dans des balises.	« zone:1, critical:yes » « zone:3, critical:no, zone:1 »
ServerId	L'identifiant du serveur tel qu'il apparaît dans la liste des serveurs Migration Hub.	`d-server-01kk9i6yw waxmp`

Vous pouvez importer des données, même si vous n'avez pas de données renseignées pour tous les champs définis dans le modèle d'importation, tant que chaque enregistrement contient au moins l'un des champs obligatoires. Les doublons sont gérés dans plusieurs requêtes d'importation à l'aide d'une clé interne ou externe correspondante. Si vous remplissez votre propre clé correspondante, `External ID`, ce champ est utilisé uniquement pour identifier et importer les enregistrements. Si aucune clé correspondante n'est spécifiée, l'importation utilise une clé correspondante générée en interne qui est dérivée de certaines colonnes du modèle d'importation. Pour plus d'informations sur cette correspondance, consultez Logique de correspondance pour les serveurs et applications découverts.

Note

L'importation de Migration Hub ne prend en charge aucun champ autre que ceux définis dans le modèle d'importation. Tous les champs personnalisés fournis sont ignorés et ne sont pas importés.

Configuration des autorisations d'importation

Avant de pouvoir importer vos données, assurez-vous que votre utilisateur IAM dispose des autorisations Amazon S3 nécessaires pour télécharger (`s3:PutObject`) votre fichier d'importation sur Amazon S3 et pour lire l'objet (`s3:GetObject`). Vous devez également établir un accès par programmation (pour AWS CLI) ou un accès à la console, en créant une politique IAM et en l'attachant à l'utilisateur IAM qui effectue les importations dans votre compte. AWS

Console Permissions

Utilisez la procédure suivante pour modifier la politique d'autorisation de l'utilisateur IAM qui effectuera des demandes d'importation dans votre AWS compte à l'aide de la console.

Pour modifier les politiques gérées attachées d'un utilisateur

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.
2. Dans le panneau de navigation, choisissez utilisateurs.
3. Choisissez le nom de l'utilisateur dont vous souhaitez modifier la politique d'autorisations.
4. Cliquez sur l'onglet Autorisations, puis sur Ajouter des autorisations.
5. Cliquez sur Attacher directement les stratégies existantes, puis sur Créer une stratégie.

    a. Dans la page Créer une stratégie qui s'ouvre, sélectionnez JSON et collez la stratégie suivante. N'oubliez pas de remplacer le nom de votre compartiment par le nom réel du compartiment dans lequel l'utilisateur IAM va charger les fichiers d'importation.

    JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    },
```

```
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::importBucket"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": ["arn:aws:s3:::importBucket/*"]
    }
  ]
}
```

b. Choisissez Examiner une politique.

c. Donnez un nouveau nom ainsi qu'une description facultative à votre stratégie, avant de passer en revue le résumé de la stratégie.

d. Choisissez Create Policy (Créer une politique).

6. Retournez à la page de la console IAM pour accorder des autorisations à l'utilisateur qui effectuera des demandes d'importation dans votre AWS compte.
7. Actualisez le tableau des stratégies et recherchez le nom de la stratégie que vous venez de créer.
8. Choisissez Suivant : Vérification.
9. Choisissez Ajouter des autorisations.

Maintenant que vous avez ajouté la politique à votre utilisateur IAM, vous êtes prêt à démarrer le processus d'importation.

AWS CLI Permissions

Utilisez la procédure suivante pour créer les politiques gérées nécessaires pour donner à un utilisateur IAM les autorisations nécessaires pour effectuer des demandes d'importation de données à l'aide du AWS CLI.

Pour créer et associer les politiques gérées

1. Utilisez la `aws iam create-policy` AWS CLI commande pour créer une politique IAM avec les autorisations suivantes. N'oubliez pas de remplacer le nom de votre compartiment par le nom réel du compartiment dans lequel l'utilisateur IAM va charger les fichiers d'importation.

   JSON

   ```
   {
     "Version":"2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Action": ["s3:ListBucket"],
         "Resource": ["arn:aws:s3:::importBucket"]
       },
       {
         "Effect": "Allow",
         "Action": [
           "s3:PutObject",
           "s3:GetObject",
           "s3:DeleteObject"
         ],
         "Resource": ["arn:aws:s3:::importBucket/*"]
       }
     ]
   }
   ```

   Pour plus d'informations sur l'utilisation de cette commande, consultez la section create-policy dans le manuel de référence des AWS CLI commandes.

2. Utilisez la `aws iam create-policy` AWS CLI commande pour créer une politique IAM supplémentaire avec les autorisations suivantes.

   JSON

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

```
        {
            "Effect": "Allow",
            "Action": [
                "discovery:ListConfigurations",
                "discovery:CreateApplication",
                "discovery:UpdateApplication",
                "discovery:AssociateConfigurationItemsToApplication",
                "discovery:DisassociateConfigurationItemsFromApplication",
                "discovery:GetDiscoverySummary",
                "discovery:StartImportTask",
                "discovery:DescribeImportTasks",
                "discovery:BatchDeleteImportData"
            ],
            "Resource": "*"
        }
    ]
}
```

3. Utilisez la `aws iam attach-user-policy` AWS CLI commande pour associer les politiques que vous avez créées au cours des deux étapes précédentes à l'utilisateur IAM qui effectuera les demandes d'importation dans votre AWS compte à l'aide du AWS CLI. Pour plus d'informations sur l'utilisation de cette commande, reportez-vous attach-user-policyà la référence des AWS CLI commandes.

Maintenant que vous avez ajouté les politiques à votre utilisateur IAM, vous êtes prêt à démarrer le processus d'importation.

N'oubliez pas que lorsque l'utilisateur IAM télécharge des objets dans le compartiment Amazon S3 que vous avez spécifié, il doit laisser les autorisations par défaut définies pour les objets afin que l'utilisateur puisse lire l'objet.

Chargement de votre fichier d'importation sur Amazon S3

Ensuite, vous devez télécharger votre fichier d'importation au format CSV dans Amazon S3 afin qu'il puisse être importé. Avant de commencer, vous devez disposer d'un compartiment Amazon S3 qui hébergera votre fichier d'importation créé et and/or choisi à l'avance.

Console S3 Upload

Pour télécharger votre fichier d'importation sur Amazon S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment dans lequel vous souhaitez charger votre objet.
3. Choisissez Charger.
4. Dans la boîte de dialogue Charger, choisissez Add files pour choisir le fichier à charger.
5. Choisissez un fichier à charger, puis choisissez Ouvrir.
6. Choisissez Charger.
7. Une fois votre fichier téléchargé, choisissez le nom de l'objet de fichier de données dans le tableau de bord de votre compartiment.
8. Dans l'onglet Présentation de la page des détails de l'objet, copiez l'URL d'objet. Vous en aurez besoin lors de la création de votre requête d'importation.
9. Accédez à la page d'importation de la console Migration Hub comme décrit dansImportation de données. Collez ensuite l'URL de l'objet dans le champ URL de l'objet Amazon S3.

AWS CLI S3 Upload

Pour télécharger votre fichier d'importation sur Amazon S3

1. Ouvrez une fenêtre de terminal et naviguez jusqu'au répertoire dans lequel votre fichier d'importation est enregistré.
2. Entrez la commande suivante :

```
aws s3 cp ImportFile.csv s3://BucketName/ImportFile.csv
```

3. Cela renvoie les résultats suivants :

```
upload: .\ImportFile.csv to s3://BucketName/ImportFile.csv
```

4. Copiez le chemin complet de l'objet Amazon S3 renvoyé. Vous en aurez besoin lorsque vous créerez votre demande d'importation.

Importation de données

Après avoir téléchargé le modèle d'importation depuis la console Migration Hub et l'avoir renseigné avec les données de votre serveur local existant, vous êtes prêt à commencer à importer les données dans Migration Hub. Les instructions suivantes décrivent deux méthodes pour ce faire, soit en utilisant la console, soit en effectuant des appels d'API via le AWS CLI.

Console Import

Lancez l'importation des données sur la page Outils de la console Migration Hub.

Pour démarrer l'importation des données

1. Dans le panneau de navigation, sous Découvrir, choisissez Outils.
2. Si vous ne disposez pas déjà d'un modèle d'importation rempli, vous pouvez télécharger le modèle en choisissant le modèle d'importation dans la zone Importation. Ouvrez le modèle téléchargé et remplissez-le avec vos données de serveur sur site existantes. Vous pouvez également télécharger le modèle d'importation depuis notre compartiment Amazon S3 à l'adresse https://s3.us-west-2.amazonaws.com/templates-7cffcf56-bd96-4b1c-b45b-a5b42f282e46/import_template.csv
3. Pour ouvrir la page Importer, choisissez Importer dans la zone Importer.
4. Sous Nom de l'importation, spécifiez le nom de l'importation.
5. Remplissez le champ URL de l'objet Amazon S3. Pour effectuer cette étape, vous devez télécharger votre fichier de données d'importation sur Amazon S3. Pour de plus amples informations, veuillez consulter Chargement de votre fichier d'importation sur Amazon S3.
6. Choisissez Importation dans la zone inférieure droite. Cela ouvre la page Importations dans laquelle vous pouvez afficher votre importation et son statut répertoriés dans le tableau.

Après avoir suivi la procédure précédente pour démarrer l'importation de vos données, la page Importations affiche les détails de chaque requête d'importation, y compris son état de progression, le délai d'exécution, et le nombre d'enregistrements réussis ou ayant échoué avec la possibilité de télécharger ces enregistrements. À partir de cet écran, vous pouvez également accéder à la page Serveurs sous Découvrir pour afficher les données importées.

Sur la page Serveurs, vous pouvez afficher une liste de tous les serveurs (périphériques) qui sont détectés ainsi que le nom de l'importation. Lorsque vous naviguez depuis la page Importations (historique des importations) en sélectionnant le nom de l'importation indiqué dans la colonne

Nom, vous êtes redirigé vers la page Serveurs où un filtre est appliqué en fonction de l'ensemble de données de l'importation sélectionné. Ensuite, vous ne voyez que les données appartenant à cette importation particulière.

L'archive est au format .zip, et contient deux fichiers : `errors-file` et `failed-entries-file`. Le fichier d'erreurs contient une liste de messages d'erreur associés à chaque ligne ayant échoué et le nom de la colonne associée du fichier de données pour lequel l'importation n'a pas abouti. Vous pouvez utiliser ce fichier pour identifier rapidement où les problèmes se sont produits. Le fichier d'entrées ayant échoué inclut chaque ligne et toutes les colonnes fournies ayant échoué. Vous pouvez apporter les modifications indiquées dans le fichier d'erreurs dans ce fichier et essayez d'importer à nouveau le fichier avec les informations corrigées.

AWS CLI Import

Pour démarrer le processus d'importation de données à partir du AWS CLI, vous AWS CLI devez d'abord l'installer dans votre environnement. Pour plus d'informations, consultez la section Installation de l'interface de ligne de AWS commande dans le guide de AWS Command Line Interface l'utilisateur.

> **Note**
>
> Si vous n'avez pas encore rempli de modèle d'importation, vous pouvez le télécharger depuis notre compartiment Amazon S3 ici : https://s3.us-west-2.amazonaws.com/templates-7cffcf56-bd96-4b1c-b45b-a5b42f282e46/import_template.csv

Pour démarrer l'importation des données

1. Ouvrez une fenêtre de terminal et saisissez la commande suivante :

```
aws discovery start-import-task --import-url s3://BucketName/ImportFile.csv --
name ImportName
```

2. Cette opération crée votre tâche d'importation et renvoie les informations d'état suivantes :

```
{
    "task": {
        "status": "IMPORT_IN_PROGRESS",
        "applicationImportSuccess": 0,
        "serverImportFailure": 0,
```

```
        "serverImportSuccess": 0,
        "name": "ImportName",
        "importRequestTime": 1547682819.801,
        "applicationImportFailure": 0,
        "clientRequestToken": "EXAMPLE1-abcd-1234-abcd-EXAMPLE1234",
        "importUrl": "s3://BucketName/ImportFile.csv",
        "importTaskId": "import-task-EXAMPLE1229949eabfEXAMPLE03862c0"
    }
}
```

Suivi de vos demandes d'importation de Migration Hub

Vous pouvez suivre l'état de vos demandes d'importation du Migration Hub à l'aide de la console ou de l'un des AWS SDKs. AWS CLI

Console Tracking

Dans le tableau de bord des importations de la console Migration Hub, vous trouverez les éléments suivants.

- Nom : nom de la demande d'importation.
- ID d'importation — L'identifiant unique de la demande d'importation.
- Heure d'importation : date et heure de création de la demande d'importation.
- État de l'importation : statut de la demande d'importation. Il peut s'agir de l'une des valeurs suivantes :
  - Importation — Ce fichier de données est en cours d'importation.
  - Importé — L'intégralité du fichier de données a été correctement importée.
  - Importé avec des erreurs : un ou plusieurs enregistrements du fichier de données n'ont pas pu être importés. Pour réparer vos enregistrements ayant échoué, choisissez Télécharger les enregistrements ayant échoué pour votre tâche d'importation, résolvez les erreurs dans le fichier .csv des enregistrements ayant échoué, et importez à nouveau.
  - Échec de l'importation : aucun des enregistrements du fichier de données n'a été importé. Pour réparer vos enregistrements ayant échoué, choisissez Télécharger les enregistrements ayant échoué pour votre tâche d'importation, résolvez les erreurs dans le fichier .csv des enregistrements ayant échoué, et importez à nouveau.
- Enregistrements importés : nombre d'enregistrements d'un fichier de données spécifique qui ont été importés avec succès.

- Enregistrements ayant échoué : nombre d'enregistrements d'un fichier de données spécifique qui n'ont pas été importés.

CLI Tracking

Vous pouvez suivre l'état de vos tâches d'importation à l'aide de la `aws discovery describe-import-tasks` AWS CLI commande.

1. Ouvrez une fenêtre de terminal et saisissez la commande suivante :

