AWS Server Migration Service

Guide de l'utilisateur

AWS Server Migration Service: Guide de l'utilisateur

Table of Contents

Qu'est-ce que AWS Server Migration Service ?

AWS Server Migration Service(AWS SMS) automatise la migration de vos machines virtuelles VMware vSphere, Microsoft Hyper-V/SCVMM et Azure sur site vers leAWScloud.AWS SMSréplique de façon incrémentielle vos machines virtuelles Server en tant qu'Amazon Machine Images (AMI) prêtes au déploiement sur Amazon EC2. En utilisant les AMI, vous pouvez facilement tester et mettre à jour vos images basées sur le Cloud avant de les déployer en production.

En utilisant AWS SMS pour gérer vos agents de migration, vous pouvez :

- Simplifier le processus de migration vers le cloud. Vous pouvez commencer par migrer un groupe de serveurs à l'aide de l'AWS CLI. Une fois la migration lancée,AWS SMSgère toutes les complexités du processus de migration, notamment la réplication automatique des volumes de serveurs en direct dansAWSet création régulière de nouvelles AMI. Vous pouvez rapidement lancer des instances EC2 à partir des AMI dans la console.
- Gérer des migrations multi-serveur. AWS SMS gère les migrations de serveurs en vous permettant de programmer des réplications et de suivre la progression d'un groupe de serveurs qui constitue une application. Vous pouvez programmer des réplications initiales, configurer des intervalles de réplication et suivre la progression de chaque serveur à l'aide de l'AWS CLI. Lorsque vous lancez une application migrée, vous pouvez appliquer des scripts de configuration personnalisés qui s'exécutent au moment du démarrage.
- Testez les migrations de serveur incrémentielles Prise en charge de la réplication incrémentielle,AWS SMSpermet la vérification rapide et évolutive des serveurs migrés. Etant donné queAWS SMSutilise la réplication incrémentielle, elle ne transfère que les modifications vers le cloud. Par conséquent, vous pouvez tester de petits changements de façon itérative et économiser de la bande passante réseau.
- Prise en charge des systèmes d'exploitation les plus fréquemment utilisés. AWS SMS prend en charge la réplication des images de système d'exploitation contenant Windows, ainsi que plusieurs distributions Linux majeures.
- Temps d'arrêt minimaux. Une réplication incrémentielle AWS SMS réduit l'impact sur l'activité associé à la période d'arrêt de l'application pendant le transfert définitif.

Les limitations liées à l'utilisation d'AWS SMS sont les suivantes :

- 50 migrations de machine virtuelle simultanées par compte, à moins qu'un client ne demande une augmentation de la limite.
- 90 jours d'utilisation des services par machine virtuelle (et non par compte), depuis la réplication initiale d'une machine virtuelle. Nous résilions une réplication en cours au bout de 90 jours, à moins qu'un client ne demande une augmentation de la limite.
- 50 migrations d'applications simultanées par compte, avec une limite de 10 groupes et de 50 serveurs dans chaque application.

Tarification

L'utilisation d'AWS Server Migration Service n'engendre pas des frais supplémentaires. Vous payez les frais standard qui s'appliquent aux instances EC2 que vous exécutez, ainsi que pour les compartiments S3, volumes EBS et opérations de transfert de données ayant servi lors du processus de migration. Pour en savoir plus, consultez Tarification de AWS Server Migration Service.

Exigences relatives à AWS Server Migration Service

Votre environnement VMware vSphere, Microsoft Hyper-V/SCVMM ou Microsoft Azure doit respecter les exigences suivantes pour pouvoir utiliser Server Migration Service afin de migrer vos serveurs virtualisés sur site vers Amazon EC2.

Prérequis

Conditions requises générales

Avant de configurer AWS SMS, assurez-vous d'avoir fait le nécessaire pour répondre à l'ensemble des exigences suivantes.

Tous les VMs

- Désactivez tout logiciel anti-virus ou de détection d'intrusions sur la machine virtuelle que vous migrez. Ces services peuvent être réactivés une fois le processus de migration terminé.
- Déconnectez tous les lecteurs de CD-ROM (virtuels ou physiques) connectés à la machine virtuelle.

Machines virtuelles Windows

- Activez Bureau à distance (Remote Desktop, RDP) pour un accès distant.
- Installez la version appropriée de .NET Framework sur la machine virtuelle. Notez que .NET Framework 4.5 ou supérieur est installé automatiquement sur votre machine virtuelle si nécessaire.

Version Windows	Version .NET Framework
Windows Server 2008 ou version antérieure	3.5 ou version ultérieure
Windows Server 2008 R2 ou version ultérieure	4.5 ou version ultérieure
Windows 8 ou version antérieure	3.5 ou version ultérieure
Windows 8.1 ou version ultérieure	4.5 ou version ultérieure

- Pendant la préparation d'une machine virtuelle Microsoft Windows à la migration, configurez une taille de fichier d'échange fixe et assurez-vous d'avoir au moins 6 Gio d'espace disponible sur le volume racine. Ceci est nécessaire pour que les pilotes soient correctement installés.
- Assurez-vous que le pare-feu hôte (comme le pare-feu Windows) autorise l'accès à RDP. Autrement, vous serez dans l'incapacité d'accéder à votre instance une fois la migration terminée.

- Appliquez les correctifs logiciels suivants :
  - `RealTimeIsUniversal`Vous ne pouvez pas modifier l'heure du système si l'entrée de Registre est activée dans Windows
  - Utilisation élevée de l'UC au cours du passage de l'heure d'été dans Windows Server 2008, Windows 7 ou Windows Server 2008 R2
- Les types d'instances suivants sont les seuls qui prennent en charge les AMIs 32 bits : `t2.nano`, `t2.micro`, `t2.small`, `t2.medium`, `c3.large`, `t1.micro`, `m1.small`, `m1.medium` et `c1.medium`. Si vous migrez une instance 32 bits, vous êtes limité à ces types d'instance et aux régions qui les prennent en charge.

Machines virtuelles Linux

- Activez Secure Shell (SSH) pour un accès distant.
- Assurez-vous que le pare-feu hôte (comme iptables) autorise l'accès à SSH. Autrement, vous serez dans l'incapacité d'accéder à votre instance une fois la migration terminée.
- Assurez-vous que vous avez configuré un utilisateur non-racine pour utiliser SSH basé sur une clé publique afin d'accéder à votre instance après son importation. L'utilisation du SSH basé sur un mot de passe et la connexion racine via SSH sont possibles, mais nous ne le recommandons pas. Nous recommandons d'utiliser des clés publiques et un utilisateur non-racine car ceux-ci sont plus sécurisés. Votre machine virtuelle Linux ne disposera pas d'un`ec2-user`compte créé dans le cadre du processus de migration.
- Assurez-vous que votre machine virtuelle Linux utilise GRUB (GRUB hérité) ou GRUB 2 comme chargeur de démarrage.
- Veillez à ce que le volume racine de votre machine virtuelle Linux utilise l'un des systèmes de fichiers suivants :
  - EXT2
  - EXT3
  - EXT4
  - Btrfs
  - JFS
  - XFS
- Les machines virtuelles Linux migrées doivent utiliser des images 64 bits. La migration d'images Linux 32 bits n'est pas prise en charge.
- Les machines virtuelles Linux migrées doivent utiliser des noyaux par défaut pour de meilleurs résultats. La migration de machines virtuelles qui utilisent des noyaux Linux personnalisés risque d'échouer.
- Lorsque vous préparez des machines virtuelles Amazon EC2 Linux pour la migration, assurez-vous d'avoir au moins 250 MiB d'espace disque disponible sur le volume racine pour installer les pilotes et les autres logiciels.

Modifications par programmation apportées aux machines virtuelles

Lors de l'importation d'une machine virtuelle,AWSmodifie le système de fichiers pour rendre la VM importée accessible au client. Les actions suivantes peuvent avoir lieu :

- [Linux] Installation de pilotes PV Citrix directement dans le système d'exploitation ou modification de initrd/initramfs pour les contenir.
- [Linux] Modification des scripts réseau pour remplacer les adresses IP statiques par des adresses IP dynamiques.
- [Linux] Modification de `/etc/fstab`, en mettant en commentaire les entrées non valides et en remplaçant les noms d'appareil par des UUID. Si aucun UUID correspondant n'est trouvé pour un appareil, l'option `nofail` est ajoutée à la description de l'appareil. Vous devrez corriger les noms

d'appareil et supprimer `nofail` après l'importation. Comme bonne pratique lors de la préparation de vos machines virtuelles pour l'importation, nous vous recommandons d'utiliser des UUID pour spécifier vos périphériques de disques de machine virtuelle plutôt que des noms d'appareil.

Les entrées dans `/etc/fstab` qui contiennent des types de système de fichiers distribués (cifs, smbfs, vboxsf, sshfs, etc.) seront désactivées.

- [Linux] Modification de paramètres de programme d'amorçage grub, comme le délai d'attente et l'entrée par défaut.
- [Windows] Modification des paramètres du registre pour rendre la machine virtuelle démarrable.

Lorsque vous écrivez un fichier modifié,AWSconserve le fichier d'origine au même emplacement sous un nouveau nom.

Operating systems

Les systèmes d'exploitation suivants peuvent être migrés vers EC2 à l'aide de SMS :

Windows (32 bits et 64 bits)

- Microsoft Windows Server 2003 (Standard, Datacenter, Enterprise) avec le Service Pack 1 (SP1) ou ultérieur (32 et 64 bits)
- Microsoft Windows Server 2003 R2 (Standard, Datacenter, Enterprise) (32 et 64 bits)
- Microsoft Windows Server 2008 (Standard, Datacenter, Enterprise) (32 et 64 bits)
- Microsoft Windows Server 2008 R2 (Standard, Web Server, Datacenter, Enterprise) (64 bits uniquement)
- Microsoft Windows Server 2012 (Standard, Datacenter) (64 bits uniquement)
- Microsoft Windows Server 2012 R2 (Standard, Datacenter) (64 bits uniquement) (installation de serveur Nano non prise en charge)
- Microsoft Windows Server 2016 (Standard, Datacenter) (64 bits uniquement)
- Microsoft Windows Server 1709 (Standard, Datacenter) (64 bits uniquement)
- Microsoft Windows Server 1803 (Standard, Datacenter) (64 bits uniquement)
- Microsoft Windows Server 2019 (Standard, Datacenter) (64 bits uniquement)
- Microsoft Windows 7 (Famille, Professionnel, Entreprise, Édition Intégrale) (Français, France) (32 et 64 bits)
- Microsoft Windows 8 (Famille, Professionnel, Entreprise) (Français, France) (32 et 64 bits)
- Microsoft Windows 8.1 (Professionnel, Entreprise) (Français, France) (64 bits uniquement)
- Microsoft Windows 10 (Famille, Professionnel, Entreprise, Education) (Français, France) (64 bits uniquement)

Linux/Unix (64 bits)

- Ubuntu 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 16.04, 16.10, 17.04, 18.04
- Red Hat Enterprise Linux (RHEL) 5.1-5.11, 6.1-6.9, 7.0-7.6 (6.0 ne dispose pas des pilotes requis)
- SUSE Linux Enterprise Server 11 avec le Service Pack 1 et le noyau 2.6.32.12-0.7
- SUSE Linux Enterprise Server 11 avec le Service Pack 2 et le noyau 3.0.13-0.27
- SUSE Linux Enterprise Server 11 avec le Service Pack 3 et le noyau 3.0.76-0.11, 3.0.101-0.8 ou 3.0.101-0.15
- SUSE Linux Enterprise Server 11 avec le Service Pack 4 et le noyau 3.0.101-63
- SUSE Linux Enterprise Server 12 avec le noyau 3.12.28-4
- SUSE Linux Enterprise Server 12 avec le Service Pack 1 et le noyau 3.12.49-11

- SUSE Linux Enterprise Server 12 avec le Service Pack 2 et le noyau 4.4
- SUSE Linux Enterprise Server 12 avec le Service Pack 3 et le noyau 4.4
- CentOS 5.1-5.11, 6.1-6.6, 7.0-7.6 (6.0 ne dispose pas des pilotes requis)
- Debian 6.0.0-6.0.8, 7.0.0-7.8.0, 8.0.0
- Oracle Linux 5.10-5.11 avec suffixe de noyau el5uek
- Oracle Linux 6.1-6.10 avec noyau compatible RHEL 2.6.32 ou noyaux UEK 3.8.13, 4.1.12
- Oracle Linux 7.0-7.6 avec noyau compatible RHEL 3.10.0 ou noyaux UEK 3.8.13, 4.1.12, 4.14.35
- Fedora Server 19-21

Types de volumes et systèmes de fichiers

AWS Server Migration Service prend en charge la migration d'instances Windows et Linux avec les systèmes de fichiers suivants :

Système d'exploitation	Système de fichiers	Architecture	Table de partition	Types de données pris en charge	Volumes de démarrage pris en
Windows	NTFS	32 bits	MBR	✓	✓
			GPT	✓	
		64 bits	MBR	✓	✓
			GPT	✓	✓ (VHDX uniquement)
	ReFS	32 bits	MBR		
			GPT		
		64 bits	MBR	✓	
			GPT	✓	
Linux/Unix	Ext2, ext3, ext4, Btrfs, JFS, XFS	64 bits	MBR	✓	✓
			GPT	✓	

Les AMI avec des volumes utilisant le chiffrement EBS ne sont pas prises en charge. Lors de la migration des serveurs avec AWS SMS, n'activez pas le chiffrement par défaut. Si le chiffrement par défaut est déjà activé et que vous rencontrez des échecs de réplication delta, désactivez cette fonction.

Configurer un utilisateur IAM pour Server Migration Connector

Pour créer un utilisateur IAM pour Server Migration Connector dans votreAWScompte

1. Créez un utilisateur IAM avec lequel votre connecteur peut communiquer avecAWS. Enregistrez la clé d'accès et la clé secrète générées pour les utiliser au cours de la configuration initiale du connecteur.

Pour plus d'informations sur la gestion des utilisateurs et des autorisations IAM, consultezCréation d'un utilisateur IAM dans votreAWSCompte.

2. Attachez la stratégie gérée IAMServerMigrationConnectorpour l'utilisateur IAM. Pour en savoir plus, consultez Stratégies gérées et stratégies en ligne.

Limites

Les limites suivantes s'appliquent.

Limites

Format d'image

- Lors de la migration de machines virtuelles gérées par Hyper-V/SCVMM, SMS prend en charge les machines virtuelles de génération 1 (utilisant le format de disque VHD ou VHDX) et de génération 2 (VHDX uniquement).
- AWS SMS ne prend pas en charge les machines virtuelles sur Hyper-V exécutant n'importe quelle version de RHEL 5 basée sur un disque VHDX. Nous vous recommandons de convertir les disques de ce format en VHD pour la migration.
- AWS SMS ne prend pas en charge les machines virtuelles qui combinent des fichiers au format de disque VHD et VHDX.
- Sur VMware, AWS SMS ne prend pas en charge les machines virtuelles qui utilisent RDM (Raw Device Mapping). Seules les images de disque VMDK sont prises en charge.

Démarrage

- Les partitions de démarrage UEFI/EFI sont prises en charge uniquement pour les volumes de démarrage Windows avec VHDX comme format d'image. Sinon, le volume de démarrage d'une machine virtuelle doit utiliser des partitions MBR (enregistrement de démarrage principal). Dans les deux cas, le volume de démarrage ne peut pas dépasser 2 Tio (non compressé) en raison de limitations liées à MBR.

  Note

  QuandAWSdétecte un volume de démarrage GPT Windows avec une partition de démarrage UEFI, il le convertit on-the-fly sur un volume de démarrage MBR avec une partition de démarrage BIOS. Cela est dû au fait qu'EC2 ne prend pas directement en charge les volumes de démarrage GPT.
- Une machine virtuelle importée peut ne pas démarrer si la partition racine ne se trouve pas sur le même disque dur virtuel que le MBR.
- Une machine virtuelle migrée peut ne pas démarrer si la partition racine ne se trouve pas sur le même disque dur virtuel que le MBR.
- La migration de machines virtuelles avec des configurations à double démarrage n'est pas prise en charge.

Réseaux

- Les interfaces réseau multiples ne sont pas prises en charge actuellement. Une fois la migration terminée, votre machine virtuelle aura une seule interface réseau virtuelle qui utilise DHCP pour attribuer des adresses. Votre instance reçoit une adresse IP privée.
- Une VM migrée dans un VPC ne reçoit pas d'adresse IP publique, quel que soit le réglage d'auto-attribution d'adresse IP publique pour le sous-réseau. Sinon, vous pouvez attribuer une adresse IP Elastic à votre compte et l'associer à votre instance.
- Les adresses IP Internet Protocol version 6 (IPv6) ne sont pas prises en charge.

Importation d'applications depuis Migration Hub

- SMS importe les serveurs liés aux applications depuis AWS Migration Hub uniquement s'ils existent dans le catalogue de serveurs SMS. Par conséquent, certaines applications peuvent être importées partiellement uniquement.
- Si aucun des serveurs d'une application Migration Hub n'existe dans le catalogue de serveurs SMS, l'importation échoue silencieusement et l'application n'est pas visible dans SMS.
- Les applications importées peuvent être migrées, mais ne peuvent pas être modifiées dans SMS. Elles peuvent toutefois être modifiées dans Migration Hub.

