AWS Server Migration Service

ユーザーガイド

AWS Server Migration Service: ユーザーガイド

Table of Contents

AWS Server Migration Service とは?

AWS Server Migration Service (AWS SMS) は、オンプレミスの VMware vSphere、Microsoft Hyper-V/SCVMM、または Azure 仮想マシンの AWS クラウドへの移行を自動化します。AWS SMS は、サーバー仮想マシンをクラウドホストの Amazon マシンイメージ (AMI) として段階的にレプリケートし、Amazon EC2 にデプロイします。AMI を使用すると、クラウドベースのイメージを簡単にテストして更新した上で、本番稼働環境にデプロイできます。

AWS SMS を使用してサーバーの移行を管理することで、以下のことができます。

- クラウドへの移行プロセスの簡素化。でサーバーのグループの移行を開始できます。AWS CLI。移行が開始すると、AWS SMS は、ライブサーバーボリュームを自動的に AWS にレプリケートしたり、新しい AMI を定期的に作成したりするなど、移行プロセスのすべての複雑性を管理します。コンソールの AMI から EC2 インスタンスをすばやく起動できます。
- 複数サーバー移行のオーケストレーション – AWS SMS では、レプリケーションのスケジュールやアプリケーションを構成するサーバーグループの進捗の追跡を行い、サーバー移行をオーケストレーションできます。を使用して、最初のレプリケーションのスケジュール、レプリケーション間隔の設定、各サーバーの進行状況の追跡ができます。AWS CLI。移行されたアプリケーションを起動するとき、スタートアップ時に実行するカスタマイズされた設定スクリプトを適用できます。
- サーバの移行を段階的にテストします。インクリメンタル· レプリケーションのサポートにより、AWS SMS移行されたサーバーをすばやくスケーラブルにテストできます。AWS SMS は増分レプリケーションを使用するので、変更された分だけをクラウドに転送します。したがって、小さな変更で繰り返しテストし、ネットワーク帯域幅を節約できます。
- 広く普及しているオペレーティングシステムのサポート – AWS SMS では、Windows や主な Linux ディストリビューションを含むオペレーティングシステムイメージのレプリケーションをサポートしています。
- ダウンタイムの最小化。AWS SMS の増分レプリケーションにより、最終カットオーバー時のアプリケーションダウンタイムに伴うビジネスへの影響を最小限に抑えることができます。

AWS SMS の使用には以下の制約があります。

- 顧客が制限の引き上げをリクエストしない限り、アカウントごとに 50 の VM が同時に移行できます。
- VM の最初のレプリケーションから開始される、VM あたり (アカウントあたりではなく) 90 日間のサービス使用。お客様が制限引き上げをリクエストしない限り、90 日を過ぎると継続的なレプリケーションは終了されます。
- アカウントごとに 50 個のアプリケーションを同時に移行できます。アプリケーションごとに 50 台のサーバーと 10 個のグループに制限されます。

料金

Server Migration Service は追加料金なしで使用できます。移行プロセス中に使用される S3 バケット、EBS ボリューム、データ転送、および実行する EC2 インスタンスに対しては標準料金がかかります。詳細については、AWS Server Migration Service 料金を参照してください。

AWS Server Migration Service の要件

Server Migration Service を使用してオンプレミスの仮想化されたサーバーをAmazon EC2 に移行するには、VMware vSphere、Microsoft Hyper-V/SCVMM、または Microsoft Azure 環境が以下の要件を満たしている必要があります。

要件

一般要件

AWS SMS をセットアップする前に、必要な操作を行って、以下のすべての要件を満たします。

すべての VM

- 移行元の VM でウイルス対策ソフトウェアまたは侵入検出ソフトウェアを無効にします。移行プロセスが完了したら、これらのサービスを再度有効にすることができます。
- VM に接続されている CD-ROM ドライブ (仮想または物理) を切断します。

Windows VM

- リモートアクセスのためのリモートデスクトップ (RDP) を有効にする
- 適切なバージョンの .NET Framework を VM にインストールします。.NET Framework 4.5 以降は、必要に応じて VM に自動的にインストールされることに注意してください。

Windows のバージョン	.NET Framework のバージョン
Windows Server 2008 以前	3.5 以降
Windows Server 2008 R2 以降	4.5 以降
Windows 8 以前	3.5 以降
Windows 8.1 以降	4.5 以降

- Microsoft Windows VM の移行を準備する場合は、固定されたページファイルサイズを設定し、少なくとも 6 GiB の空き容量がルートボリュームで使用可能であることを確認します。これはドライバーを正常にインストールするために必要です。
- ホストのファイアウォール (Windows ファイアウォールなど) で RDP へのアクセスが許可されていることを確認します。そうしないと、移行した後にインスタンスにアクセスできなくなります。

- 以下の hotfix を適用します。
  - `RealTimeIsUniversal`You cannot change system time if registry entry is enabled in Windows (Windows で RealTimeIsUniversal レジストリエントリが有効になっている場合、システム時刻を変更できない)
  - High CPU usage during DST changeover in Windows Server 2008, Windows 7, or Windows Server 2008 R2 (Windows Server 2008、Windows 7、Windows Server 2008 R2 で DST への切り替え時に CPU 使用率が高くなる)
- 32 ビット AMIs をサポートするのは以下のインスタンスタイプのみです。`t2.nano`、`t2.micro`、`t2.small`、`t2.medium`、`c3.large`、`t1.micro`、`m1.small`、`m1.medium`、および `c1.medium`。32 ビットインスタンスを移行する場合は、これらのインスタンスタイプと、これらのインスタンスタイプをサポートするリージョンに制限されます。

Linux VM

- リモートアクセスの Secure Shell (SSH) を有効にします。
- ホストのファイアウォール (iptables など) で SSH へのアクセスが許可されていることを確認します。そうしないと、移行した後にインスタンスにアクセスできなくなります。
- インポート後に、非ルートユーザーはパブリックキーベースの SSH を使用してインスタンスにアクセスするように設定されていることを確認します。パスワードベースの SSH の利用と SSH を介したルートログインはどちらも可能ですが推奨されません。安全性を向上させるため、パブリックキーおよび非ルートユーザーの使用が推奨されます。Linux VM には移行プロセスの一部として作成された `ec2-user` アカウントはありません。
- Linux VM でブートローダーとして GRUB (GRUB レガシー) または GRUB 2 が使用されていることを確認します。
- Linux VM のルートボリュームで以下のいずれかのファイルシステムが使用されていることを確認します。
  - EXT2
  - EXT3
  - EXT4
  - Btrfs
  - JFS
  - XFS
- 移行された Linux VM は 64 ビットイメージを使用する必要があります。32 ビット Linux イメージの移行は、サポートされていません。
- 移行された Linux VM では、最良の結果を得るためにデフォルトのカーネルを使用してください。カスタム Linux カーネルを使用する VM は正常に移行されない場合があります。
- Amazon EC2 Linux VM を移行のために準備する場合は、ドライバとその他のソフトウェアをインストールするために、少なくとも 250 MiB のディスク容量がルートボリュームで使用可能であることを確認します。

プログラムによる VM への変更

VM をインポートするときに、AWS はファイルシステムを変更し、インポートされた VM をお客様に対してアクセス可能にします。以下のアクションが発生する場合があります。

- [Linux] Citrix PV ドライバを直接 OS にインストールするか、initrd/initramfs を変更してそれらを含める。
- [Linux] 静的 IP アドレスを動的 IP アドレスに置き換えるようにネットワークスクリプトを変更する。
- [Linux] `/etc/fstab` を変更し、無効なエントリをコメントアウトして、デバイス名を UUID で置き換える。一致する UUID がデバイスに対して見つからない場合、`nofail` オプションがデバイスの説明に追加されます。デバイス名を修正し、インポート後に `nofail` を削除する必要があります。ベストプラク

ティスとして、インポートのために VM を準備中に、デバイス名ではなく UUID によって VM ディスクデバイスを指定することをお勧めします。

分散ファイルシステムの種類 (nfs、cifs、smbfs、vboxsf、sshfs など) を含む、`/etc/fstab` のエントリは無効になります。

- [Linux] デフォルトのエントリとタイムアウトなど、grub ブートローダー設定を変更する。
- [Windows] VM を起動可能にするためにレジストリ設定を変更する。

変更されたファイルを書き込むときに、AWS は元のファイルを同じ場所に新しい名前で保持します。

オペレーティングシステム

SMS を使用して EC2 に移行できる オペレーティングシステムは以下のとおりです。

Windows (32 ビットおよび 64 ビット)

- Microsoft Windows Server 2003 (Standard、Datacenter、Enterprise) (Service Pack 1 を適用済み) 以降 (32 ビットと 64 ビット)
- Microsoft Windows Server 2003 R2 (Standard、Datacenter、Enterprise) (32 ビットと 64 ビット)
- Microsoft Windows Server 2008 (Standard、Datacenter、Enterprise) (32 ビットと 64 ビット)
- Microsoft Windows Server 2008 R2 (Standard、Web Server、Datacenter、Enterprise) (64 ビットのみ)
- Microsoft Windows Server 2012 (Standard、Datacenter) (64 ビットのみ)
- Microsoft Windows Server 2012 R2 (Standard、Datacenter) (64 ビットのみ) (Nano Server のインストールはサポートされていません)
- Microsoft Windows Server 2016 (Standard、Datacenter) (64 ビットのみ)
- Microsoft Windows Server 1709 (Standard、Datacenter) (64 ビットのみ)
- Microsoft Windows Server 1803 (Standard、Datacenter) (64 ビットのみ)
- Microsoft Windows Server 1803 (Standard、Datacenter) (64 ビットのみ)
- Microsoft Windows 7 (Home、Professional、Enterprise、Ultimate) (英語版) (32 ビットと 64 ビット)
- Microsoft Windows 8 (Home、Professional、Enterprise) (米国英語版) (32 ビットと 64 ビット)
- Microsoft Windows 8.1 (Professional、Enterprise) (米国英語版) (64 ビットのみ)
- Microsoft Windows 10 (Home、Professional、Enterprise、Education) (米国英語版) (64 ビットのみ)

Linux/Unix (64 ビットのみ)

- 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 は必要なドライバが存在しません)
- SUSE Linux Enterprise Server 11 Service Pack 1 およびカーネル 2.6.32.12-0.7
- SUSE Linux Enterprise Server 11 Service Pack 2 およびカーネル 3.0.13-0.27
- SUSE Linux Enterprise Server 11 Service Pack 3 およびカーネル 3.0.76-0.11、3.0.101-0.8、または 3.0.101-0.15
- SUSE Linux Enterprise Server 11 Service Pack 4 およびカーネル 3.0.101-63
- SUSE Linux Enterprise Server 12 およびカーネル 3.12.28-4
- SUSE Linux Enterprise Server 12 Service Pack 1 およびカーネル 3.12.49-11
- SUSE Linux Enterprise Server 12 Service Pack 2 およびカーネル 4.4

- SUSE Linux Enterprise Server 12 Service Pack 3 およびカーネル 4.4
- CentOS 5.1 ~ 5.11、6.1 ~ 6.6、7.0 ~ 7.6 (6.0 には必要なドライバがありません)
- Debian 6.0.0 ~ 6.0.8、7.0.0 ~ 7.8.0、8.0.0
- Oracle Linux 5.10-5.11 (kernel サフィックス el5uek)
- Oracle Linux 6.1-6.10 (RHEL 互換の kernel 2.6.32 または UEK kernels 3.8.13、4.1.12 を使用)
- Oracle Linux 7.0-7.6 (RHEL 互換の kernel 3.10.0 または UEK kernels 3.8.13、4.1.12、4.14.35 を使用)
- Fedora Server 19 ~ 21

ボリュームタイプとファイルシステム

AWS Server Migration Service は、以下のファイルシステムを使用する Windows および Linux インスタンスの移行をサポートしています。

オペレーティングシステム	ファイルシステム	アーキテクチャ	テーブルパーティション	サポートされるデータボリューム	サポートされるブートボリューム
Windows	NTFS	32 ビット	MBR	✓	✓
			GPT	✓	
		64 ビット	MBR	✓	✓
			GPT	✓	✓ (VHDX のみ)
	ReFS	32 ビット	MBR		
			GPT		
		64 ビット	MBR	✓	
			GPT	✓	
Linux/UNIX	ext2、ext3、ext4、btrfs、JFS、XFS	64 ビット	MBR	✓	✓
			GPT	✓	

EBS の暗号化を使用したボリュームを持つ AMI はサポートされていません。AWS SMS を使用してサーバーを移行する場合は、デフォルトでの暗号化を有効にしないでください。デフォルトでの暗号化がすでに有効になっていて、デルタレプリケーションエラーが発生している場合は、この機能を無効にしてください。

Server Migration Connector の IAM ユーザーの設定

AWS アカウントで Server Migration Connector の IAM ユーザーを作成するには

1. コネクタが AWS と通信するための新しい IAM ユーザーを作成します。生成されたアクセスキーとシークレットキーを保存し、コネクタの初期設定に使用します。IAM ユーザーとアクセス許可の管理については、「AWS アカウントでの IAM ユーザーの作成」を参照してください。
2. マネージド IAM ポリシー ServerMigrationConnector を IAM ユーザーにアタッチします。詳細については、「管理ポリシーとインラインポリシー」を参照してください。

制約事項

以下の制限が適用されます。

制約事項

イメージ形式

- Hyper-V/SCVMM で管理される VM を移行する場合、SMS は第 1 世代の VM (VHD または VHDX ディスク形式を使用) および 第 2 世代の VM (VHDX のみ) の両方をサポートします。
- VHDX ディスクでバックアップされている場合、AWS SMS は、RHEL 5 の任意のバージョンを実行している Hyper-V 上の VM はサポートしません。この形式のディスクを移行用の VHD に変換することをお勧めします。
- AWS SMS は、VHD および VHDX ディスクファイルの組み合わせを含む VM をサポートしていません。
- VMware では、AWS SMS は Raw デバイスマッピング (RDM) を使用する VM をサポートしていません。VMDK ディスクイメージのみがサポートされています。

起動

- UEFI/EFI ブートパーティションは、イメージ形式として VHDX を使用する Windows ブートボリュームでのみサポートされています。それ以外の場合は、VM のブートボリュームはマスターブートレコード (MBR) パーティションを使用する必要があります。いずれの場合も、MBR の制限によりブートボリュームは 2 TiB (非圧縮) を超えることはできません。