```
aws discovery describe-import-tasks
```

2. Cette action renvoie une liste de toutes vos tâches d'importation au format JSON, avec l'état et d'autres informations utiles. Vous pouvez également filtrer les résultats pour renvoyer un sous-ensemble de vos tâches d'importation.

Lors du suivi de vos tâches d'importation, vous pouvez constater que la valeur `serverImportFailure` retournée est supérieure à zéro. Le cas échéant, votre fichier d'importation contient une ou plusieurs entrées qui n'ont pas pu être importées. Cela peut être résolu en téléchargeant votre archive d'enregistrements ayant échoué, en consultant les fichiers qu'elle contient et en effectuant une autre requête d'importation dans le fichier .csv modifié des entrées ayant échoué.

Après la création de votre tâche d'importation, vous pouvez effectuer des actions supplémentaires pour vous aider à gérer et suivre vos données de migration. Par exemple, vous pouvez télécharger une archive d'enregistrements ayant échoué pour une requête spécifique. Pour plus d'informations sur l'utilisation de l'archive d'enregistrements ayant échoué pour résoudre les problèmes d'importation, consultez Résolution des problèmes d'importation ayant échoué.

Afficher et explorer les données découvertes

Application Discovery Service Agentless Collector (Agentless Collector) et AWS Discovery Agent (Discovery Agent) fournissent des données de performance du système basées sur l'utilisation moyenne et maximale. Vous pouvez utiliser les données de performance du système collectées pour établir un coût total de possession (TCO) élevé. Les agents de découverte collectent des données plus détaillées, notamment des séries chronologiques pour les informations sur les performances du système, les connexions réseau entrantes et sortantes et les processus exécutés sur le serveur. Vous pouvez utiliser ces données pour comprendre les dépendances réseau entre les serveurs et regrouper les serveurs connexes en applications afin de planifier la migration.

Dans cette section, vous trouverez des instructions sur la façon d'afficher et d'utiliser les données découvertes par Agentless Collector et Discovery Agent à la fois depuis la console et le AWS CLI.

Rubriques

Afficher les données collectées à l'aide de la console Migration Hub

Pour Application Discovery Service Agentless Collector (Agentless Collector) et AWS Discovery Agent (Discovery Agent), une fois le processus de collecte de données lancé, vous pouvez utiliser la console pour consulter les données collectées sur vos serveurs et. VMs Les données apparaissent dans la console environ 15 minutes après le début de la collecte des données. Vous pouvez également afficher ces données au format CSV en exportant les données collectées en effectuant des appels d'API à l'aide du AWS CLI.

Pour consulter les données collectées sur les serveurs découverts dans la console, suivez les étapes décrites dansAffichage des serveurs dans la AWS Migration Hub console. Pour en savoir plus sur l'utilisation de la console pour afficher, trier et étiqueter les serveurs découverts par vos Agentless Collectors ou Discovery Agents, consultezDécouvrir des données à l'aide de la AWS Migration Hub console.

Le module de collecte de données de base de données et d'analyse Agentless Collector télécharge les données collectées dans le compartiment Amazon S3. Vous pouvez consulter les données de ce compartiment dans la console AWS DMS. Pour consulter les données collectées sur les serveurs de

base de données et d'analyse découverts, suivez les étapes décrites dansAfficher les données que vous avez collectées.

Logique de correspondance pour les serveurs et applications découverts

AWS Application Discovery Service (Application Discovery Service) possède une logique de correspondance intégrée qui identifie le moment où les serveurs découverts correspondent à des entrées existantes. Lorsque cette logique trouve une correspondance, elle met à jour les informations du serveur détecté déjà existant avec de nouvelles valeurs.

Cette logique de correspondance gère les serveurs dupliqués provenant de sources multiples, notamment l'importation AWS Migration Hub (Migration Hub), l'application Discovery Service Agentless Collector (Agentless Collector), AWS l'Application Discovery Agent (Discovery Agent) et d'autres outils de migration. Pour plus d'informations sur l'importation du Migration Hub, consultez la section Migration Hub Import.

Lorsque la détection du serveur se produit, chaque entrée est confrontée aux enregistrements précédemment importés afin de s'assurer que le serveur importé n'existe pas déjà. Si aucune correspondance n'est trouvée, un nouvel enregistrement est créé et un nouvel identifiant de serveur unique est attribué. Si une correspondance est trouvée, une nouvelle entrée est créée, mais elle se voit attribuer le même identifiant de serveur unique en tant que serveur existant. Lorsque vous consultez ce serveur dans la console Migration Hub, vous ne trouvez qu'une seule entrée unique pour le serveur.

Les attributs du serveur associés à cette entrée sont fusionnés pour afficher les valeurs d'attribut d'un enregistrement précédemment disponible, ainsi que de l'enregistrement nouvellement importé. S'il existe plus d'une valeur pour un attribut de serveur donné à partir de plusieurs sources (par exemple, deux valeurs différentes pour la `Total RAM` associée à un serveur donné détecté à l'aide de l'importation mais aussi par l'agent de détection), la valeur la plus récemment mise à jour est affichée dans l'enregistrement correspondant du serveur.

Champs correspondants

Les champs suivants sont utilisés pour mettre en correspondance les serveurs lorsque des outils de détection sont utilisés.

- ExternalId— Il s'agit du champ principal utilisé pour faire correspondre les serveurs. Si la valeur de ce champ est identique à celle d'une autre entrée, Application Discovery Service fait correspondre les deux entrées, que les autres champs correspondent ou non. `ExternalId`

- IPAddress
- HostName
- MacAddress
- VMware. MoRefIdet VMware. vCenterId — Ces deux valeurs doivent être identiques aux champs respectifs d'une autre entrée pour qu'Application Discovery Service puisse établir une correspondance.

Exploration des données dans Amazon Athena

L'exploration des données dans Amazon Athena vous permet d'analyser les données collectées à partir de tous les serveurs locaux découverts par Discovery Agent en un seul endroit. Une fois que l'exploration des données dans Amazon Athena est activée depuis la console Migration Hub (ou à l'aide de l' StartContinousExport API) et que la collecte de données pour les agents est activée, les données collectées par les agents sont automatiquement stockées dans votre compartiment S3 à intervalles réguliers. Pour de plus amples informations, veuillez consulter Exploration des données dans Amazon Athena.

L'exploration des données dans Amazon Athena vous permet d'analyser les données collectées à partir de tous les serveurs locaux découverts par les Discovery Agents en un seul endroit. Une fois que l'exploration des données dans Amazon Athena est activée depuis la console Migration Hub (ou à l'aide de l' StartContinousExport API) et que la collecte de données pour les agents est activée, les données collectées par les agents sont automatiquement stockées dans votre compartiment S3 à intervalles réguliers.

Vous pouvez ensuite visiter Amazon Athena pour exécuter des requêtes prédéfinies afin d'analyser les performances chronologiques du système pour chaque serveur, le type de processus exécutés sur chaque serveur et les dépendances réseau entre les différents serveurs. En outre, vous pouvez écrire vos propres requêtes personnalisées à l'aide d'Amazon Athena, télécharger des sources de données existantes supplémentaires, telles que les exportations de bases de données de gestion des configurations (CMDB), et associer les serveurs découverts aux applications métier réelles. Vous pouvez également intégrer la base de données Athena à Amazon Quick pour visualiser les résultats des requêtes et effectuer des analyses supplémentaires.

Les rubriques de cette section décrivent les manières dont vous pouvez utiliser vos données dans Athena pour évaluer et planifier la migration de votre environnement local vers celui-ci. AWS

Activer l'exploration des données dans Amazon Athena

L'exploration des données dans Amazon Athena est activée en activant l'exportation continue à l'aide de la console Migration Hub ou d'un appel d'API depuis le. AWS CLI Vous devez activer l'exploration des données avant de pouvoir voir et commencer à explorer les données que vous avez découvertes dans Amazon Athena.

Lorsque vous activez l'exportation continue, le rôle lié au service `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` est automatiquement utilisé par votre compte. Pour de plus amples informations sur ce rôle lié à un service, consultez Autorisations de rôle liées à un service pour Application Discovery Service.

Les instructions suivantes indiquent comment activer l'exploration des données dans Amazon Athena à l'aide de la console et du. AWS CLI

Turn on with the console

L'exploration des données dans Amazon Athena est activée par l'activation implicite de l'exportation continue lorsque vous choisissez « Démarrer la collecte de données » ou que vous cliquez sur le bouton intitulé « Exploration des données dans Amazon Athena » sur la page des collecteurs de données de la console Migration Hub.

Pour activer l'exploration des données dans Amazon Athena depuis la console

1. Dans le volet de navigation, choisissez Data Collectors (Collecteurs de données).
2. Choisissez l'onglet Agents.
3. Choisissez Démarrer la collecte de données ou, si la collecte de données est déjà activée, cliquez sur le bouton Exploration des données dans Amazon Athena.
4. Dans la boîte de dialogue générée à partir de l'étape précédente, cochez la case acceptant les coûts associés et choisissez Continue (Continuer) ou Enable (Activer).

> **Note**
>
> Vos agents fonctionnent désormais en mode « exportation continue », ce qui vous permettra de consulter et d'utiliser les données que vous avez découvertes dans Amazon Athena. La première fois que cette option est activée, l'affichage de vos données dans Amazon Athena peut prendre jusqu'à 30 minutes.

Enable with the AWS CLI

L'exploration des données dans Amazon Athena est activée par l'activation explicite de l'exportation continue via un appel d'API depuis le. AWS CLI Pour ce faire, AWS CLI il faut d'abord l'installer dans votre environnement.

Pour installer AWS CLI et activer l'exploration des données dans Amazon Athena

1. Installez le AWS CLI pour votre système d'exploitation (Linux, macOS ou Windows). Consultez le guide de AWS Command Line Interface l'utilisateur pour obtenir des instructions.
2. Ouvrez l'invite de commande (Windows) ou le Terminal (Linux ou macOS).
   a. Tapez `aws configure` et appuyez sur Entrer.
   b. Entrez votre identifiant de clé d' AWS accès et votre clé d'accès AWS secrète.
   c. Saisissez `us-west-2` pour Default region name (Nom de la région par défaut).
   d. Saisissez `text` pour Default output format (Format de sortie par défaut).
3. Saisissez la commande suivante :

```
aws discovery start-continuous-export
```

> **Note**
>
> Vos agents fonctionnent désormais en mode « exportation continue », ce qui vous permettra de consulter et d'utiliser les données que vous avez découvertes dans Amazon Athena. La première fois que cette option est activée, l'affichage de vos données dans Amazon Athena peut prendre jusqu'à 30 minutes.

Exploration des données directement dans Amazon Athena

Après avoir activé l'exploration des données dans Amazon Athena, vous pouvez commencer à explorer et à utiliser les données actuelles détaillées découvertes par vos agents en interrogeant les données directement dans Athena. Vous pouvez utiliser ces données pour générer des feuilles de calcul, exécuter une analyse des coûts, porter la requête vers un programme de visualisation pour établir un diagramme des dépendances réseau, etc.

Les instructions suivantes expliquent comment explorer les données de votre agent directement dans la console Athena. Si vous n'avez aucune donnée dans Athena ou si vous n'avez pas activé l'exploration des données dans Amazon Athena, une boîte de dialogue vous invite à activer l'exploration des données dans Amazon Athena, comme expliqué dans. Activer l'exploration des données dans Amazon Athena

Pour explorer les données découvertes par les agents directement dans Athena

1. Dans la AWS Migration Hub console, choisissez Servers dans le volet de navigation.
2. Pour ouvrir la console Amazon Athena, choisissez Explorer les données dans Amazon Athena.
3. Dans la page Query Editor (Éditeur de requête), dans le volet de navigation sous Database (Base de données), assurez-vous que application_discovery_service_database est sélectionné.

   > **Note**
   >
   > Sous Tables, les tables suivantes représentent les jeux de données regroupés par les agents.
   >
   > - os_info_agent
   > - network_interface_agent
   > - sys_performance_agent
   > - processes_agent
   > - inbound_connection_agent
   > - outbound_connection_agent
   > - id_mapping_agent

4. Interrogez les données dans la console Amazon Athena en écrivant et en exécutant des requêtes SQL dans l'éditeur de requêtes Athena. Par exemple, vous pouvez utiliser la requête suivante pour afficher toutes les adresses IP de serveur découvertes.

   ```
   SELECT * FROM network_interface_agent;
   ```

   Pour d'autres exemples de requête, veuillez consulter Utilisation de requêtes prédéfinies dans Amazon Athena.

Visualisation des données Amazon Athena

Pour visualiser vos données, une requête peut être portée vers un programme de visualisation tel qu'Amazon Quick ou d'autres outils de visualisation open source tels que Cytoscape, yEd ou Gelphi. Utilisez ces outils pour afficher des diagrammes réseau, des tableaux récapitulatifs et d'autres représentations graphiques. Lorsque cette méthode est utilisée, vous vous connectez à Athena via le programme de visualisation afin qu'elle puisse accéder à vos données collectées en tant que source pour produire la visualisation.

Pour visualiser vos données Amazon Athena à l'aide de Quick

1. Connectez-vous à Amazon Quick.
2. Choisissez Connect to another data source or upload a file (Se connecter à une autre source de données ou charger un fichier).
3. Choisissez Athéna. La boîte de dialogue de la source de données New Athena s'affiche.
4. Entrez un nom dans le champ Data source name (Nom de la source de données).
5. Choisissez Create data source.
6. Sélectionnez le gents-servers-os tableau A dans la boîte de dialogue Choisissez votre table, puis sélectionnez Sélectionner.
7. Dans la boîte de dialogue Finish dataset creation (Terminer la création d'un ensemble de données), sélectionnez Import to SPICE for quicker analytics (Importer vers SPICE pour des analyses plus rapides), puis choisissez Visualize (Visualiser).

   Votre visualisation est rendue.

Utilisation de requêtes prédéfinies dans Amazon Athena

Cette section contient un ensemble de requêtes prédéfinies qui exécutent des cas d'utilisation standard, comme l'analyse du coût total de possession et la visualisation du réseau. Vous pouvez utiliser ces requêtes en l'état ou les modifier en fonction de vos besoins.

Pour utiliser une requête prédéfinie

1. Dans la AWS Migration Hub console, choisissez Servers dans le volet de navigation.
2. Pour ouvrir la console Amazon Athena, choisissez Explorer les données dans Amazon Athena.

3. Dans la page Query Editor (Éditeur de requête), dans le volet de navigation sous Database (Base de données), assurez-vous que application_discovery_service_database est sélectionné.
4. Choisissez le signe plus (+) dans l'éditeur de requête pour créer un onglet pour une nouvelle requête.
5. Copiez l'une des requêtes à partir de Requêtes prédéfinies.
6. Collez la requête dans le volet de requête du nouvel onglet de requête que vous venez de créer.
7. Choisissez Run Query.

Requêtes prédéfinies

Choisissez un titre pour afficher les informations sur la requête.

Obtenir les adresses IP et les noms d'hôte pour les serveurs

Cette fonction d'assistant de vue récupère les adresses IP et les noms d'hôte d'un serveur donné. Vous pouvez utiliser cette vue dans d'autres requêtes. Pour plus d'informations sur la création d'une vue, consultez CREATE VIEW dans le guide de l'utilisateur d'Amazon Athena.

```
CREATE OR REPLACE VIEW hostname_ip_helper AS
SELECT DISTINCT
  "os"."host_name"
, "nic"."agent_id"
, "nic"."ip_address"
FROM
  os_info_agent os
, network_interface_agent nic
WHERE ("os"."agent_id" = "nic"."agent_id");
```

Identifiez les serveurs avec ou sans agents

Cette requête peut vous aider à effectuer une validation des données. Si vous avez déployé des agents sur un certain nombre de serveurs dans votre réseau, vous pouvez utiliser cette requête pour trouver s'il existe d'autres serveurs dans votre réseau dans lesquels aucun agent n'a été déployé. Dans cette requête, nous allons examiner le trafic réseau entrant et sortant, et filtrer le trafic pour les adresses IP privées uniquement. Autrement dit, les adresses IP commençant par `192`, `10`, ou `172`.

```
SELECT DISTINCT "destination_ip" "IP Address" ,
         (CASE
    WHEN (
```

```
    (SELECT "count"(*)
    FROM network_interface_agent
    WHERE ("ip_address" = "destination_ip") ) = 0) THEN
        'no'
        WHEN (
        (SELECT "count"(*)
        FROM network_interface_agent
        WHERE ("ip_address" = "destination_ip") ) > 0) THEN
            'yes' END) "agent_running"
    FROM outbound_connection_agent
WHERE ((("destination_ip" LIKE '192.%')
        OR ("destination_ip" LIKE '10.%'))
        OR ("destination_ip" LIKE '172.%'))
UNION
SELECT DISTINCT "source_ip" "IP ADDRESS" ,
         (CASE
    WHEN (
    (SELECT "count"(*)
    FROM network_interface_agent
    WHERE ("ip_address" = "source_ip") ) = 0) THEN
        'no'
        WHEN (
        (SELECT "count"(*)
        FROM network_interface_agent
        WHERE ("ip_address" = "source_ip") ) > 0) THEN
            'yes' END) "agent_running"
    FROM inbound_connection_agent
WHERE ((("source_ip" LIKE '192.%')
        OR ("source_ip" LIKE '10.%'))
        OR ("source_ip" LIKE '172.%'));
```

Analyser les données de performance du système pour les serveurs dotés d'agents

Vous pouvez utiliser cette requête pour analyser les performances système et le modèle d'utilisation des données de vos serveurs sur site dans lesquels des agents ont été installés. La requête associe la table `system_performance_agent` avec la table `os_info_agent` pour identifier le nom d'hôte de chaque serveur. Cette requête renvoie les données d'utilisation des séries chronologiques (à intervalles de 15 minutes) pour tous les serveurs dans lesquels des agents sont en cours d'exécution.