Divers

- Une tâche de réplication SMS échouera pour les machines virtuelles avec plus de 22 volumes attachés.
- Les AMI avec des volumes utilisant le chiffrement EBS ne sont pas prises en charge. Lors de la migration des serveurs avec AWS SMS, n’activez pas le chiffrement par défaut. Si le chiffrement par défaut est déjà activé et que vous rencontrez des échecs de réplication delta, désactivez cette fonction.
- AWS SMS crée des AMI qui utilisent la virtualisation HVM. Il ne peut pas créer d'AMI qui utilisent la virtualisation PV. Les pilotes PVHVM Linux sont pris en charge au sein des machines virtuelles migrées.
- Les machines virtuelles qui sont créées suite à une conversion P2V ne sont pas prises en charge. Une conversion P2V a lieu lorsqu'une image de disque est créée en effectuant un processus d'installation Linux ou Windows sur une machine physique, puis en important une copie de cette installation Linux ou Windows dans une machine virtuelle.
- AWS SMS n'installe pas les pilotes Single-Root I/O virtualization (SR-IOV), sauf avec les importations de machine virtuelles Microsoft Windows Server 2012 R2. Ces pilotes ne sont pas nécessaires, sauf si vous envisagez d'utiliser la mise en réseau améliorée qui offre des performances (paquet par seconde) plus élevées, ainsi qu'une instabilité et une latence réseau réduites. Pour les machines virtuelles Microsoft Windows Server 2012 R2, les pilotes SR-IOV sont installés automatiquement dans le cadre du processus de migration.
- Les disques indépendants n'étant pas affectés par les instantanés, AWS SMS ne prend pas en charge la réplication avec intervalle pour les VMDK en mode indépendant.
- Les packs de langues Windows qui utilisent des caractères UTF-16 (ou non-ASCII) ne sont pas pris en charge pour l'importation. Nous vous recommandons d'utiliser le pack de langue anglaise lors de l'importation de machines virtuelles Windows Server 2003, Windows Server 2008 et Windows Server 2012 R1.
- Pour Windows Server 2003, désactivez les vérifications de signature de pilote Windows avant la migration.

Options de licence pourAWS SMS

Lorsque vous créez une nouvelle tâche de réplication, leAWS Server Migration ServiceAPI etAWS CLIinclut une option License type. Si vous choisissez un type de licence incompatible avec votre VM, la tâche de réplication échoue et un message d'erreur apparaît. Les valeurs possibles sont :

- Auto (par défaut)

  Détecte le système d'exploitation (OS) source-système et applique la licence adéquate à la machine virtuelle (VM) migrée.
- AWS

  Remplace la licence du système source par unAWSlicence, le cas échéant, sur la VM migrée.
- BYOL

  Conserve la licence source-système, le cas échéant, sur la VM migrée.

AWS CLIexemple :

```
aws sms create-replication-job --license-type value
```

La valeur du`--license-type`paramètre peut être`AWS`ou`BYOL`. La valeur par défaut est `Auto`.

Choix de licence pour Linux

Les systèmes d'exploitation Linux prennent en charge les licences BYOL uniquement. ChoixAuto(valeur par défaut) signifie que SMS utilise une licence BYOL.

Les machines virtuelles Red Hat Enterprise Linux (RHEL) migrées doivent utiliser des licences Cloud Access (BYOL). Pour plus d'informations, voir Red Hat Cloud Access sur le site Web de Red Hat.

Les machines virtuelles SUSE Linux Enterprise Server migrées doivent utiliser des licences SUSE Public Cloud Program (BYOS). Pour plus d'informations, consultez le document SUSE Public Cloud Program—Bring Your Own Subscription.

Choix de licence pour Windows

Les systèmes d'exploitation Windows Server prennent en charge BYOL ouAWSlicences. Les systèmes d'exploitation de client Windows (par exemple, Windows 10) prennent en charge les licences BYOL uniquement.

Si vous choisissezAuto(valeur par défaut),AWS SMSutilise leAWSsi la VM dispose d'un système d'exploitation de serveur. Si la VM dispose d'un système d'exploitation client, la licence BYOL est utilisée.

Les règles suivantes s'appliquent lorsque vous utilisez votre licence Microsoft BYOL, soit par MSDN, soit par Windows Software Assurance Per User :

- Vos instances BYOL sont facturées selon la tarification des instances Linux Amazon EC2 en vigueur, dans la mesure où vous entrez dans les conditions suivantes :
  - Exécutez sur un hôte dédié (Hôtes dédiés)
  - Lancez depuis les VM provenant de binaires logiciels fournis par vous-même à l'aide d'AWS SMS, sujet aux termes et capacités actuels d'AWS SMS
  - Désignez les instances en tant qu'instance BYOL

  - Exécutez les instances au sein de votre instance désignéeAWSRégions et oùAWSpropose le modèle BYOL
  - Activez à l'aide des clés Microsoft que vous fournissez ou qui sont utilisées dans votre système de gestion de clé
- Vous devez tenir compte du fait que lorsque vous démarrez une instance Amazon EC2, celle-ci peut s'exécuter sur n'importe quel des nombreux serveurs au sein d'une zone de disponibilité. Cela signifie que chaque fois que vous démarrez une instance Amazon EC2 (y compris avec un arrêt/démarrage), celle-ci peut s'exécuter sur un serveur différent au sein d'une zone de disponibilité. Vous devez tenir compte de ce fait en gardant à l'ESPRIT les limitations concernant la réaffectation de licence décrites dans les conditions relatives aux produits de licences en volume de Microsoft, disponibles sur l'Conditions de licence, ou consultez vos droits d'utilisation spécifiques pour déterminer si ceux-ci sont cohérents avec cette utilisation.
- Vous devez être éligible pour utiliser le programme BYOL pour le logiciel Microsoft applicable dans le cadre de votre ou vos accords avec Microsoft, par exemple, dans le cadre de vos droits d'utilisateur MSDN ou de vos droits Windows Software Assurance par utilisateur. Vous assumez l'entière responsabilité d'obtenir toutes les licences requises et de vous conformer à toutes les exigences concernant les licences, y compris les PUR/PT. En outre, vous devez avoir accepté le Contrat de Licence Utilisateur Final de Microsoft (CLUF Microsoft), et en utilisant le logiciel Microsoft dans le cadre du programme BYOL, vous acceptez le CLUF Microsoft.
- AWSvous recommande de consulter vos propres conseillers juridiques et autres pour comprendre les exigences relatives aux licences Microsoft applicables et vous y conformer. L'utilisation du paramètre Services (y compris l'utilisation du paramètre licenseType et de l'indicateur BYOL) en violation de vos accords avec Microsoft n'est pas autorisée.

Autres exigences

Prise en charge de VMware vMotion

AWS Server Migration Service prend partiellement en charge vMotion, Storage vMotion et d'autres fonctions basées sur la migration de machines virtuelles (comme DRS et Storage DRS) soumises aux limitations suivantes :

- La migration d'une machine virtuelle vers un nouvel hôte ESXi ou un magasin de données une fois qu'un cycle de réplication est terminé et avant que le prochain cycle ne démarre, est prise en charge tant que le compte du service vCenter du Server Migration Connector du Server Migration Connector dispose des autorisations nécessaires sur l'hôte ESXi, les magasins de données et le centre de données et sur le machine virtuelle elle-même au nouvel emplacement.
- La migration d'une machine virtuelle vers un nouvel hôte ESXi, un magasin de données et/ou un centre de données n'est pas prise en charge quand un cycle de réplication est en cours, c'est-à-dire pendant le chargement d'une machine virtuelle.
- L'utilisation de Cross vCenter vMotion n'est pas prise en charge avecAWS SMS.

Prise en charge de VMware vSAN

Les machines virtuelles sur les magasins de données vSAN sont uniquement prises en charge lorsque le paramètre Replication job type de la page Configure replication jobs settings est défini sur One-time migration.

Prise en charge des volumes virtuels VMware (VVol)

AWSne prend pas en charge la migration des volumes virtuels VMware. Cependant, certaines implémentations peuvent fonctionner.

Machines virtuelles VMware avec des instantanés

AWS SMS prend en charge que la migration unique sur les machines virtuelles où un logiciel de sauvegarde basé sur un instantané est utilisé. De plus, évitez de créer des instantanés sur des machines virtuelles répliquées via AWS SMS.

Points de contrôle Hyper-V

AWS SMSne prend pas en charge les machines virtuelles dotées de points de contrôle existants.

Disque de différenciation Hyper-V

AWS SMSne prend pas en charge les machines virtuelles dotées de disques différenciés.

Installation du connecteur de migration de serveur

Le connecteur de migration de serveur est une machine virtuelle FreeBSD que vous pouvez installer dans votre environnement de virtualisation sur site. Les plates-formes prises en charge sont VMware vSphere, Microsoft Hyper-V/SCVMM et Microsoft Azure.

Table des matières

Installation du connecteur de migration de serveur sur VMware

Utilisez les informations suivantes pour installer le connecteur de migration de serveur afin de pouvoir utiliserAWS SMSpour migrer des machines virtuelles depuis un environnement VMware vers Amazon EC2.

Ces informations s'appliquent uniquement à des machines virtuelles dans un environnement VMware sur site. Pour plus d'informations sur l'installation du connecteur sur d'autres environnements, consultez Installation du connecteur de migration de serveur (p. 11).

Exigences pour le connecteur VMware

- vCenter version 5.1 ou supérieure (jusqu'à la version 6.7)
- ESXi 5.1 ou supérieure (jusqu'à la version 6.7)
- Minimum : 8 Gio de RAM
- Capacité minimum de stockage de disque de 20 Gio (allocation dynamique) ou de 250 Gio (allocation fixe)
- Prise en charge des services réseau suivants. Notez que vous devrez peut-être reconfigurer votre pare-feu pour autoriser des connexions sortantes avec état à partir du connecteur vers ces services.
  - DNS : autorisez le connecteur à initier des connexions vers le port 53 pour la résolution des noms.
  - HTTPS sur vCenter : permet au connecteur d'initier des connexions Web sécurisées vers le port 443 de vCenter. Vous pouvez également configurer un port autre que le port par défaut, à votre discrétion. Si votre vCenter Server est configuré pour utiliser un port autre le port par défaut, spécifiez le port et le nom d'hôte de vCenter, séparé par deux points (à titre d'exemple, `HOSTNAME:PORT` or `IP:PORT`) sur la page vCenter Service Account dans Connector setup.
  - HTTPS sur ESXi : permet au connecteur d'initier des connexions Web sécurisées vers le port 443 des hôtes ESXi comprenant les machines virtuelles que vous prévoyez de migrer.
  - NTP : autorise (si besoin) le accès sortant du du connecteur au port 123 pour la synchronisation de l'heure. Si le connecteur synchronise son horloge avec l'hôte ESXi, cela n'est pas nécessaire.
- Autorisez les connexions depuis le connecteur vers les URL suivantes :
  - *.amazonaws.com
  - *.aws.amazon.com

Pour configurer le connecteur pour un environnement VMware

1. Téléchargez le connecteur pour les environnements VMware à partir du lien suivant :https://s3.amazonaws.com/sms-connector/AWS-SMS-Connector.ova. Le connecteur est une machine virtuelle FreeBSD préconfigurée au format OVA qui est prête pour le déploiement dans votre vCenter.

   Somme de contrôle d'intégrité

   - MD5—https://s3.amazonaws.com/sms-connector/AWS-SMS-Connector.ova.md5
   - SHA256—https://s3.amazonaws.com/sms-connector/AWS-SMS-Connector.ova.sha256
2. Configurez votre compte de service vCenter. Créez un utilisateur vCenter avec les autorisations nécessaires pour créer et supprimer des instantanés sur des machines virtuelles qui doivent être migrées versAWSet téléchargez leurs disques Delta.

   Note

   La bonne pratique consiste à limiter les autorisations vCenter pour le compte de service du connecteur uniquement aux centres de données vCenter qui contiennent les machines virtuelles que vous prévoyez de migrer. Nous vous conseillons également de verrouiller vos autorisations d'accès au compte de service vCenter en affectant le NoAccess dans vCenter sur les hôtes, les dossiers et les magasins de données qui n'ont aucune machine virtuelle à migrer.
3. Créez un rôle dans vCenter avec les privilèges suivants :

   - Datastore > Browse datastore and Low level file operations (Datastore.Browse and Datastore.FileManagement)
   - Host > Configuration > System Management (Host.Config.SystemManagement)
   - vApp > Export (VApp.Export)
   - Virtual Machine > Snapshot management > Create snapshot and Remove Snapshot (VirtualMachine.State.CreateSnapshot et VirtualMachine.State.RemoveSnapshot)
4. Attribuez le rôle comme suit :

   a. Attribuez ce rôle vCenter au compte de service que le connecteur utilisera pour se connecter à vCenter.

   b. Attribuez ce rôle avec les autorisations qui en découlent aux centres de données qui contiennent les machines virtuelles à migrer.
5. Pour vérifier manuellement les autorisations de votre compte de service vCenter, vérifiez que vous pouvez vous connecter à vSphere Client avec vos informations d'identification de compte de service de connecteur. Ensuite, exportez vos machines virtuelles sous forme de modèles OVF, utilisez le navigateur du magasin de données pour télécharger les fichiers des magasins de données qui contiennent vos machines virtuelles et affichez les propriétés dans l'onglet Summary des hôtes ESXi de vos machines virtuelles.

Pour configurer le connecteur

1. Déployez le connecteur OVA téléchargé au cours de la procédure précédente dans votre environnement VMware à l'aide de vSphere Client.
2. Ouvrez la console de machine virtuelle du connecteur et connectez-vous en tant que `ec2-user` avec le mot de passe `ec2pass`. Indiquez une nouveau mot de passe si vous y êtes invité.
3. Obtenez l'adresse IP du connecteur comme suit :

   a. Exécutez la commande sudo setup.rb. Cela entraîne l'affichage du menu de configuration :

```
Choose one of the following options:
      1. Reset password
```

```
      2. Reconfigure network settings
      3. Restart services
      4. Factory reset
      5. Delete unused upgrade-related files
      6. Enable/disable SSL certificate validation
      7. Display connector's SSL certificate
      8. Generate log bundle
      0. Exit
Please enter your option [1-9]:
```

b. Entrez l'option 2. Vous affichez ainsi des informations sur le réseau en cours et un sous-menu pour apporter des modifications aux paramètres du réseau. La sortie doit ressembler à ce qui suit :

```
Current network configuration: DHCP
IP: 192.0.2.100
Netmask: 255.255.254.0
Gateway: 192.0.2.1
DNS server 1: 192.0.2.200
DNS server 2: 192.0.2.201
DNS suffix search list: subdomain.example.com
Web proxy: not configured

Reconfigure your network:
      1. Renew or acquire a DHCP lease
      2. Set up a static IP
      3. Set up a web proxy for AWS communication
      4. Set up a DNS suffix search list
      5. Exit
Please enter your option [1-5]:
```

Vous devez entrer cette adresse IP dans des procédures ultérieures.

4. [Facultatif] Configurez une adresse IP statique pour le connecteur. Cela vous évite de devoir reconfigurer les listes d'hôtes de confiance sur votre réseau local chaque fois que DHCP attribue une nouvelle adresse au connecteur.

   DansReconfigure votre réseaumenu, saisissez l'option2. Un formulaire permettant de fournir des paramètres réseau s'affiche :

   Pour chaque champ, indiquez une valeur appropriée et appuyez sur Entrée. Vous devez voir des résultats similaires à ce qui suit :

```
Setting up static IP:
      1. Enter IP address: 192.0.2.50
      2. Enter netmask: 255.255.254.0
      3. Enter gateway: 192.0.2.1
      4. Enter DNS 1: 192.0.2.200
      5. Enter DNS 2: 192.0.2.201

Static IP address configured.
```

5. Dans le menu de configuration réseau du connecteur, configurez les valeurs de suffixe de domaine pour la liste de recherche de suffixes DNS.
6. Si votre environnement utilise un proxy Web pour accéder à Internet, configurez-le maintenant.
7. Avant de quitter la console du connecteur, utilisezpingpour vérifier l'accès réseau aux cibles suivantes à l'intérieur et à l'extérieur de votre réseau local :

   - À l'intérieur de votre réseau local, vers vos hôtes ESXi et vCenter par nom d'hôte, nom de domaine complet et adresse IP
   - En dehors de votre réseau local, pourAWS

8. Dans un navigateur Web, accédez à la machine virtuelle du connecteur à partir de son adresse IP (https ://*adresse IP du connecteur*/) pour ouvrir l'assistant de configuration, puis choisissezPour commencer ».
9. Lisez le contrat de licence, sélectionnez la case à cocher, puis choisissez Next (Suivant).
10. Créez un mot de passe pour le connecteur.
11. ChoisissezChargement automatique de journauxetMise à niveau automatique du connecteur de migration automatique.
12. PourAWSRegion (Région), choisissez votre région dans la liste. PourAWSInformations d'identification, entrez les informations d'identification IAM que vous avez créées dansConfigurer un utilisateur IAM pour Server Migration Connector (p. 5). Choisissez Next (Suivant).
13. Dans vCenter Service Account, entrez le nom d'hôte, le nom d'utilisateur et le mot de passe vCenter de l'étape 3. Choisissez Next (Suivant).
14. Après avoir accepté le certificat vCenter, terminez l'inscription et affichez le tableau de bord de configuration.
15. Vérifiez que le connecteur que vous avez enregistré s'affiche sur la page Connectors. Si vous rencontrez un problème lors de l'enregistrement du connecteur, contactezsms-service@amazon.com.