  Note

  メトリックAWSUEFI ブートパーティションを使用する Windows GPT ブートボリュームをが検出すると、変換されます。 on-the-fly BIOS ブートパーティションを持つ MBR ブートボリュームに。これは、EC2 で GPT ブートボリュームが直接サポートされていないためです。
- ルートパーティションが MBR と同じ仮想ハードドライブにない場合は、インポートした VM が起動しないこともあります。
- ルートパーティションが MBR と同じ仮想ハードディスクにない場合は、移行した VM が起動しないこともあります。
- デュアルブート設定の VM の移行設定はサポートされていません。

ネットワーク

- 現在、複数のネットワークインターフェイスはサポートされていません。移行後、VM にはアドレスの割り当てに DHCP を使用する 1 つの仮想ネットワークインターフェイスが与えられます。インスタンスはプライベート IP アドレスを受け取ります。
- VPC に移行された VM は、サブネットの自動割り当てパブリック IP の設定にかかわらず、パブリック IP アドレスを受け取りません。その代わり、Elastic IP アドレスをアカウントに割り当て、それをインスタンスに関連付けます。

- インターネットプロトコルバージョン 6 (IPv6) の IP アドレスはサポートされていません。

Migration Hub からのアプリケーションのインポート

- SMS は、SMS サーバーカタログに存在している場合のみ、AWS Migration Hub からアプリケーション関連サーバーをインポートします。その結果、一部のアプリケーションは部分的にしか移行されない場合があります。
- SMS サーバーカタログに Migration Hub アプリケーションが 1 つも存在しない場合、インポートはメッセージが表示されずに失敗し、アプリケーションは SMS に表示されなくなります。
- インポートされたアプリケーションは移行できますが、SMS で編集することはできません。ただし、それらは Migration Hub で編集できます。

雑則

- 22 を超えるボリュームがアタッチされている VM では、SMS レプリケーションジョブは失敗します。
- EBS の暗号化を使用したボリュームを持つ AMI はサポートされていません。AWS SMS を使用してサーバーを移行する場合は、デフォルトでの暗号化を有効にしないでください。デフォルトでの暗号化がすでに有効になっていて、デルタレプリケーションエラーが発生している場合は、この機能を無効にしてください。
- AWS SMS は、ハードウェア仮想マシン (HVM) 仮想化を使用する AMI を作成します。準仮想化 (PV) を使用する AMI は作成できません。Linux PVHVM ドライバーは、移行された VM 内でサポートされます。
- P2V 変換の結果として作成された VM はサポートされません。P2V 変換は、物理マシンで Linux または Windows インストールプロセスを実行し、その Linux または Windows インストールのコピーを VM にインポートすることでディスクイメージを作成するときに行われます。
- AWS SMS によってシングルルート I/O 仮想化 (SR-IOV) ドライバーはインストールされません。ただし、Microsoft Windows Server 2012 R2 VM をインポートする場合は除きます。これらのドライバは、より優れたパフォーマンス (パケット毎秒)、レイテンシーとストレスの低減を可能にする拡張ネットワーキングを使用しない場合は不要です。Microsoft Windows Server 2012 R2 VM の場合、SR-IOV ドライバーは移行プロセスの一部として自動的にインストールされます。
- 独立したディスクは、スナップショットの影響を受けないため、AWS SMS は、独立モードでは VMDK の間隔レプリケーションはサポートしません。
- UTF-16 文字 (または ASCII 以外の文字) を使用する Windows 言語パックでインポートはサポートされません。Windows Server 2003、Windows Server 2008、Windows Server 2012 R1 VM をインポートするときは、英語の言語パックを使用することをお勧めします。
- Windows Server 2003 では、移行前に Windows ドライバによる署名チェックを無効にします。

AWS SMS のライセンスオプション

新しいレプリケーションジョブを作成すると、AWS Server Migration ServiceAPIとAWS CLIライセンスタイプオプションを含めます。VM と互換性のないライセンスタイプを選択すると、レプリケーションジョブはエラーメッセージを表示して失敗します。指定できる値は以下のとおりです。

- Auto (デフォルト)

  ソースシステムのオペレーティングシステム (OS) を検出し、移行された仮想マシン (VM) に適切なライセンスを適用します。
- AWS

  移行された VM で、必要に応じてソースシステムのライセンスを AWS のライセンスに置き換えます。

- BYOL

  移行された VM で、必要に応じてソースシステムのライセンス維持します。

AWS CLI例:

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

`--license-type` パラメータの値は、`AWS` または `BYOL` です。デフォルト値は、「`Auto`」です。

Linux のライセンス

Linux オペレーティングシステムは BYOL ライセンスのみをサポートします。[Auto] (デフォルト) を選択すると、SMS は BYOL ライセンスを使用します。

移行された Red Hat Enterprise Linux (RHEL) VM は Cloud Access (BYOL) ライセンスを使用する必要があります。詳細については、Red Hat ウェブサイトの「Red Hat Cloud Access」を参照してください。

移行した SUSE Linux Enterprise Server VM では、SUSE パブリッククラウドプログラム (BYOS) ライセンスを使用する必要があります。詳細については、「SUSE Public Cloud Program—Bring Your Own Subscription」を参照してください。

Windows のライセンス

Windows Server オペレーティングシステムは、BYOL ライセンスまたは AWS ライセンスをサポートします。Windows クライアントオペレーティングシステム (Windows 10 など) は BYOL ライセンスのみをサポートします。

[Auto] (デフォルト) を選択すると、VM にサーバー OS がある場合、AWS SMS は AWS のライセンスを使用します。VM にクライアント OS がある場合は、BYOL ライセンスが使用されます。

MSDN または Windows Software Assurance Per User 経由で BYOL Microsoft ライセンスを使用する場合、以下のルールが適用されます。

- BYOL インスタンスの価格は Amazon EC2 Linux インスタンスの一般料金表によって決まります。ただし、次の条件に従うものとします。
  - Dedicated Host (Dedicated Host) で実行する
  - AWS SMS の現行の条件および機能に従って、AWS SMS を使用してお客様提供のソフトウェアバイナリをソースとする VM から起動する
  - インスタンスを BYOL インスタンスとして指定する
  - AWS が BYOL モデルを提供している指定 AWS リージョン内でのインスタンスの実行
  - ユーザーが提供した Microsoft キーまたはキー管理システムで使用されている Microsoft キーを使用したアクティブ化
- Amazon EC2 インスタンスを起動すると、そのインスタンスはアベイラビリティーゾーン内のいずれかのサーバーで実行されることを考慮する必要があります。つまり、Amazon EC2 インスタンスの起動 (停止/起動を含む) のたびに、そのインスタンスはアベイラビリティーゾーン内の別のサーバーで実行される可能性があります。このような使用方法においては、ライセンス条項に掲載されている Microsoft ボリューム ライセンス製品条項で記載されているライセンス再割り当ての制限が適用されるかどうか、取得済みの使用権限が適用されるかどうかを判断してください。
- Microsoft との契約の下で、たとえば、MSDN のユーザー権限または Windows Software Assurance per User の権利の下で、該当する Microsoft ソフトウェアの BYOL プログラムを使用できる必要があります。お客様は、必要なすべてのライセンスの取得、および該当するすべての Microsoft ライセンスの要件 (PUR または PT など) の遵守に全責任を負うものとします。また、Microsoft の使用許諾契約 (Microsoft EULA) に同意する必要があります。さらに、BYOL プログラムの下で Microsoft ソフトウェアを使用することで、Microsoft EULA に同意したとみなされます。

- AWS では、該当する Microsoft ライセンスの要件の遵守について、社内の法務部署およびその他の顧問に相談することをお勧めします。Microsoft との契約に違反したサービスの使用方法 (licenseType パラメータと BYOL フラグの使用を含む) は承認も許可もされません。

その他の要件

VMware vMotion のサポート

AWS Server Migration Service は、vMotion、Storage vMotion、その他の仮想マシンの移行に基づく機能 (DRS や Storage DRS など) を部分的にサポートします。ただし、以下の制約が適用されます。

- 仮想マシンを新しい ESXi ホストまたはデータストアに移行する場合、1 つのレプリケーション実行が終わってから次のレプリケーション実行が始まるまでの移行は、移行先の ESXi ホスト、データストア、データセンター、および新しい場所での仮想マシン自体に対して、Server Migration Connector の vCenter サービスアカウントに十分なアクセス許可がある場合に限ってサポートされます。
- 仮想マシンの新しい ESXi ホスト、データストア、データセンターへの移行は、レプリケーションの進行中 (仮想マシンのアップロード中) はサポートされません。
- クロス vCenter vMotion は、AWS SMS との連携でサポートされません。

VMware vSAN のサポート

vSAN データストアの VM は、[Configure replication jobs settings] ページの [Replication job type] が [One-time migration] に設定されている場合にのみサポートされます。

VMware 仮想ボリューム (VVol) のサポート

AWS は、VMware 仮想ボリュームの移行サポートを提供していません。ただし、一部の実装は動作する場合があります。

スナップショットを含む VMware VM

AWS SMS は、スナップショットベースのバックアップソフトウェアが使用されている VM で、1 回のみの移行をサポートします。また、AWS SMS を通じてレプリケートされた VM でスナップショットを作成することは避けてください。

Hyper-V のチェックポイント

AWS SMS は、既存のチェックポイントがある VM をサポートしていません。

Hyper-V の差分ディスク

AWS SMS は、差分ディスクがある仮想マシンをサポートしていません。

Server Migration Connector をインストールする

Server Migration Connector は、オンプレミスの仮想化環境にインストールする FreeBSD VM です。サポートされるプラットフォームは、VMware vSphere、Microsoft Hyper-V/SCVMM、Microsoft Azure です。

目次

VMware への Server Migration Connector のインストール

以下の情報を使用して Server Migration Connector を VMware にインストールします。これにより、AWS SMS を使用して VM を VMware 環境から Amazon EC2 に移行できるようになります。

この情報は、オンプレミスの VMware 環境にある VM にのみ適用されます。他の環境へのコネクタのインストールについては、「Server Migration Connector をインストールする (p. 10)」を参照してください。

VMware コネクタの要件

- vCenter バージョン 5.1 以降 (6.7 まで検証済み)
- ESXi 5.1 以降 (6.7 まで検証済み)
- 8 GiB 以上の RAM
- 20 GiB (シンプロビジョニング) または 250 GiB (シックプロビジョニング) 以上の使用可能なディスクストレージ
- 以下のネットワークサービスのサポート。これらのサービスに対するコネクタからのステートフルなアウトバウンド接続を許可するために、ファイアウォールの再構成が必要になる場合がありますのでご注意ください。
  - DNS — 名前解決のためにポート 53 への接続を開始することをコネクタに許可します。
  - HTTPS on vCenter—vCenter のポート — 443 にセキュアなウェブ接続を開始することをコネクタに許可します。必要に応じて、デフォルトでないポートを設定することもできます。vCenter Server でデフォルトでないポートを使用するように設定した場合は、vCenter サービスアカウントページの [Connector setup] に、vCenter のホスト名とポートの両方をコロンで区切って指定します (例: `HOSTNAME:PORT` または `IP:PORT`)。
  - HTTPS on ESXi — 移行元の VM を含む ESXi ホストのポート 443 にセキュアなウェブ接続を開始することをコネクタに許可します。
  - NTP - 必要に応じて時刻同期のためにポート 123 へのコネクタのアウトバウンドアクセスを許可します。コネクタと ESXi ホストのクロックが同期している場合、この設定は不要です。
- コネクタからの以下の URL 範囲へのアウトバウンド接続を許可します。
  - *.amazonaws.com
  - *.aws.amazon.com

VMware 環境用にコネクタをセットアップするには

1. 次のリンクを使用して VMware 環境のコネクタをダウンロードします。https://s3.amazonaws.com/sms-connector/AWS-SMS-Connector.ova。コネクタは、OVA 形式で事前設定された FreeBSD VM であり、vCenter にデプロイする準備が完了しています。

   整合性チェックサム

   - 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. vCenter サービスアカウントをセットアップします。AWS に移行する必要のある VM 上でスナップショットを作成および削除し、差分ディスクをダウンロードするために必要なアクセス許可を持つ vCenter ユーザーを作成します。

   Note

   ベストプラクティスとして、コネクタのサービスアカウントの vCenter のアクセス許可を、移行する VM が格納されている vCenter データセンターのみに制限することをお勧めします。また、vCenter サービスアカウントのアクセス許可をこのユーザーに割り当てます。NoAccess vCenter のロール。移行する VM のないホスト、フォルダ、およびデータストア上の vCenter のロール。

3. vCenter で以下の権限を持つロールを作成します。

   - [Datastore] > [Browse datastore and Low level file operations] (Datastore.Browse および Datastore.FileManagement)
   - ホスト > 設定 > システム管理 (Host.Config.SystemManagement)
   - [vApp] > [Export] (VApp.Export)
   - [Virtual Machine] > [Snapshot management] > [Create snapshot and Remove Snapshot] (VirtualMachine.State.CreateSnapshot および VirtualMachine.State.RemoveSnapshot)

4. 次のようにロールを割り当てます。

   a. この vCenter ロールを、コネクタのサービスアカウントに割り当て、vCenter へのログインに使用します。

   b. このロールを伝達権限と共に VM の移行元のデータセンターに割り当てます。

5. vCenter サービスアカウントのアクセス許可を手動で確認するには、コネクタのサービスアカウントの認証情報を使用して vSphere Client にログインできることを確認します。次に、VM を OVF テンプレートとしてエクスポートし、データストアのブラウザを使用して VM を含むデータストアからファイルをダウンロードし、VM の ESXi ホストの [Summary] タブのプロパティを表示します。

コネクタを設定するには

1. vSphere Client を使用して、前の手順でダウンロードしたコネクタ OVA を VMware 環境にデプロイします。
2. コネクタの仮想マシンコンソールを開き、パスワード `ec2pass` で `ec2-user` としてログインします。求められたら、新しいパスワードを指定します。
3. 次に示すようにコネクタの IP アドレスを取得します。

   a. sudo setup.rb コマンドを実行します。これにより設定メニューが表示されます。

```
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. オプション「2」を入力します。現在のネットワーク情報と、ネットワーク設定を変更するサブメニューが表示されます。出力は次のようになります。