```
SELECT "OS"."os_name" "OS Name" ,
    "OS"."os_version" "OS Version" ,
    "OS"."host_name" "Host Name" ,
     "SP"."agent_id" ,
```

```
    "SP"."total_num_cores" "Number of Cores" ,
    "SP"."total_num_cpus" "Number of CPU" ,
    "SP"."total_cpu_usage_pct" "CPU Percentage" ,
    "SP"."total_disk_size_in_gb" "Total Storage (GB)" ,
    "SP"."total_disk_free_size_in_gb" "Free Storage (GB)" ,
    ("SP"."total_disk_size_in_gb" - "SP"."total_disk_free_size_in_gb") "Used
 Storage" ,
    "SP"."total_ram_in_mb" "Total RAM (MB)" ,
    ("SP"."total_ram_in_mb" - "SP"."free_ram_in_mb") "Used RAM (MB)" ,
    "SP"."free_ram_in_mb" "Free RAM (MB)" ,
    "SP"."total_disk_read_ops_per_sec" "Disk Read IOPS" ,
    "SP"."total_disk_bytes_written_per_sec_in_kbps" "Disk Write IOPS" ,
    "SP"."total_network_bytes_read_per_sec_in_kbps" "Network Reads (kbps)" ,
    "SP"."total_network_bytes_written_per_sec_in_kbps" "Network Write (kbps)"
FROM "sys_performance_agent" "SP" , "OS_INFO_agent" "OS"
WHERE ("SP"."agent_id" = "OS"."agent_id") limit 10;
```

Suivez les communications sortantes entre les serveurs en fonction du numéro de port et des détails du processus

Cette requête permet d'obtenir les détails relatifs au trafic sortant pour chaque service, ainsi que le numéro de port et les détails du processus.

Avant d'exécuter la requête, si vous ne l'avez pas déjà fait, vous devez créer la table `iana_service_ports_import` qui contient la base de données de registre des ports IANA téléchargée depuis IANA. Pour plus d'informations sur la création de cette table, veuillez consulter Création de la table d'importation du registre des ports IANA.

Une fois la table `iana_service_ports_import` créée, créez deux fonctions d'assistant de vue pour suivre le trafic sortant. Pour plus d'informations sur la création d'une vue, consultez CREATE VIEW dans le guide de l'utilisateur d'Amazon Athena.

Pour créer des fonctions d'assistant de suivi sortant

1. Ouvrez la console à l'adresse https://console.aws.amazon.com/athena/.
2. Créez la `valid_outbound_ips_helper` vue à l'aide de la fonction d'assistance suivante qui répertorie toutes les adresses IP de destination sortantes distinctes.

   ```
   CREATE OR REPLACE VIEW valid_outbound_ips_helper AS
   SELECT DISTINCT "destination_ip"
   FROM outbound_connection_agent;
   ```

3. Créez la vue `outbound_query_helper` à l'aide de la fonction d'assistant suivante, qui détermine la fréquence de communication pour le trafic sortant.

```
CREATE OR REPLACE VIEW outbound_query_helper AS
SELECT "agent_id" ,
         "source_ip" ,
         "destination_ip" ,
         "destination_port" ,
         "agent_assigned_process_id" ,
         "count"(*) "frequency"
FROM outbound_connection_agent
WHERE (("ip_version" = 'IPv4')
        AND ("destination_ip" IN
    (SELECT *
    FROM valid_outbound_ips_helper )))
GROUP BY  "agent_id", "source_ip", "destination_ip", "destination_port",
 "agent_assigned_process_id";
```

4. Après avoir créé la table `iana_service_ports_import` et vos deux fonctions d'assistant, vous pouvez exécuter la requête suivante pour obtenir les détails relatifs au trafic sortant pour chaque service, ainsi que le numéro de port et les détails de traitement.

```
SELECT hip1.host_name "Source Host Name",
         outbound_connections_results0.source_ip "Source IP Address",
         hip2.host_name "Destination Host Name",
         outbound_connections_results0.destination_ip "Destination IP Address",
         outbound_connections_results0.frequency "Connection Frequency",
         outbound_connections_results0.destination_port "Destination Communication
 Port",
         outbound_connections_results0.servicename "Process Service Name",
         outbound_connections_results0.description "Process Service Description"
FROM
    (SELECT DISTINCT o.source_ip,
         o.destination_ip,
         o.frequency,
         o.destination_port,
         ianap.servicename,
         ianap.description
    FROM outbound_query_helper o, iana_service_ports_import ianap
    WHERE o.destination_port = TRY_CAST(ianap.portnumber AS integer)) AS
 outbound_connections_results0 LEFT OUTER
JOIN hostname_ip_helper hip1
    ON outbound_connections_results0.source_ip = hip1.ip_address LEFT OUTER
```

```
JOIN hostname_ip_helper hip2
    ON outbound_connections_results0.destination_ip = hip2.ip_address
```

Suivez les communications entrantes entre les serveurs en fonction du numéro de port et des détails du processus

Cette requête permet d'obtenir des informations sur le trafic entrant pour chaque service, ainsi que le numéro de port et les détails du processus.

Avant d'exécuter cette requête, si vous ne l'avez pas déjà fait, vous devez créer la table `iana_service_ports_import` qui contient la base de données de registre des ports IANA téléchargée depuis IANA. Pour plus d'informations sur la création de cette table, veuillez consulter Création de la table d'importation du registre des ports IANA.

Une fois la table `iana_service_ports_import` créée, créez deux fonctions d'assistant de vue pour le suivi du trafic entrant. Pour plus d'informations sur la création d'une vue, consultez CREATE VIEW dans le guide de l'utilisateur d'Amazon Athena.

Pour créer des fonctions d'assistant de suivi d'importation

1. Ouvrez la console à l'adresse https://console.aws.amazon.com/athena/.
2. Créez la vue `valid_inbound_ips_helper` à l'aide de la fonction d'assistant suivante, qui répertorie toutes les adresses IP source entrantes distinctes.

   ```
   CREATE OR REPLACE VIEW valid_inbound_ips_helper AS
   SELECT DISTINCT "source_ip"
   FROM inbound_connection_agent;
   ```

3. Créez la vue `inbound_query_helper` à l'aide de la fonction d'assistant suivante, qui détermine la fréquence de communication pour le trafic entrant.

   ```
   CREATE OR REPLACE VIEW inbound_query_helper AS
   SELECT "agent_id" ,
            "source_ip" ,
            "destination_ip" ,
            "destination_port" ,
            "agent_assigned_process_id" ,
            "count"(*) "frequency"
   FROM inbound_connection_agent
   WHERE (("ip_version" = 'IPv4')
   ```

```
        AND ("source_ip" IN
    (SELECT *
    FROM valid_inbound_ips_helper )))
GROUP BY  "agent_id", "source_ip", "destination_ip", "destination_port",
 "agent_assigned_process_id";
```

4. Maintenant que vous disposez de la table `iana_service_ports_import` et de vos deux fonctions d'assistant, vous pouvez exécuter la requête suivante pour obtenir les détails sur le trafic entrant pour chaque service, ainsi que le numéro de port et les détails de traitement.

```
SELECT hip1.host_name "Source Host Name",
         inbound_connections_results0.source_ip "Source IP Address",
         hip2.host_name "Destination Host Name",
         inbound_connections_results0.destination_ip "Destination IP Address",
         inbound_connections_results0.frequency "Connection Frequency",
         inbound_connections_results0.destination_port "Destination Communication
 Port",
         inbound_connections_results0.servicename "Process Service Name",
         inbound_connections_results0.description "Process Service Description"
FROM
    (SELECT DISTINCT i.source_ip,
         i.destination_ip,
         i.frequency,
         i.destination_port,
         ianap.servicename,
         ianap.description
    FROM inbound_query_helper i, iana_service_ports_import ianap
    WHERE i.destination_port = TRY_CAST(ianap.portnumber AS integer)) AS
 inbound_connections_results0 LEFT OUTER
JOIN hostname_ip_helper hip1
    ON inbound_connections_results0.source_ip = hip1.ip_address LEFT OUTER
JOIN hostname_ip_helper hip2
    ON inbound_connections_results0.destination_ip = hip2.ip_address
```

Identifiez le logiciel en cours d'exécution à partir du numéro de port

Cette requête identifie le logiciel en cours d'exécution en fonction des numéros de port.

Avant d'exécuter cette requête, si vous ne l'avez pas déjà fait, vous devez créer la table `iana_service_ports_import` qui contient la base de données de registre des ports IANA téléchargée depuis IANA. Pour plus d'informations sur la création de cette table, veuillez consulter Création de la table d'importation du registre des ports IANA.

La requête suivante peut être utilisée pour identifier le logiciel en cours d'exécution en fonction des numéros de port.

```
SELECT o.host_name "Host Name",
       ianap.servicename "Service",
       ianap.description "Description",
       con.destination_port,
       con.cnt_dest_port "Destination Port Count"
FROM   (SELECT agent_id,
               destination_ip,
               destination_port,
               Count(destination_port) cnt_dest_port
        FROM   inbound_connection_agent
        GROUP  BY agent_id,
                  destination_ip,
                  destination_port) con,
       (SELECT agent_id,
               host_name,
               Max("timestamp")
        FROM   os_info_agent
        GROUP  BY agent_id,
                  host_name) o,
       iana_service_ports_import ianap
WHERE  ianap.transportprotocol = 'tcp'
       AND con.destination_ip NOT LIKE '172%'
       AND con.destination_port = ianap.portnumber
       AND con.agent_id = o.agent_id
ORDER BY cnt_dest_port DESC;
```

Création de la table d'importation du registre des ports IANA

Certaines des requêtes prédéfinies nécessitent une table nommée `iana_service_ports_import` qui contient des informations téléchargées depuis Internet Assigned Numbers Authority (IANA).

Pour créer la table iana_service_ports_import

1. Téléchargez le fichier CSV de la base de données de registre de ports IANA à partir de Service Name and Transport Protocol Port Number Registry sur iana.org.
2. Téléchargez le fichier sur Amazon S3. Pour plus d'informations, consultez Comment charger des fichiers ou dossiers vers un compartiment S3 ?.

3. Créez une nouvelle table dans Athéna nommée. `iana_service_ports_import` Pour obtenir des instructions, consultez la section Créer une table dans le guide de l'utilisateur d'Amazon Athena. Dans l'exemple suivant, vous devez remplacer `my_bucket_name` par le nom du compartiment S3 dans lequel vous avez téléchargé le fichier CSV à l'étape précédente.