Installation du connecteur de migration de serveur sur Hyper-V

AWS SMS prend en charge la migration selon deux modes : à partir de serveurs Hyper-V autonomes, ou depuis des serveurs Hyper-V gérés par System Center Virtual Machine Manager (SCVMM). Utilisez les informations suivantes pour installer le connecteur de migration de serveur sur Hyper-V afin de pouvoir utiliserAWS SMSpour migrer des machines virtuelles d'Hyper-V vers Amazon EC2.

Ces informations s'appliquent uniquement à des machines virtuelles dans un environnement Hyper-V sur site. Pour plus d'informations sur l'installation du connecteur sur d'autres environnements, consultez Installation du connecteur de migration de serveur (p. 11).

Considérations sur les scénarios de migration

- Les procédures d'installation pour un environnement Hyper-V autonome et des environnements SCVMM ne sont pas interchangeables.
- Lorsqu'une appliance Server Migration Connector est configurée en mode SCVMM, elle prend en charge la migration à partir d'un environnement SCVMM (qui peut gérer plusieurs serveurs Hyper-V).
- Lorsqu'une appliance Server Migration Connector est configurée en mode Hyper-V autonome, elle prend en charge la migration à partir de plusieurs serveurs Hyper-V.
- AWS SMSprend en charge le déploiement de n'importe quel nombre d'appliances de connecteur en vue d'assurer la migration à partir de plusieurs environnements SCVMM et de plusieurs serveurs Hyper-V autonomes en parallel.

Exigences pour le connecteur Hyper-V

- Rôle Hyper-V sur Windows Server 2012 R2 ou Windows Server 2016
- Active Directory 2012 ou version supérieure
- [Facultatif] SCVMM 2012 SP1 ou SCVMM 2016
- Minimum : 8 Gio de RAM
- Stockage sur disque disponible minimum de 300 Gio

- Prise en charge des services réseau suivants. Notez que vous devrez peut-être reconfigurer votre pare-feu pour autoriser des connexions sortantes avec état à partir du connecteur vers ces services.
  - DNS : autorisez le connecteur à initier des connexions vers le port 53 pour la résolution des noms.
  - HTTPS sur le port WinRM 5986 sur votre hôte SCVMM ou Hyper-V autonome
  - HTTPS entrant sur le port 443 du connecteur : permet au connecteur de recevoir des connexions Web sécurisées sur le port 443 en provenance d'hôtes Hyper-V comprenant les machines virtuelles que vous prévoyez de migrer.
  - NTP : autorise (si besoin) le accès sortant du du connecteur au port 123 pour la synchronisation de l'heure. Si le connecteur synchronise son horloge avec l'hôte Hyper-V, cela n'est pas nécessaire.
- Autorisez les connexions depuis le connecteur vers les URL suivantes :
  - *.amazonaws.com
  - *.aws.amazon.com

Table des matières

À propos du script d'installation du connecteur de migration de serveur

Le script de configuration d'AWS SMS automatise la création des autorisations appropriées et des connexions réseau qui permettent à AWS SMS d'exécuter des tâches sur votre environnement Hyper-V. Vous devez exécuter le script en tant qu'administrateur sur chaque hôte Hyper-V et SCVMM que vous prévoyez d'utiliser lors de la migration de machines virtuelles. Lorsque vous exécutez le script, celui-ci effectue les actions suivantes :

1. [Tous les systèmes] Vérifie si le service Gestion à distance de Windows (WinRM) est activé sur SCVMM et tous les hôtes Hyper-V, l'active si nécessaire et le configure de sorte qu'il démarrer automatiquement lors de l'initialisation.
2. [Tous les systèmes]Active PowerShell à distance, ce qui permet au connecteur d'exécuter des commandes PowerShell sur cet hôte via une connexion WinRM.
3. [Tous les systèmes] Crée un certificat X.509 auto-signé, crée un écouteur HTTPS WinRM et lie le certificat à l'écouteur.
4. [Tous les systèmes] Crée une règle de pare-feu pour accepter les connexions entrantes vers l'écouteur WinRM.
5. [Tous les systèmes]Ajoute l'adresse IP ou le nom de domaine du connecteur à la liste des hôtes approuvés dans la configuration WinRM. Vous devez configurer cette adresse IP ou ce nom de domaine avant d'exécuter le script, afin de pouvoir fournir cette information de manière interactive.
6. [Tous les systèmes] Active l'authentification CredSSP (Credential Security Support Provider) avec WinRM.
7. [Tous les systèmes] Accorde les autorisations de lecture et d'exécution à un utilisateur Active Directory préconfiguré sur WinRM configSDDL. Cet utilisateur est le même que le compte de service décrit ci-après dans Étape 1 : Créer un compte de service pour Server Migration Connector dans Active Directory (p. 16).

8. [Hyper-V autonome uniquement] Ajoute l'utilisateur Active Directory aux groupes Administrateurs et Utilisateurs de gestion à distance Hyper-V sur votre hôte Hyper-V.
9. [Hyper-V autonome uniquement] Accorde les autorisations en lecture seule sur tous les dossiers de données de machine virtuelle gérés par cette machine virtuelle Hyper-V.
10. [SCVMM uniquement] Accorde les autorisations « Méthodes d'exécution », « Activer le compte » et « Appel à distance autorisé » à l'utilisateur Active Directory sur deux objets WMI, CIMV2 et SCVMM.
11. [SCVMM uniquement] Crée un rôle Administrateur délégué dans SCVMM avec des autorisations d'accès à tous les hôtes Hyper-V. Le rôle est affecté à l'utilisateur Active Directory. Vous pouvez supprimer l'accès aux hôtes de manière sélective en modifiant ce rôle dans SCVMM.
12. [SCVMM uniquement] Vérifie si un chemin de réseau sécurisé (HTTPS) existe entre SCVMM et les hôtes Hyper-V. Si le script ne détecte pas de canal sécurisé, il renvoie une erreur et génère des instructions pour que l'administrateur sécurise le canal.
13. [SCVMM uniquement] Itère sur tous les hôtes Hyper-V gérés par SCVMM et accorde à l'utilisateur Active Directory des autorisations en lecture seule sur tous les dossiers de machine virtuelle sur chaque hôte Hyper-V.

Étape 1 : Créer un compte de service pour Server Migration Connector dans Active Directory

Le connecteur de migration de serveur requiert un compte de service dans Active Directory. À mesure que le script de configuration du connecteur est exécuté sur chaque hôte SCVMM et Hyper-V, il accorde à ce compte les autorisations sur ces hôtes.

> Note
>
> Une fois configuré en mode SCVMM, l'hôte SCVMM et tous les hôtes Hyper-V qu'il gère doivent être regroupés dans un domaine Active Directory unique. Si vous avez plusieurs domaines Active Directory, configurez un connecteur pour chacun d'eux.

Pour créer l'utilisateur Active Directory

1. À l'aide du Centre d'administration Active Directory de l'ordinateur Windows sur lequel votre forêt Active Directory est installée, créez un nouvel utilisateur et attribuez-lui un mot de passe.
2. Ajoutez le nouvel utilisateur au groupe Utilisateurs de gestion à distance.

Étape 2 : Télécharger et déployer le connecteur de migration de serveur

Télécharger leConnecteur de migration de serveur pour Hyper-V et SCVMMsur votre environnement sur site et installez-le sur un hôte Hyper-V.

Pour configurer le connecteur pour un environnement Hyper-V

1. Téléchargez le connecteur pour Hyper-V en utilisant le lien suivant :https://s3.amazonaws.com/sms-connector/AWS-SMS-Connector-for-SCVMM-HyperV.zip.

   Somme de contrôle d'intégrité

   - MD5—https://s3.amazonaws.com/sms-connector/AWS-SMS-Connector-for-SCVMM-HyperV.zip.md5
   - SHA256—https://s3.amazonaws.com/sms-connector/AWS-SMS-Connector-for-SCVMM-HyperV.zip.sha256

2. Transférez le fichier de connecteur téléchargé vers votre hôte Hyper-V, décompressez-le et importez le connecteur en tant que machine virtuelle.
3. Ouvrez la console de machine virtuelle du connecteur et connectez-vous en tant que `ec2-user` avec le mot de passe `ec2pass`. Indiquez une nouveau mot de passe si vous y êtes invité.
4. Obtenez l'adresse IP du connecteur comme suit :

   a. Exécutez la commande sudo setup.rb. Cela entraîne l'affichage du menu de configuration :

```
Choose one of the following options:
      1. Reset password
      2. Reconfigure network settings
      3. Restart services
      4. Factory reset
      5. Delete unused upgrade-related files
      6. Enable/disable SSL certificate validation
      7. Display connector's SSL certificate
      8. Generate log bundle
      0. Exit
Please enter your option [1-9]:
```

   b. Entrez l'option 2. Vous affichez ainsi des informations sur le réseau en cours et un sous-menu pour apporter des modifications aux paramètres du réseau. La sortie doit ressembler à ce qui suit :

```
Current network configuration: DHCP
IP: 192.0.2.100
Netmask: 255.255.254.0
Gateway: 192.0.2.1
DNS server 1: 192.0.2.200
DNS server 2: 192.0.2.201
DNS suffix search list: subdomain.example.com
Web proxy: not configured

Reconfigure your network:
      1. Renew or acquire a DHCP lease
      2. Set up a static IP
      3. Set up a web proxy for AWS communication
      4. Set up a DNS suffix search list
      5. Exit
Please enter your option [1-5]:
```

   Vous devez entrer cette adresse IP dans des procédures ultérieures.
5. [Facultatif] Configurez une adresse IP statique pour le connecteur. Cela vous évite de devoir reconfigurer les listes d'hôtes de confiance sur votre réseau local chaque fois que DHCP attribue une nouvelle adresse au connecteur.

   DansReconfigure votre réseaumenu, saisissez l'option2. Un formulaire permettant de fournir des paramètres réseau s'affiche :

   Pour chaque champ, indiquez une valeur appropriée et appuyez sur Entrée. Vous devez voir des résultats similaires à ce qui suit :

```
Setting up static IP:
      1. Enter IP address: 192.0.2.50
      2. Enter netmask: 255.255.254.0
      3. Enter gateway: 192.0.2.1
      4. Enter DNS 1: 192.0.2.200
      5. Enter DNS 2: 192.0.2.201

Static IP address configured.
```

6. Dans le menu de configuration réseau du connecteur, configurez les valeurs de suffixe de domaine pour la liste de recherche de suffixes DNS.
7. Si votre environnement utilise un proxy Web pour accéder à Internet, configurez-le maintenant.
8. Avant de quitter la console du connecteur, utilisezpingpour vérifier l'accès réseau aux cibles suivantes à l'intérieur et à l'extérieur de votre réseau local :

   - À l'intérieur de votre réseau local, vers vos hôtes Hyper-V et SCVMM par nom d'hôte, nom de domaine complet et adresse IP
   - En dehors de votre réseau local, pourAWS

Étape 3 : Télécharger et installer le script de configuration Hyper-V/SCVMM

AWS SMSfournit un logiciel téléchargeable PowerShell afin de configurer l'environnement Windows de sorte qu'il prenne en charge les communications avec le connecteur de migration de serveur. Le même script est utilisé pour la configuration d'un hôte Hyper-V autonome ou SCVMM. Ce script est signé de façon chiffrée par AWS.

Téléchargez le script et les fichiers de hachage à partir des URL suivantes :

Fichier	URL
Script d'installation	https://s3.amazonaws.com/sms-connector/aws-sms-hyperv-setup.ps1
hachage MD5	https://s3.amazonaws.com/sms-connector/aws-sms-hyperv-setup.ps1.md5
hachage SHA256	https://s3.amazonaws.com/sms-connector/aws-sms-hyperv-setup.ps1.sha256

Après avoir téléchargé les fichiers, transférez-les vers le ou les ordinateurs sur lesquels vous prévoyez d'exécuter le script.

Étape 4 : Valider l'intégrité et la signature cryptographique du fichier de script

Avant d'exécuter le script, nous vous recommandons de valider son intégrité et sa signature. Ces procédures supposent que vous avez téléchargé le script et les fichiers de hachage, que ceux-ci sont installés sur le bureau de l'ordinateur où vous prévoyez d'exécuter le script, et que vous êtes connecté en tant qu'administrateur. Vous devrez peut-être modifier les procédures en fonction de votre configuration.

Pour valider l'intégrité du script à l'aide de hachages cryptographiques (PowerShell)

1. Utilisez les fichiers de hachage téléchargés pour valider l'intégrité du fichier de script, ce qui garantit qu'il n'a pas été modifié lors de l'acheminement vers votre ordinateur.

   a. Pour procéder à la validation avec le hachage MD5, exécutez la commande suivante dans un PowerShell fenêtre :

```
PS C:\Users\Administrator> Get-FileHash aws-sms-hyperv-setup.ps1 -Algorithm MD5
```

Les informations renvoyées devraient être semblables à ce qui suit :

```
Algorithm         Hash
---------         ----
MD5               1AABAC6D068EEF6EXAMPLEDF50A05CC8
```

b. Pour procéder à la validation avec le hachage SHA256, exécutez la commande suivante dans un PowerShell fenêtre :

```
PS C:\Users\Administrator> Get-FileHash aws-sms-hyperv-setup.ps1 -Algorithm SHA256
```

Les informations renvoyées devraient être semblables à ce qui suit :

```
Algorithm         Hash
---------         ----
SHA256            6B86B273FF34FCE19D6B804EFF5A3F574EXAMPLE22F1D49C01E52DDB7875B4B
```

2. Comparez les valeurs de hachage renvoyées avec les valeurs fournies dans les fichiers téléchargés, `aws-sms-hyperv-setup.ps1.md5` et `aws-sms-hyperv-setup.ps1.sha256`.

Ensuite, utilisez l'interface utilisateur Windows ou PowerShell pour vérifier que le fichier de script inclut une signature valide duAWS.

Pour vérifier la validité de la signature cryptographique d'un fichier de script (interface utilisateur Windows)

1. Dans Windows Explorer, ouvrez le menu contextuel (clic droit) et choisissez Propriétés, Signatures numériques, Amazon Web Services et Détails.
2. Vérifiez que les informations affichées contiennent « Cette signature numérique est valide. » et que « Amazon Web Services, Inc. » est le signataire.

Pour vérifier la validité de la signature cryptographique d'un fichier de script (PowerShell)

- Dans un PowerShell , exécutez la commande suivante :

```
PS C:\Users\Administrator> Get-AuthenticodeSignature aws-sms-hyperv-setup.ps1 | Select
 *
```

Un fichier de script correctement signé doit renvoyer des informations similaires à ce qui suit :

```
SignerCertificate          : [Subject]
                               CN="Amazon Web Services, Inc." ...
                             [Issuer]
                               CN=DigiCert EV Code Signing CA (SHA2), OU=www.digicert.com,
 O=DigiCert Inc, C=US
...

TimeStamperCertificate     :
Status                     : Valid
StatusMessage              : Signature verified.
Path                       : C:\Users\Administrator\Desktop\aws-sms-hyperv-setup.ps1

...
```

Étape 5 : Exécutez le script

Cette procédure suppose que vous avez téléchargé le script sur le bureau de l'ordinateur où vous prévoyez de l'exécuter, et que vous êtes connecté en tant qu'administrateur. Vous devrez peut-être modifier la procédure en fonction de votre configuration.

> **Note**
>
> Si vous utilisez SCVMM, vous devez d'abord exécuter ce script sur chaque hôte Hyper-V à partir duquel vous prévoyez de procéder à une migration, puis l'exécuter sur SCVMM.

Exécuter le script sur chaque hôte

1. À l'aide du protocole RDP, connectez-vous à votre système SCVMM ou à votre hôte Hyper-V autonome en tant qu'administrateur.
2. Exécutez le script à l'aide des éléments suivants PowerShell Commande de l' :

```
PS C:\Users\Administrator> .\aws-sms-hyperv-setup.ps1
```

> **Note**
>
> Si vos recettes PowerShell La stratégie d'exécution est définie pour vérifier les scripts signés. Vous êtes invité à fournir une autorisation lors de l'exécution du script de configuration. Vérifiez que le script est publié par « Amazon Web Services, Inc. » et choisissez « R » pour courir une fois. Vous pouvez consulter ce paramètre en utilisant Get-ExecutionPolicy et le modifier en utilisant Set-ExecutionPolicy.