```
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]:
```

この IP アドレスは後の手順で必要になります。

4. (オプション) コネクタの静的 IP アドレスの設定 これにより、DHCP がコネクタに新しいアドレスを割り当てるたびに、LAN 上の信頼できるホストリストを再設定する必要がなくなります。

   [Reconfigure your network] (ネットワークの再設定) メニューにオプション「2」を入力します。ネットワーク設定を指定するフォームが表示されます。

   各フィールドに適切な値を入力し、Enter キーを押します。次のような出力が表示されます。

```
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. コネクタのネットワーク構成メニューで、DNS サフィックス検索リストのドメインサフィックス値を設定します。
6. 環境で Web プロキシを使用してインターネットにアクセスしている場合は、ここで設定を行います。
7. コネクタコンソールを離れる前に、ping を使用して、LAN 内外の次のターゲットへのネットワークアクセスを検証します。

   - LAN 内で、ホスト名、FQDN、および IP アドレスを使用して ESXi ホストと vCenter へのアクセスを確認します。
   - LAN の外で、AWS へのアクセスを確認します。
8. ウェブブラウザで、IP アドレス (https://*ip-address-of-connector*/) で VM にアクセスしてセットアップウィザードを開き、[Get started now] (今すぐ開始) を選択します。
9. ライセンス契約を確認し、チェックボックスをオンにして、[Next (次へ)] を選択します。
10. コネクタのパスワードを作成します。

11. [Upload logs automatically] (ログを自動的にアップロード) および [Server Migration Connector auto-upgrade] (Server Migration Connector の自動アップグレード) を選択します。
12. [AWS Region] (AWS リージョン) で、リストからリージョンを選択します。を使用する場合AWS認証情報で、「」で作成した IAM 認証情報を入力します。Server Migration Connector の IAM ユーザーの設定 (p. 5)。[Next] (次へ) を選択します。
13. [vCenter Service Account] に、ステップ 3 の vCenter ホスト名、ユーザー名、パスワードを入力します。[Next] (次へ) を選択します。
14. vCenter 証明書の受理後に、登録を完了し、コネクタ設定ダッシュボードを表示します。
15. 登録したコネクタが [Connectors] ページに表示されることを確認します。コネクタの登録時に問題が発生した場合は、sms-service@amazon.com に連絡してください。

Hyper-V への Server Migration Connector のインストール

AWS SMS は、スタンドアロンの Hyper-V サーバーからの移行、System Center Virtual Machine Manager (SCVMM) によって管理される Hyper-V サーバーからの移行という、2 つのいずれかのモードでの移行をサポートします。以下の情報を使用して Server Migration Connector を Hyper-V にインストールします。これにより、AWS SMS を使用して VM を Hyper-V から Amazon EC2 に移行できるようになります。

この情報は、オンプレミスの Hyper-V 環境にある VM にのみ適用されます。他の環境へのコネクタのインストールについては、「Server Migration Connector をインストールする (p. 10)」を参照してください。

移行シナリオに関する考慮事項

- スタンドアロンの Hyper-V および SCVMM 環境のインストール手順は、互換性がありません。
- SCVMM モードで設定すると、1 つの Server Migration Connector アプライアンスが (複数の Hyper-V サーバーを管理できる) 1 つの SCVMM からの移行をサポートします。
- スタンドアロン Hyper-V モードで設定すると、1 つの Server Migration Connector アプライアンスが複数の Hyper-V サーバーからの移行をサポートします。
- AWS SMS は、複数の SCVMM および複数のスタンドアロン Hyper-V サーバからの移行を並行してサポートするために、任意の数のコネクタプライアンスのデプロイをサポートします。

Hyper-V コネクタの要件

- Windows Server 2012 R2 または Windows Server 2016 の Hyper-V ロール
- Active Directory 2012 以降
- (オプション) SCVMM 2012 SP1 または SCVMM 2016
- 8 GiB 以上の RAM
- 300 GiB 以上の使用可能なディスクストレージ
- 以下のネットワークサービスのサポート。これらのサービスに対するコネクタからのステートフルなアウトバウンド接続を許可するために、ファイアウォールの再構成が必要になる場合がありますのでご注意ください。
  - DNS — 名前解決のためにポート 53 への接続を開始することをコネクタに許可します。
  - SCVMM またはスタンドアロン Hyper-V ホスト上の WinRM ポート 5986 上の HTTPS
  - コネクタのポート 443 上のインバウンド HTTPS - コネクタが、移行する VM が格納されている Hyper-V ホストからポート 443 で安全なウェブ接続を受信できるようにします。
  - NTP - 必要に応じて時刻同期のためにポート 123 へのコネクタのアウトバウンドアクセスを許可します。コネクタが Hyper-V ホストとクロックを同期する場合、これは不要です。

- コネクタからの以下の URL 範囲へのアウトバウンド接続を許可します。
  - *.amazonaws.com
  - *.aws.amazon.com

目次

Server Migration Connector のインストールスクリプトについて

AWS SMS 設定スクリプトは、AWS SMS が Hyper-V 環境でタスクを実行できるようにする適切なアクセス許可とネットワーク接続の作成を自動化します。VM の移行に使用する各 Hyper-V および SCVMM ホストで、スクリプトを管理者として実行する必要があります。スクリプトを実行すると、次のアクションが実行されます。

1. [すべてのシステム] SCVMM およびすべての Hyper-V ホストで Windows Remote Management (WinRM) サービスが有効になっているかどうかを確認し、必要に応じて有効にして、起動時に自動的に開始するように設定します。
2. [すべてのシステム] PowerShell リモート処理を有効にします。これにより、 は WinRM 接続を介してそのホスト上で PowerShell コマンドを実行できます。
3. [すべてのシステム] 自己署名の X.509 証明書を作成し、WinRM HTTPS リスナーを作成して、証明書をリスナーにバインドします。
4. [すべてのシステム] WinRM リスナーへの着信接続を受け入れるためのファイアウォールルールを作成します。
5. [すべてのシステム] コネクタの IP アドレスまたはドメイン名を WinRM 設定の信頼できるホストの一覧に追加します。インタラクティブで提供できるように、スクリプトを実行する前にこの IP アドレスまたはドメイン名を設定する必要があります。
6. [すべてのシステム] WinRM で Credential Security Support Provider (CredSSP) 認証を有効にします。
7. [すべてのシステム] WinRM configSDDL 上の事前設定された Active Directory ユーザーに対して、読み取りと実行のアクセス許可を与えます。このユーザーは、後述の ステップ 1: Active Directory で Server Migration Connector のサービスアカウントを作成する (p. 15) で説明するサービスアカウントと同じです。
8. [スタンドアロン Hyper-V のみ] Active Directory ユーザーを、Hyper-V ホスト上の Hyper-V 管理者およびリモート管理ユーザーのグループに追加します。
9. [スタンドアロン Hyper-V のみ] この Hyper-V によって管理されているすべての VM データフォルダに読み取り専用アクセス許可を与えます。
10. (SCVMM のみ) 2 つの WMI オブジェクト (CIMV2 および SCVMM) の Active Directory ユーザーに対して、「メソッドの実行」、「アカウントの有効化」、および「リモート有効化」のアクセス許可を付与します。
11. (SCVMM のみ) SCVMM に、すべての Hyper-V ホストにアクセスする権限を持つ委任管理者ロールを作成します。Active Directory ユーザーにロールを割り当てます。SCVMM でこのロールを編集することにより、ホストへのアクセスを選択的に削除することができます。

12(SCVMM のみ) SCVMM と Hyper-V ホスト間に安全な (HTTPS) ネットワークパスが存在するかどうかを確認します。スクリプトが安全なチャネルを検出しない場合は、エラーを返し、管理者がチャネルを保護するための指示を生成します。

13(SCVMM のみ) SCVMM によって管理されるすべての Hyper-V ホストを反復処理し、Active Directory ユーザーに各 Hyper-V ホスト上のすべての VM フォルダーに対する読み取り専用のアクセス許可を付与します。

ステップ 1: Active Directory で Server Migration Connector のサービスアカウントを作成する

Server Migration Connector では、Active Directory のサービスアカウントが必要です。コネクタの設定スクリプトは各 SCVMM および Hyper-V ホストで実行されるため、これらのホストに対するアクセス許可がこのアカウントに付与されます。

> Note
>
> SCVMM モードで設定する場合、SCVMM ホストとそれが管理するすべての Hyper-V ホストを単一の Active Directory ドメインに配置する必要があります。複数の Active Directory ドメインがある場合は、それぞれのコネクタを設定します。

Active Directory ユーザーを作成するには

1. Active Directory フォレストがインストールされている Windows コンピュータで Active Directory 管理センターを使用して、新しいユーザーを作成し、パスワードを割り当てる必要があります。
2. [Remote Management Users] グループに新しいユーザーを追加します。

ステップ 2: Server Migration Connector をダウンロードしてデプロイする

Hyper-V および SCVMM 用の Server Migration Connector をオンプレミス環境にダウンロードし、Hyper-V ホストにインストールします。

Hyper-V 環境用にコネクタをセットアップするには

1. 次のリンクを使用して Hyper-V のコネクタをダウンロードします。https://s3.amazonaws.com/sms-connector/AWS-SMS-Connector-for-SCVMM-HyperV.zip。

   整合性チェックサム

   - 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. ダウンロードしたコネクタファイルを Hyper-V ホストに転送し、解凍してコネクタを VM としてインポートします。
3. コネクタの仮想マシンコンソールを開き、パスワード `ec2pass` で `ec2-user` としてログインします。求められたら、新しいパスワードを指定します。
4. 次に示すようにコネクタの IP アドレスを取得します。

   a. sudo setup.rb コマンドを実行します。これにより設定メニューが表示されます。

   ```
   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. オプション「2」を入力します。現在のネットワーク情報と、ネットワーク設定を変更するサブメニューが表示されます。出力は次のようになります。

```
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]:
```

この IP アドレスは後の手順で必要になります。

5. (オプション) コネクタの静的 IP アドレスの設定 これにより、DHCP がコネクタに新しいアドレスを割り当てるたびに、LAN 上の信頼できるホストリストを再設定する必要がなくなります。

   [Reconfigure your network] (ネットワークの再設定) メニューにオプション「2」を入力します。ネットワーク設定を指定するフォームが表示されます。

   各フィールドに適切な値を入力し、Enter キーを押します。次のような出力が表示されます。

```
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. コネクタのネットワーク構成メニューで、DNS サフィックス検索リストのドメインサフィックス値を設定します。
7. 環境で Web プロキシを使用してインターネットにアクセスしている場合は、ここで設定を行います。
8. コネクタコンソールを離れる前に、ping を使用して、LAN 内外の次のターゲットへのネットワークアクセスを検証します。

   - LAN 内で、ホスト名、FQDN、および IP アドレスを使用して Hyper-V ホストおよび SCVMM へのアクセスを確認します。
   - LAN の外で、AWS へのアクセスを確認します。

ステップ 3: Hyper-V/SCVMM 設定スクリプトをダウンロードしてインストールする

AWS SMSダウンロード可能 PowerShell スクリプトを使用して、Server Migration Connectorとの通信をサポートするように Windows 環境を設定するためのスクリプトです。スタンドアロンの Hyper-V または SCVMM の設定には、同じスクリプトを使用します。このスクリプトは、AWS によって暗号で署名されます。

次の URL からスクリプトとハッシュファイルをダウンロードしてください。

File	URL
インストールスクリプト	https://s3.amazonaws.com/sms-connector/aws-sms-hyperv-setup.ps1
MD5 ハッシュ	https://s3.amazonaws.com/sms-connector/aws-sms-hyperv-setup.ps1.md5
SHA256 ハッシュ	https://s3.amazonaws.com/sms-connector/aws-sms-hyperv-setup.ps1.sha256

ダウンロード後、ダウンロードしたファイルを、スクリプトを実行するコンピュータに転送します。

ステップ 4: スクリプトファイルの整合性と暗号署名を検証する

スクリプトを実行する前に、整合性と署名を検証することをお勧めします。これらの手順では、スクリプトを実行するコンピュータのデスクトップにインストールされているスクリプトとハッシュファイルをダウンロードし、管理者としてサインインしていることを前提としています。セットアップに合わせて手順を変更する必要がある場合があります。

暗号化ハッシュ (PowerShell) を使用してスクリプトの整合性を検証するには

1. ダウンロードしたハッシュファイルの一方または両方を使用して、スクリプトファイルの整合性を検証し、コンピュータへの転送中に変更されていないことを確認します。

   a. MD5 ハッシュで検証するには、次のコマンドを PowerShell Windows:

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

   これにより、次のような情報が返されます。

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

   b. SHA256 ハッシュで検証するには、次のコマンドを PowerShell Windows:

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

   これにより、次のような情報が返されます。

   ```
   Algorithm       Hash
   ```

```
---------          ----
SHA256             6B86B273FF34FCE19D6B804EFF5A3F574EXAMPLE22F1D49C01E52DDB7875B4B
```

2. 返されたハッシュ値をダウンロードされたファイル `aws-sms-hyperv-setup.ps1.md5` および `aws-sms-hyperv-setup.ps1.sha256` と比較します。

次に、Windows ユーザーインターフェイスまたは PowerShell スクリプトファイルにの有効な署名が含まれていることを確認するにはAWS。

有効な暗号署名 (Windows GUI) のスクリプトファイルを確認するには

1. Windows エクスプローラで、スクリプトファイルのコンテキスト (右クリック) メニューを開き、[Properties]、[Digital Signatures]、[Amazon Web Services]、 [Details] を選択します。
2. 表示された情報に「このデジタル署名は問題ありません。」が含まれており、署名者が「Amazon Web Services, Inc.」 であることを確認します。

有効な暗号署名 (PowerShell) のスクリプトファイルを確認するには

- で PowerShell ウィンドウで、以下のコマンドを実行します。

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

正しく署名されたスクリプトファイルは、次のような情報を返します。

```
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

...
```

ステップ 5: スクリプトを実行します。

この手順では、スクリプトを実行するコンピュータのデスクトップにスクリプトをダウンロードし、管理者としてサインインしていることを前提としています。セットアップに合わせて表示されている手順を変更する必要がある場合があります。