```
CREATE EXTERNAL TABLE IF NOT EXISTS iana_service_ports_import (
         ServiceName STRING,
         PortNumber INT,
         TransportProtocol STRING,
         Description STRING,
         Assignee STRING,
         Contact STRING,
         RegistrationDate STRING,
         ModificationDate STRING,
         Reference STRING,
         ServiceCode STRING,
         UnauthorizedUseReported STRING,
         AssignmentNotes STRING
)
ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.lazy.LazySimpleSerDe'
WITH SERDEPROPERTIES (
  'serialization.format' = ',',
  'quoteChar' = '"',
  'field.delim' = ','
) LOCATION 's3://my_bucket_name/'
TBLPROPERTIES ('has_encrypted_data'='false',"skip.header.line.count"="1");
```

Découvrir des données à l'aide de la AWS Migration Hub console

AWS Application Discovery Service (Application Discovery Service) est intégré à AWS Migration Hub (Migration Hub) et les clients peuvent consulter et gérer leurs collecteurs de données, leurs serveurs et leurs applications au sein de Migration Hub. Lorsque vous utilisez la console Application Discovery Service, vous êtes redirigé vers la console Migration Hub. L'utilisation de la console Migration Hub ne nécessite aucune étape ou configuration supplémentaire de votre part.

Dans cette section, vous découvrirez comment gérer et surveiller Application Discovery Service Agentless Collector (Agentless Collector) et AWS Application Discovery Agent (Discovery Agent) à l'aide de la console.

Rubriques

Affichage des données dans le tableau de bord AWS Migration Hub de la console

Pour afficher le tableau de bord principal, choisissez Dashboard dans le volet de navigation de la console AWS Migration Hub (Migration Hub). Dans le tableau de bord principal de Migration Hub, vous pouvez consulter des statistiques de haut niveau sur les serveurs, les applications et les collecteurs de données tels que Application Discovery Service Agentless Collector (Agentless Collector) et AWS Application Discovery Agent (Discovery Agent).

Le tableau de bord principal recueille les données des tableaux de bord Discover et Migrate dans un emplacement central. Il comporte quatre volets d'état et d'informations, ainsi qu'une liste de liens pour

accès rapide. À l'aide des volets, vous pouvez afficher un état résumé de vos dernières applications mises à jour. Vous pouvez également obtenir un accès rapide à l'une de vos applications, une vue d'ensemble des applications dans différents états et suivre la progression de la migration au fil du temps.

Pour afficher le tableau de bord principal, choisissez Tableau de bord dans le volet de navigation situé sur le côté gauche de la page d'accueil de la console Migration Hub.

Démarrage et arrêt des collecteurs de données dans la AWS Migration Hub console

Application Discovery Service Agentless Collector (Agentless Collector) et AWS Application Discovery Agent (Discovery Agent) sont les outils de collecte de données utilisés par AWS Application Discovery Service (Application Discovery Service) pour vous aider à découvrir votre infrastructure existante. Les étapes suivantes expliquent comment télécharger et déployer ces outils de collecte de données de découverte, Déployer un collecteur sans agent etAWS Agent de découverte d'applications.

Ces outils de collecte de données stockent leurs données dans le référentiel du Service de découverte d'applications, fournissant des détails sur chaque serveur et les processus qui y sont exécutés. Lorsque l'un de ces outils est déployé, vous pouvez démarrer, arrêter et consulter les données collectées depuis la console AWS Migration Hub (Migration Hub).

Une fois l'agent de découverte d' AWS applications (agent de découverte) déployé, vous pouvez démarrer ou arrêter le processus de collecte de données sur la page Data Collectors de la console AWS Migration Hub (Migration Hub).

Pour démarrer ou arrêter les outils de collecte de données

1. À l'aide de votre AWS compte, 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, sous Discover, sélectionnez Data collectors.
3. Choisissez l'onglet Agents.
4. Cochez la case de l'outil de collecte que vous voulez démarrer ou arrêter.
5. Choisissez Start data collection (Démarrer la collecte des données) ou Stop data collection (Arrêter la collecte des données).

Tri des collecteurs de données dans la AWS Migration Hub console

Si vous avez déployé de nombreux collecteurs de données, vous pouvez trier la liste affichée des collecteurs déployés sur la page Collecteurs de données de la console. Vous triez la liste en appliquant des filtres dans la barre de recherche. Vous pouvez rechercher et filtrer sur la plupart des critères spécifiés dans la liste Data Collectors (Collecteurs de données).

Le tableau suivant indique les critères de recherche que vous pouvez utiliser pour les agents, notamment les opérateurs, les valeurs et une définition des valeurs.

Critère de recherche	Opérateur	Valeur : Définition
ID de l'agent	==	Tout identifiant d'agent sélectionné dans la liste préremplie à partir de laquelle un outil de collecte est installé.
Hostname	== !=	Pour les agents, n'importe quel nom d'hôte sélectionné à partir de la liste préremplie des hôtes où un agent est installé.
État de la collecte	== !=	Démarré : les données sont collectées et envoyées à Application Discovery Service Start scheduled : le démarrage de la collecte des données est programmé. Les données seront envoyées à Applicati on Discovery Service lors du prochain ping, et le statut passera à Started. Arrêté : les données ne sont ni collectées ni envoyées à Application Discovery Service.

Critère de recherche	Opérateur	Valeur : Définition
		Stop scheduled : l'arrêt de la collecte des données est programmé. Les données cesseront d'être envoyées à Application Discovery Service lors du prochain ping, et le statut passera à Arrêté.
Santé	== !=	Healthy : la collecte des données n'est pas activée. L'outil fonctionne normaleme nt. Unhealthy : l'outil est dans un état d'erreur. Les données ne sont pas collectées ou rapportées. Unknown : aucune connexion établie sur une heure. Shutdown : l'outil a dernièrem ent communiqué un message « shutting down (arrêt) » en raison d'un arrêt du système, du service ou d'un démon. S'il se produit un redémarrage ou une mise à niveau de l'outil, le statut est modifié en un autre état lors du premier cycle de création de rapports. Exécution : la collecte des données est activée. L'outil fonctionne normalement.

Critère de recherche	Opérateur	Valeur : Définition
Adresse IP	== !=	Toute adresse IP sélectionnée dans la liste préremplie où un outil de collecte est installé.

Le tableau suivant indique les critères de recherche que vous pouvez utiliser pour les collecteurs sans agent, notamment les opérateurs, les valeurs et une définition des valeurs.

Critère de recherche	Opérateur	Valeur : Définition
ID	==	Tout identifiant de collecteur sans agent sélectionné dans la liste préremplie à partir de laquelle un outil de collecte est installé.
Hostname	== !=	Pour les collecteurs sans agent, tout nom d'hôte sélectionné dans la liste préremplie des hôtes sur lesquels un collecteur sans agent est installé.
Statut	== !=	Collecte de données : la collecte de données est activée. L'outil fonctionne normalement. Prêt à être configuré : la collecte de données n'est pas activée. L'outil fonctionne normalement. Nécessite de l'attention : l'outil est dans un état d'erreur

Critère de recherche	Opérateur	Valeur : Définition
		et nécessite une attention particulière. Unknown : aucune connexion établie sur une heure. Arrêt : l'outil a indiqué pour la dernière fois qu'il s'était « arrêté » en raison de l'arrêt d'un système, d'un service ou d'un démon. S'il se produit un redémarrage ou une mise à niveau de l'outil, le statut est modifié en un autre état lors du premier cycle de création de rapports.
Adresse IP	== !=	Toute adresse IP sélectionnée dans la liste préremplie où un outil de collecte est installé.

Pour trier les collecteurs de données en appliquant les filtres de recherche

1. À l'aide de votre AWS compte, 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, sous Discover, sélectionnez Data Collectors.
3. Choisissez l'onglet Collecteurs sans agent ou Agents.
4. Cliquez dans la barre de recherche et sélectionnez un critère de recherche dans la liste.
5. Choisissez un opérateur dans la liste suivante.
6. Choisissez une valeur dans la dernière liste.

Affichage des serveurs dans la AWS Migration Hub console

La page Serveurs fournit les données relatives à la configuration du système et aux performances de chaque instance de serveur connue des outils de collecte des données. Vous pouvez afficher les informations sur le serveur, trier les serveurs avec des filtres, baliser les serveurs avec des paires clé-valeur, et exporter les informations serveur et système détaillées.

Vous pouvez obtenir une vue générale et une vue détaillée des serveurs détectés par les outils de collecte de données.

Pour afficher les serveurs détectés

1. À l'aide de votre AWS compte, 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, sous Discover, sélectionnez Servers. Les serveurs détectés apparaissent dans la liste des serveurs.
3. Pour plus d'informations sur un serveur, choisissez son lien dans la colonne Server info (Informations sur le serveur). Un écran qui décrit le serveur s'affiche alors.

L'écran des détails du serveur affiche les informations relatives au système et les métriques des performances. Vous pouvez également trouver un bouton pour exporter les dépendances réseau et les informations relatives aux processus. Pour exporter les informations détaillées sur le serveur, consultez Utilisation AWS Migration Hub pour exporter les données du serveur.

Tri des serveurs dans la AWS Migration Hub console

Pour trouver facilement des serveurs spécifiques, appliquez des filtres de recherche afin de trier tous les serveurs détectés par les outils de collecte. Vous pouvez rechercher et filtrer sur de nombreux critères.

Pour trier les serveurs en appliquant les filtres de recherche

1. À l'aide de votre AWS compte, 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, sous Discover, sélectionnez Servers.
3. Cliquez dans la barre de recherche et sélectionnez un critère de recherche dans la liste.
4. Choisissez un opérateur dans la liste suivante.

5. Saisissez une valeur sensible à la casse pour le critère de recherche que vous avez sélectionné, puis appuyez sur Entrée.
6. Plusieurs filtres peuvent être appliqués en répétant les étapes 2 à 4.

Marquage des serveurs dans la console AWS Migration Hub

Pour faciliter la planification de la migration et rester organisé, vous pouvez créer plusieurs balises pour chaque serveur. Les balises sont des paires clé/valeur définies par l'utilisateur pouvant stocker des données ou des métadonnées sur les serveurs. Vous pouvez étiqueter un ou plusieurs serveurs en une seule opération. AWS Application Discovery Service Les balises (Application Discovery Service) sont similaires aux AWS balises, mais les deux types de balises ne peuvent pas être utilisés de manière interchangeable.

Vous pouvez ajouter ou supprimer une ou plusieurs balises d'un ou de plusieurs serveurs depuis la page principale Serveurs. Sur la page des détails d'un serveur, vous pouvez ajouter ou supprimer une ou plusieurs balises pour le serveur sélectionné. Vous pouvez effectuer n'importe quel type de tâche de balisage impliquant plusieurs serveurs ou balises en une seule opération. Vous pouvez aussi supprimer des balises.

Pour ajouter des balises à un ou plusieurs serveurs

1. À l'aide de votre AWS compte, 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, sous Discover, sélectionnez Servers.
3. Dans la colonne Server info (Informations sur le serveur), choisissez le lien relatif au serveur pour lequel vous souhaitez ajouter des balises. Pour ajouter des balises à plusieurs serveurs à la fois, cliquez sur les cases à cocher de plusieurs serveurs.
4. Choisissez Ajouter des balises, puis choisissez Ajouter une nouvelle étiquette.
5. Dans la boîte de dialogue, tapez une clé dans le champ Clé, et éventuellement une valeur dans le champ Valeur.

   Ajoutez d'autres balises en choisissant Ajouter une nouvelle étiquette et en ajoutant des informations supplémentaires.
6. Choisissez Enregistrer.

Pour supprimer les balises d'un ou de plusieurs serveurs

1. À l'aide de votre AWS compte, 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, sous Discover, sélectionnez Servers.
3. Dans la colonne Server info (Informations sur le serveur), choisissez le lien relatif au serveur pour lequel vous souhaitez supprimer des balises. Cochez les cases de plusieurs serveurs pour supprimer les balises de plusieurs serveurs à la fois.
4. Choisissez Supprimer les tags.
5. Sélectionnez chaque étiquette que vous souhaitez supprimer.
6. Choisissez Confirmer.

Utilisation AWS Migration Hub pour exporter les données du serveur

Cette rubrique explique comment exporter les données du serveur à l'aide de l' AWS Management Console API AWS Command Line Interface, de ou de l'API.

Pour utiliser le AWS Management Console pour exporter les données du serveur pour tous les serveurs

1. 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 gauche, sous Discover, sélectionnez Servers.
3. Choisissez Actions, puis Exporter les données de découverte.
4. Dans la section Exports (Exportations) en bas de l'écran, choisissez Export server details (Exporter les détails du serveur). Cette action génère un fichier .zip qui inclut les fichiers .csv décrits dans le tableau suivant.

Nom de fichier	Description
{account_id} _Application.csv	Détails de chaque application, y compris le nombre de serveurs, le nom et la description.

Nom de fichier	Description
{identifiant de compte} _ .csv ApplicationResourceAssociation	La relation entre les serveurs et les applications.
{identifiant de compte} _ ImportTemplate	Résumé de l'application et des balises de chaque serveur. Ce fichier peut être modifié et réimporté pour mettre à jour l'application associée au serveur.
{identifiant de compte} _ .csv NetworkInterface	Détails de chaque interface réseau, y compris le serveur, l'adresse et le commutateur associés.
{account_id} _Server.csv	Détails de chaque serveur, y compris le système d'exploitation, le nom d'hôte et l'hyperviseur.
{identifiant de compte} _ .csv SystemPerformance	Détails de chaque serveur, y compris la configuration du processeur, de la mémoire et du stockage, ainsi que les performances.
{account_id} _Tags.csv	Détails de chaque balise associée à un serveur.
{account_id} _ Info.csv VMware	Détails de chaque VMware configuration, y compris MoRef, VMname et vCenter.

Pour utiliser le AWS Management Console pour exporter les données d'agent pour un serveur spécifique

1. 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 gauche, sous Discover, sélectionnez Servers.
3. Placez le curseur dans le champ de recherche sous Serveurs. Une liste déroulante apparaît. Dans cette liste, sous Propriétés, choisissez Source, puis l'opérateur =, puis Source = Agent.

4. Dans les résultats de recherche, choisissez le nom du serveur pour lequel vous souhaitez exporter les données. Cette action vous amène à la page de détails de ce serveur.
5. Entrez une heure de début et une heure de fin, puis choisissez Exporter. Le fichier .zip exporté inclut les fichiers .csv décrits dans le tableau suivant.

{identifiant de compte} _ .csv destinati onProcessConnection	Détails des connexions entrantes vers le serveur.
{account_id} _networkInterface.csv	Détails de chaque interface réseau, y compris l'adresse, le masque et le nom
{account_id} _osInfo.csv	Détails du système d'exploitation, y compris le type de processeur, l'hyperviseur et le nom du système d'exploitation.
{account_id} _process.csv	Détails des processus exécutés sur le serveur.
{identifiant de compte} _ .csv sourcePro cessConnection	Détails de la connexion sortante provenant du serveur.
{account_id} _systemPerformance.csv	Détails de la configuration et des performan ces du processeur, de la mémoire et du stockage du serveur.

Pour utiliser l'API AWS Command Line Interface ou l'API pour exporter les données du serveur

1. Exécutez start-export-task. L'opération d'API correspondante est StartExportTask
2. Exécutez describe-export-tasks. L'opération d'API correspondante est DescribeExportTasks.

Regroupement de serveurs dans la AWS Migration Hub console

Certains de vos serveurs détectés peuvent avoir besoin d'être migrés conjointement afin de rester fonctionnels. Dans ce cas, vous pouvez définir et regrouper de manière logique les serveurs détectés dans les applications.

Dans le cadre du processus de regroupement, vous pouvez rechercher, filtrer et ajouter des balises.

Pour regrouper des serveurs dans une application nouvelle ou existante

1. À l'aide de votre AWS compte, 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, sous Discover, sélectionnez Servers.
3. Dans la liste des serveurs, sélectionnez chaque serveur que vous souhaitez regrouper dans une application nouvelle ou existante.

   Pour vous aider à choisir les serveurs de votre groupe, vous pouvez rechercher et filtrer sur tous les critères que vous spécifiez dans la liste des serveurs. Cliquez dans la barre de recherche et sélectionnez un élément dans la liste, choisissez un opérateur à partir de la liste suivante, puis entrez vos critères.
4. Facultatif : pour chaque serveur sélectionné, choisissez Add tag (Ajouter une balise), saisissez une valeur pour Key (Clé), puis, le cas échéant, tapez une valeur pour Value (Valeur).
5. Choisissez Group as application (Regrouper comme application) pour créer votre application ou l'ajouter à une application existante.
6. Dans la boîte de dialogue Group as application (Regrouper comme application), choisissez Group as a new application (Regrouper comme nouvelle application) ou Add to an existing application (Ajouter à une application existante).

   a. Si vous choisissez Group as a new application (Regrouper comme nouvelle application), entrez un nom dans Application name (Nom de l'application). Le cas échéant, vous pouvez entrer une description pour Application description (Description de l'application).

   b. Si vous choisissez Add to an existing application (Ajouter à une application existante), sélectionnez le nom de l'application à ajouter à la liste.
7. Choisissez Enregistrer.

Utilisation de l'API Application Discovery Service pour interroger les éléments de configuration découverts

Un élément de configuration est un actif informatique découvert dans votre centre de données par un agent ou par une importation. Lorsque vous utilisez AWS Application Discovery Service (Application Discovery Service), vous utilisez l'API pour spécifier des filtres et interroger des éléments de configuration spécifiques pour les actifs du serveur, de l'application, du processus et de la connexion. Pour plus d'informations sur l'API, consultez la section Application Discovery Service API Reference.

Les tableaux des sections suivantes répertorient les filtres d'entrée et les options de tri de sortie disponibles pour deux actions Application Discovery Service :

- `DescribeConfigurations`
- `ListConfigurations`

Les options de filtrage et de tri sont organisées en fonction du type la de ressource à laquelle elles s'appliquent (serveur, application, processus ou connexion).

> **Important**
>
> Les résultats ont été renvoyés par `DescribeConfigurationsListConfigurations`, et `StartExportTask` peuvent ne pas contenir de mises à jour récentes. Pour de plus amples informations, veuillez consulter the section called "Cohérence à terme".

Utilisation de l'**`DescribeConfigurations`**action

L'`DescribeConfigurations`action récupère les attributs d'une liste de configurations IDs. Tous les éléments fournis IDs doivent concerner le même type de ressource (serveur, application, processus ou connexion). Les champs de sortie sont spécifiques au type de ressource sélectionné. Par exemple, la sortie d'un élément de configuration de serveur inclut une liste d'attributs relatifs au serveur, tels que le nom d'hôte, le système d'exploitation et le nombre de cartes réseau. Pour plus d'informations sur la syntaxe des commandes, consultez DescribeConfigurations.

L'action `DescribeConfigurations` ne prend pas en charge le filtrage.

Champs de sortie pour **`DescribeConfigurations`**

Les tableaux suivants, organisés par type de ressource, répertorient les champs de sortie pris en charge de l'action `DescribeConfigurations`. Les champs marqués comme obligatoires sont toujours présents dans la sortie.

Ressources de serveur

Champ	Obligatoire
`server.agentId`	
`server.applications`	
`server.applications.hasMore Values`	
`server.configurationId`	x
`server.cpuType`	
`server.hostName`	
`server.hypervisor`	
`server.networkInterfaceInfo`	
`server.networkInterfaceInfo .hasMoreValues`	
`server.osName`	
`server.osVersion`	
`server.tags`	
`server.tags.hasMoreValues`	
`server.timeOfCreation`	x
`server.type`	

Champ	Obligatoire
server.performance.avgCpuUsagePct	
server.performance.avgDiskReadIOPS	
server.performance.avgDiskReadsPerSecondInKB	
server.performance.avgDiskWriteIOPS	
server.performance.avgDiskWritesPerSecondInKB	
server.performance.avgFreeRAMInKB	
server.performance.avgNetworkReadsPerSecondInKB	
server.performance.avgNetworkWritesPerSecondInKB	
server.performance.maxCpuUsagePct	
server.performance.maxDiskReadIOPS	
server.performance.maxDiskReadsPerSecondInKB	
server.performance.maxDiskWriteIOPS	
server.performance.maxDiskWritesPerSecondInKB	

Champ	Obligatoire
server.performance.maxNetwo rkReadsPerSecondInKB	
server.performance.maxNetwo rkWritesPerSecondInKB	
server.performance.minFreeR AMInKB	
server.performance.numCores	
server.performance.numCpus	
server.performance.numDisks	
server.performance.numNetwo rkCards	
server.performance.totalRAMInKB	

Ressources de processus

Champ	Obligatoire
process.commandLine	
process.configurationId	x
process.name	
process.path	
process.timeOfCreation	x

Ressources d'application

Champ	Obligatoire
`application.configurationId`	x
`application.description`	
`application.lastModifiedTime`	h/24, j/7
`application.name`	h/24, j/7
`application.serverCount`	h/24, j/7
`application.timeOfCreation`	x

Utilisation de l'**`ListConfigurations`**action

L'action `ListConfigurations` récupère une liste d'éléments de configuration en fonction des critères que vous spécifiez dans un filtre. Pour plus d'informations sur la syntaxe des commandes, consultez ListConfigurations.

Champs de sortie pour **`ListConfigurations`**

Les tableaux suivants, organisés par type de ressource, répertorient les champs de sortie pris en charge de l'action `ListConfigurations`. Les champs marqués comme obligatoires sont toujours présents dans la sortie.

Ressources de serveur

Champ	Obligatoire
`server.configurationId`	x
`server.agentId`	
`server.hostName`	
`server.osName`	
`server.osVersion`	

Champ	Obligatoire
server.timeOfCreation	x
server.type	

Ressources de processus

Champ	Obligatoire
process.commandLine	
process.configurationId	x
process.name	
process.path	
process.timeOfCreation	h/24, j/7
server.agentId	
server.configurationId	x

Ressources d'application

Champ	Obligatoire
application.configurationId	x
application.description	
application.name	h/24, j/7
application.serverCount	h/24, j/7
application.timeOfCreation	h/24, j/7
application.lastModifiedTime	x

Ressources de connexion

Champ	Obligatoire
`connection.destinationIp`	x
`connection.destinationPort`	h/24, j/7
`connection.ipVersion`	h/24, j/7
`connection.latestTimestamp`	h/24, j/7
`connection.occurrence`	h/24, j/7
`connection.sourceIp`	x
`connection.transportProtocol`	
`destinationProcess.configurationId`	
`destinationProcess.name`	
`destinationServer.configurationId`	
`destinationServer.hostName`	
`sourceProcess.configurationId`	
`sourceProcess.name`	
`sourceServer.configurationId`	
`sourceServer.hostName`	

Filtres pris en charge pour **`ListConfigurations`**

Les tableaux suivants, organisés par type de ressource, répertorient les filtres pris en charge pour l'action `ListConfigurations`. Les filtres et les valeurs sont dans une key/value relation définie par l'une des conditions logiques prises en charge. Vous pouvez trier la sortie des filtres indiqués.

Ressources de serveur

Filtre	Conditions prises en charge	Valeurs prises en charge	Tri pris en charge
`server.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• Tout ID de configuration de serveur valide	Aucune
`server.hostName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`server.osName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`server.osVersion`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`server.agentId`	• EQUALS • NOT_EQUALS • EQ	• String	Aucune

Filtre	Conditions prises en charge	Valeurs prises en charge	Tri pris en charge
	• NE		
`server.connectorId`	• EQUALS • NOT_EQUALS • EQ • NE	• String	Aucune
`server.type`	• EQUALS • NOT_EQUALS • EQ • NE	Chaîne avec une des valeurs suivantes : • EC2 • OTHER • VMWARE_VM • VMWARE_HOST • VMWARE_VM_TEMPLATE	Aucune
`server.vmWareInfo.morefId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Aucune
`server.vmWareInfo.vcenterId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Aucune

Filtre	Conditions prises en charge	Valeurs prises en charge	Tri pris en charge
`server.vmWareInfo.hostId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Aucune
`server.networkInterfaceInfo.portGroupId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Aucune
`server.networkInterfaceInfo.portGroupName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Aucune
`server.networkInterfaceInfo.virtualSwitchName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Aucune

Filtre	Conditions prises en charge	Valeurs prises en charge	Tri pris en charge
`server.networkInterfaceInfo.ipAddress`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Aucune
`server.networkInterfaceInfo.macAddress`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Aucune
`server.performance.avgCpuUsagePct`	• GE • LE • GT • LT	• Pourcentage	Aucune
`server.performance.totalDiskFreeSizeInKB`	• GE • LE • GT • LT	• Double	Aucune
`server.performance.avgFreeRAMInKB`	• GE • LE • GT • LT	• Double	Aucune

Filtre	Conditions prises en charge	Valeurs prises en charge	Tri pris en charge
`server.tag.value`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Aucune
`server.tag.key`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Aucune
`server.application.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Aucune
`server.application.description`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Aucune

Filtre	Conditions prises en charge	Valeurs prises en charge	Tri pris en charge
`server.application.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• Tout ID de configuration d'application valide	Aucune
`server.process.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	Aucune
`server.process.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Aucune
`server.process.commandLine`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	Aucune

Ressources d'application

Filtre	Conditions prises en charge	Valeurs prises en charge	Tri pris en charge
`application.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ApplicationId	Aucune
`application.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`application.description`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`application.serverCount`	Filtrage non pris en charge.	Filtrage non pris en charge.	• ASC • DESC
`application.timeOfCreation`	Filtrage non pris en charge.	Filtrage non pris en charge.	• ASC • DESC
`application.lastModifiedTime`	Filtrage non pris en charge.	Filtrage non pris en charge.	• ASC • DESC

Filtre	Conditions prises en charge	Valeurs prises en charge	Tri pris en charge
`server.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ServerId	Aucune

Ressources de processus

Filtre	Conditions prises en charge	Valeurs prises en charge	Tri pris en charge
`process.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	
`process.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`process.commandLine`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC

Filtre	Conditions prises en charge	Valeurs prises en charge	Tri pris en charge
`server.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ServerId	
`server.hostName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`server.osName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`server.osVersion`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC

Filtre	Conditions prises en charge	Valeurs prises en charge	Tri pris en charge
`server.agentId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	

Ressources de connexion

Filtre	Conditions prises en charge	Valeurs prises en charge	Tri pris en charge
`connection.sourceIp`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• IP	• ASC • DESC
`connection.destinationIp`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• IP	• ASC • DESC
`connection.destinationPort`	• EQUALS • NOT_EQUALS • EQ • NE	• Entier	• ASC • DESC

Filtre	Conditions prises en charge	Valeurs prises en charge	Tri pris en charge
`sourceServer.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ServerId	
`sourceServer.hostName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`destinationServer.osName`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`destinationServer.osVersion`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC

Filtre	Conditions prises en charge	Valeurs prises en charge	Tri pris en charge
`destinationServer.agentId`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	
`sourceProcess.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	
`sourceProcess.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`sourceProcess.commandLine`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`destinationProcess.configurationId`	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	

Filtre	Conditions prises en charge	Valeurs prises en charge	Tri pris en charge
`destinationProcess.name`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC
`destinationprocess.commandLine`	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• String	• ASC • DESC

Cohérence éventuelle de l' AWS Application Discovery Service API

Les opérations de mise à jour suivantes sont finalement cohérentes. Les mises à jour peuvent ne pas être immédiatement visibles lors des opérations de lecture StartExportTaskDescribeConfigurations, et ListConfigurations.

- AssociateConfigurationItemsToApplication
- CreateTags
- DeleteApplications
- DeleteTags
- DescribeBatchDeleteConfigurationTask
- DescribeImportTasks
- DisassociateConfigurationItemsFromApplication
- UpdateApplication

Suggestions pour gérer une éventuelle cohérence :

- Lorsque vous invoquez les opérations de lecture StartExportTaskDescribeConfigurations, ou ListConfigurations(ou AWS CLI les commandes correspondantes), utilisez un algorithme de réduction exponentielle afin de laisser suffisamment de temps à toute opération de mise à jour précédente pour se propager dans le système. Pour ce faire, exécutez l'opération de lecture à plusieurs reprises, en commençant par un temps d'attente de deux secondes, puis en augmentant progressivement jusqu'à cinq minutes.
- Ajoutez un temps d'attente entre les opérations suivantes, même si une opération de mise à jour renvoie une réponse 200 - OK. Appliquez un algorithme de backoff exponentiel en commençant par quelques secondes d’attente, puis augmentez progressivement jusqu’à environ cinq minutes.

Accès AWS Application Discovery Service via un point de terminaison d'interface (AWS PrivateLink)

Vous pouvez l'utiliser AWS PrivateLink pour créer une connexion privée entre votre VPC et. AWS Application Discovery Service Vous pouvez accéder à Application Discovery Service comme s'il se trouvait dans votre VPC, sans utiliser de passerelle Internet, de périphérique NAT, de connexion VPN ou Direct Connect de connexion. Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour accéder à Application Discovery Service.

Vous établissez cette connexion privée en créant un point de terminaison d'interface optimisé par AWS PrivateLink. Nous créons une interface réseau de point de terminaison dans chaque sous-réseau que vous activez pour le point de terminaison d'interface. Il s'agit d'interfaces réseau gérées par les demandeurs qui servent de point d'entrée pour le trafic destiné à Application Discovery Service.

Pour plus d'informations, consultez Accès aux Services AWS via AWS PrivateLink dans le Guide AWS PrivateLink .

Considérations relatives à Application Discovery Service

Avant de configurer un point de terminaison d'interface pour Application Discovery Service, consultez la section Accès à un AWS service à l'aide d'un point de terminaison VPC d'interface dans le AWS PrivateLink Guide.

Application Discovery Service prend en charge deux interfaces : l'une pour appeler toutes ses actions d'API, et l'autre pour que le collecteur sans agent et l'agent de découverte AWS d'applications envoient des données de découverte.

Création d'un point de terminaison d'interface

Vous pouvez créer un point de terminaison d'interface à l'aide de la console Amazon VPC ou de l' AWS Command Line Interface (AWS CLI). Pour plus d'informations, consultez la section Accès à un AWS service à l'aide d'un point de terminaison VPC d'interface dans le AWS PrivateLink Guide.

For Application Discovery Service

Créez un point de terminaison d'interface pour Application Discovery Service en utilisant le nom de service suivant :