3. À mesure que le script s'exécute, il vous invite à indiquer plusieurs informations. Soyez prêt à répondre aux invites suivantes :

Action du script	Invite du client	Action du client
Invite à choisir une option selon le mode de fonctionnement du connecteur (migration à partir d'un Hyper-V autonome ou migration à l'aide de SCVMM), ce qui détermine les modifications devant être apportées à votre environnement Windows.	0. Quitter 1. Reconfigure standalone Hyper-V... 2. Reconfigure Hyper-V managed by SCVMM... 3. Reconfigure SCVMM... 4. Help/Support	Choisissez 0 pour quitter le script. Choisissez 1 pour reconfigurer un hôte Hyper-V autonome afin de permettre la migration de ses machines virtuelles invitées. Choisissez 2 pour reconfigurer un hôte Hyper-V afin d'autoriser SCVMM à gérer la migration de ses machines virtuelles invitées. Choisissez 3 pour reconfigurer SCVMM afin d'autoriser la migration des machines virtuelles invitées sur tous les hôtes Hyper-V qu'il gère. Option4liens vers ce document et vers des informations surAWSSupport.
Invite à indiquer l'utilisateur Active Directory que le connecteur utilise lors de la	Enter the AD user that the connector will use (DOMAIN \user)	Indiquez l'utilisateur Active Directory que vous avez configuré précédemment. Pour plus d'informations,

Action du script	Invite du client	Action du client
communication avec SCVMM et Hyper-V.		consultez Étape 1 : Créer un compte de service pour Server Migration Connector dans Active Directory (p. 16).
Demande l'adresse IP ou le nom d'hôte du connecteur.	Enter the IP Address or Hostname of the connector appliance	Fournissez l'adresse IP ou le nom d'hôte que vous avez configuré sur le connecteur.
Invite à confirmer votre choix avant la modification de votre environnement Windows.	Make changes to Windows system configuration? (Enter "yes" or "no")	Tapez « yes » et appuyez sur Entrée pour commencer la reconfiguration. Tapez « no » pour quitter le script.

Étape 6 : Configurez le connecteur

Lorsque la configuration du connecteur du a été correctement exécutée, accédez à l'interface Web du connecteur :

```
https://ip-address-of-connector/
```

Effectuez les étapes ci-dessous pour configurer le nouveau connecteur.

Pour configurer le connecteur

1. Sur la page de destination du connecteur, choisissez Get started now (Démarrer maintenant).
2. Lisez le contrat de licence, sélectionnez la case à cocher, puis choisissez Next (Suivant).
3. Créez un mot de passe pour le connecteur. Le mot de passe doit répondre aux critères affichés. Choisissez Next (Suivant).
4. Dans la pageInfos sur le réseau, vous pouvez, entre autres tâches, attribuer une adresse IP statique au connecteur si vous ne l'avez pas déjà fait. Choisissez Next (Suivant).
5. Dans la pageEnregistrez les téléchargements et les mises à niveau, sélectionnezChargement automatique de journauxetMise à niveau automatique du connecteur de migration automatique, et choisissezSuivant.
6. Sur la page Server Migration Service (Service de migration de serveur), fournissez les informations suivantes :

   - PourAWSRegion (Région), choisissez votre région dans la liste.
   - PourAWSInformations d'identification, entrez les informations d'identification IAM que vous avez créées dansConfigurer un utilisateur IAM pour Server Migration Connector (p. 5). Choisissez Next (Suivant).
7. Sur la page Choisir votre type de gestionnaire de machines virtuelles, sélectionnez Microsoft® System Center Virtual Manager (SCVMM) ou Microsoft® Hyper-V en fonction de votre environnement. SélectionVMware® vCenterUne erreur s'affiche si vous avez installé le connecteur Hyper-V. Choisissez Next (Suivant).
8. Dans la pageHyper-V : Configuration du compte d'hôte et de serviceouSCVMM : Configuration du compte d'hôte et de service, fournissez les informations de compte pour l'utilisateur Active Directory que vous avez créé dansÉtape 1 : Créer un compte de service pour Server Migration Connector dans Active Directory (p. 16), y comprisNom d'utilisateuretMot de passe.
9. - [SCVMM uniquement] Fournissez le nom d'hôte SCVMM devant être géré par ce connecteur et choisissezSuivant. Inspectez le certificat pour l'hôte, puis choisissez Approbation si le certificat est valide.

- [Hyper-V autonome uniquement] Fournissez le nom d'hôte Hyper-V devant être traité par ce connecteur. Pour ajouter des hôtes supplémentaires, utilisez le symbole plus. Pour inspecter le certificat pour chaque hôte, choisissez Verify Certificate (Vérifier le certificat), puis Approbation si le certificat est valide. Choisissez Next (Suivant).

Vous pouvez également sélectionner l'option spécifique à l'hôte pour Ignorer les erreurs de non-correspondance de nom d'hôte et d'expiration... pour les certificats SCVMM ou Hyper-V. Nous vous déconseillons de remplacer la sécurité en production, mais cela peut être utile pendant les tests.

Note

Si vous avez des hôtes Hyper-V situés dans plusieurs domaines Active Directory, nous vous recommandons de configurer un connecteur distinct pour chaque domaine.

10. Si vous avez authentifié avec succès le connecteur, vous devriez voir leFélicitations. Pour afficher l'état de santé du connecteur, choisissezAccéder au tableau de bord du connecteur.
11. Pour vérifier que le connecteur que vous avez enregistré est désormais répertorié, ouvrez leConnecteurssur leAWS Server Migration Serviceconsole Si vous rencontrez un problème lors de l'enregistrement du connecteur, contactezsms-service@amazon.com.

Installation du connecteur de migration de serveur sur Azure

Utilisez les informations suivantes pour installer le connecteur de migration de serveur sur Azure afin de pouvoir utiliserAWS SMSPour migrer des machines virtuelles depuis Azure vers Amazon EC2.

Ces informations ne s'appliquent qu'aux machines virtuelles hébergées par Azure. Pour plus d'informations sur l'installation du connecteur sur d'autres environnements, consultez Installation du connecteur de migration de serveur (p. 11).

Considérations sur les scénarios de migration

- Une même appliance Server Migration Connector ne peut migrer de machines virtuelles que sous un seul abonnement et une seule région Azure.
- Une fois qu'une appliance Server Migration Connector est déployée, vous ne pouvez pas changer son abonnement ou sa région, sauf si vous déployez un autre connecteur dans le nouvel abonnement et la nouvelle région.
- AWS SMSprend en charge le déploiement de n'importe quel nombre de machines virtuelles d'appliance Server Migration Connector pour prendre en charge la migration à partir de plusieurs abonnements et régions Azure en parallel.
- Server Migration Connector ne prend pas en charge les régions Azure Government.

Prérequis pour le connecteur Azure

- La taille de la machine virtuelle recommandée pour le connecteur Azure est F4s - 4 vCPU et 8 Go de RAM. Vérifiez que vous avez un quota d'UC Azure suffisant dans la région dans laquelle vous déployez le connecteur.
- Un compte de stockage standard (autre que Premium) sous lequel le connecteur peut être déployé.
- Un réseau virtuel sur lequel le connecteur peut être déployé.
- Accès entrant sur le port 443 (HTTPS), à partir du réseau virtuel du connecteur (recommandé) ou ouvert au public (non recommandé), pour l'enregistrement du connecteur et l'affichage du tableau de bord du connecteur.

- Accès Internet sortant pour accéder aux services AWS et Azure afin de procéder aux mises à jour du système d'exploitation du connecteur, etc.

Table des matières

Étape 1 : Télécharger le script d'installation du connecteur

AWSSMS fournit un logiciel téléchargeable PowerShell pour déployer le connecteur dans votre environnement Azure. Ce script est signé de façon chiffrée par AWS. Effectuez cette procédure pour exécuter la commande PowerShell Script et installez le connecteur automatiquement dans votre environnement Azure. Le script nécessite PowerShell 5.1 ou version ultérieure.

> Note
>
> AWS recommande d'utiliser le script d'installation, mais vous pouvez également installer le connecteur manuellement. Pour plus d'informations, consultez (Alternative) Déployez manuellement le connecteur de migration de serveur (p. 26).

Pour télécharger le script et les fichiers de hachage

1. Télécharger le PowerShell script et fichiers de hachage à partir des URL suivantes :

Fichier	URL
Script d'installation	https://s3.amazonaws.com/sms-connector/aws-sms-azure-setup.ps1
hachage MD5	https://s3.amazonaws.com/sms-connector/aws-sms-azure-setup.ps1.md5
hachage SHA256	https://s3.amazonaws.com/sms-connector/aws-sms-azure-setup.ps1.sha256

2. Après avoir téléchargé les fichiers, transférez-les vers le ou les ordinateurs sur lesquels vous prévoyez d'exécuter le script.

Étape 2 : Valider l'intégrité et la signature cryptographique du fichier de script

Avant d'exécuter le script, nous vous recommandons de valider son intégrité et sa signature, en veillant à ce qu'il n'ait pas changé lors du chargement sur votre ordinateur. Ces procédures supposent que vous avez téléchargé le script et les fichiers de hachage, que ceux-ci sont installés sur le bureau de l'ordinateur où vous prévoyez d'exécuter le script, et que vous êtes connecté en tant qu'administrateur. Vous devrez peut-être modifier les procédures en fonction de votre configuration.

Pour valider l'intégrité du script à l'aide de hachages cryptographiques (PowerShell)

1. Utilisez l'un et/ou l'autre des fichiers de hachage téléchargés pour valider l'intégrité du fichier de script.

   a. Pour procéder à la validation avec le hachage MD5, exécutez la commande suivante dans un PowerShell fenêtre :

   ```
   PS C:\Users\Administrator> Get-FileHash aws-sms-azure-setup.ps1 -Algorithm MD5
   ```

   Les informations renvoyées devraient être semblables à ce qui suit :

   ```
   Algorithm         Hash
   ---------         ----
   MD5               1AABAC6D068EEF6EXAMPLEDF50A05CC8
   ```

   b. Pour procéder à la validation avec le hachage SHA256, exécutez la commande suivante dans un PowerShell fenêtre :

   ```
   PS C:\Users\Administrator> Get-FileHash aws-sms-azure-setup.ps1 -Algorithm SHA256
   ```

   Les informations renvoyées devraient être semblables à ce qui suit :

   ```
   Algorithm         Hash
   ---------         ----
   SHA256            6B86B273FF34FCE19D6B804EFF5A3F574EXAMPLE22F1D49C01E52DDB7875B4B
   ```

2. Comparez les valeurs de hachage renvoyées avec les valeurs fournies dans les fichiers téléchargés, `aws-sms-azure-setup.ps1.md5` et `aws-sms-azure-setup.ps1.sha256`.

Ensuite, utilisez l'une ou l'autre PowerShell ou l'interface utilisateur de Windows pour vérifier que le fichier de script inclut une signature valide à partir duAWS.

Pour vérifier la validité de la signature cryptographique d'un fichier de script (PowerShell)

- Dans un PowerShell , exécutez la commande suivante :

```
PS C:\Users\Administrator> Get-AuthenticodeSignature aws-sms-azure-setup.ps1 | Select *
```

Un fichier de script correctement signé doit renvoyer des informations similaires à ce qui suit :

```
SignerCertificate          : [Subject]
                              CN="Amazon Web Services, Inc." ...
                             [Issuer]
                              CN=DigiCert EV Code Signing CA (SHA2), OU=www.digicert.com,
 O=DigiCert Inc, C=US
...

TimeStamperCertificate     :
Status                     : Valid
StatusMessage              : Signature verified.
Path                       : C:\Users\Administrator\Desktop\aws-sms-azure-setup.ps1

...
```

Pour vérifier la validité de la signature cryptographique d'un fichier de script (interface utilisateur Windows)

1. Dans Windows Explorer, ouvrez le menu contextuel (clic droit) et choisissez Propriétés, Signatures numériques, Amazon Web Services et Détails.
2. Vérifiez que les informations affichées contiennent « Cette signature numérique est valide. » et que « Amazon Web Services, Inc. » est le signataire.

Étape 3 : Exécutez le script

Exécutez ce script à partir de n'importe quel ordinateur avec PowerShell 5.1 ou version ultérieure installé.

> Note
>
> Si vos recettes PowerShell La stratégie d'exécution est définie pour vérifier les scripts signés. Vous êtes invité à fournir une autorisation lors de l'exécution du script de configuration. Vérifiez que le script est publié par « Amazon Web Services, Inc. » et choisissez « R » pour courir une fois. Vous pouvez consulter ce paramètre en utilisant Get-ExecutionPolicy et le modifier en utilisant Set-ExecutionPolicy.

```
PS C:\Users\Administrator> .\aws-sms-azure-setup.ps1 -StorageAccountName name -
ExistingVNetName name -SubscriptionId id -SubnetName name
```

`StorageAccountName`

Nom du compte de stockage dans lequel vous souhaitez déployer le connecteur.

`ExistingVNetName`

Nom du réseau virtuel dans lequel vous souhaitez déployer le connecteur.

`SubscriptionId`

(Facultatif) ID de l'abonnement à utiliser. Si vous ne spécifiez pas ce paramètre, l'abonnement par défaut pour le compte est utilisé.

`SubnetName`

(Facultatif) Nom du sous-réseau dans le réseau virtuel. Si vous ne spécifiez pas ce paramètre, le sous-réseau nommé « default » est utilisé.

Lorsque le script vous invite à indiquer un identifiant de connexion Azure, utilisez-en un qui a les autorisations administrateur sous lesquelles vous déployez le connecteur.

Lorsque le script est terminé, le connecteur est déployé dans votre compte. Le script imprime l'adresse IP privée du connecteur et l'ID d'objet de l'identité affectée par le système à la machine virtuelle du connecteur. Vous avez besoin de ces deux éléments pour effectuer l'étape suivante.

Étape 4 : Configurez le connecteur

À partir d'une autre machine virtuelle du même réseau virtuel où vous avez déployé le connecteur, accédez à l'interface Web du connecteur à l'aide de l'URL suivante, qui inclut l'adresse IP privée du connecteur que vous avez obtenu à l'étape précédente :

```
https://ip-address-of-connector
```

Pour configurer le connecteur

1. Sur la page de destination du connecteur, choisissez Get started now (Démarrer maintenant).
2. Lisez le contrat de licence, sélectionnez la case à cocher, puis choisissez Next (Suivant).
3. Créez un mot de passe pour le connecteur. Le mot de passe doit répondre aux critères affichés. Choisissez Next (Suivant).
4. Dans la pageInfos sur le réseau, vous trouverez des instructions pour effectuer des tâches liées au réseau, telles que la configurationAWSproxy pour le connecteur. Choisissez Next (Suivant).
5. Sur la page Log Uploads (Chargements de journaux), sélectionnez Upload logs automatically (Charger les journaux automatiquement) et choisissez Next (Suivant).
6. Sur la page Server Migration Service (Service de migration de serveur), fournissez les informations suivantes :
   - PourAWSRegion (Région), choisissez votre région dans la liste.
   - PourAWSInformations d'identification, entrez les informations d'identification IAM que vous avez créées dansConfigurer un utilisateur IAM pour Server Migration Connector (p. 5). Choisissez Next (Suivant).
7. Sur la page Azure Account Verification (Vérification de compte Azure), vérifiez que l'ID d'abonnement et l'emplacement Azure sont corrects. Ce connecteur peut migrer des machines virtuelles sous cet abonnement et cet emplacement. Fournissez l'ID d'objet de l'identité affectée par le système de la machine virtuelle du connecteur, fournie comme sortie du script de déploiement.
8. Si vous avez configuré correctement le connecteur, la page Congratulations (Félicitations s'affiche. Pour afficher le statut d'intégrité du connecteur, choisissez Go to connecteur dashboard (Accéder au tableau de bord du connecteur).
9. Pour vérifier que le connecteur que vous avez enregistré est répertorié, ouvrez leConnecteurssur la console Systems Manager.

(Alternative) Déployez manuellement le connecteur de migration de serveur

Suivez la procédure ci-dessous pour installer le connecteur manuellement dans votre environnement Azure.

Pour installer le connecteur manuellement

1. Connectez-vous au portail Azure en tant qu'utilisateur doté des autorisations administrateur pour l'abonnement sous lequel vous déployez ce connecteur.
2. Assurez-vous que vous êtes prêt à fournir un compte de stockage, son groupe de ressources, un Virtual Network et la région Azure, comme décrit dansPrérequis pour le connecteur Azure (p. 22).
3. Téléchargez le VHD du connecteur et les fichiers associés à partir des URL indiquées dans le tableau ci-dessous.