Note

SCVMM を使用している場合は、移行元の各 Hyper-V ホストでこのスクリプトを実行してから、SCVMM で実行する必要があります。

各ホストでスクリプトを実行するには

1. RDP を使用して、SCVMM システムまたはスタンドアロンの Hyper-V ホストに管理者としてログインします。
2. 次のを使用してスクリプトを実行します。 PowerShell コマンド:

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

Note

もしあなたの PowerShell 実行ポリシーが署名付きスクリプトを確認するように設定されている場合は、コネクタ設定スクリプトの実行時に承認を求められます。スクリプトが「Amazon Web Services, Inc.」によって発行されていることを確認し、「R」をクリックして一度実行します。この設定は、Get-ExecutionPolicy を使用して表示し、Set-ExecutionPolicy を使用して変更できます。

3. スクリプトが実行されると、いくつかの情報が求められます。次のプロンプトに対応する準備をしてください。

スクリプトアクション	カスタマープロンプト	カスタマーアクション
コネクタのオペレーションモード (スタンドアロン Hyper-V から移行するか、または SCVMM を使用して移行するか) に基づいて、Windows 環境にどのような変更を加える必要があるかを決定するオプションが求められます。	0. Exit 1. スタンドアロンの Hyper-V を再設定する 2. SCVMM によって管理される Hyper-V を再設定する 3. SCVMM を再設定する 4. ヘルプ/サポート	スクリプトを終了するには、0 を選択します。 スタンドアロン Hyper-V ホストを再設定してゲスト VM の移行を許可するには、1 を選択します。 Hyper-V ホストを再設定して SCVMM がゲスト VM の移行を管理することを許可するには、2 を選択します。 SCVMM を再設定して、管理するすべての Hyper-V ホスト上のゲスト VM の移行を許可するには、3 を選択します。 オプション「4」は、このドキュメントと AWS サポートに関する情報にリンクしています。
コネクタが SCVMM および Hyper-V と通信するときに使用する Active Directory ユーザーのプロンプトを表示します。	コネクタが使用する AD ユーザーを入力します (DOMAIN\user)	以前に設定した Active Directory ユーザーを提供します。詳細については、「ステップ 1: Active Directory で Server Migration Connector のサービスアカウントを作成する (p. 15)」を参照してください。
コネクタの IP アドレスまたはホスト名のプロンプト。	コネクタアプライアンスの IP アドレスまたはホスト名を入力する	コネクタに設定した IP アドレスまたはホスト名を入力します。
Windows 環境を変更する前に確認を求めるプロンプトが表示されます。	Windows システム設定を変更しますか? (「yes」または「no」を入力してください)	「yes」と入力し Enter キーを押すと、再設定を開始します。「no」と入力すると、スクリプトを終了します。

ステップ 6: コネクタの設定

コネクタの設定が正常に実行されたら、コネクタのウェブインターフェイスを参照します。

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

新しいコネクタをセットアップするには、次のステップを完了します。

コネクタを設定するには

1. コネクタのランディングページで、[今すぐ始める] を選択します。
2. ライセンス契約を確認し、チェックボックスをオンにして、[Next (次へ)] を選択します。
3. コネクタのパスワードを作成します。パスワードは、表示された基準を満たしている必要があります。[Next] (次へ) を選択します。
4. [Network Info] (ネットワーク情報) ページで、(他のタスクと共に) コネクタにまだ静的 IP アドレスを割り当てていない場合は、それを割り当てることができます。[Next] (次へ) を選択します。
5. [Log Uploads and Upgrades] (ログのアップロードとアップグレード) ページで、[Upload logs automatically (ログの自動アップロード)] および [Server Migration Connector auto-upgrade] (Server Migration Connector の自動アップグレード) を選択して [次へ] を選択します。
6. [Server Migration Service (サーバー移行サービス)] ページで、以下の情報を提供します。
   - [AWS Region] (AWS リージョン) で、リストからリージョンを選択します。
   - を使用する場合AWS認証情報で、「」で作成した IAM 認証情報を入力します。Server Migration Connector の IAM ユーザーの設定 (p. 5)。[Next] (次へ) を選択します。
7. [Choose your VM manager type] (VM Manager のタイプを選択) ページで、環境に応じて [Microsoft® System Center Virtual Manager (SCVMM)] または [Microsoft® Hyper-V] のどちらかを選択します。Hyper-V コネクタがインストールされている場合は [VMware® vCenter] を選択すると、エラーが発生します。[Next] (次へ) を選択します。
8. リポジトリの []Hyper-V: ホストおよびサービスアカウントのセットアップまたはSCVMM: ホストおよびサービスアカウントのセットアップページで、で作成した Active Directory ユーザーのアカウント情報を提供します。ステップ 1: Active Directory で Server Migration Connector のサービスアカウントを作成する (p. 15)を含むユーザーネームそしてパスワード。
9. - [SCVMM only] (SCVMM のみ) このコネクタによって処理される SCVMM ホスト名を指定し、[Next] (次へ) を選択します。ホストの証明書を調べて、証明書が有効であれば [Trust (信頼する)] を選択します。
   - [Stand-alone Hyper-V only] (スタンドアロン Hyper-V のみ) このコネクタによって処理される各ホストの Hyper-V ホスト名を指定します。さらにホストを追加するには、プラス記号を使用します。各ホストの証明書を調べるには、[Verify Certificate (証明書の確認)] を選択し、証明書が有効であれば [Trust (信頼する)] を選択します。[Next] (次へ) を選択します。

   または、ホスト固有オプションを、SCVMM または Hyper-V ホスト証明書でホスト名の不一致と有効期限のエラーは無視するように選択することもできます。本稼働環境でセキュリティを上書きすることはお勧めしませんが、テスト中は役に立つことがあります。

   Note

   複数の Active Directory ドメインに Hyper-V ホストがある場合は、個別のコネクタを各ドメインに設定することをお勧めします。
10. コネクタで正常に認証された場合、[Congratulations] (認証完了) ページが表示されます。コネクタのヘルスステータスを表示するには、[Go to connector dashboard] (コネクタダッシュボードに移動) を選択します。

11. 登録したコネクタがリストに登録されていることを確認するには、AWS Server Migration Service コンソールの [Connectors] (コネクタ) ページを開きます。コネクタの登録時に問題が発生した場合は、sms-service@amazon.com に連絡してください。

Azure への Server Migration Connector のインストール

以下の情報を使用して Server Migration Connector を Azure にインストールします。これにより、AWS SMS を使用して VM を Azure から Amazon EC2 に移行できるようになります。

この情報は、Azure でホストされる VM にのみ適用されます。他の環境へのコネクタのインストールについては、「Server Migration Connector をインストールする (p. 10)」を参照してください。

移行シナリオに関する考慮事項

- 単一の Server Migration Connector アプライアンスでは、1 つのサブスクリプションと 1 つの Azure リージョンにある VM のみを移行できます。
- Server Migration Connector アプライアンスがデプロイされたら、新しいサブスクリプションとリージョンで別のコネクタをデプロイしない限り、このアプライアンスのサブスクリプションやリージョンを変更することはできません。
- AWS SMS は、複数の Azure サブスクリプションおよびリージョンから並行して移行できるように、任意の数の Server Migration Connector アプライアンス VM のデプロイをサポートしています。
- Server Migration Connector は Azure Government リージョンをサポートしていません。

Azure コネクタの要件

- Azure コネクタの推奨される VM サイズは、F4 (4 個の vCPU と 8 GB の RAM) です。コネクタをデプロイしているリージョンに Azure CPU の十分なクォータがあることを確認します。
- コネクタをデプロイできる標準ストレージアカウント (プレミアムではできません)。
- コネクタをデプロイできる仮想ネットワーク。
- コネクタの登録およびコネクタダッシュボードの表示を目的とした、コネクタの仮想ネットワーク内 (推奨)、または一般公開 (推奨されていません) からのポート443 (HTTPS) でのインバウンドアクセス。
- AWS サービス、Azure サービス、コネクタ OS の更新などを実行するためのアウトバウンドインターネットアクセス。

目次

ステップ 1: コネクタのインストールスクリプトをダウンロードする

AWSSMSはダウンロード可能なものを提供します PowerShell Azure 環境にコネクタをデプロイするためのスクリプトです。このスクリプトは、AWS によって暗号で署名されます。この手順を実行して、

PowerShell Azure 環境にコネクタを自動的にスクリプト化してインストールします。スクリプトには次のものが必要です。 PowerShell 5.1 以降。

Note

AWS では、スクリプトによるコネクタのインストールを推奨していますが、手動でインストールすることもできます。詳細については、「(別の方法) Server Migration Connector を手動でデプロイする (p. 25)」を参照してください。

スクリプトとハッシュファイルをダウンロードするには

1. のダウンロード PowerShell 次の URL からのスクリプトとハッシュファイル:

File	URL
インストールスクリプト	https://s3.amazonaws.com/sms-connector/aws-sms-azure-setup.ps1
MD5 ハッシュ	https://s3.amazonaws.com/sms-connector/aws-sms-azure-setup.ps1.md5
SHA256 ハッシュ	https://s3.amazonaws.com/sms-connector/aws-sms-azure-setup.ps1.sha256

2. ダウンロード後、スクリプトを実行するコンピュータにそのファイルを転送します。

ステップ 2: スクリプトファイルの整合性と暗号署名を検証する

スクリプトを実行する前に、その整合性と署名を検証すし、コンピュータへの転送中に変更されていないことを確認することをお勧めします。これらの手順では、スクリプトを実行するコンピュータのデスクトップにインストールされているスクリプトとハッシュファイルをダウンロードし、管理者としてサインインしていることを前提としています。セットアップに合わせて手順を変更する必要がある場合があります。

暗号化ハッシュ (PowerShell) を使用してスクリプトの整合性を検証するには

1. ダウンロードしたハッシュファイルの 1 つまたは両方を使用して、スクリプトファイルの整合性を検証します。

   a. MD5 ハッシュで検証するには、次のコマンドを PowerShell Windows:

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

   これにより、次のような情報が返されます。

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

   b. SHA256 ハッシュで検証するには、次のコマンドを PowerShell Windows:

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

   これにより、次のような情報が返されます。

   ```
   Algorithm         Hash
   ```

```
---------          ----
SHA256             6B86B273FF34FCE19D6B804EFF5A3F574EXAMPLE22F1D49C01E52DDB7875B4B
```

2. 返されたハッシュ値をダウンロードされたファイル aws-sms-azure-setup.ps1.md5 および aws-sms-azure-setup.ps1.sha256 と比較します。

次に、次のいずれかを使用します。 PowerShell または Windows ユーザーインターフェイスを使用して、スクリプトファイルにの有効な署名が含まれていることを確認します。AWS。

有効な暗号署名 (PowerShell) のスクリプトファイルを確認するには

- で PowerShell ウィンドウで、以下のコマンドを実行します。

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

正しく署名されたスクリプトファイルは、次のような情報を返します。

```
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

...
```

有効な暗号署名 (Windows GUI) のスクリプトファイルを確認するには

1. Windows エクスプローラで、スクリプトファイルのコンテキスト (右クリック) メニューを開き、[Properties]、[Digital Signatures]、[Amazon Web Services]、 [Details] を選択します。
2. 表示された情報に「このデジタル署名は問題ありません。」が含まれており、署名者が「Amazon Web Services, Inc.」 であることを確認します。

ステップ 3: スクリプトを実行します。

このスクリプトは、次のコンピュータから実行します。 PowerShell 5.1 以降がインストールされています。

> **Note**
>
> もしあなたの PowerShell 実行ポリシーが署名付きスクリプトを確認するように設定されている場合は、コネクタ設定スクリプトの実行時に承認を求められます。スクリプトが「Amazon Web Services, Inc.」によって発行されていることを確認し、「R」をクリックして一度実行します。この設定は、Get-ExecutionPolicy を使用して表示し、Set-ExecutionPolicy を使用して変更できます。

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

`StorageAccountName`

コネクタをデプロイするストレージアカウントの名前。

`ExistingVNetName`

コネクタをデプロイする仮想ネットワークの名前。

`SubscriptionId`

(オプション) 使用するサブスクライバーの ID。このパラメータを指定しない場合、アカウントのデフォルトのサブスクリプションが使用されます。

`SubnetName`

(オプション) 仮想ネットワーク内のサブネットの名前。このパラメータを指定しない場合、「default」という名前のサブネットが使用されます。

スクリプトによって Azure へのログインを求められたら、このコネクタをデプロイしているサブスクリプションの管理者のアクセス許可を持つログインを使用します。

スクリプトが完了したら、コネクタはお客様のアカウントにデプロイされます。スクリプトは、コネクタのプライベート IP アドレスと、コネクタ VM のシステム割り当て ID のオブジェクト ID を出力します。次のステップを完了するには、これらの両方が必要です。

ステップ 4: コネクタの設定

コネクタをデプロイしたのと同じ仮想ネットワーク内の別の VM から、以下の URL を使用してコネクタのウェブインターフェイスを参照します。この URL には、前のステップで取得したコネクタのプライベート IP アドレスが含まれています。

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

コネクタを設定するには

1. コネクタのランディングページで、[今すぐ始める] を選択します。
2. ライセンス契約を確認し、チェックボックスをオンにして、[Next (次へ)] を選択します。
3. コネクタのパスワードを作成します。パスワードは、表示された基準を満たしている必要があります。[Next] (次へ) を選択します。
4. [Network Info] (ネットワーク情報) ページで、コネクタ用の AWS プロキシの設定など、ネットワーク関連のタスクを実行する手順が見つかります。[Next] (次へ) を選択します。
5. [Log Uploads (ログのアップロード)] ページで、[Upload logs automatically (ログを自動的にアップロード)] を選択し、[Next (次へ)] を選択します。
6. [Server Migration Service (サーバー移行サービス)] ページで、以下の情報を提供します。
   - [AWS Region] (AWS リージョン) で、リストからリージョンを選択します。
   - を使用する場合AWS認証情報で、「」で作成した IAM 認証情報を入力します。Server Migration Connector の IAM ユーザーの設定 (p. 5)。[Next] (次へ) を選択します。
7. [Azure Account Verification (Azure アカウントの確認)] ページで、Azure のサブスクリプション ID と場所が正しいことを確認します。このコネクタは、このサブスクリプションと場所で VM を移行できます。デプロイスクリプトからの出力として表示された、コネクタ VM のシステム割り当てアイデンティティのオブジェクト ID を指定します。
8. コネクタが正常に設定されると、[Congratulations (設定完了)] ページが表示されます。コネクタのヘルスステータスを表示するには、[Go to connector dashboard (コネクタダッシュボードに移動)] を選択します。
9. 登録したコネクタがリストされていることを確認するには、Systems Manager コンソールの [Connectors] (コネクタ) ページを開きます。