```
com.amazonaws.region.discovery
```

Si vous activez le DNS privé pour le point de terminaison de l'interface, vous pouvez envoyer des demandes d'API à Application Discovery Service en utilisant son nom DNS régional par défaut. Par exemple, `discovery.us-east-1.amazonaws.com`.

For Agentless Collector and AWS Application Discovery Agent

Créez un point de terminaison d'interface en utilisant le nom de service suivant :

```
com.amazonaws.region.arsenal-discovery
```

Si vous activez le DNS privé pour le point de terminaison de l'interface, vous pouvez envoyer des demandes d'API à Application Discovery Arsenal en utilisant son nom DNS régional par défaut. Par exemple, `arsenal-discovery.us-east-1.amazonaws.com`.

Création d'une politique de point de terminaison pour votre point de terminaison d'interface

Une politique de point de terminaison est une ressource IAM que vous pouvez attacher à votre point de terminaison d'interface. La politique de point de terminaison par défaut permet un accès complet à un AWS service via le point de terminaison de l'interface. Pour contrôler l'accès autorisé à un AWS service depuis votre VPC, associez une politique de point de terminaison personnalisée au point de terminaison de l'interface.

Une politique de point de terminaison spécifie les informations suivantes :

- Les principaux qui peuvent effectuer des actions (Comptes AWS, utilisateurs IAM et rôles IAM).
- Les actions qui peuvent être effectuées.

Pour plus d'informations, consultez Contrôle de l'accès aux services à l'aide de politiques de point de terminaison dans le Guide AWS PrivateLink .

Exemple : politiques relatives aux points de terminaison VPC

Voici un exemple de politique de point de terminaison. Lorsque vous attachez cette politique à votre point de terminaison d'interface, elle accorde l'accès aux actions répertoriées pour tous les principaux sur toutes les ressources.

Example policy for Application Discovery Service

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "discovery:action-1",
            "discovery:action-2",
            "discovery:action-3"
         ],
         "Resource":"*"
      }
   ]
}
```

Example policy for the Agentless Collector and AWS Application Discovery Agent

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "arsenal:RegisterOnPremisesAgent"
         ],
         "Resource":"*"
      }
   ]
}
```

Utilisation du point de terminaison VPC pour le collecteur sans agent et AWS l'agent de découverte d'applications

Le collecteur sans agent et l'agent de découverte AWS d'applications ne prennent pas en charge les points de terminaison configurables. Utilisez plutôt la fonctionnalité DNS privé pour le point de `arsenal-discovery` terminaison Amazon VPC.

- Configurez la table de Direct Connect routage pour acheminer les adresses IP AWS privées vers le VPC. Par exemple, destination = 10.0.0.0/8 et cible = local. Pour cette configuration, vous devez au moins acheminer les adresses IP privées du point de terminaison `arsenal-discovery` Amazon VPC vers le VPC.
- Utilisez la fonctionnalité DNS privé des points de terminaison `arsenal-discovery` Amazon VPC, car le collecteur sans agent ne prend pas en charge les points de terminaison Arsenal configurables.
- Configurez le point de terminaison `arsenal-discovery` Amazon VPC dans un sous-réseau privé avec le même VPC vers lequel vous acheminez le trafic. Direct Connect
- Configurez le point de terminaison `arsenal-discovery` Amazon VPC avec un groupe de sécurité qui active le trafic entrant depuis le VPC (par exemple, 10.0.0.0/8).
- Configurez un résolveur entrant Amazon Route 53 pour acheminer la résolution DNS pour le nom DNS privé du point de terminaison Amazon `arsenal-discovery` VPC, qui sera résolu en adresse IP privée du point de terminaison VPC. Si vous ne le faites pas, le collecteur effectuera la résolution DNS à l'aide du résolveur local et utilisera le point de terminaison public Arsenal, et le trafic ne transitera pas par le VPC.
- Si tout le trafic public est désactivé, la fonctionnalité de mise à jour automatique échouera. Cela est dû au fait que le collecteur sans agent récupère les mises à jour en envoyant des demandes au point de terminaison Amazon ECR. Pour que la fonctionnalité de mise à jour automatique fonctionne sans envoyer de demandes via Internet public, configurez un point de terminaison VPC pour le service Amazon ECR et activez la fonctionnalité DNS privé pour ce point de terminaison.

Sécurité dans AWS Application Discovery Service

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture 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 cette notion par les termes sécurité du cloud et 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. L'efficacité de notre sécurité est régulièrement testée et vérifiée par des auditeurs tiers dans le cadre des programmes 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 la sensibilité de vos données, les exigences de votre organisation, et la législation et la réglementation applicables.

Pour utiliser l' AWS Application Discovery Agent ou l'Application Discovery Service Agentless Collector, vous devez fournir des clés d'accès à votre AWS compte. Ces informations sont ensuite stockées sur votre infrastructure locale. Dans le cadre du modèle de responsabilité partagée, vous êtes responsable de la sécurisation de l'accès à votre infrastructure.

Cette documentation vous aidera à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation d'Application Discovery Service. Les rubriques suivantes expliquent comment configurer Application Discovery Service pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui peuvent vous aider à surveiller et à sécuriser vos ressources Application Discovery Service.

Rubriques

Identity and Access Management pour AWS Application Discovery Service

Gestion des identités et des accès AWS (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 Application Discovery Service. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez Gestion des identités et des accès AWS (IAM) varie en fonction de votre rôle :

- Utilisateur du service : demandez des autorisations à votre administrateur si vous ne pouvez pas accéder aux fonctionnalités (voir Résolution des problèmes AWS Application Discovery Service d'identité et d'accès)
- Administrateur du service : déterminez l'accès des utilisateurs et soumettez les demandes d'autorisation (voir Comment AWS Application Discovery Service fonctionne avec IAM)
- Administrateur IAM : rédigez des politiques pour gérer l'accès (voir AWS Application Discovery Service exemples de politiques basées sur l'identité)

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 en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en tant qu'identité fédérée à l'aide d'informations d'identification provenant d'une source d'identité telle que AWS IAM Identity Center (IAM Identity Center), d'une authentification unique ou d'informations d'identification. Google/Facebook Pour plus d'informations sur la connexion, consultez Connexion à votre Compte AWS dans le Guide de l'utilisateur Connexion à AWS .

Pour l'accès par programmation, AWS fournit un SDK et une CLI pour signer les demandes de manière cryptographique. Pour plus d'informations, consultez Signature AWS Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une seule identité de connexion appelée utilisateur Compte AWS root qui dispose d'un accès complet à toutes Services AWS les ressources. Il est vivement déconseillé d'utiliser l'utilisateur racine pour vos tâches quotidiennes. Pour les tâches qui requièrent des informations d'identification de l'utilisateur racine, consultez Tâches qui requièrent les informations d'identification de l'utilisateur racine dans le Guide de l'utilisateur IAM.

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité qui dispose d'autorisations spécifiques pour une seule personne ou application. Nous vous recommandons d'utiliser ces informations d'identification temporaires au lieu des utilisateurs IAM avec des informations d'identification à long terme. Pour plus d'informations, voir Exiger des utilisateurs humains qu'ils utilisent la fédération avec un fournisseur d'identité pour accéder à AWS l'aide d'informations d'identification temporaires dans le guide de l'utilisateur IAM.

Les groupes IAM spécifient une collection d'utilisateurs IAM et permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. 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 dotée d'autorisations spécifiques qui fournit des informations d'identification temporaires. Vous pouvez assumer un rôle en passant d'un rôle d'utilisateur à un rôle

IAM (console) ou en appelant une opération d' AWS API AWS CLI ou d'API. Pour plus d'informations, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM sont utiles pour l'accès des utilisateurs fédérés, les autorisations temporaires des utilisateurs IAM, les accès intercompte, les accès entre services et les applications exécutées sur Amazon EC2. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Gestion de l'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 définit les autorisations lorsqu'elles sont associées à une identité ou à une ressource. AWS évalue ces politiques lorsqu'un directeur fait une demande. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations les documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

À l'aide de politiques, les administrateurs précisent qui a accès à quoi en définissant 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. Un administrateur IAM crée des politiques IAM et les ajoute aux rôles, que les utilisateurs peuvent ensuite assumer. Les politiques IAM définissent les autorisations quelle que soit la méthode que vous utilisez pour exécuter l'opération.

Politiques basées sur l'identité

Les stratégies basées sur l'identité sont des documents de stratégie d'autorisations JSON que vous attachez à une identité (utilisateur, groupe ou rôle). Ces politiques contrôlent les actions que peuvent exécuter ces identités, 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 des politiques intégrées (intégrées directement dans une seule identité) ou des politiques gérées (politiques autonomes associées à plusieurs identités). Pour découvrir comment choisir entre des politiques gérées et 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. Les exemples incluent les politiques de confiance de rôle IAM et les stratégies de compartiment Amazon S3. 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. Vous devez spécifier un principal dans une politique basée sur les ressources.

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 des types de politiques supplémentaires qui peuvent définir les autorisations maximales accordées par les types de politiques les plus courants :

- Limites d'autorisations : une limite des autorisations définit le nombre maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM. Pour plus d'informations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCPs) — Spécifiez les autorisations maximales pour une organisation ou une unité organisationnelle dans AWS Organizations. Pour plus d'informations, consultez Politiques de contrôle de service dans le Guide de l'utilisateur AWS Organizations .
- Politiques de contrôle des ressources (RCPs) : définissez le maximum d'autorisations disponibles pour les ressources de vos comptes. Pour plus d'informations, voir Politiques de contrôle des ressources (RCPs) dans le guide de AWS Organizations l'utilisateur.
- Politiques de session : politiques avancées que vous passez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. 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 AWS Application Discovery Service fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à Application Discovery Service, vous devez connaître les fonctionnalités IAM disponibles avec Application Discovery Service. Pour obtenir une vue d'ensemble de la façon dont Application Discovery Service et les autres AWS services fonctionnent avec IAM, consultez la section AWS Services That Work with IAM dans le guide de l'utilisateur IAM.

Rubriques

- Politiques basées sur l'identité d'Application Discovery Service
- Politiques basées sur les ressources d'Application Discovery Service
- Autorisation basée sur les balises Application Discovery Service
- Rôles IAM du Service de découverte d'applications

Politiques basées sur l'identité d'Application Discovery Service

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. Application Discovery Service prend en charge des actions, des ressources et des clés de condition spécifiques. Pour en savoir plus sur 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.

Actions

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

Les actions de stratégie dans Application Discovery Service utilisent le préfixe suivant avant l'action : `discovery:` Les déclarations de politique doivent inclure un élément `Action` ou `NotAction`. Application Discovery Service définit son propre ensemble d'actions décrivant les tâches que vous pouvez effectuer avec ce service.

Pour spécifier plusieurs actions dans une seule déclaration, séparez-les par des virgules comme suit :

```
"Action": [
      "discovery:action1",
      "discovery:action2"
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `Describe`, incluez l'action suivante :

```
"Action": "discovery:Describe*"
```

Pour consulter la liste des actions d'Application Discovery Service, reportez-vous à la section Actions définies par AWS Application Discovery Service dans le guide de l'utilisateur IAM.