Fichier	URL
VHD du connecteur	https://awssmsconnector.blob.core.windows.net/release/AWS-SMS-Connector-for-Azure.vhd
hachage MD5	https://s3.amazonaws.com/sms-connector/AWS-SMS-Connector-for-Azure.vhd.md5
hachage SHA256	https://s3.amazonaws.com/sms-connector/AWS-SMS-Connector-for-Azure.vhd.sha256

4. Vérifiez l'intégrité cryptographique du VHD du connecteur à l'aide de procédures similaires à celles décrites dans Étape 2 : Valider l'intégrité et la signature cryptographique du fichier de script (p. 23).
5. Chargez le VHD du connecteur et les fichiers associés dans votre compte de stockage.
6. Créez un disque géré avec les valeurs de paramètre suivantes :

   - Groupe de ressources : Sélectionner le groupe de ressources
   - Nom : N'importe quel nom - par exemple, sms-connector-disk-westus
   - Region (Région) : Sélectionner votre région Azure
   - Zone de disponibilité : Aucun
   - Type de source : Stockage Blob (Choisissez le blob VHD que vous avez chargé à l'étape 3.c.)
   - OSType : Linux
   - Taille : Disque dur standard de 60 Go/
7. Choisissez Créer une machine virtuelle pour créer une machine virtuelle depuis le disque géré que vous avez créé. Affectez les valeurs de paramètre suivantes :

   Sous l'onglet Informations de base :

   - Groupe de ressources : Entrez votre groupe de ressources
   - Nom de machine virtuelle : Tous les noms, par exemple sms-connector-vm-westus
   - Region (Région) : Sélectionner votre région Azure
   - Taille : F4
   - Ports d'entrée publics : Aucun

   Sous l'onglet Disques :

   - Type de disque du SE : HDD Standard

   Sous l'onglet Mise en réseau :

   - Réseau virtuel : Entrez le nom de votre réseau virtuel
   - Sous-réseau : Laissez la valeur par défaut ou choisissez un sous-réseau spécifique
   - IP publique : Laissez comme nouveau
   - Groupe de sécurité réseau de la carte réseau : Base
   - Ports d'entrée publics : Aucun
   - Acceptez les valeurs par défaut des champs restants.

   Sous l'onglet Gestion :

   - Diagnostic du démarrage : Activé
   - Diagnostics d'exploitation invité : Désactivé
   - Diagnostics Storage : Compte de stockage
   - Identité managée affectée par : Activé
   - Activer l'arrêt automatique : Désactivé
8. Vérifiez et créez la machine virtuelle. Ce sera la machine virtuelle de votre connecteur.
9. Téléchargez les deux documents de rôle :

   - https://s3.amazonaws.com/sms-connector/SMSConnectorRole.json
   - https://s3.amazonaws.com/sms-connector/SMSConnectorRoleSA.json
10. (Important) Personnalisez les documents de rôle.

Modification `SMSConnectorRole.json`. Remplacez la valeur du champ `name` par `sms-connector-role-`*`id_abonnement`*. Remplacez la valeur du champ `AssignableScopes` afin de refléter votre ID d'abonnement.

Modification `SMSConnectorRoleSA.json`. Remplacez la valeur du champ `name` par `sms-connector-role-`*`compte_stockage`*. Par exemple, si votre compte est testStorage, le nom du champ doit être `sms-connector-role-testStorage`. Modifiez ensuite le champ `AssignableScopes` pour qu'il corresponde aux valeurs Abonnement, Groupe de ressources et Compte de stockage.

11. Créez une définition de rôle. Actuellement, il n'est pas possible de créer une définition de rôle dans le portail Azure. Vous devez utiliser l'interface de ligne de commande Az ou Az PowerShell pour cette étape. Utilisez la commande New-AzRoleDefinition (Az PowerShell) ou az role definition create (Az CLI) pour créer ces rôles personnalisés dans votre abonnement à l'aide des fichiers JSON que vous avez créés à l'étape précédente.
12. Affectez des rôles à la machine virtuelle du connecteur. Dans le portail Azure, choisissez Compte de stockage, Contrôle d'accès, Rôles, >Ajouter, Ajouter une attribution de rôle. Choisissez le rôle `sms-connector-role`, attribuez l'accès à Machine virtuelle et sélectionnez, dans la liste, l'identité affectée par le système à la machine virtuelle. Répétez cette procédure pour le rôle `sms-connector-role-`*`storage_account`*.
13. Redémarrez la machine virtuelle du connecteur pour activer les attributions de rôle.
14. Passez au Étape 4 : Configurez le connecteur (p. 25).

Répliquer des machines virtuelles en utilisantAWS CLICommandes de l' pourAWS SMS

Vous pouvez utiliser le pluginAWS Command Line Interface(AWS CLI) pour inventorier et migrer vos serveurs sur site vers Amazon EC2.

Prérequis

- Installation du connecteur de migration de serveur comme décrit dans laInstallation du connecteur de migration de serveur (p. 11).
- Vous devez utiliser les éléments suivants :rôle lié à la création d'un servicepour créer le rôle lié à un service requis.

```
aws iam create-service-linked-role --aws-service-name sms.amazonaws.com
```

  Pour plus d'informations, consultez Rôles lié à un service pour AWS SMS (p. 44).

Considérations

- Vous pouvez répliquer vos serveurs sur site dans AWS pendant 90 jours maximum par serveur. Le temps d'utilisation est calculé dès le lancement d'une réplication de serveur et jusqu'à l'arrêt de la tâche de réplication. Votre tâche de réplication est automatiquement arrêtée après 90 jours. Vous pouvez demander une extension à partir de AWS Support.
- Si vous avez activé l'intégration entreAWS SMSetAWS Migration Hub, votre catalogue de serveurs SMS est également visible sur le Migration Hub. Pour plus d'informations, consultez Importer des applications depuis Migration Hub (p. 36).
- Pendant le processus de réplication,AWS SMScrée un compartiment Amazon S3 dans la région en votre nom, avec le chiffrement côté serveur activé et une stratégie de compartiment définie pour supprimer tous les éléments du compartiment après sept jours.AWS SMSréplique les volumes de serveur de votre environnement vers ce compartiment, puis crée des instantanés EBS à partir des volumes. Si vous ne supprimez pas ce compartiment, AWS SMS l'utilise pour toutes les tâches de réplication dans cette région.
- Au cours du processus de création de l'AMI,AWS SMSdéfinit le`DeleteOnTermination`pour le volume racine à false, remplaçant la valeur par défaut. Vous pouvez supprimer le volume racine manuellement après avoir terminé l'instance, ou vous pouvez définir l'attribut sur true afin qu'Amazon EC2 supprime le volume racine à la fin de l'instance. Pour plus d'informations, consultez Conservation des volumes Amazon EBS lors de la résiliation des instances dans le Guide de l'utilisateur Amazon EC2.

Pour répliquer un serveur à l'aide de l'interface de ligne de commande

1. Utilisez la commande get-connectors pour obtenir la liste des connecteurs enregistrés pour vous.

```
aws sms get-connectors
```

2. Une fois qu'un connecteur a été installé et enregistré, utilisez l'import-serveur-catalogue-serveurpour créer un inventaire de vos serveurs. Ce processus peut prendre jusqu'à 1 minute.

```
aws sms import-server-catalog
```

3. Utilisation de l'get-serverpour afficher la liste des serveurs pouvant être importés dans Amazon EC2.

```
aws sms get-servers
```

La sortie doit ressembler à ce qui suit :

```
{
    "serverList": [
        {
            "serverId": "s-12345678",
            "serverType": "VIRTUAL_MACHINE",
            "vmServer": {
                "vmManagerName": "vcenter.yourcompany.com",
                "vmServerAddress": {
                    "vmManagerId": "your-vcenter-instance-uuid",
                    "vmId": "vm-123"
                },
                "vmName": "your-linux-vm",
                "vmPath": "/Datacenters/DC1/vm/VM Folder Path/your-linux-vm",
                "vmManagerType": "vSphere"
            }
        },
        {
            "replicationJobTerminated": false,
            "serverId": "s-23456789",
            "serverType": "VIRTUAL_MACHINE",
            "replicationJobId": "sms-job-12345678",
            "vmServer": {
                "vmManagerName": "vcenter.yourcompany.com",
                "vmServerAddress": {
                    "vmManagerId": "your-vcenter-instance-uuid",
                    "vmId": "vm-234"
                },
                "vmName": "Your Windows VM",
                "vmPath": "/Datacenters/DC1/vm/VM Folder Path/Your Windows VM",
                "vmManagerType": "vSphere"
            }
        }
    ]
}
```

Si vous n'avez pas encore importé de catalogue de serveurs, vous verrez un résultat similaire à ce qui suit s'afficher :

```
{
    "lastModifiedOn": 1477006131.856,
    "serverCatalogStatus": "NOT IMPORTED",
    "serverList": []
}
```

Un statut de catalogue DELETED ou EXPIRED indique également qu'aucun serveur n'existe dans le catalogue.

4. Sélectionnez un serveur à répliquer, notez l'ID du serveur et spécifiez l'ID dans la commande create-replication-job.

```
aws sms create-replication-job --server-id s-12345678 \
    --frequency 12 \
```

```
    --seed-replication-time 2016-10-24T15:30:00-07:00 \
    --role-name AWSServiceRoleForSMS
```

Une fois que la réplication est configurée, la réplication démarrera automatiquement à l'heure indiquée par le paramètre `--seed-replication-time`, exprimé en secondes au format d'heure Unix epoch ou conformément à la norme ISO 8601. Pour plus d'informations, veuillez consulter Spécification de valeurs de paramètre pour l'AWS Command Line Interface. Par la suite, la réplication se répète selon un intervalle spécifié par le paramètre `--frequency`, exprimé en heures.

5. Vous pouvez afficher les détails de toutes les tâches de réplication à l'aide de la commande get-replication-jobs. Si vous ne spécifiez aucun paramètre, la commande répertorie toutes vos tâches de réplication.

   La sortie générée lors de l'exécution de cette commande est semblable à ce qui suit :

```
{
    "replicationJobList": [
        {
            "vmServer": {
                "vmManagerName": "vcenter.yourcompany.com",
                "vmServerAddress": {
                    "vmManagerId": "your-vcenter-instance-uuid",
                    "vmId": "vm-1234"
                },
                "vmName": "VM name in vCenter",
                "vmPath": "/Datacenters/DC1/vm/VM Folder Path/VM name in vCenter"
            },
            "replicationRunList": [
                {
                    "scheduledStartTime": 1487007010.0,
                    "state": "Deleted",
                    "type": "Automatic",
                    "statusMessage": "Uploading",
                    "replicationRunId": "sms-run-12345678"
                }
            ],
            "replicationJobId": "sms-job-98765432",
            "state": "Deleted",
            "frequency": 12,
            "seedReplicationTime": 1477007049.0,
            "roleName": "sms"
        },
        {
            "vmServer": {
                "vmManagerName": "vcenter.yourcompany.com",
                "vmServerAddress": {
                    "vmManagerId": "your-vcenter-instance-uuid",
                    "vmId": "vm-2345"
                },
                "vmName": "win2k12",
                "vmPath": "/Datacenters/DC1/vm/VM Folder Path/win2k12"
            },
            "replicationRunList": [
                {
                    "scheduledStartTime": 1477008789.0,
                    "state": "Active",
                    "type": "Automatic",
                    "statusMessage": "Converting",
                    "replicationRunId": "sms-run-12345679"
                }
            ],
            "replicationJobId": "sms-job-23456789",
            "state": "Active",
            "frequency": 24,
```

```
            "seedReplicationTime": 1477008789.0,
            "roleName": "sms"
        }
    ]
}
```

6. Vous pouvez également utiliser la commande get-replication-runs pour récupérer des informations sur tous les cycles de réplication pour une tâche de réplication spécifique. Pour ce faire, spécifiez un ID de tâche de réplication comme suit :

```
aws sms get-replication-runs --replication-job-id sms-job-12345678
```

Cette commande renvoie une liste de tous les cycles de réplication pour la tâche de réplication indiquée, ainsi que les détails de cette dernière, dont le contenu est similaire à ce qui suit :

```
{
    "replicationRunList": [
        {
            "scheduledStartTime": 1477310423.0,
            "state": "Active",
            "type": "Automatic",
            "statusMessage": "Converting",
            "replicationRunId": "sms-run-23456789"
        },
        {
            "amiId": "ami-abcdefab",
            "state": "Completed",
            "completedTime": 1477227683.652,
            "scheduledStartTime": 1477224023.0,
            "replicationRunId": "sms-run-34567890",
            "type": "Automatic",
            "statusMessage": "Completed"
        },
        {
            "amiId": "ami-efababcd",
            "state": "Completed",
            "completedTime": 1477144823.486,
            "scheduledStartTime": 1477137623.0,
            "replicationRunId": "sms-run-45678903",
            "type": "Automatic",
            "statusMessage": "Completed"
        }
    ]
}
```

7. Pour modifier les paramètres d'une tâche de réplication qui a été créée, utilisez la commande update-replication-job en indiquant l'ID de la tâche de réplication et les autres paramètres à modifier.

```
aws sms update-replication-job --replication-job-id sms-job-12345678 --frequency 24 --
next-replication-run-start-time 2016-10-24T15:30:00-07:00
```

8. Outre les cycles de réplication prévus, vous pouvez également démarrer jusqu'à deux cycles de réplication à la demande par 24 heures. Pour ce faire, utilisez la commande start-on-demand-replication-run, qui permet de démarrer un cycle de réplication immédiatement. Si un autre cycle de réplication est en cours, un cycle de réplication à la demande ne pourra pas être lancé.

```
aws sms start-on-demand-replication-run --replication-job-id sms-job-12345678
```

Si un cycle de réplication planifié doit démarrer pendant qu'un cycle de réplication à la demande est en cours, il sera ignoré et reprogrammé pendant l'intervalle suivant.

9. Une fois que la réplication d'un serveur est terminée, vous pouvez arrêter la tâche de réplication à l'aide de la commande delete-replication-job. Cela interrompt la tâche de réplication et élimine tous les artefacts créés par le service (par exemple, le compartiment S3 de la tâche). Cela ne supprime pas les AMI créées lors des cycles de la tâche interrompue.

```
aws sms delete-replication-job --replication-job-id sms-job-12345678
```

10. Quand vous n'avez plus besoin de conserver votre catalogue de serveurs, utilisez la commande delete-server-catalog pour supprimer le catalogue de serveurs géré par le service.

```
aws sms delete-server-catalog
```

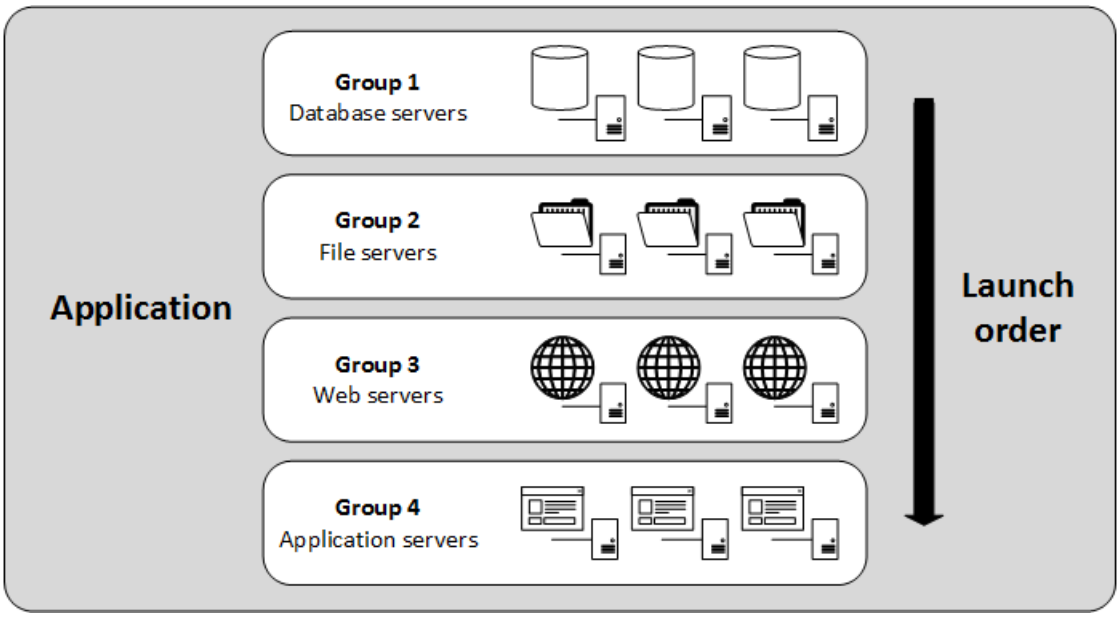
11. Quand vous avez fini d'utiliser un connecteur, utilisez la commande disassociate-connector pour annuler l'inscription de ce connecteur à partir de AWS SMS. Appelez cette commande uniquement après que toutes les réplications utilisant ce connecteur sont terminées.

```
aws sms disassociate-connector --connector-id c-12345678901234567
```

Migration d'applications à l'aide deAWS SMS

AWS Server Migration Serviceprend en charge la migration automatique des piles d'applications multi-serveurs de vos centres de données sur site vers Amazon EC2. Lorsque la migration du serveur est effectuée par réplication d'un seul serveur tel qu'une Amazon Machine Image (AMI), la migration de l'application réplique tous les serveurs dans une application comme des AMI et génère un modèle AWS CloudFormation pour les lancer de façon coordonnée.

Les applications peuvent également être subdivisées en plusieurs groupes pour vous permettre de lancer des niveaux de serveurs dans un ordre défini. Le schéma suivant illustre un exemple d'application Web basée sur une base de données :



Dans cet exemple, l'application est divisée en quatre groupes dont chacun possède trois serveurs. Le modèle AWS CloudFormation démarre les serveurs dans l'ordre suivant : bases de données, serveurs de fichiers, serveurs Web et serveurs d'applications.