(別の方法) Server Migration Connector を手動でデプロイする

コネクタを手動で Azure 環境にインストールするには、この手順を実行します。

コネクタを手動でインストールするには

1. このコネクタをデプロイしているサブスクリプションに対する管理者のアクセス許可を持つユーザーとして、Azure ポータルにログインします。
2. 「Azure コネクタの要件 (p. 21)」に示されているように、ストレージアカウント、そのリソースグループ、仮想ネットワーク、および Azure リージョンを指定する準備が整っていることを確認してください。
3. コネクタ VHD と関連ファイルを次の表の URL からダウンロードします。

File	URL
コネクタ VHD	https://awssmsconnector.blob.core.windows.net/release/AWS-SMS-Connector-for-Azure.vhd
MD5 ハッシュ	https://s3.amazonaws.com/sms-connector/AWS-SMS-Connector-for-Azure.vhd.md5
SHA256 ハッシュ	https://s3.amazonaws.com/sms-connector/AWS-SMS-Connector-for-Azure.vhd.sha256

4. ステップ 2: スクリプトファイルの整合性と暗号署名を検証する (p. 22) に示されているのと同様の手順を使用して、コネクタ VHD の暗号化の完全性を検証します。
5. コネクタ VHD と関連ファイルをストレージアカウントにアップロードします。
6. 次のパラメータ値を使用して新しい Managed Disks を作成します。

   - Resource Group: リソースグループを選択する
   - 名前: 任意の名前 (例:sms-connector-disk-westus)
   - リージョン: Azure リージョンを選択する
   - アベイラビリティーゾーン: なし
   - Source タイプ: Storage Blob (ストレージ Blob) (ステップ 3.c. でアップロードした VHD blob を選択します。)
   - OSType: Linux
   - サイズ: 60 GB/スタンダード HDD
7. 作成した Managed Disks から新しい仮想マシンを作成するには、[VM の作成] を選択します。次のパラメータ値を割り当てます。

   [Basics (基本)] タブ:

   - Resource Group: リソースグループに入力する
   - 仮想マシン名: 任意の名前 (例:sms-connector-vm-westus)
   - リージョン: Azure リージョンを選択する
   - サイズ: F4s
   - パブリックインバウンドポート: なし

   [Disks (ディスク)] タブ:

   - OS ディスクタイプ: HDD 標準HDD

[ネットワーキング] タブ:

- 仮想ネットワーク: 仮想ネットワーク名を入力する
- サブネット: デフォルトのままにするか、特定のサブネットを選択する
- パブリック IP: 新規のままにしておきます
- NIC ネットワークセキュリティグループ: Basic (ベーシック)
- パブリックインバウンドポート: なし
- 残りのフィールドは、デフォルトのままにします。

管理タブ:

- 起動診断: On
- OS ゲスト診断: オフ
- 診断ストレージアカウント: ストレージアカウント
- システム割り当てマネージド ID: On
- 自動シャットダウンを有効にします: オフ

8. VM を確認し、作成します。これがコネクタ VM になります。
9. 2 つのロールドキュメントをダウンロードします。

   - https://s3.amazonaws.com/sms-connector/SMSConnectorRole.json
   - https://s3.amazonaws.com/sms-connector/SMSConnectorRoleSA.json
10. (重要) ロールドキュメントをカスタマイズします。

    編集 `SMSConnectorRole.json. name` フィールドを `sms-connector-role-`*`subscription_id`* に変更します。次に、サブスクリプション ID に合うように、`AssignableScopes` フィールドを変更します。

    編集 `SMSConnectorRoleSA.json. name` フィールドを `sms-connector-role-`*`storage_account`* に変更します。たとえば、アカウントが testStorage の場合、名前フィールドは `sms-connector-role-testStorage` にする必要があります。その後、サブスクリプション、リソースグループ、ストレージアカウントの値に合うように、`AssignableScopes` フィールドを変更します。
11. ロール定義を作成します。現時点では、Azure ポータルからロール定義を作成する方法はありません。Az CLI または Az を使用する必要があります PowerShell このステップです。New-AzRoleDefinition (Az PowerShell) または az role definition create (Az CLI) コマンドと、前のステップで作成した JSON ファイルを使用して、サブスクリプションにこれらのカスタムロールを作成します。
12. ロールをコネクタ VM に割り当てます。Azure ポータルで、[ストレージアカウント]、[アクセスコントロール]、[ロール]、[追加]、[ロール割り当ての追加] の順に選択します。ロール `sms-connector-role` を選択し、仮想マシンへのアクセスを割り当て、リストからコネクタ VM のシステム割り当てのアイデンティティを選択します。ロール `sms-connector-role-`*`storage_account`* に対してこのステップを繰り返します。
13. コネクタ VM を再起動して、ロールの割り当てをアクティブ化します。
14. 「ステップ 4: コネクタの設定 (p. 24)」に進んでください。

AWS SMS の AWS CLI コマンドを使用した VM のレプリケート

AWS Command Line Interface (AWS CLI) を使用して、オンプレミスサーバーのインベントリと Amazon EC2 への移行を行うことができます。

前提条件

- 「Server Migration Connector をインストールする (p. 10)」の説明に従って Server Migration Connector をインストールします。
- 次のものを使用する必要があります。サービスリンクロールの作成コマンドを実行して、サービスにリンクされた必要なロールを作成する

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

詳細については、「AWS SMS のサービスリンクロール (p. 42)」を参照してください。

考慮事項

- サーバーあたり最大 90 日までオンプレミスサーバーを AWS にレプリケートできます。使用時間は、サーバーのレプリケーションを開始した時点からレプリケーションジョブを終了するまで計算されます。90 日後、レプリケーションジョブは自動的に終了します。AWS Support から延長をリクエストすることができます。
- AWS SMS と AWS Migration Hub の間の統合を有効にしている場合、SMS サーバーカタログも Migration Hub に表示されます。詳細については、「Migration Hub からのアプリケーションのインポート (p. 34)」を参照してください。
- レプリケーションプロセス中に、AWS SMS は、サーバー側の暗号化を有効にして、リージョンに Amazon S3 バケットを作成します。また、7 日後にバケット内のアイテムを削除するバケットポリシーを定義します。AWS SMS は、サーバーボリュームをお客様の環境からこのバケットにレプリケートし、そのボリュームから EBS スナップショットを作成します。このバケットを削除しない場合、AWS SMS はこのリージョンのすべてのレプリケーションジョブにそのバケットを使用します。
- AMI の作成プロセスで、AWS SMS は、ルートボリュームの `DeleteOnTermination` 属性を false に設定し、デフォルト設定を上書きします。インスタンスを終了した後にルートボリュームを手動で削除するか、属性を true に設定して、インスタンスの終了時に Amazon EC2 がルートボリュームを削除するようにすることができます。詳細については、次を参照してください。インスタンスの終了時の Amazon EBS ボリュームの保持のAmazon EC2 ユーザーガイド。

CLI を使用してサーバーをレプリケートするには

1. get-connectors コマンドを使用して、登録されているコネクタのリストを取得します。

```
aws sms get-connectors
```

2. コネクトをインストールして登録したら、サーバーカタログのインポートコマンドを使用して、サーバーのインベントリを作成します。このプロセスには 1 分程かかることがあります。

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

3. get-servers コマンドを使用して Amazon EC2 にインポートできるサーバーのリストを表示します。

```
aws sms get-servers
```

出力は次の例のようになります:

```
{
    "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"
            }
        }
    ]
}
```

サーバーカタログをまだインポートしていない場合は、次のような出力が表示されます。

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

カタログのステータスが DELETED または EXPIRED である場合も、サーバーがカタログにないことを示します。

4. レプリケートするサーバーを選択し、サーバー ID を書き留めます。この ID を create-replication-job コマンドに指定します。

```
aws sms create-replication-job --server-id s-12345678 \
    --frequency 12 \
    --seed-replication-time 2016-10-24T15:30:00-07:00 \
    --role-name AWSServiceRoleForSMS
```

レプリケーションジョブをセットアップすると、`--seed-replication-time` パラメータに Unix エポックまたは ISO 8601 表記形式の秒単位で指定した時刻に、レプリケーションが自動的に開始されます。詳細については、「AWS Command Line Interface のパラメータ値の指定」を参照してください。以後は、`--frequency` パラメータに時間単位で指定した間隔でレプリケーションが繰り返されます。

5. すべての実行中のレプリケーションジョブについては、get-replication-jobs で詳細を確認できます。パラメータを指定しない場合、コマンドはすべてのレプリケーションジョブを一覧表示します。

   このコマンドは、次のような出力を返します：

```
{
    "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. get-replication-runs コマンドを使用して特定のレプリケーションジョブに関するすべてのレプリケーション実行の詳細を取得することもできます。これを行うには、次のようにレプリケーションジョブ ID を指定します。

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

このコマンドは、次に示すように、指定したレプリケーションジョブに関するすべてのレプリケーション実行のリストと詳細を返します。

```
{
    "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. 一度作成したレプリケーションジョブのパラメータを変更するには、update-replication-job コマンドを使用し、レプリケーションジョブ ID および変更するパラメータを指定します。

```
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. スケジュールしたレプリケーション実行に加えて、24 時間あたり最大 2 回までのレプリケーション実行をオンデマンドで開始することもできます。そのためには、start-on-demand-replication-run コマンドを使用して、レプリケーション実行をすぐに開始します。別のレプリケーション実行が進行中である場合、オンデマンドのレプリケーション実行を開始することはできません。

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

オンデマンドのレプリケーション実行が進行中のときに、スケジュールされたレプリケーション実行の開始時刻になると、このスケジュールされたレプリケーション実行はスキップされて次回に持ち越されます。

9. サーバーのレプリケーションが終了したら、delete-replication-job コマンドを使用してレプリケーションジョブを停止できます。これにより、レプリケーションジョブが停止され、サービスで作成された

すべてのアーティファクト (ジョブの S3 バケットなど) がクリーンアップされます。停止したジョブの実行で作成された AMI は削除されません。

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

10. サーバーのカタログを維持する必要がなくなった場合は、delete-server-catalog コマンドを使用して、サーバーで維持されているサーバーのカタログをクリアできます。

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

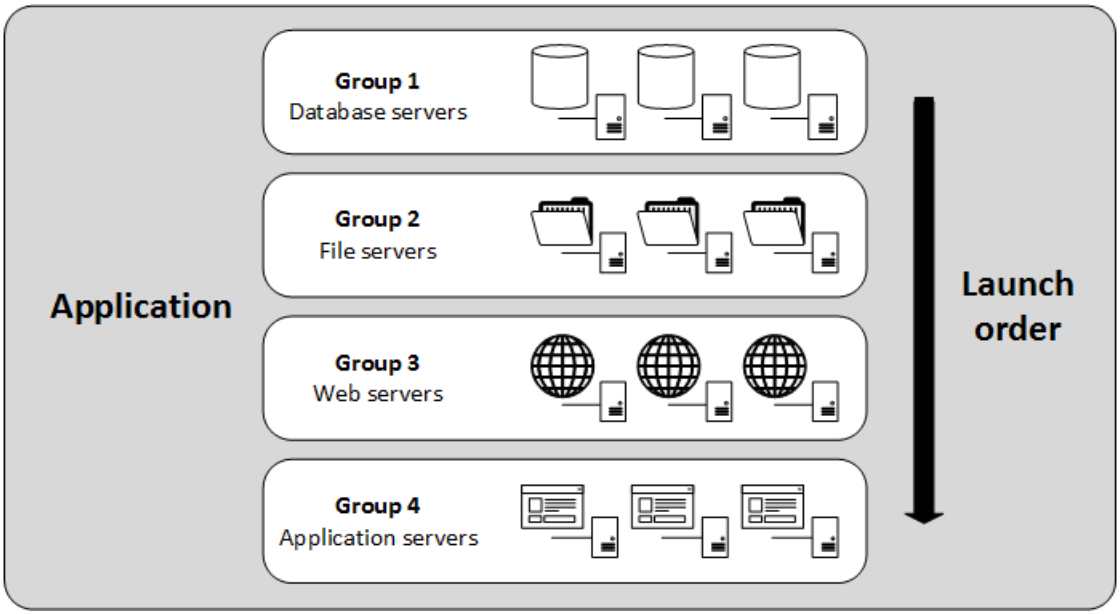
11. コネクタを使い終わったら、disassociate-connector コマンドを使用して AWS SMS からコネクタを登録解除します。このコマンドは、このコネクタを使用するすべてのレプリケーションが完了した後でのみ呼び出します。

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

AWS SMS を使用したアプリケーションの移行

AWS Server Migration Service は、オンプレミスのデータセンターから Amazon EC2 へのマルチサーバーアプリケーションスタックの自動移行をサポートしています。サーバーの移行は 1 台のサーバーを Amazon マシンイメージ (AMI) としてレプリケートすることにより実現されます。一方、アプリケーションの移行は、アプリケーション内のすべてのサーバーを AMI としてレプリケートし、適切に起動するように調整した AWS CloudFormation テンプレートを生成します。

定義された順でサーバーの階層を起動できるグループに、アプリケーションをさらに細分化できます。次の図では、データベースと連携するウェブアプリケーションの例を示します。



この例では、アプリケーションは 4 つのグループに分かれ、それぞれ 3 台のサーバーで構成されます。AWS CloudFormation テンプレートは次の順序でサーバーを起動します。データベース、ファイルサーバー、ウェブサーバー、アプリケーションサーバーです。

各サーバーがアプリケーション用に編成され、各グループが起動された後、レプリケーションの頻度を指定し、設定スクリプトを準備して、サーバーを起動するターゲット VPC を設定できます。アプリケーションを起動するときに、AWS SMS は生成したテンプレートに基づいてそれを設定します。

アプリケーションの移行は「Server Migration Connector をインストールする (p. 10)」に記載されたオンプレミスリソースを検出するための手順で決まります。サーバカタログをにインポートした後AWS SMSServer Migration Connector を使用して、アプリケーション、レプリケーション、および起動の設定に加えて、AWS SMSのAWS SMSアピ、AWSCLI、またはAWSSDK。

考慮事項

- サーバーあたり最大 90 日までオンプレミスサーバーを AWS にレプリケートできます。使用時間は、サーバーのレプリケーションを開始した時点からレプリケーションジョブを終了するまで計算されま

す。90 日後、レプリケーションジョブは自動的に終了します。AWS Support から延長をリクエストすることができます。

- AMI の作成プロセスで、AWS SMS は、ルートボリュームの `DeleteOnTermination` 属性を false に設定し、デフォルト設定を上書きします。インスタンスを終了した後にルートボリュームを手動で削除するか、属性を true に設定して、インスタンスの終了時に Amazon EC2 がルートボリュームを削除するようにすることができます。詳細については、次を参照してください。インスタンスの終了時の Amazon EBS ボリュームの保持のAmazon EC2 ユーザーガイド。
- Microsoft Azure 環境からのアプリケーション移行はサポートされていますが、現時点では Azure 用の Server Migration Connector はアプリケーション内のサーバースナップショットの近さを保証するものではありません。

アプリケーションの移行の使用

以下のタスクを実行できます。

[Tasks] (タスク)

アプリケーションの作成

アプリケーションを作成するには、AWS SMS create-appコマンドのAWS CLIコマンドリファレンス。

アプリケーション設定を構成します。

アプリケーションのレプリケーション設定については、を参照してください。AWS SMS 更新レプリケーションジョブコマンドのAWS CLIコマンドリファレンス。

起動設定の構成

ネットワーク設定を構成する前に、RunInstances Amazon EC2 API アクションの説明に従って、仮想プライベートクラウド、サブネット、およびセキュリティグループを設定する必要があります。

アプリケーションの起動設定については、を参照してください。AWS SMS アプリ起動構成を入れてコマンドのAWS CLIコマンドリファレンス。

レプリケーションの開始

アプリケーションのレプリケーションを開始するには、AWS SMS アプリレプリケーションの開始コマンドのAWS CLIコマンドリファレンス。

アプリケーションの起動

アプリケーションを起動するには、AWS SMS アプリを起動するコマンドのAWS CLIコマンドリファレンス。

の生成 CloudFormation テンプレート

を調べるためにAWS CloudFormationアプリケーションの起動時に自動的に生成されるテンプレートについては、AWS SMS テンプレートを生成するコマンドのAWS CLIコマンドリファレンス。

Migration Hub からのアプリケーションのインポート

アプリケーションの移行では、AWS Migration Hub で検出されたアプリケーションのインポートおよび移行がサポートされています。

Migration Hub からアプリケーションをインポートするには、AWS SMS アプリカタログのインポートコマンドのAWS CLIコマンドリファレンス。

> Note
>
> SMS は、アプリケーション関連サーバーが SMS サーバーカタログに存在し、既存の SMS アプリケーションの一部ではない場合のみ、Migration Hub からアプリケーション関連サーバーをインポートします。その結果、一部のアプリケーションは部分的にしかインポートされない場合があります。SMS によってアクティブにレプリケート中または起動中のアプリケーションを再インポートすることはできません。この競合が発生した場合は、レプリケーションを中止するか、開始して再インポートします。

AWS SMS での Amazon CloudWatch Events と AWS Lambda の使用

移行ワークフローに基づいてアクションを自動化するには、AWS Server Migration Service で Amazon CloudWatch Events を使用できます。そのためには、Lambda が継承する IAM ポリシー、イベントを処理する Lambda 関数、および受信イベントを照合して Lambda 関数にルーティングする CloudWatch Events ルールを作成する必要があります。

AWS SMS の CloudWatch Events ルールの処理

次の手順では、AWS Lambda 関数を使用して AWS SMS ジョブの状態の変更をモニタリングし、AMI ID が作成されるたびに Amazon EC2 instance インスタンスを起動します。

ジョブの状態の変更をモニタリングする Lambda 関数を作成するには

1. IAM コンソール(https://console.aws.amazon.com/iam/)を開きます。
2. CloudWatch Events によって呼び出されたときに (Lambda によって呼び出される) アクションの実行と CloudWatch ログへの書き込みを行うためのアクセス許可を提供する IAM ポリシーを作成します。次は、`RunInstances` アクションを実行するアクセス許可の例です。このポリシーを CloudWatch イベントを処理するユーザーの IAM ロールに割り当てます。