Ressources

Application Discovery Service ne prend pas en charge la spécification de ressources ARNs dans une politique. Pour séparer l'accès, créez et utilisez séparément Comptes AWS.

Clés de condition

Application Discovery Service ne fournit aucune clé de condition spécifique au service, mais il prend en charge l'utilisation de certaines clés de condition globales. Pour voir toutes les clés de condition AWS globales, consultez la section Clés contextuelles de condition AWS globale dans le guide de l'utilisateur IAM.

Exemples

Pour consulter des exemples de politiques basées sur l'identité d'Application Discovery Service, consultez. AWS Application Discovery Service exemples de politiques basées sur l'identité

Politiques basées sur les ressources d'Application Discovery Service

Application Discovery Service ne prend pas en charge les politiques basées sur les ressources.

Autorisation basée sur les balises Application Discovery Service

Application Discovery Service ne prend pas en charge le balisage des ressources ni le contrôle d'accès en fonction des balises.

Rôles IAM du Service de découverte d'applications

Un rôle IAM est une entité de votre AWS compte qui possède des autorisations spécifiques.

Utilisation d'informations d'identification temporaires avec Application Discovery Service

Application Discovery Service ne prend pas en charge l'utilisation d'informations d'identification temporaires.

Rôles liés à un service

Les rôles liés aux AWS services permettent aux services d'accéder aux ressources d'autres services pour effectuer une action en votre nom. Les rôles liés à un service s'affichent dans votre compte IAM et sont la propriété du service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Application Discovery Service prend en charge les rôles liés aux services. Pour plus d'informations sur la création ou la gestion des rôles liés au service Application Discovery Service, consultez. Utilisation de rôles liés à un service pour Application Discovery Service

Rôles du service

Cette fonction permet à un service d'endosser une fonction du service en votre nom. Ce rôle autorise le service à accéder à des ressources d'autres services pour effectuer une action en votre nom. Les rôles de service s'affichent dans votre compte IAM et sont la propriété du compte. Cela signifie qu'un administrateur IAM peut modifier les autorisations associées à ce rôle. Toutefois, une telle action peut perturber le bon fonctionnement du service.

Application Discovery Service prend en charge les rôles de service.

AWS politiques gérées pour AWS Application Discovery Service

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 occasionnellement des autorisations à une politique gérée par AWS 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 très susceptibles de mettre à jour une politique gérée par AWS quand une nouvelle fonctionnalité est lancée ou quand 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 : AWSApplication DiscoveryServiceFullAccess

La `AWSApplicationDiscoveryServiceFullAccess` politique accorde à un compte utilisateur IAM l'accès à l'Application Discovery Service et au Migration Hub APIs.

Un compte utilisateur IAM associé à cette politique peut configurer Application Discovery Service, démarrer et arrêter les agents, démarrer et arrêter la découverte sans agent et interroger les données de la base de données AWS Discovery Service. Pour un exemple de cette stratégie, consultez Octroi d'un accès complet à Application Discovery Service.

AWS politique gérée : AWSApplication DiscoveryAgentlessCollectorAccess

La politique `AWSApplicationDiscoveryAgentlessCollectorAccess` gérée accorde à l'Application Discovery Service Agentless Collector (Agentless Collector) l'accès pour s'enregistrer et communiquer avec l'Application Discovery Service, ainsi qu'avec d'autres AWS services.

Cette politique doit être attachée à l'utilisateur IAM dont les informations d'identification sont utilisées pour configurer le collecteur sans agent.

Détails de l’autorisation

Cette politique inclut les autorisations suivantes.

- `arsenal`— Permet au collecteur de s'enregistrer auprès de l'application Application Discovery Service. Cela est nécessaire pour pouvoir renvoyer les données collectées à AWS.
- `ecr-public`— Permet au collecteur d'appeler le Amazon Elastic Container Registry Public (Amazon ECR Public) où se trouvent les dernières mises à jour relatives au collecteur.
- `mgh`— Permet au collecteur d'appeler AWS Migration Hub pour récupérer la région d'origine du compte utilisé pour configurer le collecteur. Cela est nécessaire pour savoir à quelle région les données collectées doivent être envoyées.
- `sts`— Permet au collecteur de récupérer un jeton porteur de service afin qu'il puisse appeler Amazon ECR Public pour obtenir les dernières mises à jour.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "arsenal:RegisterOnPremisesAgent"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecr-public:DescribeImages"
            ],
            "Resource": "arn:aws:ecr-
public::446372222237:repository/6e5498e4-8c31-4f57-9991-13b4b992ff7b"
        },
        {
```

```
            "Effect": "Allow",
            "Action": [
                "ecr-public:GetAuthorizationToken"

            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "mgh:GetHomeRegion"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "sts:GetServiceBearerToken"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS politique gérée : AWSApplication DiscoveryAgentAccess

La `AWSApplicationDiscoveryAgentAccess` politique accorde à l'agent Application Discovery l'accès pour s'enregistrer et communiquer avec Application Discovery Service.

Vous associez cette politique à tout utilisateur dont les informations d'identification sont utilisées par Application Discovery Agent.

Cette stratégie permet également à l'utilisateur d'accéder à Arsenal. Arsenal est un service d'agent géré et hébergé par AWS. Arsenal transmet les données à Application Discovery Service dans le cloud. Pour un exemple de cette stratégie, consultez Octroi de l'accès aux agents de découverte.

AWS politique gérée : AWSAgentless DiscoveryService

La `AWSAgentlessDiscoveryService` politique accorde au connecteur AWS Agentless Discovery qui s'exécute sur votre serveur VMware vCenter Server l'accès pour enregistrer, communiquer et partager les indicateurs de santé du connecteur avec Application Discovery Service.

Vous attachez cette stratégie à un utilisateur dont les informations d'identification sont utilisées par le connecteur.

AWS politique gérée : ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

Si cette `AWSApplicationDiscoveryServiceFullAccess` politique est associée à votre compte IAM, elle `ApplicationDiscoveryServiceContinuousExportServiceRolePolicy` est automatiquement associée à votre compte lorsque vous activez l'exploration des données dans Amazon Athena.

Cette politique permet AWS Application Discovery Service de créer des flux Amazon Data Firehose pour transformer et transmettre les données collectées par les AWS Application Discovery Service agents vers un compartiment Amazon S3 de votre AWS compte.

En outre, cette politique crée une nouvelle base AWS Glue Data Catalog de données appelée application_discovery_service_database et des schémas de table pour mapper les données collectées par les agents. Pour un exemple de cette stratégie, consultez Octroi d'autorisations pour la collecte des données des agents.

AWS politique gérée : AWSDiscovery ContinuousExportFirehosePolicy

La `AWSDiscoveryContinuousExportFirehosePolicy` politique est requise pour utiliser l'exploration des données dans Amazon Athena. Il permet à Amazon Data Firehose d'écrire des données collectées depuis Application Discovery Service vers Amazon S3. Pour plus d'informations sur l'utilisation de cette stratégie, consultez Création du AWSApplication DiscoveryServiceFirehose rôle. Pour un exemple de cette stratégie, consultez Octroi d'autorisations pour l'exploration des données.

Création du AWSApplication DiscoveryServiceFirehose rôle

Un administrateur associe des politiques gérées à votre compte utilisateur IAM. Lors de l'utilisation de la `AWSDiscoveryContinuousExportFirehosePolicy` politique, l'administrateur doit d'abord créer un rôle nommé AWSApplicationDiscoveryServiceFirehoseFirehose en tant qu'entité de confiance, puis associer la `AWSDiscoveryContinuousExportFirehosePolicy` politique au rôle, comme indiqué dans la procédure suivante.

Pour créer le rôle AWSApplicationDiscoveryServiceFirehoseIAM

1. Dans la console IAM, sélectionnez Rôles dans le volet de navigation.
2. Choisissez Create Role (Créer un rôle).

3. Choisissez Kinesis.
4. Choisissez Amazon Kinesis Firehose en tant que cas d'utilisation.
5. Choisissez Suivant : Autorisations.
6. Sous Politiques de filtrage, recherchez AWSDiscoveryContinuousExportFirehosePolicy.
7. Cochez la case AWSDiscoveryContinuousExportFirehosePolicyci-contre, puis choisissez Suivant : Révision.
8. Entrez le AWSApplicationDiscoveryServiceFirehosenom du rôle, puis choisissez Créer un rôle.

Application Discovery Service : mises à jour des politiques AWS gérées

Consultez les détails des mises à jour apportées aux politiques AWS gérées pour Application Discovery Service depuis que ce service a commencé à suivre ces modifications. Pour obtenir des alertes automatiques sur les modifications apportées à cette page, abonnez-vous au flux RSS de la page Historique du document pour AWS Application Discovery Service.

Modifier	Description	Date
AWSApplicationDiscoveryAgentlessCollectorAccess— Nouvelle politique rendue disponible avec le lancement d'Agentless Collector	Application Discovery Service a ajouté la nouvelle politique gérée `AWSApplicationDiscoveryAgentlessCollectorAccess` qui accorde au collecteur sans agent l'accès à l'enregistrement et à la communication avec l'Application Discovery Service, ainsi qu'à la communication avec d'autres AWS services.	16 août 2022
Application Discovery Service a commencé à suivre les modifications	Application Discovery Service a commencé à suivre les	1er mars 2021

Modifier	Description	Date
	modifications apportées AWS à ses politiques gérées.	

AWS Application Discovery Service exemples de politiques basées sur l'identité

Par défaut, les utilisateurs et les rôles IAM ne sont pas autorisés à créer ou à modifier les ressources Application Discovery Service. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l' AWS API AWS Management Console AWS CLI, ou. Un administrateur IAM doit créer des politiques IAM autorisant les utilisateurs et les rôles à exécuter des opérations d'API spécifiques sur les ressources spécifiées dont ils ont besoin. Il doit ensuite attacher ces politiques aux utilisateurs ou aux groupes IAM ayant besoin de ces autorisations.

Pour savoir comment créer une stratégie IAM basée sur l'identité à l'aide de ces exemples de documents de stratégie JSON, veuillez consulter Création de stratégies dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Rubriques

- Bonnes pratiques en matière de politiques
- Octroi d'un accès complet à Application Discovery Service
- Octroi de l'accès aux agents de découverte
- Octroi d'autorisations pour la collecte des données des agents
- Octroi d'autorisations pour l'exploration des données
- Octroi d'autorisations pour utiliser le schéma réseau de la console Migration Hub

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources Application Discovery Service 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 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.

Octroi d'un accès complet à Application Discovery Service

La politique AWSApplication DiscoveryServiceFullAccess gérée accorde au compte utilisateur IAM l'accès à l'Application Discovery Service et au Migration Hub APIs.

Un utilisateur IAM dont cette politique est associée à son compte peut configurer Application Discovery Service, démarrer et arrêter les agents, démarrer et arrêter la découverte sans agent et interroger les données de la base de données AWS Discovery Service. Pour plus d'informations sur cette politique, consultez AWS politiques gérées pour AWS Application Discovery Service.

Example AWSApplicationDiscoveryServiceFullAccess politique

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "mgh:*",
                "discovery:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "iam:GetRole"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Octroi de l'accès aux agents de découverte

La politique AWSApplication DiscoveryAgentAccess gérée accorde à l'agent Application Discovery l'accès pour s'enregistrer et communiquer avec Application Discovery Service. Pour plus

d'informations sur cette politique, consultez AWS politiques gérées pour AWS Application Discovery Service.

Associez cette politique à tout utilisateur dont les informations d'identification sont utilisées par Application Discovery Agent.

Cette stratégie permet également à l'utilisateur d'accéder à Arsenal. Arsenal est un service d'agent géré et hébergé par AWS. Arsenal transmet les données à Application Discovery Service dans le cloud.

Example AWSApplicationDiscoveryAgentAccess Politique

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "arsenal:RegisterOnPremisesAgent"
            ],
            "Resource": "*"
        }
    ]
}
```

Octroi d'autorisations pour la collecte des données des agents

La politique ApplicationDiscoveryServiceContinuousExportServiceRolePolicy gérée permet de AWS Application Discovery Service créer des flux Amazon Data Firehose pour transformer et transmettre les données collectées par les agents d'Application Discovery Service vers un compartiment Amazon S3 de votre AWS compte.

En outre, cette politique crée un catalogue de AWS Glue données avec une nouvelle base de données appelée `application_discovery_service_database` et des schémas de table pour mapper les données collectées par les agents.

Pour plus d'informations sur l'utilisation de cette stratégie, consultez AWS politiques gérées pour AWS Application Discovery Service.

Example ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

JSON

```
{
   "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "glue:CreateDatabase",
                "glue:UpdateDatabase",
                "glue:CreateTable",
                "glue:UpdateTable",
                "firehose:CreateDeliveryStream",
                "firehose:DescribeDeliveryStream",
                "logs:CreateLogGroup"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "firehose:DeleteDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch",
                "firehose:UpdateDestination"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-application-
discovery-service*"
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:PutBucketLogging",
                "s3:PutEncryptionConfiguration"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::aws-application-discovery-service*"
        },
        {
            "Action": [
```

```
                "s3:GetObject"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::aws-application-discovery-service*/*"
        },
        {
            "Action": [
                "logs:CreateLogStream",
                "logs:PutRetentionPolicy"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:logs:*:*:log-group:/aws/application-discovery-
service/firehose*"
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/
AWSApplicationDiscoveryServiceFirehose",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "firehose.amazonaws.com"
                }
            }
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/service-role/
AWSApplicationDiscoveryServiceFirehose",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "firehose.amazonaws.com"
                }
            }
        }
    ]
}
```

Octroi d'autorisations pour l'exploration des données

La AWSDiscovery ContinuousExportFirehosePolicy politique est requise pour utiliser l'exploration des données dans Amazon Athena. Il permet à Amazon Data Firehose d'écrire des données collectées depuis Application Discovery Service vers Amazon S3. Pour plus d'informations sur l'utilisation de cette stratégie, consultez Création du AWSApplication DiscoveryServiceFirehose rôle.

Example AWSDiscoveryContinuousExportFirehosePolicy

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "glue:GetTableVersions"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:GetBucketLocation",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::aws-application-discovery-service-*",
                "arn:aws:s3:::aws-application-discovery-service-*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
```

```
                "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose:log-stream:*"
            ]
        }
    ]
}
```

Octroi d'autorisations pour utiliser le schéma réseau de la console Migration Hub

Pour accorder l'accès au schéma réseau de la AWS Migration Hub console lors de la création d'une politique basée sur l'identité qui autorise ou refuse l'accès à Application Discovery Service ou à Migration Hub, vous devrez peut-être ajouter l'`discovery:GetNetworkConnectionGraph`action à la stratégie.

Vous devez utiliser cette `discovery:GetNetworkConnectionGraph` action dans les nouvelles politiques ou mettre à jour les anciennes politiques si les deux conditions suivantes s'appliquent à la stratégie :

- La politique autorise ou refuse l'accès à Application Discovery Service ou au Migration Hub.
- La politique accorde des autorisations d'accès en utilisant une autre action de découverte spécifique, comme `discovery:`*`action-name`* plutôt que`discovery:*`.

L'exemple suivant montre comment utiliser l'`discovery:GetNetworkConnectionGraph`action dans une politique IAM.