Une fois que vos serveurs sont organisés en applications et groupes de lancement, vous pouvez spécifier une fréquence de réplication, fournir des scripts de configuration, puis configurer une cible VPC dans laquelle vous les lancerez. Lorsque vous lancez une application, AWS SMS la configure en fonction du modèle généré.

La migration d'applications s'appuie sur les procédures pour découvrir les ressources sur site décrites dans Installation du connecteur de migration de serveur (p. 11). Une fois que vous avez importé un catalogue de serveurs dansAWS SMSà l'aide du connecteur de migration de serveur, vous pouvez configurer les paramètres relatifs aux applications, à la réplication et au lancement, puis surveiller le statut de la migration à l'aide des ressources deAWS SMSdans leAWS SMSAPI,AWSInterface de ligne de commande, ouAWSKits SDK.

Considérations

- Vous pouvez répliquer vos serveurs sur site dans AWS pendant 90 jours maximum par serveur. Le temps d'utilisation est calculé dès le lancement d'une réplication de serveur et jusqu'à l'arrêt de la tâche

de réplication. Votre tâche de réplication est automatiquement arrêtée après 90 jours. Vous pouvez demander une extension à partir de AWS Support.

- Au cours du processus de création de l'AMI,AWS SMSdéfinit le`DeleteOnTermination`pour le volume racine à false, remplaçant la valeur par défaut. Vous pouvez supprimer le volume racine manuellement après avoir terminé l'instance, ou vous pouvez définir l'attribut sur true afin qu'Amazon EC2 supprime le volume racine à la fin de l'instance. Pour plus d'informations, consultez Conservation des volumes Amazon EBS lors de la résiliation des instances dans le Guide de l'utilisateur Amazon EC2.
- La migration d'applications à partir de Microsoft Azure est prise en charge, mais le connecteur de migration de serveur pour Azure ne garantit pas actuellement la proximité des instantanés de serveur dans l'application.

Utiliser la migration des applications

Vous pouvez exécuter les tâches suivantes.

Tâches

Création d'une application

Pour créer une application, consultez leAWS SMS create-appdans la commandeAWS CLIRéférence des commandes.

Configurer des paramètres de réplication

Pour configurer les paramètres de réplication pour une application, consultez leAWS SMS tâche de mise à jour de réplicationdans la commandeAWS CLIRéférence des commandes.

Configurer des paramètres de lancement

Avant de pouvoir configurer les paramètres réseau, vous devez configurer un cloud privé virtuel, un sous-réseau et un groupe de sécurité, comme décrit pour leRunInstancesAction d'API Amazon EC2.

Pour configurer les paramètres de lancement d'une application, consultez leAWS SMS configuration de lancement de put-appdans la commandeAWS CLIRéférence des commandes.

Démarrer la réplication

Pour commencer la réplication d'une application, consultez leAWS SMS réplication Start-Appdans la commandeAWS CLIRéférence des commandes.

Lancement d'une application

Pour lancer une application, consultez leAWS SMS application de lancementdans la commandeAWS CLIRéférence des commandes.

Générer un rapport CloudFormation modèle

Pour examiner leAWS CloudFormationmodèle généré automatiquement lorsque vous lancez l'application, consultez leAWS SMS générer un modèledans la commandeAWS CLIRéférence des commandes.

Importer des applications depuis Migration Hub

La migration des applications prend en charge l'importation et la migration des applications détectées par AWS Migration Hub.

Pour importer des applications depuis Migration Hub, consultez leAWS SMS import-app-cataloguedans la commandeAWS CLIRéférence des commandes.

> Note
>
> SMS importe les serveurs liés aux applications de Migration Hub uniquement s'ils existent dans le catalogue de serveurs SMS et s'ils ne font pas partie d'une application SMS existante. Par conséquent, certaines applications peuvent être importées partiellement uniquement. Une application ne peut pas être importée à nouveau si elle est répliquée ou lancée activement par SMS. Si ce conflit a lieu, arrêtez la réplication ou lancez et réimportez.

Utilisation d'Amazon CloudWatch Events etAWS LambdaavecAWS SMS

Vous pouvez utiliser Amazon CloudWatch Events avecAWS Server Migration Servicepour automatiser des actions en fonction de votre flux de travail de migration. Cela vous permet de créer une stratégie IAM qui sera assumée par Lambda, une fonction Lambda pour gérer l'événement, et une règle CloudWatch Events qui fait correspondre les événements entrants et les achemine vers la fonction Lambda.

Gestion des règles CloudWatch Events pourAWS SMS

La procédure suivante utilise unAWS Lambdacontrôle de fonctionAWS SMSl'état de tâche change et lance une instance Amazon EC2 chaque fois qu'un ID d'AMI a été créé.

Pour créer une fonction Lambda qui surveille les modifications d'état de tâche

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Créez une stratégie IAM pour fournir des autorisations afin d'exécuter une action (appelée par Lambda) et d'écrire dans le journal CloudWatch lors d'un appel par CloudWatch Events. L'exemple suivant fournit des autorisations pour exécuter une action `RunInstances`. Attribuez la stratégie au rôle IAM de l'utilisateur qui gérera l'événement CloudWatch.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "logs:CreateLogGroup",
            "logs:CreateLogStream",
            "logs:PutLogEvents"
         ],
         "Resource":"arn:aws:logs:*:*:*"
      },
      {
         "Effect":"Allow",
         "Action":[
            "ec2:RunInstances"
         ],
         "Resource":"*"
      }
   ]
}
```

3. Ouvrez la console AWS Lambda à l'adresse https://console.aws.amazon.com/lambda/.
4. Sélectionnez Créer une fonction.

5. Pour vous assurer que votre fonction Lambda est disponible à partir de la console CloudWatch, créez-la dans la région où l'événement CloudWatch doit se produire. Pour plus d'informations, consultez le Manuel du développeur AWS Lambda. Nommez la fonction `LaunchInstanceFromAMI` et sélectionnez Python 2.7 comme environnement d'exécution.
6. Pour Rôle, sélectionnez Choisir un rôle de existant. Sous Existing role (Rôle existant), dans la liste des rôles disponibles, choisissez le rôle auquel vous avez ajouté votre stratégie.
7. ChoisissezCréation de fonctionet définissez une fonction Lambda similaire à celle ci-dessous. Cet exemple de fonction, écrite en Python 2.7, est appelé par CloudWatch Events lorsqu'uneAWS SMSl'achèvement de la tâche envoie un événement avec un ID AMI. Lorsqu'elle est appelée, elle lance une instance `t2.micro` dans la région de l'événement.

```
# Sample Lambda function to launch an EC2 instance from all AMI ID's created from a
# Server Migration Service replication job

import boto3

# main function
def lambda_handler(event, context):

    # create an ec2 client
    ec2 = boto3.client('ec2', region_name=event['region'])

    # match any event that returns an ami-id
    if 'ami-id' in event['detail']:
        imageId = event['detail']['ami-id']

        # launch instance from the AMI ID
        ec2.run_instances(
            ImageId=imageId,
            MaxCount=123,
            MinCount=1,
            InstanceType='t2.micro'
        )
        print 'launched instance with ami id: ' + imageId
    else:
        print 'did not launch instance'
```

8. Ouvrez la console CloudWatch à l'adresse https://console.aws.amazon.com/cloudwatch/.
9. Choisissez Événements, Créer une règle. Pour Service Name (Nom du service), choisissez Server Migration Service (SMS). Pour Event Type (Type d'événement), choisissez Server Migration Job State Change (Modification de l'état de tâche de migration de serveur).
10. Choisissez Target, puis Add Target.
11. Dans le champ Lambda function, sélectionnez la fonction Lambda que vous avez créée précédemment, puis choisissez Configure details.
12. Sur la page Configure rule details, tapez les valeurs de Name et Description. Sélectionnez la case à cocher State pour activer la fonction (en la définissant sur Enabled).
13. Choisissez Create rule.

Votre règle doit désormais apparaître sur l'onglet Rules. Dans l'exemple présenté, l'événement configuré doit lancer une instance EC2 chaque fois que vous recevez un ID d'AMI.

Journalisation des appels d'API AWS Server Migration Service avec AWS CloudTrail

AWS Server Migration Serviceest intégré àAWS CloudTrail, un service qui enregistre les actions réalisées par un utilisateur, un rôle ou unAWSservice enAWS SMS. CloudTrail capture les appels d'API pourAWS SMScomme événements. Les appels capturés incluent les appels de code vers leAWS SMSOpérations d'API Si vous créez un journal de suivi, vous pouvez diffuser en continu CloudTrail événements vers un compartiment Amazon S3, y compris des événements pourAWS SMS. Si vous ne configurez pas de journal d'activité, vous pouvez toujours afficher les événements les plus récents dans la console CloudTrail dans Historique des événements. En utilisant les informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été envoyée à AWS SMS, l'adresse IP, l'auteur et la date de la demande, ainsi que d'autres détails.

Pour plus d'informations, consultez le Guide de l'utilisateur AWS CloudTrail.

AWS SMS Informations dans CloudTrail

CloudTrail est activé dans votre compte AWS lors de la création de ce dernier. Lorsque l'activité se produit dansAWS SMS, cette activité est enregistrée dans un CloudTrail événement avec d'autresAWSévénements de service dansHistorique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre AWS compte. Pour de plus amples informations, veuillez consulterAffichage des événements avec CloudTrail Historique des événements.

Pour enregistrer en continu les événements dans votre compte AWS, y compris les événements d'AWS SMS, créez un journal d'activité. UNsentierpermet CloudTrail pour diffuser des fichiers journaux vers un compartiment Amazon S3. Par défaut, lorsque vous créez un journal de suivi dans la CloudTrail console, la piste s'applique à tousAWSRégions. Le journal d'activité consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Simple Storage Service (Amazon S3) de votre choix. De plus, vous pouvez configurer d'autresAWSservices permettant d'analyser plus en profondeur les données d'événement collectées dans CloudTrail bûches. Pour en savoir plus, consultez les ressources suivantes :

- Présentation de la création d'un journal d'activité
- Intégrations et services pris en charge par CloudTrail
- Configuration des Notifications de Amazon SNS pour CloudTrail
- Réception CloudTrail Journaux de plusieurs régionsetRéception CloudTrail Journaux de plusieurs comptes

TousAWS SMSLes actions sont consignées par CloudTrail et sont documentés dans leAWS SMSAPI Reference. Par exemple, les appels aux`CreateReplicationJob`,`GetConnectors`, et`ImportServerCatalog`les actions génèrent des entrées dans la CloudTrail fichiers journaux

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

- Si la demande a été effectuée avec les informations d'identification utilisateur racine ou AWS Identity and Access Management (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 requête a été effectuée par un autre service AWS.

Pour plus d'informations, consultez Élément userIdentity CloudTrail.

Présentation des AWS SMS entrées des fichiers journaux

Un journal de suivi est une configuration qui permet la livraison d'événements sous forme de fichiers journaux vers un compartiment Amazon S3 que vous spécifiez. CloudTrail Les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande individuelle émise à partir d'une source quelconque et comprend 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 série ordonnée retraçant les appels d'API publics. Ils ne suivent aucun ordre précis.

L'exemple suivant montre un CloudTrail qui illustre l'action`CreateReplicationJob`action.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "0123456789abcdef01234",
        "arn": "arn:aws:iam::0123456789ab:user/sms-user",
        "accountId": "0123456789ab",
        "accessKeyId": "0123456789abcdef0123",
        "userName": "sms-user"
    },
    "eventTime": "2018-09-04T16:34:49Z",
    "eventSource": "sms.amazonaws.com",
    "eventName": "CreateReplicationJob",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "1.2.3.4",
    "userAgent": "aws-sdk-java/example-sdk-version Linux/example-kernel-version …",
    "requestParameters": {
        "roleName": "sms",
        "serverId": "s-01234567",
        "runOnce": true,
        "seedReplicationTime": "Sep 4, 2018 4:36:48 PM"
    },
    "responseElements": {
        "replicationJobId": "sms-job-012345677"
    },
    "requestID": "00000000-1111-2222-3333-444444444444",
    "eventID": "55555555-6666-7777-8888-999999999999",
    "eventType": "AwsApiCall",
    "recipientAccountId": "0123456789ab"
}
```

Sécurité dans AWS Server Migration Service

Chez AWS, la sécurité dans le cloud est notre priorité numéro 1. En tant que client AWS, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des organisations les plus pointilleuses en termes de sécurité.

La sécurité est une responsabilité partagée entre AWS et vous. Le modèle de responsabilité partagéede décrit ceci comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est responsable de la protection de l'infrastructure qui exécute des services AWS dans le cloud AWS. AWS vous fournit également les services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des AWS programmes de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent àAWS Server Migration Service(AWS SMS), voirAWSServices concernés par le programme de conformité.
- Sécurité dans le cloud : votre responsabilité est déterminée par le service AWS que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre entreprise,et la législation et la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de AWS SMS. Elle vous montre comment configurer AWS SMS pour atteindre vos objectifs en matière de sécurité et de conformité. Vous apprendrez également à utiliser d'autres services AWS pour surveiller et sécuriser vos ressources AWS SMS.

Table des matières

Protection des données dans AWS Server Migration Service

Le modèle de responsabilité partagée AWS s'applique à la protection des données dans AWS Server Migration Service. Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure globale sur laquelle l'ensemble du AWS Cloud s'exécute. La gestion du contrôle de votre contenu hébergé sur cette infrastructure est de votre responsabilité. Ce contenu comprend les tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour en savoir plus sur la confidentialité des données, veuillez consulter Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, veuillez consulter le billet de blog AWS Modèle de responsabilité partagée et RGPD sur le AWSBlog de sécurité.

À des fins de protection des données, nous vous recommandons de protéger les informations d'identification Compte AWS et de configurer les comptes utilisateur individuels avec AWS Identity

and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multi-facteur (MFA) avec chaque compte.
- Utilisez SSL/TLS pour communiquer avec les ressources AWS. Nous recommandons TLS 1.2 ou version ultérieure.
- Configurez une API et la journalisation des activités utilisateur avec AWS CloudTrail.
- Utilisez des solutions de chiffrement AWS, ainsi que tous les contrôles de sécurité par défaut au sein des services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données personnelles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés FIPS 140-2 lorsque vous accédez à AWS via une CLI ou une API, utilisez un point de terminaison FIPS. Pour en savoir plus sur les points de terminaison FIPS disponibles, consultez Norme de traitement de l'information fédérale (Federal Information Processing Standard (FIPS)) 140-2.

Nous vous recommandons vivement de ne jamais placer d'informations confidentielles ou sensibles, telles que des adresses e-mail, dans des identifications ou des champs de format libre tels que Nom. Cela s'applique aussi lorsque vous utilisez AWS SMS ou d'autres services AWS à l'aide de la console, d'une API, de la AWS CLI ou des kits SDK AWS. Toutes les données que vous entrez dans des identifications ou des champs de format libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification non chiffrées dans l'URL pour valider votre demande adressée au serveur.

Chiffrement au repos

Lorsque vous répliquez des volumes de serveur à partir de votre environnement local, AWS SMS stocke temporairement les données dans un compartiment S3 intermédiaire. Une fois la réplication terminée,AWS SMSsupprime ces données stockées dans Amazon S3. Sinon, AWS SMS ne stocke pas vos données au repos.

Chiffrement en transit

Les données en transit sont chiffrées à l'aide du protocole TLS. Cela inclut le trafic depuis le connecteur de migration de serveur vers Amazon S3 et le connecteur de migration de serveur versAWS SMS.

Gestion des identités et des accès pour AWS Server Migration Service

AWS Identity and Access Management (IAM) est un AWS service qui aide un administrateur à contrôler en toute sécurité l'accès aux AWS ressources. Des administrateurs IAM contrôlent les personnes qui s'authentifient (sont connectées) et sont autorisées (disposent d'autorisations) à utiliserAWSAWS. IAM vous permet de créer des utilisateurs et des groupes sous votreAWS. Vous contrôlez les autorisations dont disposent les utilisateurs pour effectuer des tâches à l'aide deAWSAWS. Vous pouvez utiliser IAM sans frais supplémentaires.

Par défaut, les utilisateurs IAM ne disposent pas d'autorisations pourAWS Server Migration Service(AWS SMS) ressources et opérations. Pour permettre aux utilisateurs IAM de gérerAWS SMS, vous devez créer une stratégie IAM qui leur donne explicitement les autorisations et attacher la stratégie aux utilisateurs ou groupes IAM qui requièrent ces autorisations.

Quand vous attachez une politique à un utilisateur ou à un groupe d'utilisateurs, elle accorde ou refuse aux utilisateurs l'autorisation d'exécuter les tâches spécifiées sur les ressources spécifiées. Pour de plus amples informations, veuillez consulterStratégies et autorisationsdans leIAM User Guideguide.