```
{
   "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. AWS Lambda コンソール (https://console.aws.amazon.com/lambda/) を開きます。
4. [関数の作成] を選択します。
5. Lambda 関数は、CloudWatch コンソールから確実に利用できるように、CloudWatch イベントが発生するリージョンで作成します。詳細については、「AWS Lambda デベロッパーガイド」を参照してください。この関数に `LaunchInstanceFromAMI` という名前を付け、ランタイムとして Python 2.7 を選択します。

6. [Role (ロール)] で、[Choose an existing role (既存のロールを選択)] を選択します。[Existing role (既存のロール)] の下に表示される利用可能なロールのリストで、ポリシーを追加したロールを選択します。
7. [Create function] (関数を作成) を選択し、次のような Lambda 関数を定義します。この Python 2.7 で記述されたサンプル関数は、AWS SMS ジョブの完了に伴ってイベントが AMI ID と共に送信されると、CloudWatch Events によって呼び出されます。この関数は、呼び出されると、イベントのリージョンで `t2.micro` インスタンスを起動します。

```
# 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. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
9. [Events]、[Create rule] の順に選択します。[Service Name (サービス名)] で、[Server Migration Service (SMS)] を選択します。[Event Type (イベントタイプ)] で、[Server Migration Job State Change (サーバー移行ジョブの状態の変更)] を選択します。
10. [Target]、[Add Target] の順に選択します。
11. [Lambda function] で、前に作成した Lambda 関数を選択し、[Configure details] を選択します。
12. [Configure rule details] ページで、[Name] と [Description] の値を入力します。[State] チェックボックスをオンにして、関数をアクティブにします ([Enabled] に設定します)。
13. [Create rule] を選択します。

作成したルールが、[Rules] タブに表示されます。この例では、AMI ID を受信するたびに、設定済みのイベントによって EC2 インスタンスが起動されます。

AWS Server Migration Serviceを使用したAWS CloudTrailAPI コールのログ記録

AWS Server Migration Serviceはと統合されていますAWS CloudTrailは、ユーザーやロール、またはによって実行されたアクションを記録するサービスです。AWSのサービスインサービスAWS SMS。 CloudTrail のすべての API コールをキャプチャしますAWS SMSイベントとして。キャプチャされる呼び出しには、へのコード呼び出しが含まれますAWS SMSAPI オペレーション。証跡を作成する場合は、の継続的な配信を有効にすることができます CloudTrail Amazon S3 バケットへのイベント (のイベントなど) AWS SMS。証跡を設定しない場合でも、 CloudTrail コンソールの [Event history (イベント履歴)] で最新のイベントを表示できます。CloudTrail で収集された情報を使用して、AWS SMS に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

詳細については、AWS CloudTrail ユーザーガイドを参照してください。

AWS SMSCloudTrail での 情報

CloudTrail は、アカウントを作成すると AWS アカウントで有効になります。アクティビティがで発生する場合AWS SMSでは、そのアクティビティは、 CloudTrail 他のイベントと一緒にイベントAWSのサービスイベントイベント履歴。AWS アカウントで最近のイベントを表示、検索、ダウンロードできます。詳細については、次を参照してください。を使用してイベントを表示する CloudTrail イベント履歴。

AWS のイベントなど、AWS SMS アカウントのイベントの継続的なレコードについては、追跡を作成します。あるトレイル可能にする CloudTrail を使用して、Amazon S3 バケットにログファイルを配信します。デフォルトでは、で証跡を作成するときに CloudTrail コンソールでは、証跡はすべてに適用されますAWS地域。追跡は、AWS パーティションのすべてのリージョンからのイベントをログに記録し、指定した Simple Storage Service (Amazon S3) バケットにログファイルを配信します。さらに、その他の設定を行うことができますAWSサービスにより、で収集されたデータをより詳細に分析し、それに基づく対応を行うことができます CloudTrail ログ。詳細については、以下を参照してください。

- 追跡を作成するための概要
- CloudTrail のサポート対象サービスと統合
- Amazon SNS の CloudTrail の通知の設定
- 受信 CloudTrail 複数のリージョンからのログファイルそして受信 CloudTrail 複数のアカウントからのログファイル

すべてAWS SMSアクションは、によってログに記録されます CloudTrail と記載されているAWS SMSAPI リファレンス。たとえば、`CreateReplicationJob`,`GetConnectors`, および`ImportServerCatalog`アクションでは、のエントリが生成されます CloudTrail ログファイル。

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。アイデンティティ情報は以下の判断に役立ちます。

- リクエストが、ルート認証情報と AWS Identity and Access Management (IAM) ユーザー認証情報のどちらを使用して送信されたか。
- リクエストが、ロールとフェデレーティッドユーザーのどちらのテンポラリセキュリティ認証情報を使用して送信されたか。

- リクエストが、別の AWS サービスによって送信されたかどうか。

詳細については、「CloudTrail userIdentity 要素」を参照してください。

AWS SMS ログファイルエントリの理解

追跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信できるようにする設定です。 CloudTrail ログファイルには、1 つ以上のログエントリが含まれます。イベントは、任意のソースからの単一の要求を表し、要求されたアクション、アクションの日時、要求パラメーターなどに関する情報が含まれます。 CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

以下に、以下に、例を示します。 CloudTrail 以下を実行するログエントリ`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"
}
```

AWS Server Migration Serviceでのセキュリティ

AWSでは、クラウドのセキュリティが最優先事項です。AWSのお客様は、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャから利点を得られます。

セキュリティは、AWSとお客様の間の共有責任です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ-AWS は、AWS クラウドでAWS のサービスを実行するインフラストラクチャを保護する責任を負います。また、AWSは、使用するサービスを安全に提供します。AWS コンプライアンスプログラム の一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。AWS Server Migration Service (AWS SMS) に適用するコンプライアンスプログラムの詳細については、コンプライアンスプログラムによる AWS 対象範囲内のサービス」および「」を参照してください。
- クラウド内のセキュリティ–お客様の責任は、使用するAWSのサービスに応じて異なります。また、お客様は、お客様のデータの機密性、企業の要件、および適用可能な法律および規制などの他の要因についても責任を担います。

このドキュメントは、AWS SMS を使用して共有責任モデルを適用する方法を理解するのに役立ちます。ここでは、セキュリティとコンプライアンスの目標を満たすように AWS SMS を設定する方法を説明します。また、AWS リソースのモニタリングや保護に役立つ、他の AWS SMS サービスの使用方法についても説明します。

目次

AWS Server Migration Serviceでのデータ保護

AWS責任共有モデルは、AWS Server Migration Serviceでのデータ保護に適用されます。このモデルで説明されているように、AWS は、AWS クラウドのすべてを実行するグローバルインフラストラクチャを保護する責任を担います。ご利用者はこのインフラストラクチャでホストされているコンテンツに対する管理を維持する責任があります。このコンテンツには、使用される AWS のサービス のセキュリティ設定と管理タスクが含まれます。データプライバシーの詳細については、「データプライバシーのよくある質問」を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿された「AWS 責任共有モデルおよび GDPR」のブログ記事を参照してください。

データを保護するため、AWS アカウントの認証情報を保護し、AWS Identity and Access Management (IAM) を使用して個々のユーザーアカウントをセットアップすることをお勧めします。この方法により、それぞれのジョブを遂行するために必要なアクセス許可のみを各ユーザーに付与できます。また、以下の方法でデータを保護することをお勧めします:

- 各アカウントで多要素認証 (MFA、Multi-Factor Authentication) を使用します。

- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 以降が推奨されています。
- AWS CloudTrail で API とユーザーアクティビティログをセットアップします。
- AWS 暗号化ソリューションを AWS サービス内のすべてのデフォルトのセキュリティ管理と一緒に使用します。
- Amazon Macie などのアドバンストマネージドセキュリティサービスを使用します。これは、Amazon S3 に保存されている個人データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API を使用して AWS にアクセスするときに FIPS 140-2 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。使用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-2」を参照してください。

顧客の E メールアドレスなどの機密または機密性の高い情報情報は、タグや名前フィールドなど自由形式フィールドには入力しないことを強くお勧めします。これには、コンソール、API、AWS CLI、または AWS を使用して、AWS SMS や AWS のその他サービスで作業を行う場合も含まれます。タグ、または名前用に使用される自由形式フィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーへの URL を提供する場合は、そのサーバーへのリクエストを検証するための認証情報を URL に含めないことを強くお勧めします。

保管中の暗号化

オンプレミス環境からサーバーボリュームをレプリケートする場合、AWS SMS は一時的に中間 S3 バケットにデータを保存します。レプリケーションが完了すると、AWS SMS は Amazon S3 に保存されたこのデータを削除します。それ以外の場合、AWS SMS は保管済みのデータを保存しません。

転送時の暗号化

転送中のデータは TLS を使用して暗号化されます。これには、サーバー移行コネクタから Amazon S3 へのトラフィック、および Server Migration Connector からへのトラフィックが含まれます。AWS SMS。

AWS Server Migration Service のためのアイデンティティおよびアクセス管理

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全にコントロールするために役立つ AWS のサービスです。IAM管理者は、誰を認証 (サインイン) し、誰に AWS リソースの使用を許可する (アクセス許可を持たせる) かを制御します。IAM では、自分の AWS アカウントの下にユーザーとグループを作成できます。ユーザーが AWS リソースを使用してタスクを実行するために必要なアクセス許可を制御します。IAM は追加料金なしでご利用いただけます。

デフォルトでは、IAM ユーザーには AWS Server Migration Service (AWS SMS) のリソースおよびオペレーションに対するアクセス許可がありません。IAM ユーザーに AWS SMS リソースの管理を許可するには、それらのユーザーに許可を明示的に付与する IAM ポリシーを作成し、許可を必要とする IAM ユーザーまたはグループにアタッチする必要があります。

ポリシーをユーザーまたはユーザーのグループに添付する場合、ポリシーによって特定リソースの特定タスクを実行するユーザーの権限が許可または拒否されます。詳細については、IAM ユーザーガイドのポリシーとアクセス許可を参照してください。