Example

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["discovery:GetNetworkConnectionGraph"],
            "Resource": "*"
        }
    ]
}
```

Pour plus d'informations sur le schéma réseau du Migration Hub, consultez la section Affichage des connexions réseau dans Migration Hub.

Utilisation de rôles liés à un service pour Application Discovery Service

AWS Application Discovery Service utilise des Gestion des identités et des accès AWS rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à Application Discovery Service. Les rôles liés à un service sont prédéfinis par Application Discovery Service et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration d'Application Discovery Service, car il n'est pas nécessaire d'ajouter manuellement les autorisations nécessaires. Application Discovery Service définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul Application Discovery Service peut assumer ses rôles. Les autorisations définies comprennent la politique de confiance et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela protège vos ressources Application Discovery Service, car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Rubriques

- Autorisations de rôle liées à un service pour Application Discovery Service
- Création d'un rôle lié à un service pour Application Discovery Service
- Suppression d'un rôle lié à un service pour Application Discovery Service

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM et recherchez les services avec un Oui dans la colonne Rôle lié à un service. Choisissez un Oui ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle liées à un service pour Application Discovery Service

Application Discovery Service utilise le rôle lié au service nommé AWSServiceRoleForApplicationDiscoveryServiceContinuousExport— Permet d'accéder aux AWS services et aux ressources utilisés ou gérés par. AWS Application Discovery Service

Le rôle AWSService RoleForApplicationDiscoveryServiceContinuousExport lié à un service fait confiance aux services suivants pour assumer le rôle :

- `continuousexport.discovery.amazonaws.com`

La politique d'autorisation des rôles permet à Application Discovery Service d'effectuer les actions suivantes :

glue

`CreateDatabase`

`UpdateDatabase`

`CreateTable`

`UpdateTable`

firehose

`CreateDeliveryStream`

`DeleteDeliveryStream`

`DescribeDeliveryStream`

`PutRecord`

`PutRecordBatch`

`UpdateDestination`

s3

`CreateBucket`

`ListBucket`

`GetObject`

journaux

`CreateLogGroup`

`CreateLogStream`

`PutRetentionPolicy`

iam

```
PassRole
```

Il s'agit de la stratégie complète qui affiche les ressources auxquelles les actions ci-dessus s'appliquent :

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "glue:CreateDatabase",
                "glue:UpdateDatabase",
                "glue:CreateTable",
                "glue:UpdateTable",
                "firehose:CreateDeliveryStream",
                "firehose:DescribeDeliveryStream",
                "logs:CreateLogGroup"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "firehose:DeleteDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch",
                "firehose:UpdateDestination"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-application-
discovery-service*"
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:PutBucketLogging",
                "s3:PutEncryptionConfiguration"
```

```
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::aws-application-discovery-service*"
        },
        {
            "Action": [
                "s3:GetObject"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::aws-application-discovery-service*/*"
        },
        {
            "Action": [
                "logs:CreateLogStream",
                "logs:PutRetentionPolicy"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:logs:*:*:log-group:/aws/application-discovery-
service/firehose*"
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/
AWSApplicationDiscoveryServiceFirehose",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "firehose.amazonaws.com"
                }
            }
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/service-role/
AWSApplicationDiscoveryServiceFirehose",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "firehose.amazonaws.com"
                }
```

```
            }
        }
    ]
}
```

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 en savoir plus, 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 Application Discovery Service

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Le rôle AWSService RoleForApplicationDiscoveryServiceContinuousExport lié à un service est automatiquement créé lorsque l'exportation continue est implicitement activée en a) en confirmant les options dans la boîte de dialogue présentée sur la page Data Collectors après avoir choisi « Démarrer la collecte de données », ou en cliquant sur le curseur intitulé « Exploration des données dans Athena », ou b) lorsque vous appelez l'API à l'aide de la CLI. StartContinuousExport AWS

> **Important**
>
> Ce rôle lié à un service peut apparaître dans votre compte si vous avez effectué une action dans un autre service qui utilise les fonctions prises en charge par ce rôle. Pour de plus amples informations, veuillez consulter Un nouveau rôle est apparu dans mon compte IAM.

Création du rôle lié à un service depuis la console Migration Hub

Vous pouvez utiliser la console Migration Hub pour créer le rôle AWSService RoleForApplicationDiscoveryServiceContinuousExport lié au service.

Pour créer le rôle lié à un service (console)

1. Dans le volet de navigation, choisissez Data Collectors (Collecteurs de données).
2. Choisissez l'onglet Agents.
3. Basculez le curseur Exploration des données dans Athena sur la position Activé.
4. Dans la boîte de dialogue générée à partir de l'étape précédente, cochez la case acceptant les coûts associés et choisissez Continue (Continuer) ou Enable (Activer).

Création du rôle lié à un service à partir du AWS CLI

Vous pouvez utiliser les commandes Application Discovery Service depuis le AWS Command Line Interface pour créer le rôle AWSService RoleForApplicationDiscoveryServiceContinuousExport lié au service.

Ce rôle lié à un service est automatiquement créé lorsque vous lancez l'exportation continue depuis le AWS CLI (AWS CLI il doit d'abord être installé dans votre environnement).

Pour créer le rôle lié au service (CLI) en démarrant l'exportation continue à partir du AWS CLI

1. Installez le AWS CLI pour votre système d'exploitation (Linux, macOS ou Windows). Consultez le guide de AWS Command Line Interface l'utilisateur pour obtenir des instructions.
2. Ouvrez l'invite de commande (Windows) ou le Terminal (Linux ou macOS).
    a. Tapez `aws configure` et appuyez sur Entrer.
    b. Entrez votre identifiant de clé d' AWS accès et votre clé d'accès AWS secrète.
    c. Saisissez `us-west-2` pour Default region name (Nom de la région par défaut).
    d. Saisissez `text` pour Default output format (Format de sortie par défaut).
3. Saisissez la commande suivante :

```
aws discovery start-continuous-export
```

Vous pouvez également utiliser la console IAM pour créer un rôle lié à un service avec le cas d'utilisation Discovery Service - Continuous Export. Dans l'interface de ligne de commande (CLI) IAM ou l'API IAM, créez un rôle lié à un service avec le nom de service `continuousexport.discovery.amazonaws.com`. Pour plus d'informations, consultez Création d'un rôle lié à un service dans le Guide de l'utilisateur IAM. Si vous supprimez ce rôle lié à un service, vous pouvez utiliser ce même processus pour créer le rôle à nouveau.

Suppression d'un rôle lié à un service pour Application Discovery Service

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer votre rôle lié à un service avant de pouvoir le supprimer manuellement.

Nettoyage du rôle lié au service

Avant de pouvoir utiliser IAM pour supprimer un rôle lié à un service, vous devez supprimer toutes les ressources utilisées par le rôle.

> **Note**
>
> Si Application Discovery Service utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les ressources Application Discovery Service utilisées par le rôle AWSService RoleForApplicationDiscoveryServiceContinuousExport lié au service depuis la console Migration Hub

1. Dans le volet de navigation, choisissez Data Collectors (Collecteurs de données).
2. Choisissez l'onglet Agents.
3. Basculez le curseur Exploration des données dans Athena sur la position Off.

Pour supprimer les ressources Application Discovery Service utilisées par le rôle AWSService RoleForApplicationDiscoveryServiceContinuousExport lié à un service dans AWS CLI

1. Installez le AWS CLI pour votre système d'exploitation (Linux, macOS ou Windows). Consultez le guide de AWS Command Line Interface l'utilisateur pour obtenir des instructions.
2. Ouvrez l'invite de commande (Windows) ou le Terminal (Linux ou macOS).
   a. Tapez `aws configure` et appuyez sur Entrer.
   b. Entrez votre identifiant de clé d' AWS accès et votre clé d'accès AWS secrète.
   c. Saisissez `us-west-2` pour Default region name (Nom de la région par défaut).
   d. Saisissez `text` pour Default output format (Format de sortie par défaut).
3. Saisissez la commande suivante :

```
aws discovery stop-continuous-export --export-id <export ID>
```

   - Si vous ne connaissez pas l'ID export de l'exportation continue que vous souhaitez arrêter, entrez la commande suivante pour afficher l'ID de l'exportation continue :

```
aws discovery describe-continuous-exports
```

4. Entrez la commande suivante pour vous assurer que l'exportation continue s'est arrêtée en vérifiant que son statut de retour est « INACTIF » :

```
aws discovery describe-continuous-export
```

Suppression manuelle du rôle lié au service

Vous pouvez supprimer le rôle AWSService RoleForApplicationDiscoveryServiceContinuousExport lié à un service à l'aide de la console IAM, de la CLI IAM ou de l'API IAM. Si vous n'avez plus besoin d'utiliser les fonctionnalités Discovery Service - Continuous Export qui nécessitent ce rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Pour en savoir plus, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

> **Note**
>
> Vous devez commencer par nettoyer votre rôle lié à un service avant de pouvoir le supprimer. Consultez Nettoyage du rôle lié au service.

Résolution des problèmes AWS Application Discovery Service d'identité et d'accès

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

Rubriques

- Je ne suis pas autorisé à effectuer iam : PassRole

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'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à Application Discovery Service.

Certains vous 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, vous devez 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 Application Discovery Service. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary n'est pas autorisée à transmettre 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 d'identification de connexion.

Journalisation des appels d'API Application Discovery Service avec AWS CloudTrail

AWS Application Discovery Service est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Application Discovery Service. Vous pouvez l'utiliser CloudTrail pour enregistrer, surveiller en permanence et conserver l'activité du compte à des fins de dépannage et d'audit. CloudTrail fournit un historique des événements de l'activité de votre AWS compte, y compris les actions effectuées via la console de AWS gestion et AWS SDKs les outils de ligne de commande.

CloudTrail capture tous les appels d'API pour Application Discovery Service sous forme d'événements. Les appels capturés incluent des appels provenant de la console Application Discovery Service et des appels de code vers les opérations de l'API Application Discovery Service.

Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Application Discovery Service. 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 envoyée à Application Discovery Service, l'adresse IP à partir de laquelle la demande a été faite, l'auteur de la demande, la date à laquelle elle a été faite, ainsi que des informations supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Informations sur le Service d'Application Discovery dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité se produit dans Application Discovery Service, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre AWS compte. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre AWS compte, y compris des événements relatifs à Application Discovery Service, créez une trace. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un parcours dans la console, celui-ci s'applique à toutes les AWS régions. 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 :

- Vue d'ensemble de la création d'un journal d'activité
- 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

Toutes les actions d'Application Discovery Service sont enregistrées CloudTrail et documentées dans le Guide de référence de l'API Application Discovery Service. Par exemple, les appels aux `CreateTagsDescribeTags`, et `GetDiscoverySummary` les actions génèrent des entrées dans les fichiers CloudTrail journaux.

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 Gestion des identités et des accès AWS (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour plus d'informations, consultez la section Élément userIdentity CloudTrail .

Comprendre les entrées du fichier journal d'Application Discovery Service

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'`DescribeTags`action.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAJBHMC4H6EKEXAMPLE:sample-user",
        "arn": "arn:aws:sts::444455556666:assumed-role/ReadOnly/sample-user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAJQABLZS4A3QDU576Q",
                "arn": "arn:aws:iam::444455556666:role/ReadOnly",
                "accountId": "444455556666",
                "userName": "sampleAdmin"
            },
            "webIdFederationData": {},
```

```
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-05-05T15:19:03Z"
            }
        }
    },
    "eventTime": "2020-05-05T17:02:40Z",
    "eventSource": "discovery.amazonaws.com",
    "eventName": "DescribeTags",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "20.22.33.44",
    "userAgent": "Coral/Netty4",
    "requestParameters": {
        "maxResults": 0,
        "filters": [
            {
                "values": [
                    "d-server-0315rfdjreyqsq"
                ],
                "name": "configurationId"
            }
        ]
    },
    "responseElements": null,
    "requestID": "mgh-console-eb1cf315-e2b4-4696-93e5-b3a3b9346b4b",
    "eventID": "7b32b778-91c9-4c75-9cb0-6c852791b2eb",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

AWS Application Discovery Service Formats d'ARN

Un Amazon Resource Name (ARN) est une chaîne qui identifie une AWS ressource de manière unique. AWS nécessite un ARN lorsque vous souhaitez spécifier une ressource sans ambiguïté dans l'ensemble. AWS AWS Application Discovery Service définit ce qui suit ARNs.

- Agent de découverte : `arn:aws:discovery:region:account:agent/discovery-agent/agentId`
- Collectionneur sans agent : `arn:aws:discovery:region:account:agent/agentless-collector/agentId`
- Migration Evaluator Collector : `arn:aws:discovery:region:account:agent/migration-evaluator-collector/agentId`
- Connecteur Discovery : `arn:aws:discovery:region:account:agent/discovery-connector/agentId`

AWS Application Discovery Service Quotas

La console Service Quotas fournit des informations sur AWS Application Discovery Service les quotas. Vous pouvez utiliser la console Service Quotas pour consulter les quotas de service par défaut ou pour demander des augmentations de quotas pour des quotas ajustables.

À l'heure actuelle, le seul quota pouvant être augmenté est celui des serveurs importés par compte.

Application Discovery Service possède les quotas par défaut suivants :

- 1 000 demandes par compte.

  Si vous atteignez ce quota et que vous souhaitez importer de nouvelles applications, vous pouvez supprimer des applications existantes à l'aide de l'action `DeleteApplications` API. Pour plus d'informations, consultez DeleteApplicationsle manuel Application Discovery Service API Reference.
- Chaque fichier d'importation peut avoir une taille maximale de 10 Mo.
- 25 000 enregistrements de serveur importés par compte.
- 25 000 suppressions d'enregistrements d'importation par jour.
- 10 000 serveurs importés par compte (vous pouvez demander à augmenter ce quota).
- 1 000 agents actifs, qui collectent et envoient des données à Application Discovery Service.
- 10 000 agents inactifs, qui répondent mais ne collectent pas de données.
- 400 serveurs par application.
- 30 balises par serveur.

Résolution des problèmes AWS Application Discovery Service

Dans cette section, vous trouverez des informations relatives à la résolution des problèmes courants liés à AWS Application Discovery Service.

Rubriques

Arrêter la collecte de données par l'exploration des données

Pour arrêter l'exploration des données, vous pouvez soit désactiver le commutateur dans la console Migration Hub sous l'onglet Découvrir > Collecteurs de données > Agents, soit appeler l'`StopContinuousExport`API. L'arrêt de la collecte de données peut prendre jusqu'à 30 minutes. Au cours de cette étape, l'interrupteur de la console et l'appel de l'`DescribeContinuousExport`API indiqueront que l'état d'exploration des données est « Stop In Progress ».

> **Note**
>
> Si à l'issue de l'actualisation de la page de la console, le bouton bascule n'est pas désélectionné et qu'un message d'erreur est émis ou que l'API `DescribeContinuousExport` retourne l'état « Stop_Failed » (Échec de l'arrêt), vous pouvez réessayer en désélectionnant le bouton bascule ou en appelant l'API `StopContinuousExport`. Si l' « exploration des données » affiche toujours une erreur et ne parvient pas à s'arrêter, veuillez contacter l' AWS assistance.

Vous pouvez également arrêter manuellement la collecte des données en procédant comme suit.

Option 1 : Arrêt de la collecte des données effectuée par des agents

Si vous avez déjà procédé à votre détection à l'aide d'agents ADS et que vous ne souhaitez plus collecter de données supplémentaires dans le référentiel de base de données ADS :

1. Dans la console Migration Hub, choisissez l'onglet Découvrir > Collecteurs de données > Agents.
2. Sélectionnez tous les agents en cours d'exécution et choisissez Stop Data Collection (Arrêter la collecte des données).

   Cela permet de vous assurer qu'aucune nouvelle donnée n'est collectée par les agents dans le référentiel de données ADS et dans votre compartiment S3. Vos données existantes restent accessibles.

Option 2 : supprimer les Amazon Kinesis Data Streams liés à l'exploration des données

Si vous souhaitez continuer à collecter des données par les agents dans le référentiel de données ADS, mais que vous ne souhaitez pas collecter de données dans votre compartiment Amazon S3 à l'aide de l'exploration de données, vous pouvez supprimer manuellement les flux Amazon Data Firehose créés par l'exploration de données :

1. Connectez-vous à Amazon Kinesis depuis la AWS console et choisissez Data Firehose dans le volet de navigation.
2. Supprimez les flux suivants créés par la fonctionnalité d'exploration de données :

   - `aws-application-discovery-service-id_mapping_agent`
   - `aws-application-discovery-service-inbound_connection_agent`
   - `aws-application-discovery-service-network_interface_agent`
   - `aws-application-discovery-service-os_info_agent`
   - `aws-application-discovery-service-outbound_connection_agent`
   - `aws-application-discovery-service-processes_agent`
   - `aws-application-discovery-service-sys_performance_agent`

Supprimer les données collectées par l'exploration des données

Pour supprimer les données collectées lors de l'exploration des données

1. Supprimez les données de l'agent de découverte stockées dans Amazon S3.

Les données collectées par AWS Application Discovery Service (ADS) sont stockées dans un compartiment S3 nomméaws-application-discover-discovery-service-*uniqueid*.