Structure d'une politique

Une politique IAM est un document JSON qui se compose d'une ou de plusieurs déclarations. Chaque déclaration est structurée comme suit :

```
{
  "Statement": [
    {
      "Effect": "effect",
      "Action": "action",
      "Resource": "arn",
      "Condition": {
        "condition": {
          "key":"value"
        }
      }
    }
  ]
}
```

Une déclaration se compose de différents éléments :

- Effect : Effect peut avoir la valeur`Allow`ou`Deny`. Comme, par défaut, les utilisateurs IAM n'ont pas la permission d'utiliser les ressources et les actions d'API, toutes les demandes sont refusées. Une autorisation explicite remplace l'autorisation par défaut. Un refus explicite remplace toute autorisation.
- Action : L'action est la spécificitéAWS SMSAction d'API pour laquelle vous accordez ou refusez l'autorisation.
- Ressource: Resource affectée par l'action. Pour AWS SMS, vous devez spécifier « * » comme ressource.
- Condition : Les conditions sont facultatives. Elles permettent de contrôler à quel moment votre politique est effective.

Exemples de politiques

Dans une déclaration de politique IAM, vous pouvez spécifier une action d'API à partir de n'importe quel service prenant en charge IAM. Pour AWS SMS, utilisez le préfixe suivant avec le nom de l'action d'API : `sms:` comme suit.

```
"Action": "sms:UpdateReplicationJob"
```

Pour spécifier plusieurs actions dans une seule déclaration, séparez-les par des virgules comme suit.

```
{
  "Statement":[
    {
      "Effect": "Allow",
      "Action": ["sms:action1", "sms:action2"],
      "Resource": "*"
    }
  ]
}
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques. Par exemple, vous pouvez spécifier toutes les actions d'API AWS SMS dont le nom commence par le mot « Get » comme suit.

```
{
  "Statement":[
    {
      "Effect": "Allow",
      "Action": "sms:Get*",
      "Resource": "*"
    }
  ]
}
```

Pour spécifier toutes les actions d'API AWS SMS, utilisez le caractère générique * comme suit.

```
{
  "Statement":[
    {
      "Effect": "Allow",
      "Action": "sms:*",
      "Resource": "*"
    }
  ]
}
```

Pour empêcher les utilisateurs d'activer le lancement automatique après la réplication, utilisez l'instruction suivante. Il ne suffit pas d'omettre`sms:LaunchApp`dans la liste des actions autorisées, car avec le lancement automatique, les utilisateurs n'appellent pas`LaunchApp`directement.

```
{
  "Statement":[
    {
      "Effect": "Deny",
      "Action": "sms:LaunchApp",
      "Resource": "*"
    }
  ]
}
```

PrédéfiniAWSpolitiques gérées

Les stratégies gérées créées par AWS octroient les autorisations requises pour les cas d'utilisation courants. Vous pouvez attacher ces stratégies à vos utilisateurs IAM, en fonction de l'accès àAWSdont ils ont besoin.

Rôles lié à un service pour AWS SMS

AWS SMS utilise un rôle lié à un service pour les autorisations dont il a besoin pour appeler d'autres services AWS en votre nom. Pour plus d'informations, consultez Utilisation des rôles liés à un service dans le IAM Guide de l'utilisateur.

Avant l'introduction d'un rôle lié à un service pour AWS SMS, vous deviez créer deux rôles IAM pour accorder à AWS SMS les autorisations requises. Ces rôles ne sont plus nécessaires pour utiliser AWS SMS. Toutefois, ils sont documentés ici par souci d'exhaustivité. Pour plus d'informations, consultez Rôles IAM hérités pourAWS SMS (p. 46).

Autorisations accordées par le rôle lié à un service

AWS SMS utilise le rôle lié au service nommé AWSServiceRoleForSMS pour permettre à AWS SMS de gérer vos tâches de réplication.

AWSServiceRoleForSMS fait confiance au mandataire du service `sms.amazonaws.com` pour assumer le rôle.

La politique d'autorisations liée au rôle permet à AWS SMS de réaliser les actions suivantes sur les ressources spécifiées :

- Utiliser des actions AWS SMS spécifiques pour créer et gérer des tâches de réplication
- Utiliser des actions AWS CloudFormation spécifiques pour créer et gérer arn:aws:cloudformation:*:*:stack/sms-app-*/*
- Utiliser des actions Amazon EC2 spécifiques pour gérer des instantanés et des images, lancer des instances et gérer des instances qui répondent à la condition de balise suivante : ec2:ResourceTag/aws:cloudformation:stack-id » : « arn:aws:cloudformation : *:*:stack/sms-app-*/*
- Utiliser des actions AWS Systems Manager spécifiques pour exécuter des scripts sur vos instances
- Utiliser `iam:GetRole` sur toutes les ressources et `iam:PassRole` sur arn:aws:cloudformation:*:*:stack/sms-app-*/*
- Utiliser des actions Amazon S3 spécifiques pour créer et gérer arn:aws:s3# :sms-app-*

Création du rôle lié à un service

Vous pouvez créer manuellement ce rôle lié à un service à l'aide de ce qui suitAWS CLI rôle lié à la création d'un servicecommande pour créerRôle AWSServiceRoleForSMS.

```
aws iam create-service-linked-role --aws-service-name sms.amazonaws.com
```

La modification du rôle lié à un service

Vous pouvez modifier la description duRôle AWSServiceRoleForSMSUtilisation d'IAM. Pour de plus amples informations, veuillez consulter Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Suppression du rôle lié à un service

Si vous n'avez plus besoin d'utiliser AWS SMS, nous vous recommandons de supprimer le rôle AWSServiceRoleForSMS. Le rôle lié à un service peut être supprimé uniquement dans les conditions suivantes :

- Le rôle lié à un service n'est pas utilisé par une tâche de réplication active
- Le rôle lié à un service n'est pas utilisé par une application associée à une tâche de réplication active
- Le rôle lié à un service n'est pas utilisé par une application qui a une pile AWS CloudFormation associée

Vous pouvez utiliser la console IAM, l'IAM CLI ou l'IAM API pour supprimer les rôles liés aux services. Pour de plus amples informations, veuillez consulter Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Après avoir supprimé le rôle AWSServiceRoleForSMS AWS SMS le crée à nouveau si vous démarrez une tâche de réplication.

Rôles IAM hérités pourAWS SMS

Avant l'introduction de AWSServiceRoleForSMS, vous auriez dû créer un rôle de service et un rôle de lancement pour accorder à AWS SMS les autorisations requises. Il n'est plus nécessaire de créer ces rôles.

Configurer un rôle de service pourAWS SMS

Utilisez la procédure suivante afin de créer un rôle IAM qui accorde des autorisations àAWS SMSPour placer des ressources migrées dans votre compte Amazon EC2.

Pour créer le rôle IAM pourAWS SMS

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Rôles, puis Créer un rôle.
3. UNDERChoisissez le service qui utilisera ce rôle, choisissezSMS,Suivant: Permissions (Autorisations).
4. UNDERAttachement des stratégies d'autorisations, confirmez que la politiqueServerMigrationServiceRoleest visible et choisissezSuivant: Review (Examiner).
5. Sous Review (Vérification), pour Role name (Nom de rôle), tapez **`sms`**.

   Note

   Vous pouvez également appliquer un autre nom. Toutefois, vous devez ensuite spécifier explicitement le nom du rôle à chaque fois que vous créez une tâche de réplication ou une application.
6. Choisissez Create role (Créer un rôle). Vous devriez maintenant voir le rôle sms dans la liste des rôles disponibles.
7. Pour des contrôles de sécurité supplémentaires, des clés contextuelles telles que`aws:SourceAccount`et`aws:SourceArn`peut être ajouté à la stratégie d'approbation de ce rôle nouvellement créé. SMS publiera le`sourceAccount`et`sourceArn`clés comme spécifié dans l'exemple ci-dessous pour assumer ce rôle.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": { "Service": "sms.amazonaws.com" },
    "Action": "sts:AssumeRole",
    "Condition": {
        "StringEquals": {
             "aws:SourceAccount": “<YOUR_AWS_ACCOUNT_ID>“
           },
         "ArnLike":    {
             "aws:SourceArn": "arn:aws:sms:*:<YOUR_AWS_ACCOUNT_ID>:*"
           }
        }
    }
}
```

Configurer un rôle de lancement pourAWS SMS

Si vous prévoyez de lancer des applications, il vous faut un rôle de lancement AWS SMS. Vous attribuez ce rôle à l'aide de l'API `PutAppLaunchConfiguration`. Lorsque l'API `LaunchApp` est appelée, le rôle est utilisé par AWS CloudFormation.

Pour créer un rôle de lancement pour AWS SMS

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Rôles, puis Créer un rôle.
3. UNDERChoisissez le service qui utilisera ce rôle, choisissezCloudFormation,Suivant: Permissions (Autorisations).
4. UNDERAttachement des stratégies d'autorisations, confirmez que la politiqueServerMigrationServiceLaunchRoleest visible et choisissezSuivant: Review (Examiner).
5. Sous Review (Vérification), pour Role name (Nom de rôle), tapez **`sms-launch`**.

   Note

   Vous pouvez également appliquer un autre nom. Toutefois, vous devez ensuite spécifier explicitement le nom du rôle à chaque fois que vous créez une configuration de lancement pour une application.
6. Choisissez Create role (Créer un rôle). Vous devriez maintenant voir le rôle sms-launch dans la liste des rôles disponibles.

Résilience dans AWS Server Migration Service

L'infrastructure mondiale d'AWS repose sur les régions et les zones de disponibilité AWS. Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à débit élevé et à forte redondance. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour en savoir plus sur les régions AWS et zones de disponibilité , consultez Infrastructure mondiale AWS.

Sécurité de l'infrastructure dans AWS Server Migration Service

En tant que service géré,AWS SMSest protégé par leAWSprocédures de sécurité du réseau mondial qui sont décrites dans leAmazon Web Services : Présentation des procédures de sécuritélivre blanc.

Vous utilisez les appels d'API publiés AWS pour accéder à AWS SMS via le réseau. Les clients doivent supporter le protocole TLS (Sécurité de la couche transport) 1.0 ou une version ultérieure. Nous recommandons TLS 1.2 ou version ultérieure. Les clients doivent aussi prendre en charge les suites de chiffrement PFS (Perfect Forward Secrecy) comme Ephemeral Diffie-Hellman (DHE) ou Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Validation de la conformité pour AWS Server Migration Service

Les auditeurs tiers évaluent la sécurité et la conformité des services de Services AWS dans le cadre de plusieurs programmes de conformité AWS, tels que SOC, PCI, FedRAMP et HIPAA.

Pour savoir si d'autres Services AWS entrent dans le champ d'application de programmes de conformité spécifiques, consultez la section Services AWS dans le champ d'application par programme de conformité. Pour obtenir des renseignements généraux, consultez Programmes de conformité AWS.

Vous pouvez télécharger les rapports de l'audit externe avec AWS Artifact. Pour plus d'informations, consultez Téléchargement de rapports dans AWS Artifact.

Votre responsabilité de conformité lors de l'utilisation de Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise, ainsi que par la législation et la réglementation applicables. AWS fournit les ressources suivantes pour faciliter le respect de la conformité :

- Guides Quick Start de la sécurité et de la conformité : ces guides de déploiement proposent des considérations architecturales et fournissent des étapes pour déployer des environnements de référence centrés sur la sécurité et la conformité sur AWS.
- Architecture pour la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent utiliser AWS pour créer des applications éligibles à la loi HIPAA.

  Note

  Tous les Services AWS ne sont pas éligibles à HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.
- Ressources de conformité AWS – Cet ensemble de manuels et de guides peut s'appliquer à votre secteur d'activité et à votre emplacement.
- Évaluation des ressources à l'aide de règles dans le Guide du développeur AWS Config : le service AWS Config évalue dans quelle mesure vos configurations de ressources sont conformes aux pratiques internes, aux directives sectorielles et aux réglementations.
- AWS Security Hub – Ce Service AWS fournit une vue complète de votre état de sécurité au sein d'AWS, ce qui vous permet de vérifier votre conformité aux normes du secteur et aux bonnes pratiques de sécurité.
- AWS Audit Manager – Ce Service AWS vous aide à auditer en continu votre utilisation d'AWS pour simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résolution des problèmes de AWS SMS

Les informations suivantes peuvent vous aider à résoudre les problèmes liés aux erreurs que vous êtes susceptible de rencontrer lors de l'utilisation d'AWS SMS. Avant d'utiliser ces procédures, vérifiez que votre configuration SMS et le serveur que vous essayez de migrer répondent aux exigences exposées dans Exigences relatives à AWS Server Migration Service (p. 2).

Table des matières

Fichiers journaux pour le connecteur

Le connecteur de migration de serveur fournit des fichiers journaux que vous pouvez utiliser pour résoudre les problèmes des tâches de réplication qui échouent avant la fin du téléchargement sur Amazon S3. Procédez comme suit pour télécharger les fichiers journaux du connecteur.

Pour télécharger les fichiers journaux du connecteur

1. Dans un navigateur Web, entrez l'adresse IP de la machine virtuelle du connecteur.
2. Connectez-vous au connecteur.
3. Vérifiez que le connecteur réussit toutes les vérifications.
4. UNDERLiens du Support, choisissezTélécharger le bundle du journal.
5. Extrayez les fichiers du groupe des journaux.

Les fichiers journaux de connecteurs suivants sont inclus dans le lot de journaux :

- `connector.log`— Vérifiez les problèmes de configuration du connecteur.
- `connectorsetup.log`— Vérifiez les informations détaillées sur la configuration initiale.
- `frontend.log`— Vérifier s'il y a des problèmes de connectivité àAWSPoints de terminaison .
- `metrics.log`— Vérifiez les statistiques de débit et les vitesses de téléchargement (voir`UploadStats`).

- `netstat.log`— Vérifiez les erreurs de paquets réseau.
- `poller.log`— Confirmez l'activité d'interrogation de la base
- `sms-replication-poller-log`— Passez en revue l'activité à partir de la validation du travail de réplication via le disque téléchargé sur Amazon S3. Par exemple, vous pouvez vérifier la progression du chargement sous forme de pourcentage et vérifier le début et la fin de chaque phase de la tâche de réplication.

Échec de l'enregistrement du connecteur

Si vous rencontrez un problème lors de l'enregistrement du connecteur, contactezsms-service@amazon.com.

Erreur de certificat lors du chargement d'une machine virtuelle sur Amazon S3

Le connecteur risque de ne pas parvenir à répliquer votre machine virtuelle, car celle-ci se trouve sur un hôte ESXi avec un problème de certificat SSL. Si cela se produit, vous verrez le message suivant s'afficher dans leMessage d'état de la dernière courseSection: « Erreur du serveur : Impossible de charger le ou les disques de base sur S3. Veuillez réessayer. Si le problème persiste, veuillez contacterAWSSupport : incompatibilité avec le nom d'hôte du certificat vSphere : Certificat pour <*somehost.somedomain.com*> ne correspond à aucun des noms alternatifs du sujet : [*domaine localhost.local*]. »

Vous pouvez résoudre ce problème de certificat d'hôte ESXi en effectuant les tâches suivantes :

Tâches

- Mise à niveau de votre connecteur (p. 50)
- Réenregistrez votre connecteur (p. 50)

Mise à niveau de votre connecteur

Cette section destinée aux clients qui effectuent une mise à niveau manuelle du connecteur. Si vous avez des mises à niveau automatiques préconfigurées, ignorez ces étapes et passez à Réenregistrez votre connecteur (p. 50)

Pour mettre à niveau votre connecteur

1. Ouvrez la console du connecteur.
2. Connectez-vous au connecteur.
3. Choisissez Upgrade (Mise à niveau).
4. Attendez que le connecteur ait terminé la mise à niveau vers la version 1.0.11.13 ou ultérieure.

Réenregistrez votre connecteur

Cette section s'applique à tous les clients qui rencontrent le problème d'incompatibilité de certificat.

Pour réenregistrer votre connecteur

1. Ouvrez la console du connecteur.

2. Connectez-vous au connecteur.
3. DansHealth générale, vérifiez que la version du connecteur est 1.0.11.13 ou ultérieure.
4. ChoisissezModifierAWS Server Migration ServiceParamètres.
5. Dans la pageInstallation, pourAWSRegion (Région), sélectionnez la région souhaitée dans la liste. PourAWSInformations d'identification, entrez la clé d'accès IAM et la clé secrète que vous avez créée lors de l'étape 2 duguide de configuration (p. 11). Choisissez Next (Suivant).
6. Sur la page vCenter Service Account (Compte de service vCenter), entrez le nom d'hôte, le nom d'utilisateur et le mot de passe vCenter que vous avez créés lors de l'étape 3 du guide de configuration (p. 11).
7. Cochez la case Ignore hostname mismatch and expiration errors for vCenter and ESXi certificates. Choisissez Next (Suivant).
8. Terminez l'enregistrement et affichez le tableau de bord de configuration du connecteur.
9. Utilisation de l'AWS SMSCLI ou API pour supprimer et redémarrer vos tâches de réplication bloquées.

Server Migration Connector ne parvient pas à se connecterAWSavec l'erreur « PKIX path building failed »

Dans certains environnements client, assurez-vous que le trafic réseau est traité par proxy via un mécanisme de revalidation du certificat pour des raisons d'audit et de gestion. Cela peut entraîner votreAWSéchouer lorsque le connecteur tente de contacterAWS SMS. Le message d'erreur « PKIX path building failed », indique qu'un certificat non valide a été présenté.