ポリシーの構造

IAM ポリシーは 1つ以上のステートメントで構成されるJSONドキュメントです。各ステートメントは次のように構成されます。

```
{
```

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

ステートメントはさまざまな工レメントで構成されます。

- [効果]: effect は`Allow`または`Deny`。デフォルトでは、IAM ユーザーはリソースおよび API アクションを使用するアクセス許可がないため、リク工ストはすべて拒否されます。明示的な許可はデフォルトに優先します。明示的な拒否はすべての許可に上書きされます。
- アクション: アクションは具体的ですAWS SMSアクセス許可を付与または拒否する、API アクションです。
- リソース: [Resource (リソース)] アクションによって影響を及ぼされるリソースです。AWS SMS では、リソースとして「*」を指定する必要があります。
- 条件: 条件はオプションです。ポリシーの発効条件を指定するために使用します。

ポリシーの例

IAM ポリシーステートメントで、IAM をサポートするすべてのサービスから任意の API アクションを指定できます。AWS SMS の場合、API アクションの名前でプレフィックスとして `sms:` を次のように使用します。

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

単一のステートメントに複数のアクションを指定するには、次のようにコンマで区切ります。

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

ワイルドカードを使用して複数のアクションを指定することもできます。たとえば、「Get」という単語で始まる名前のすべての AWS SMS API アクションは、以下のように指定できます。

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

AWS SMS API アクションをすべて指定するには、* ワイルドカードを以下のように使用します。

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

レプリケーション後にユーザーが自動起動を有効にすることを禁止するには、次のステートメントを使用します。自動起動ではユーザーは `sms:LaunchApp` を直接呼び出さないので、許可されたアクションのリストから `LaunchApp` を省略するだけでは不十分です。

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

事前定義の AWS 管理ポリシー

AWS によって作成された管理ポリシーは、一般的ユースケースに必要なアクセス権限を付与します。AWS に対して必要とされるアクセス許可に基づいて、これらのポリシーを IAM ユーザーにアタッチできます。

AWS SMS のサービスリンクロール

AWS SMS は、ユーザーに代わって他の AWS サービスを呼び出すために必要なアクセス許可を持つサービスにリンクされたロールを使用します。詳細については、IAM ユーザーガイドの「サービスにリンクされたロールの使用」を参照してください。https://docs.aws.amazon.com/IAM/latest/UserGuide/using-service-linked-roles.html

AWS SMS のサービスにリンクされたロールの導入前は、2 つの IAM ロールを作成して、必要なアクセス許可を AWS SMS に付与する必要がありました。これらのロールは、AWS SMS を使用するために必要なくなりました。ただし、完全を期すためにここで説明しています。詳細については、「AWS SMS のレガシー IAM ロール (p. 43)」を参照してください。

サービスにリンクされたロールによって付与されるアクセス許可

AWS SMS は、AWSServiceRoleForSMS という名前のサービスにリンクされたロールを使用して、AWS SMS がレプリケーションジョブを管理できるようにします。

AWSServiceRoleForSMS は、そのロールを引き受けるために、`sms.amazonaws.com` サービスプリンシパルを信頼します。

ロールのアクセス許可ポリシーは、指定したリソースに対して以下のアクションを実行することを AWS SMS に許可します。

- 特定の AWS SMS アクションを使用してレプリケーションジョブを作成および管理する
- 特定の AWS CloudFormation アクションを使用して、arn:aws:cloudformation:*:*:stack/sms-app-*/* を作成および管理する
- 特定の Amazon EC2 アクションを使用して、スナップショットとイメージの管理、インスタンスの起動、およびタグ条件 (ec2:ResourceTag/aws:cloudformation:stack-id": "arn:aws:cloudformation:*:*:stack/sms-app-*/*) を満たすインスタンスの管理を行う
- 特定の AWS Systems Manager アクションを使用してインスタンスでスクリプトを実行する
- すべてのリソースでの `iam:GetRole` の使用、および arn:aws:cloudformation:*:*:stack/sms-app-*/* での`iam:PassRole` の使用
- 特定の Amazon S3 アクションを使用して、arn:aws:s3:::sms-app-* を作成および管理する

サービスにリンクされたロールの作成

サービスにリンクされたこのロールを手動で作成するには、以下を使用します。AWS CLI サービスリンクロールの作成作成するコマンドAWSServiceRoleForSMS。

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

サービスにリンクされたロールを編集する

IAM を使用して、AWSServiceRoleForSMS の説明を編集できます。詳細については、IAM ユーザーガイドの「サービスにリンクされたロールの編集」を参照してください。

サービスにリンクされたロールを削除する

AWS SMS を使用する必要がなくなった場合は、[AWSServiceRoleForSMS] ロールを削除することをお勧めします。サービスにリンクされたロールは以下の条件でのみ削除できます。

- サービスにリンクされたロールが、アクティブなレプリケーションジョブによって使用されていない
- サービスにリンクされたロールが、アクティブなレプリケーションジョブが関連付けられているアプリケーションによって使用されていない
- サービスにリンクされたロールが、AWS CloudFormation スタックが関連付けられているアプリケーションによって使用されていない

サービスにリンクされたロールは、IAM コンソール、IAM CLI、または IAM API を使用して削除することができます。詳細については、IAM ユーザーガイドの「サービスにリンクされたロールの削除」を参照してください。

AWSServiceRoleForSMS ロールを削除した後、レプリケーションジョブを開始した場合は、AWS SMS によってそのロールが再度作成されます。

AWS SMS のレガシー IAM ロール

AWSServiceRoleForSMS の導入前は、サービスロールと起動ロールを作成して、必要なアクセス許可を AWS SMS に付与する必要がありました。これらのロールを作成する必要はなくなりました。

AWS SMS のサービスロールの設定

以下の手順を使用して、移行したリソースを Amazon EC2 アカウントに配置するためのアクセス権限を AWS SMS に付与する IAM ロールを作成します。

AWS SMS 用の IAM ロールを作成するには

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで [Roles]、[Create role] の順に選択します。
3. []このロールを使用するサービスを選択で、SMS,次へ: アクセス許可.
4. []許可ポリシー・アミッションで、ポリシーを確認します。ServerMigrationServiceRole表示され、[] を選択します。次へ: 確認.
5. [確認] の [ロール名] に **sms** と入力します。

   Note

   または、別の名前を適用することができます。ただし、その場合はレプリケーションジョブまたはアプリケーションを作成するたびに、ロール名を明示的に指定する必要があります。
6. [Create role] (ロールの作成) を選択します。これで、[sms] ロールが使用可能なロールのリストに表示されるようになります。
7. 追加のセキュリティコントロールに対して、この新しく作成したロールの信頼ポリシーに `aws:SourceAccount` や `aws:SourceArn` のようなコンテキストキーを追加できます。SMS は、次の例に示すように、`sourceAccount` および `sourceArn` キーを公開して、このキーを継承します。

```
{
  "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>:*"
           }
        }
    }
}
```

AWS SMS 用起動ロールの設定

アプリケーションを起動する予定の場合、AWS SMS 起動ロールが必要になります。`PutAppLaunchConfiguration` API を使用してこのロールを割り当てます。`LaunchApp` API が呼び出されると、ロールが AWS CloudFormation によって使用されます。

AWS SMS の起動ロールを作成するには

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで [Roles]、[Create role] の順に選択します。
3. []このロールを使用するサービスを選択で、CloudFormation,次へ: アクセス許可.
4. []許可ポリシー・アミッションで、ポリシーを確認します。ServerMigrationServiceLaunchRole表示され、[] を選択します。次へ: 確認.
5. [確認] の [ロール名] に **sms-launch** と入力します。

   Note

   または、別の名前を適用することができます。ただし、その場合はアプリケーションの起動設定を作成するたびに、ロール名を明示的に指定する必要があります。

6. [Create role] (ロールの作成) を選択します。これで、[sms-launch] ロールが使用可能なロールのリストに表示されるようになります。

AWS Server Migration Service での耐障害性

AWS のグローバルインフラストラクチャは AWS リージョンとアベイラビリティーゾーンを中心として構築されます。リージョンには、低レイテンシー、高いスループット、そして高度の冗長ネットワークで接続されている複数の物理的に独立および隔離されたアベイラビリティーゾーンがあります。アベイラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、耐障害性、および拡張性が優れています。

AWS リージョンとアベイラビリティーゾーンの詳細については、[AWS Global Infrastructure] (グローバルインフラストラクチャ) を参照してください。

AWS Server Migration Serviceでのインフラストラクチャセキュリティ

マネージドサービスとして、AWS SMSによって保護されているAWSで説明されているグローバルネットワークセキュリティ手順Amazon Web Services: セキュリティプロセスの概要ホワイトペーパー。

AWS 公開版 API コールを使用して、ネットワーク経由で AWS SMS にアクセスします。クライアントで Transport Layer Security (TLS) 1.0 以降がサポートされている必要があります。TLS 1.2 以降を推奨します。また、Ephemeral Diffie-Hellman (DHE)や Elliptic Curve Ephemeral Diffie-Hellman (ECDHE)などの Perfect Forward Secrecy (PFS)を使用した暗号スイートもクライアントでサポートされている必要があります。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。

また、リクエストは、アクセスキーID と、IAMプリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token Service (AWS STS) を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

AWS Server Migration Service のコンプライアンス検証

サードパーティーの監査人は、SOC、PCI、FedRAMP、HIPAA など複数の AWS コンプライアンス プログラムのパートとして、AWS のサービス のセキュリティとコンプライアンスを評価します。

その他の AWS のサービス が特定のコンプライアンスプログラムの対象であるかどうかを確認するには、「コンプライアンスプログラムによる対象範囲内の AWS のサービス」を参照してください。一般的な情報については、「AWS コンプライアンスプログラム」を参照してください。

AWS Artifact を使用して、サードパーティーの監査レポートをダウンロードできます。詳細については、「AWS Artifact におけるダウンロードレポート」を参照してください。

AWS のサービス を使用する際のユーザーのコンプライアンス責任は、ユーザーのデータの機密性や貴社のコンプライアンス目的、適用される法律および規制によって決まります。AWS では、コンプライアンスに役立つ次のリソースを提供しています。

- 「Security and Compliance Quick Start Guides」(セキュリティおよびコンプライアンスのクイックスタートガイド) - これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスを重視したベースライン環境を AWS でデプロイするステップを説明します。

- 「Architecting for HIPAA Security and Compliance on Amazon Web Services」(アマゾン ウェブ サービスでの HIPAA のセキュリティとコンプライアンスのためのアーキテクチャ) – このホワイトペーパーは、企業が AWS を使用して HIPAA 対象アプリケーションを作成する方法を説明しています。

  Note

  すべての AWS のサービス が HIPAA 適格であるわけではありません。詳細については、「HIPAA 対応サービスのリファレンス」を参照してください。
- AWS コンプライアンスのリソース– このワークブックおよびガイドのコレクションは、お客様の業界と拠点に適用されるものである場合があります。
- 「AWS Config デベロッパーガイド」の「ルールでのリソースの評価」 — AWS Config のサービスでは、自社のプラクティス、業界ガイドライン、および規制に対するリソースの設定の準拠状態を評価します。
- AWS Security Hub — この AWS のサービス では、AWS 内のセキュリティ状態が包括的に示されており、セキュリティ業界の標準およびベストプラクティスへの準拠の確認に役立ちます。
- AWS Audit Manager - この AWS のサービス は AWS の使用状況を継続的に監査し、リスクの管理方法やコンプライアンスを業界スタンダードへの準拠を簡素化するために役立ちます。

AWS SMS のトラブルシューティング

以下の情報は、AWS SMS の使用時に発生する可能性があるエラーに関する問題のトラブルシューティングに役立ちます。これらの手順を使用する前に、SMS の設定と移行しようとしているサーバーが「AWS Server Migration Service の要件 (p. 2)」の要件を満たしていることを確認します。

目次

コネクタのログファイル

Server Migration Connector は、Amazon S3 へのアップロードが完了する前に失敗したレプリケーションジョブのトラブルシューティングに使用できるログファイルを提供します。コネクタログファイルをダウンロードするには、次の手順に従います。

コネクタログファイルをダウンロードするには

1. ウェブブラウザで、コネクタ VM の IP アドレスを入力します。
2. コネクタにログインします。
3. コネクタがすべてのチェックに合格していることを確認します。
4. [Support Links] (サポートリンク) で、[Download Log Bundle] (ログバンドルのダウンロード) を選択します。
5. ログバンドル内のファイルを抽出します。

ログバンドルには、次のコネクタログファイルが含まれています。

- `connector.log` — コネクタ構成の問題をチェックします。
- `connectorsetup.log` — 初期設定に関する詳細情報をチェックします。
- `frontend.log` — AWS エンドポイントへの接続に関する問題をチェックします。

- `metrics.log` — スループット統計とアップロード速度をチェックします (「`UploadStats`」を参照)。
- `netstat.log` — ネットワークパケットエラーをチェックします。
- `poller.log` — データベースのポーリングアクティビティをチェックします。
- `sms-replication-poller-log` — ディスクを介したレプリケーションジョブの検証のレビューアクティビティが Amazon S3 にアップロードされます。例えば、アップロードの進行状況をパーセンテージで確認し、レプリケーションジョブの各フェーズの開始と終了を確認できます。

コネクタの登録時の問題

コネクタの登録時に問題が発生した場合は、sms-service@amazon.com に連絡してください。

VM を Amazon S3 にアップロードする際の証明書エラー

VM がある ESXi ホストに SSL 証明書の問題にある場合、コネクタは VM のレプリケーションに失敗する場合があります。この場合、次のエラーメッセージが表示されます。最新実行のステータスメッセージセクションに追加します。「サーバーエラー: ベースディスクを S3 にアップロードできませんでした。もう一度試してください。問題が解決しない場合は、お問い合わせください。AWSSupport: vSphere 証明書のホスト名の不一致: < の証明書*somehost.somedomain.com*> どのサブジェクトの代替名にも一致しません:[*#######.localdomain*]。」

この ESXi ホスト証明書問題は、以下のタスクを実行することで回避できます。

[Tasks] (タスク)

- コネクタのアップグレード (p. 48)
- コネクタの再登録 (p. 48)

コネクタのアップグレード

このセクションは、コネクタを手動でアップグレードするお客様向けです。自動アップグレードを設定済みの場合は、以下のステップをスキップして「コネクタの再登録 (p. 48)」に進んでください。

コネクタをアップグレードするには

1. コネクタコンソールを開きます。
2. コネクタにログインします。
3. [アップグレード] を選択します。
4. コネクタがバージョン 1.0.11.13 以降にアップグレードするのを待ちます。