> **Note**
>
> La suppression du compartiment Amazon S3 ou de l'un des objets qu'il contient alors que l'exploration des données est activée dans Amazon Athena provoque une erreur. Il continue d'envoyer de nouvelles données d'agent de découverte à S3. Les données supprimées ne seront également plus accessibles dans Athena.

2. Supprimer AWS Glue Data Catalog.

   Lorsque l'exploration des données dans Amazon Athena est activée, un compartiment Amazon S3 est créé dans votre compte pour stocker les données collectées par les agents ADS à intervalles réguliers. En outre, il crée également un AWS Glue Data Catalog pour vous permettre d'interroger les données stockées dans un compartiment Amazon S3 à partir d'Amazon Athena. Lorsque vous désactivez l'exploration des données dans Amazon Athena, aucune nouvelle donnée n'est stockée dans votre compartiment Amazon S3, mais les données précédemment collectées sont conservées. Si vous n'avez plus besoin de ces données et que vous souhaitez rétablir l'état de votre compte avant l'activation de l'exploration des données dans Amazon Athena.

   a. Accédez à Amazon S3 depuis la AWS console et supprimez manuellement le compartiment nommé « aws-application-discover-discovery -service-uniqueid »

   b. Vous pouvez supprimer manuellement le catalogue de données AWS Glue Data Catalog d'exploration des données en supprimant la application-discovery-service-databasebase de données et toutes les tables suivantes :

      - `os_info_agent`
      - `network_interface_agent`
      - `sys_performance_agent`
      - `processes_agent`
      - `inbound_connection_agent`
      - `outbound_connection_agent`
      - `id_mapping_agent`

Suppression de vos données de AWS Application Discovery Service

Pour que toutes vos données soient supprimées d'Application Discovery Service, contactez le AWS Support et demandez la suppression complète des données.

Résoudre les problèmes courants liés à l'exploration des données dans Amazon Athena

Dans cette section, vous trouverez des informations sur la résolution des problèmes courants liés à l'exploration des données dans Amazon Athena.

Rubriques

- L'exploration des données dans Amazon Athena ne démarre pas car les rôles liés aux services et les AWS ressources requises ne peuvent pas être créés
- Les données des nouveaux agents ne s'affichent pas dans Amazon Athena
- Vous ne disposez pas d'autorisations suffisantes pour accéder à Amazon S3, Amazon Data Firehose ou AWS Glue

L'exploration des données dans Amazon Athena ne démarre pas car les rôles liés aux services et les AWS ressources requises ne peuvent pas être créés

Lorsque vous activez l'exploration des données dans Amazon Athena, le rôle lié au service est créé dans votre compte`AWSServiceRoleForApplicationDiscoveryServiceContinuousExport`, qui lui permet de créer les AWS ressources nécessaires pour rendre les données collectées par l'agent accessibles dans Amazon Athena, notamment un compartiment Amazon S3, des flux Amazon Kinesis et. AWS Glue Data Catalog Si votre compte ne dispose pas des autorisations nécessaires pour explorer les données dans Amazon Athena afin de créer ce rôle, il ne pourra pas être initialisé. Reportez-vous à AWS politiques gérées pour AWS Application Discovery Service.

Les données des nouveaux agents ne s'affichent pas dans Amazon Athena

Si aucune nouvelle donnée ne parvient à Athena, que cela fait plus de 30 minutes qu'un agent a démarré et que le statut d'exploration des données est actif, consultez les solutions répertoriées ci-dessous :

- AWS Agents de découverte

  Vérifiez que le statut Collection (Collecte) de l'agent est marqué comme Started (Démarré) et que le statut Health (État) est marqué comme Running (En cours d'exécution).

- Rôle Kinesis

  Assurez-vous de disposer du rôle `AWSApplicationDiscoveryServiceFirehose` dans votre compte.

- État du Firehose

  Assurez-vous que les flux de diffusion Firehose suivants fonctionnent correctement :

  - `aws-application-discovery-service/os_info_agent`
  - `aws-application-discovery-service-network_interface_agent`
  - `aws-application-discovery-service-sys_performance_agent`
  - `aws-application-discovery-service-processes_agent`
  - `aws-application-discovery-service-inbound_connection_agent`
  - `aws-application-discovery-service-outbound_connection_agent`
  - `aws-application-discovery-service-id_mapping_agent`

- AWS Glue Data Catalog

  Assurez-vous que la `application-discovery-service-database` base de données est bien insérée AWS Glue. Vérifiez que les tables suivantes sont présentes dans AWS Glue :

  - `os_info_agent`
  - `network_interface_agent`
  - `sys_performance_agent`
  - `processes_agent`
  - `inbound_connection_agent`
  - `outbound_connection_agent`
  - `id_mapping_agent`

- Compartiment Amazon S3

Assurez-vous qu'un compartiment Amazon S3 est nommé `aws-application-discovery-service-uniqueid` dans votre compte. Si des objets du compartiment ont été déplacés ou supprimés, ils ne s'afficheront pas correctement dans Athena.

- Serveurs sur site

  Vérifiez que vos serveurs sont en cours d'exécution afin que vos agents puissent collecter et envoyer des données à AWS Application Discovery Service.

Vous ne disposez pas d'autorisations suffisantes pour accéder à Amazon S3, Amazon Data Firehose ou AWS Glue

Si vous utilisez AWS Organizations et que l'initialisation pour l'exploration des données dans Amazon Athena échoue, cela peut être dû au fait que vous n'êtes pas autorisé à accéder à Amazon S3, Amazon Data Firehose, Athena ou. AWS Glue

Vous aurez besoin d'un utilisateur IAM doté de droits d'administrateur pour accéder à ces services. Un administrateur peut utiliser son compte pour accorder cet accès. Consultez AWS politiques gérées pour AWS Application Discovery Service.

Pour garantir le bon fonctionnement de l'exploration des données dans Amazon Athena, ne modifiez ni ne supprimez les AWS ressources créées par l'exploration des données dans Amazon Athena, notamment le compartiment Amazon S3, Amazon Data Firehose Streams et. AWS Glue Data Catalog Si vous supprimez ou modifiez accidentellement ces ressources, arrêtez et démarrez la fonction Data Exploration (Exploration des données) qui recréera alors automatiquement ces ressources. Si vous supprimez le compartiment Amazon S3 créé par l'exploration des données, vous risquez de perdre les données collectées dans le compartiment.

Résolution des problèmes d'importation ayant échoué

L'importation du Migration Hub vous permet d'importer les détails de votre environnement sur site directement dans Migration Hub sans utiliser le Discovery Connector ou le Discovery Agent. Cela vous donne ainsi la possibilité de réaliser l'évaluation et la planification de la migration directement à partir de vos données importées. Vous pouvez également regrouper vos appareils en tant qu'applications et suivre leur statut de migration.

Lors de l'importation des données, il est possible de rencontrer des erreurs. En général, ces erreurs se produisent pour l'une des raisons suivantes :

- Un quota lié à l'importation a été atteint — Un quota est associé aux tâches d'importation. Si vous faites une demande de tâche d'importation qui dépasse les quotas, la demande échouera et renverra une erreur. Pour de plus amples informations, veuillez consulter AWS Application Discovery Service Quotas.
- Une virgule supplémentaire (,) a été insérée dans le fichier d'importation. Les virgules des fichiers .CSV sont utilisées pour différencier un champ du suivant. Les virgules ne sont pas prises en charge dans les champs, car elles divisent toujours les champs. Cela peut entraîner une cascade d'erreurs de formatage. Assurez-vous que les virgules sont utilisées uniquement entre les champs, et n'apparaissent pas autrement dans vos fichiers d'importation.
- Un champ possède une valeur en dehors de sa plage prise en charge. Certains champs, par exemple, `CPU.NumberOfCores` doivent avoir une plage de valeurs qu'ils prennent en charge. Si vous avez une valeur supérieure ou inférieure à cette plage prise en charge, l'importation de l'enregistrement échoue.

Si des erreurs se produisent avec votre requête d'importation, téléchargez vos enregistrements ayant échoué pour votre tâche d'importation, et résolvez les erreurs dans le fichier .CSV des entrées ayant échoué, puis importez à nouveau.

Console

Pour télécharger votre archive d'enregistrements ayant échoué

1. Connectez-vous à la AWS Management Console console Migration Hub et ouvrez-la à l'adressehttps://console.aws.amazon.com/migrationhub.
2. Dans le volet gauche de navigation, sous Découvrir, choisissez Outils.
3. À partir de Discovery Tools (Outils de détection), choisissez View imports (Afficher les importations).
4. À partir du tableau de bord de Importations, choisissez le bouton radio associé une requête d'importation avec un certain nombre d'enregistrements ayant échoué.
5. Choisissez Télécharger les enregistrements ayant échoué au-dessus du tableau dans le tableau de bord. Cela ouvre la boîte de dialogue de téléchargement de votre navigateur pour télécharger le fichier d'archive.

AWS CLI

Pour télécharger votre archive d'enregistrements ayant échoué

1. Ouvrez une fenêtre de terminal et saisissez la commande suivante, où *ImportName* `is the name of the import task with the failed entries that you want to correct.` :

   ```
   aws discovery describe-import-tasks - -name ImportName
   ```

2. Dans la sortie, copiez l'ensemble du contenu de la valeur renvoyée pour `errorsAndFailedEntriesZip`, sans les guillemets.
3. Ouvrez un navigateur Web, collez le contenu dans la zone de texte de l'URL, et appuyez sur ENTER. Cela va télécharger l'archive des enregistrements ayant échoué, compressée au format .zip.

Maintenant que vous avez téléchargé l'archive des enregistrements ayant échoué, vous pouvez extraire les deux fichiers qu'elle contient et corriger les erreurs. Notez que si vos erreurs sont liées aux limites basées sur les services, vous devez demander une augmentation de la limite, ou supprimer suffisamment des ressources associées de manière à ce que votre compte reste dans la limite. L'archive contient les fichiers suivants :

- errors-file.csv — Ce fichier est votre journal des erreurs. Il enregistre la ligne, le nom de la colonne et un message d'erreur descriptif pour chaque enregistrement raté de chaque entrée échouée. `ExternalId`
- failed-entries-file.csv — Ce fichier contient uniquement les entrées échouées de votre fichier d'importation d'origine.

Pour corriger les non-limit-based erreurs que vous avez rencontrées, utilisez le `errors-file.csv` pour corriger les problèmes du `failed-entries-file.csv` fichier, puis importez ce fichier. Pour plus d'informations sur l'importation des fichiers, consultez Importation de données.

Historique du document pour AWS Application Discovery Service

Dernière mise à jour de la documentation du guide de l'utilisateur : 16 mai 2023

Le tableau suivant décrit les modifications importantes apportées au guide de l'utilisateur d'Application Discovery Service après le 18 janvier 2019. Pour recevoir des notifications en cas de mise à jour de cette documentation, abonnez-vous au flux RSS.

Modification	Description	Date
Mode de maintenance	AWS Application Discovery Service n'est plus ouvert aux nouveaux clients. Vous pouvez également utiliser celui AWS Transform qui fournit des fonctionnalités similaires. Pour plus d'informations, consultez la section Modification de la disponibilité d'AWS Application Discovery Service.	7 novembre 2025
Transition de Discovery Connector vers Agentless Collector	Nous recommandons aux clients qui utilisent actuellement Discovery Connector de passer au nouveau collecteur sans agent. À compter du 17 novembre 2025, AWS Application Discovery Service nous cesserons d'accepter de nouvelles données en provenance de Discovery Connectors. Pour plus d'informations, consultez Discovery Connector.	12 novembre 2024

Lancement du module de collecte de données réseau Agentless Collector	Le module de collecte de données réseau vous permet de découvrir les dépendances entre les serveurs de votre centre de données sur site. Pour plus d'informations, consultez la section Utilisation du module de collecte de données réseau Agentless Collector.	8 novembre 2024
Support pour la collecte sans agent pour le mappage des dépendances	Pour plus d'informations, consultez la section Utilisation du module de collecte de données VMware vCenter Agentless Collector.	24 octobre 2024
A publié la version 2 d'Agentless Collector basée sur Amazon Linux 2023	Pour plus d'informations, consultez la section Conditions requises pour Agentless Collector.	26 septembre 2024
Conditions requises pour Agentless Collector mises à jour	Pour plus d'informations, consultez la section Conditions requises pour Agentless Collector.	9 septembre 2024
Cohérence éventuelle de l'API	Pour plus d'informations, consultez la section Cohérence éventuelle dans l' AWS Application Discovery Service API.	20 juin 2024

Mises à jour du collecteur Agentless	Nous avons ajouté `sts.amazonaws.com` à la liste des domaines nécessitant un accès sortant. Pour plus d'informations, consultez Configurer le pare-feu pour l'accès sortant aux domaines AWS.	20 juin 2024
Pour séparer les accès, créez et utilisez des comptes AWS distincts.	Pour plus d'informations, consultez Actions, ressources et clés de condition pour AWS Application Discovery Service.	5 avril 2024
Présentation de la base de données Agentless Collector et du module de collecte de données analytiques	Le module de collecte de données de base de données et d'analyse est le nouveau module d'Application Discovery Service Agentless Collector (Agentless Collector). Vous pouvez utiliser ce module de collecte de données pour vous connecter à votre environnement et collecter des métadonnées et des indicateurs de performance à partir de votre base de données et de vos serveurs d'analyse sur site. Pour plus d'informations, voir Module de collecte de données de base de données et d'analyse.	16 mai 2023

Présentation d'Application Discovery Service Agentless Collector	Application Discovery Service Agentless Collector (Agentless Collector) est la nouvelle application AWS Application Discovery Service locale qui collecte des informations par le biais de méthodes sans agent concernant votre environnement sur site afin de vous aider à planifier efficacement votre migration vers le. AWS Cloud Pour plus d'informations, consultez Agentless Collector.	16 août 2022
Mise à jour IAM	L'`discovery:GetNetworkConnectionGraph` action Gestion des identités et des accès AWS (IAM) est désormais disponible pour accorder l'accès au schéma réseau de la AWS Migration Hub console lors de la création d'une politique basée sur l'identité. Pour plus d'informations, consultez la section Octroi d'autorisations pour utiliser le diagramme de réseau.	24 mai 2022

Présentation de la région d'origine	La région d'origine du Migration Hub fournit un référentiel unique d'informations de découverte et de planification de migration pour l'ensemble de votre portefeuille, ainsi qu'une vue unique des migrations vers plusieurs AWS régions.	20 novembre 2019
Présentation de la fonctionnalité d'importation de Migration Hub	L'importation du Migration Hub vous permet d'importer des informations sur vos serveurs et applications locaux dans Migration Hub, notamment les spécifications du serveur et les données d'utilisation. Vous pouvez également utiliser ces données pour suivre l'état des migrations d'application. Pour plus d'informations, consultez Migration Hub Import.	18 janvier 2019

Le tableau suivant décrit les versions de documentation du Guide de l'utilisateur d'Application Discovery Service publiées avant le 18 janvier 2019 :

Modifier	Description	Date
Nouvelle fonction	Documentation mise à jour pour faciliter l'exploration des données dans Amazon Athena et ajout d'un chapitre sur la résolution des problèmes.	09 août 2018
Révision en profondeur	Restructuration de l'ensemble du document ; réécriture des	25 mai 2018

Modifier	Description	Date
	informations relatives à l'utilisation et aux sorties.	
Discovery Agent 2.0	Publication d'une nouvelle version améliorée de l'agent de détection d'applications.	19 octobre 2017
Console	Le AWS Management Console a été ajouté.	19 décembre 2016
Détection sans agent	Cette version décrit l'installation et la configuration de la détection sans agent.	28 juillet 2016
Nouvelles informations relatives à Microsoft Windows Server et résolution de problèmes de commande	Ajout d'informations relatives à Microsoft Windows Server. Ajouts de correctifs concernant des problèmes de commande.	20 mai 2016
Publication initiale	Il s'agit de la première version du Guide de l'utilisateur d'Application Discovery Service.	12 mai 2016

AWS Glossaire

Pour la AWS terminologie la plus récente, consultez le AWS glossaire dans la Glossaire AWS référence.

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.