Pour que le connecteur puisse fonctionner dans un tel environnement, le certificat de nouvelle validation (un certificat utilisateur que votre organisation approuvent et utilise pour signer les paquets sortants) doit être ajouté au référentiel d'approbations, comme décrit dans les étapes suivantes.

Pour ajouter le nouveau certificat validé au référentiel d'approbations du connecteur

1. Dans votre système de connecteur, désactivez le filtre de paquet FreeBSD et activez le service SSH à l'aide des commandes suivantes :

```
sudo service pf stop
sudo service sshd onestart
```

2. Copiez votre certificat utilisateur dans le connecteur grâce à une méthode telle que celle-ci :

```
scp userCertFile ec2-user@10.0.0.100:/tmp/
```

3. Ajoutez le certificat utilisateur au référentiel d'approbations.

```
keytool -importcert -keystore /usr/local/amazon/connector/config/jetty/trustStore -
storepass AwScOnNeCtOr -file /tmp/userCertFileName -alias userCertName
```

4. Redémarrez les services à l'aide de la commande suivante (dans le cadre d'AWS Management Portal for vCenter) :

```
sudo setup.rb
```

   Sélectionnez l'option 3 et tapez « yes ».
5. Réactivez le filtre de paquet :

```
sudo service pf start
```

Ce certificat d'autorité de certification racine n'est pas approuvé

Lorsque vous accédez à l'adresse IP d'une machine virtuelle que vous avez installée sur site, vous pouvez recevoir le message suivant :

```
This CA Root certificate is not trusted. To enable trust,
install this certificate in the Trusted Root Certifications
Authorities store.
```

Vous pouvez ignorer ce message sans risque.

L'exécution de la réplication échoue pendant la phase de préparation

Dans certains cas, AWS SMS permet à une tâche de réplication de continuer à planifier des exécutions de réplication incrémentielle, même lorsque la dernière exécution de réplication a échoué. Lorsque le nombre maximal autorisé d'échecs consécutifs est atteint, le comportement par défaut pour une tâche de réplication doit être suspendu. La tâche peut être reprise dans un délai de quatre jours, après quoi elle est supprimée. Dans de tels cas, les instantanés Amazon EBS de la dernière exécution de réplication sont partagés avec le compte client, et un message de statut relatif à l'échec de l'exécution de réplication est envoyé. Le message contient les ID d'instantané et indique la raison de l'échec. Voici un exemple typique de message de statut :

```
EBS snapshot(s) created with snapshot ID(s): snap-12345678abcdefgh. Another run
has been scheduled after the last run failed due to an import failure. 2 re-try run(s)
remaining before the job will be failed.
```

La raison des échecs d'exécution de la réplication (y compris les échecs au premier démarrage) est souvent en lien étroit avec les échecs observés lorsque Amazon EC2 VM Import/Export est utilisé pour la migration de machines virtuelles. Pour plus d'informations, consultez Résolution des problèmes liés à VM Import/Export.

Si vous avez besoin d'aide pour résoudre un problème, contactez AWS Support. Les instantanés EBS générés au cours d'un échec de migration sont partagés avec votre compte, et les ID d'instantané sont inclus au message de statut relatif à la tâche de réplication. Vérifiez que ces détails sont disponibles lorsque vous contactezAWSSupport.

L'AMI répliquée ne prend pas en charge certains types d'instances pour le lancement

Certaines instances nécessitent la prise en charge ENA. Si la migration n'active pas la prise en charge ENA, l'AMI répliquée ne vous autorise pas à lancer des instances qui requièrent la prise en charge ENA.

Vérifiez qu'ENA est activé. Pour de plus amples informations, veuillez consulterActivation de la mise en réseau améliorée sur WindowsouActivation de la mise en réseau améliorée sur Linuxdans la documentation Amazon EC2.

ServerError : Échec du chargement du ou des disques de base sur Amazon S3

Causes possibles :

- Le VMDK n'est pas une table de capture instantanée ou la machine virtuelle a monté des ISO.
- La connexion à l'hyperviseur (hôte Hyper-V ou ESXi) a expiré pendant que le connecteur télécharge des données mises en mémoire tampon vers Amazon S3.
- La maintenance est en cours pendant que le travail de réplication télécharge des disques sur Amazon S3.
- Il y a un problème de compression avec le disque virtuel.
- Une erreur de validation s'est produite avec le certificat de l'hyperviseur.
- Le statut du connecteur est`Unhealthy`.
- Le connecteur ne peut pas atteindreAWSPoints de terminaison .

ServerError : Impossible de valider la tâche de réplication

Causes possibles :

- Il y a un changement dans le chemin de la machine virtuelle.
- Il y a un changement dans les autorisations IAM.
- Les autorisations des utilisateurs ou des comptes sont modifiées pour l'environnement virtuel.
- WinRM (Hyper-V) pose un problème de configuration.
- Il y a un échec de résolution DNS.
- Une erreur de configuration NTP s'est produite sur la machine virtuelle du connecteur.

Une erreur interne s'est produite. Confirmation que votreAWSles informations d'identification et les identifiants VM Manager sont corrects.

Causes possibles :

- Les autorisations IAM ne sont pas suffisantes pour terminer la configuration du connecteur.
- Les autorisations d'utilisateur ou de compte pour l'environnement virtuel ne sont pas suffisantes.
- Il y a des problèmes avec les rôles IAM pourAWS SMS.
- Il manque des conditions préalables.
- L'environnement de machine virtuelle n'est pas préparé.

- Des caractères spéciaux ont été utilisés lors de la configuration du connecteur (Hyper-V).

Erreurs liées aux instantanés (VMware)

Causes possibles :

- Le VMDK est configuré en tant que disque indépendant.
- L'hôte ESXi ne peut pas prendre d'instantané.
- Le VMDK est verrouillé.
- La chaîne de clichés est cassée. Assurez-vous qu'aucun instantané n'est pris entre les exécutions de réplication, manuellement ou par un logiciel tiers.
- Une précédente exécution de réplication n'a pas consolidé les instantanés.

Erreurs de point de contrôle (Hyper-V)

Causes possibles :

- La machine virtuelle possède des points de contrôle existants.
- Il existe des points de contrôle créés manuellement ou par des logiciels tiers.
- Le VHD ou le VHDX est verrouillé.
- L'hôte Hyper-V ne peut pas créer de point de contrôle.

Delta de réplication incrémentielle dépasse 1 To

Le connecteur est conçu pour gérer une réplication fréquente avec de petits deltas. Le connecteur ne prend pas en charge les deltas supérieure à 1 To. Si vous n'effectuez pas des réplications régulières, le delta peut dépasser cette limite et la réplication échoue.

Pour éviter ce problème, configurez des cycles de réplication incrémentielle fréquents. Si vous ne pouvez pas effectuer des réplications régulières, vous pouvez augmenter la limite de charge du delta. Par exemple, exécutez les commandes suivantes sur le connecteur pour augmenter la taille des chargements S3 de 25 Mo à 100 Mo. Lorsque vous y êtes invité, sélectionnez l’option 3.

```
sudo sms-connector-config -set slotSizeMB 100
sudo setup.rb
```

L'augmentation de la limite de chargement impacte les performances et l'utilisation de la mémoire du connecteur. N’augmentez pas la limite de chargement pendant que le connecteur est en train de charger plusieurs deltas.

Notes de mise à jour pour le connecteur de migration

Les tableaux suivants décrivent l'historique des versions du connecteur de migration de serveur.

Versions

Versions pour les environnements vCenter

Pour télécharger le dernier connecteur pour les environnements vCenter, ouvrezhttps://s3.amazonaws.com/sms-connector/AWS-SMS-Connector.ova.

Date de publication	Version	Commentaire
11 janvier 2022	1.0.13.2156	• Système d'exploitation mis à niveau vers FreeBSD 12.3-RELEASE.
14 décembre 2021	1.0.13.2011	• Cette version inclut le correctif pour une vulnérabilité de 0 jours d'exécution de code Apache Log4j2 (CVE02021-44228).
28 avril 2020	1.0.13.245	• Ajout de la prise en charge de la région Région Europe (Milan)
22 avril 2020	1.0.13.242	• Ajout de la prise en charge de la région Région Afrique (Le Cap)
23 mars 2020	1.0.13.227	• Correction d'un bug qui bloquait les migrations dans la région Moyen-Orient (Bahreïn) • Correction d'une erreur de fin prématurée de fichier (EOF) lors du téléchargement de l'instantané
29 mai 2019	1.0.13.106	• Correction d'un bogue qui bloquait l'enregistrement de l'appliance Connector en raison d'erreurs de connectivité avecAWS
3 mai 2019	1.0.13.90	• Correction d'un bug qui bloquait les migrations dans

Date de publication	Version	Commentaire
		leAWSRégion GovCloud (USA Est)
12 décembre 2018	1.0.13.15	• Ajout de la prise en charge de la région Europe (Stockholm)
5 décembre 2018	1.0.13.1	• Connecteur optimisé pour la fonction de migration des applications
19 octobre 2018	1.0.12.109	• Correction de la fin de fichier prématurée(EOF) provoquée par la reprise du chargement de disque de machine virtuelle après des interruptions d'infrastructure sur site ou de réseau
18 septembre 2018	1.0.12.88	• Correctifs permettant de reprendre les transferts de disques de machines virtuelles interrompus par des pannes réseau sur site
11 juin 2018	1.0.12.3	• Ajout de la prise en charge des machines virtuelles avec des disques de plus de 4 To à l'aide de la fonctionnalité de manifeste S3 • Correctifs de bogues mineurs
26 avril 2018	1.0.11.34	• Ajout de la prise en charge de la région Amérique du Sud (São Paulo) • Correctifs de bogues mineurs et améliorations de performances
29 janvier 2018	1.0.10.x	• Ajout de la prise en charge des régions suivantes : Europe (Londres), Europe (Paris), USA Ouest (Californie du Nord) et Chine (Beijing) • Correctifs de bogues mineurs et améliorations de performances
08 novembre 2017	1.0.9.x	• Amélioration de la résilience dans les chargements de disque • Correctifs de bogues mineurs et améliorations de performances

Date de publication	Version	Commentaire
29 août 2017	1.0.8.x	• Ajout du support linguistique pour le français, le chinois, le coréen et le japonais • Amélioration des vitesses de chargement de disque pour les machines virtuelles • Correctifs de bogues mineurs
02 juin 2017	1.0.7.12	• Ajout de la prise en charge deAWSRégion GovCloud (US-West)
5 mai 2017	1.0.5.2	• Ajout de la prise en charge de vCenter 5.1 • Ajout de la prise en charge de la migration unique • Amélioration des messages d'erreur et correctifs de bogues liés à la sécurité
3 nov 2016	1.0.0.84	• Appliance virtuelle Server Migration Connector pour les environnements VMware • Console AWS Server Migration Service pour gérer les migrations de machine virtuelle et les tâches de réplication SMS à l'aide d'une interface graphique • Interface de ligne de commande AWS Server Migration Service pour gérer les migrations de machine virtuelle et les tâches de réplication SMS à l'aide de la ligne de commande

Versions pour les environnements Hyper-V/SCVMM

Pour télécharger le dernier connecteur pour les environnements Hyper-V/SCVMM, ouvrezhttps://s3.amazonaws.com/sms-connector/AWS-SMS-Connector-for-SCVMM-HyperV.zip.

Date de publication	Version	Commentaire
27 janvier 2022	1.1.0.1474	• Système d'exploitation mis à niveau vers FreeBSD 12.3-RELEASE.
15 décembre 2021	1.1.0.1319	• Cette version inclut le correctif pour une vulnérabilité de 0 jours d'exécution

Date de publication	Version	Commentaire
		de code Apache Log4j2 (CVE-2021-44228).
9 novembre 2020	1.1.0.801	• Correction d'un problème lié au processus de création des ensembles de journaux de connecteurs avec lesquels vous partagezAWSpour le dépannage.
28 avril 2020	1.1.0.522	• Ajout de la prise en charge de la région Région Europe (Milan)
22 avril 2020	1.1.0.515	• Ajout de la prise en charge de la région Région Afrique (Le Cap)
6 avril 2020	1.1.0.505	• Correction des problèmes d'enregistrement des connecteurs dans les régions suivantes : Moyen-Orient (Bahreïn), Europe (Stockholm) et Asie-Pacifique (Hong Kong) • Correction d'un problème avec le téléchargement des paquets de journaux
12 décembre 2018	1.1.0.378	• Ajout de la prise en charge de la région Europe (Stockholm)
5 décembre 2018	1.1.0.364	• Connecteur optimisé pour la fonction de migration des applications
9 octobre 2018	1.1.0.357	• Migration de machine virtuelle Windows Hyper-V génération 2 • Correctifs de bogues mineurs
11 juin 2018	1.1.0.304	• Ajout de la prise en charge des machines virtuelles avec des disques de plus de 4 To à l'aide de la fonctionnalité de manifeste S3 • Correctifs de bogues mineurs
le 25 avril 2018	1.1.0.287	• Ajout de la prise en charge de la migration de machine virtuelle à partir de plusieurs serveurs Hyper-V à l'aide d'un seul connecteur • Ajout de la prise en charge de la région Amérique du Sud (São Paulo) • Correctifs de bogues mineurs

Date de publication	Version	Commentaire
28 février 2018	1.1.0.x	• Ajout de la prise en charge des régions suivantes : Europe (Londres), Europe (Paris), USA Ouest (Californie du Nord) et Chine (Beijing) • Correctifs de bogues mineurs
14 décembre 2017	1.1.0.76	• Ajout de la prise en charge de l'environnement Hyper-V de Microsoft

Versions pour les environnements Azure

Pour télécharger le dernier connecteur pour les environnements Azure, ouvrezhttps://s3.amazonaws.com/sms-connector/aws-sms-azure-setup.ps1.

Date de publication	Version	Commentaire
16 décembre 2021	1.2.0.2038	• Cette version inclut des corrections de bugs mineurs et le correctif pour une vulnérabilité de 0 jours d'exécution de code Apache Log4j2 (CVE-2021-44228).
27 février 2020	1.2.0.350	• Correctifs de bogues mineurs
31 mai 2019	1.2.0.286	• Le script de déploiement prend en charge les abonnements personnalisés • Correctifs de bogues mineurs et améliorations de performances
18 avril 2019	1.2.0.269	• Ajout de la prise en charge de l'environnement Azure de Microsoft

Historique du document pour AWS SMS

Le tableau suivant décrit toutes les versions d'AWS SMS.

update-history-change	update-history-description	update-history-date
obsolecence de la console (p. 60)	Suppression de la prise en charge deAWS SMSconsole en ligne avecAWS SMSobsolecence de la console. LeAWS SMSLes API seront prises en charge jusqu'au 31 mars 2023.	1er avril 2022
La validation des applications (p. 60)	Ajout de la prise en charge de la validation des applications avant de les lancer. Avec la validation des applications, vous exécutez des scripts de validation sur vos instances EC2 à l'aide deAWS Systems Manager. Avec la validation d'instance, vous pouvez exécuter un script de configuration lorsque votre instance EC2 démarre pour la première fois à l'aide des données utilisateur Amazon EC2.	10 août 2020
Prise en charge d'Azure (p. 60)	Ajout de la prise en charge de Microsoft Azure.	18 avril 2019
Intégration à AWS Migration Hub (p. 60)	Ajout de la prise en charge de l'importation et de la migration des applications découvertes par Migration Hub.	22 février 2019
Migration d'applications (p. 60)	Ajout de la prise en charge de la migration de groupes de serveurs organisés sous forme d'applications, et/ou du lancement automatisé d'applications à l'aide de CloudFormation.	5 décembre 2018
Prise en charge des disques de grande taille (p. 60)	Ajout de la prise en charge des machines virtuelles avec des disques de plus de 4 To à l'aide de la fonctionnalité de manifeste S3.	11 juin 2018

Migration de plusieurs serveurs avec un seul connecteur (p. 60)	Ajout de la prise en charge de la migration de machines virtuelle à partir de plusieurs serveurs Hyper-V à l'aide d'un seul connecteur.	le 25 avril 2018
Prise en charge Hyper-V (p. 60)	Ajout de la prise en charge de l'environnement Hyper-V de Microsoft.	14 décembre 2017
Résilience du chargement (p. 60)	Amélioration de la résilience dans les chargements de disque.	8 novembre 2017
Amélioration de la vitesse d' (p. 60)	Amélioration des vitesses de chargement de disque pour les machines virtuelles.	29 août 2017
vCenter 5.1 ; migration unique ; messages d'erreur ; sécurité (p. 60)	Ajout de la prise en charge de vCenter 5.1. Prise en charge de la migration unique. Amélioration des messages d'erreur et correctifs de bogues liés à la sécurité.	5 mai 2017
Première version (p. 60)	Appliance virtuelle Server Migration Connector pour les environnements VMware.AWS Server Migration ServiceConsole pour gérer les migrations de machine virtuelle et les tâches de réplication SMS à l'aide d'une interface graphique.AWS Server Migration Service Interface de ligne de commande pour gérer les migrations de machine virtuelle et les tâches de réplication SMS à l'aide de la ligne de commande.	3 novembre 2016

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.