コネクタの再登録

このセクションは、証明書の不一致問題が発生しているすべてのお客様向けです。

コネクタを再登録するには

1. コネクタコンソールを開きます。
2. コネクタにログインします。

3. [General Health] (全般的なヘルス) セクションで、 バージョンが 1.0.11.13 以降であることを確認します。
4. [Edit AWS Server Migration Service Settings] (WS Server Migration Service 設定の編集) を選択します。
5. [Setup] (セットアップ) ページの [AWS Region] (AWS リージョン) で、リストから目的のリージョンを選択します。[AWS Credentials] (AWS 認証情報) に、セットアップガイド (p. 10)のステップ 2 で作成した IAM のアクセスキーとシークレットキーを入力します。[Next] (次へ) を選択します。
6. [vCenter Service Account] ページに、セットアップガイド (p. 10)のステップ 3 で作成した vCenter ホスト名、ユーザー名、パスワードを入力します。
7. [Ignore hostname mismatch and expiration errors for vCenter and ESXi certificates] チェックボックスを選択します。[Next] (次へ) を選択します。
8. 登録を完了して、コネクタ設定ダッシュボードを表示します。
9. を使用するAWS SMSスタックしたレプリケーションジョブを削除して再起動する CLI または API。

エラー「PKIX path building failed」で Server Migration Connector が AWS への接続に失敗する

お客様の環境によっては、監査と管理の目的で証明書の再署名機構を通じてセキュアなネットワークトラフィックがプロキシされます。これにより、コネクタから AWS SMS に接続しようとすると AWS 認証情報が失敗する場合があります。エラーメッセージ "PKIX パスの構築エラー" は、無効な証明書が提示されたことを示します。

このような環境でコネクタが機能するには、以下のステップで示すように、再署名証明書 (所属組織または団体名が信頼してアウトバウンドパケットの署名に使用するユーザー証明書) をコネクタの信頼ストアに追加する必要があります。

再署名証明書をコネクタの信頼ストアに追加するには

1. コネクタシステムで、以下のコマンドを使用し、FreeBSD パケットフィルターを無効にして、SSH を有効にします。

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

2. 次のようなメソッドを使用して、ユーザー証明書をコネクタにコピーします。

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

3. ユーザー証明書を信頼ストアに追加します。

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

4. 次のコマンド (AWS Management Portal for vCenter の一部) を使用してサービスを再起動します。

```
sudo setup.rb
```

   オプション [3] を選択し、「yes」と入力します。
5. パケットフィルタを再有効化します。

```
sudo service pf start
```

この CA ルート証明書は信頼されていません

オンプレミスでインストールした仮想マシンの IP アドレスにアクセスすると、次のメッセージが表示されることがあります。

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

このエラーを無視しても問題ありません。

準備段階でレプリケーション実行が失敗する

場合によっては、直前のレプリケーション実行が失敗したときでも、AWS SMS は、レプリケーションジョブで増分レプリケーション実行のスケジュール設定を中止しません。連続エラーの最大許可数に達した場合のレプリケーションジョブのデフォルトの動作は、一時停止です。削除後 4 日以内なら、ジョブは再起動できます。このような場合、直前のレプリケーションの Amazon EBS スナップショットが顧客のアカウントで共有され、エラーが発生したレプリケーション実行のステータスメッセージが送信されます。メッセージにはスナップショット ID が含まれ、エラーの理由が記載されます。一般的なステータスメッセージは次のようになります。

```
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.
```

レプリケーション実行のエラー (初回起動時エラーを含む) の理由は Amazon EC2 VM Import/Export を VM の移行に使用したときに確認されるエラーと関係があることがあります。詳細については、「VM Import/Export のトラブルシューティング」を参照してください。

問題を解決するためのヘルプ情報がさらに必要な場合は、AWS Support にお問い合わせください。移行に失敗した際に生成された EBS スナップショットはアカウントと共有され、スナップショット ID はレプリケーションジョブのステータスメッセージに含まれています。AWS サポートにお問い合わせの際には必ずこれらの詳細を準備してください。

レプリケートされた AMI で一部のインスタンスタイプを起動できない

一部のインスタンスでは ENA のサポートが必要です。移行により ENA のサポートが有効にならない場合は、レプリケートされた AMI で ENA のサポートを必要とするインスタンスを起動できません。

ENA が有効になっていることを確認します。詳細については、Amazon EC2 ドキュメントの「Windows の拡張ネットワークの有効化」または「Linux の拡張ネットワークの有効化」を参照してください。

ServerError: ベースディスクを Amazon S3 にアップロードできませんでした。

考えられる原因

- VMDK がスナップショット可能でないか、仮想マシンに ISO がマウントされています。

- コネクタがバッファリングされたデータを Amazon S3 にアップロードしている間にハイパーバイザー (Hyper-V または ESXi ホスト) への接続がタイムアウトしました。
- レプリケーションジョブが Amazon S3 にディスクをアップロードしている間にメンテナンスが実行されています。
- 仮想ディスクに圧縮の問題があります。
- ハイパーバイザー証明書に検証エラーがあります。
- コネクタのステータスが `Unhealthy` です。
- コネクタが AWS エンドポイントに到達できません。

ServerError: レプリケーションジョブの検証に失敗しました

考えられる原因

- 仮想マシンのパスに変更があります。
- IAM アクセス許可に変更があります。
- 仮想環境のユーザーまたはアカウントのアクセス許可に変更があります。
- WinRM (Hyper-V) の構成に問題があります。
- DNS 解決の失敗があります。
- コネクタ仮想マシンに NTP 構成エラーがあります。

内部エラーが発生しました。AWS 認証情報と VM Manager 認証情報が正しいことを確認します。

考えられる原因

- IAM アクセス許可がコネクタのセットアップを完了するのに十分ではありません。
- 仮想環境のユーザーまたはアカウントのアクセス許可が不十分です。
- AWS SMS の IAM ロールに問題があります。
- 前提条件が不足しています。
- VM 環境が準備されていません。
- コネクタ (Hyper-V) の設定時に特殊文字が使用されました。

スナップショット関連のエラー (VMware)

考えられる原因

- VMDK が独立ディスクとして構成されています。
- ESXi ホストはスナップショットを作成できません。
- VMDK がロックされています。
- スナップショットチェーンが壊れています。手動またはサードパーティーソフトウェアによって、レプリケーションが実行されていないときにスナップショットが作成されないことを確認します。
- 前回のレプリケーション実行でスナップショットが統合されませんでした。

チェックポイントエラー (Hyper-V)

考えられる原因

- VM に既存のチェックポイントがあります。
- 手動またはサードパーティー・ソフトウェアによって作成されるチェックポイントがあります。
- VHD または VHDX がロックされています。
- Hyper-V ホストはチェックポイントを作成できません。

増分レプリケーションの差分が 1 TB を超える

コネクタは、小さい差分の頻繁なレプリケーションを処理するように設計されています。1 TB を超える差分をサポートしていません。レプリケーションを定期的に実行しない場合、差分がこの制限を超え、レプリケーションの実行に失敗する可能性があります。

この問題を回避するには、増分レプリケーションが頻繁に実行されるように設定します。レプリケーションを頻繁に実行できない場合は、差分アップロードの上限を引き上げることができます。たとえば、コネクタで以下のコマンドを実行して、S3 アップロードの部分サイズを 25 MB から 100 MB に増やします。プロンプトが表示されたら、オプション 3 を選択します。

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

アップロードの上限を引き上げると、コネクタのパフォーマンスとメモリ使用量に影響します。コネクタが複数の差分をアップロードしている間は、アップロードの上限を引き上げないでください。

Server Migration Connector のリリースノート

次の表に、Server Migration Connector のリリース履歴を示します。

リリース

vCenter 環境用のリリース

vCenter 環境の最新のコネクタをダウンロードするには、https://s3.amazonaws.com/sms-connector/AWS-SMS-Connector.ova を開きます。

リリース日	バージョン	コメント
2022 年 1 月 11 日	1.0.13.2156	• OSをFreeBSD 12.3-RELEASE にアップグレードした。
2021 年 12 月 14 日	1.0.13.2011	• このバージョンには、Apache Log4j2 コード実行0日間の脆弱性 (CVE02021-44228) のパッチが含まれています。
2020 年 4 月 28 日	1.0.13.245	• 欧州 (ミラノ) リージョンのサポートを追加
2020 年 4 月 22 日	1.0.13.242	• アフリカ (ケープタウン) リージョンのサポートを追加
2020年3月23日	1.0.13.227	• 中東 (バーレーン) リージョンでの移行をブロックするバグを修正 • スナップショットのアップロード中のファイルの早期終了 (EOF) エラーを修正
2019 年 5 月 29 日	1.0.13.106	• AWS との接続エラーによりコネクタプライアンスの登録がブロックされていたバグを修正
2019 年 5 月 3 日	1.0.13.90	• AWS GovCloud (米国東部) リージョンでの移行をブロックするバグを修正
2018 年 12 月 12 日	1.0.13.15	• 欧州 (ミラノ) リージョンのサポートを追加
2018 年 12 月 5 日	1.0.13.1	• コネクタをアプリケーション移行機能向けに最適化

リリース日	バージョン	コメント
2018 年 10 月 19 日	1.0.12.109	• オンプレミスのインフラストラクチャまたはネットワークの障害後に VM ディスクのアップロード再開によって発生する「EOF (早期終了)」を修正
2018 年 9 月 18 日	1.0.12.88	• オンプレミスのネットワーク障害によって中断された VM ディスクの転送を再開するように修正
2018 年 6 月 11 日	1.0.12.3	• S3 マニフェスト機能を使用して 4 TB を超えるディスクサイズの VM を新たにサポート • 軽微なバグを修正
2018 年 4 月 26 日	1.0.11.34	• 南米 (サンパウロ) リージョンへのサポートを追加 • 軽微なバグの修正とパフォーマンスの向上
2018 年 1 月 29 日	1.0.10.x	• 以下のリージョンのサポートを追加しました。欧州 (ロンドン)、欧州 (パリ)、米国西部 (北カリフォルニア)、中国 (北京) • 軽微なバグの修正とパフォーマンスの向上
2017 年 11 月 08 日	1.0.9.x	• ディスクアップロード時のレジリエンスの向上 • 軽微なバグの修正とパフォーマンスの向上
2017 年 8 月 29 日	1.0.8.x	• フランス語、中国語、韓国語、日本語を新たにサポート • VM ディスクのアップロード速度の向上 • 軽微なバグを修正
2017 年 6 月 02 日	1.0.7.12	• AWS GovCloud (米国西部) リージョンのサポートを追加
2017 年 5 月 5 日	1.0.5.2	• vCenter 5.1 のサポートが追加されました • 1 回のみの移行のサポートが追加されました • エラーメッセージの見直しとセキュリティ関連のバグの修正

リリース日	バージョン	コメント
2016 年 11 月 3 日	1.0.0.84	• VMware 環境用の Server Migration Connector 仮想アプライアンス • AWS Server Migration Service コンソールのグラフィカルインターフェイスを使用して VM の移行タスクと SMS のレプリケーションタスクを管理 • AWS Server Migration Service CLI のコマンドラインを使用して VM の移行タスクと SMS のレプリケーションタスクを管理

Hyper-V/SCVMM 環境用のリリース

Hyper-V/SCVMM 環境の最新のコネクタをダウンロードするには、https://s3.amazonaws.com/sms-connector/AWS-SMS-Connector-for-SCVMM-HyperV.zip を開きます。

リリース日	バージョン	コメント
2022 年 1 月 27 日	1.1.0.1474	• OSをFreeBSD 12.3-RELEASE にアップグレードした。
2021 年 12 月 15 日	1.1.0.1319	• このバージョンには、Apache Log4j2 コード実行0日間の脆弱性 (CVE-2021-44228) のパッチが含まれています。
2020 年 11 月 9 日	1.1.0.801	• トラブルシューティングの目的で AWS と共有するコネクタログバンドルの作成プロセスの問題を修正
2020 年 4 月 28 日	1.1.0.522	• 欧州 (ミラノ) リージョンのサポートを追加
2020 年 4 月 22 日	1.1.0.515	• アフリカ (ケープタウン) リージョンのサポートを追加
2020 年 4 月 6 日	1.1.0.505	• 以下のリージョンでのコネクタ登録に関する問題を修正しました。中東 (バーレーン)、欧州 (ストックホルム)、アジアパシフィック (香港) • ログバンドルのダウンロードに関する問題を修正しました。
2018 年 12 月 12 日	1.1.0.378	• 欧州 (ミラノ) リージョンのサポートを追加

リリース日	バージョン	コメント
2018 年 12 月 5 日	1.1.0.364	• コネクタをアプリケーション移行機能向けに最適化
2018 年 10 月 9 日	1.1.0.357	• Windows Hyper-V 第 2 世代 VM の移行 • 軽微なバグを修正
2018 年 6 月 11 日	1.1.0.304	• S3 マニフェスト機能を使用して 4 TB を超えるディスクサイズの VM を新たにサポート • 軽微なバグを修正
2018 年 4 月 25 日	1.1.0.287	• 1 つのコネクタを使用した複数の Hyper-V サーバーからの VM の移行を新たにサポート • 南米 (サンパウロ) リージョンへのサポートを追加 • 軽微なバグを修正
2018 年 2 月 28 日	1.1.0.x	• 以下のリージョンのサポートを追加しました。欧州 (ロンドン)、欧州 (パリ)、米国西部 (北カリフォルニア)、中国 (北京) • 軽微なバグを修正
2017 年 12 月 14 日	1.1.0.76	• Microsoft の Hyper-V 環境のサポートが追加されました

Azure 環境用のリリース

Azure 環境の最新のコネクタをダウンロードするには、https://s3.amazonaws.com/sms-connector/aws-sms-azure-setup.ps1 を開きます。

リリース日	バージョン	コメント
2021 年 12 月 16 日	1.2.0.2038	• このバージョンには、マイナーなバグ修正と Apache Log4j2 コード実行0日の脆弱性（CVE-2021-44228）のパッチが含まれています。
2020 年 2 月 27 日	1.2.0.350	• 軽微なバグを修正
2019 年 5 月 31 日	1.2.0.286	• デプロイスクリプトがデフォルト以外のサブスクリプションをサポート • 軽微なバグの修正とパフォーマンスの向上
2019 年 4 月 18 日	1.2.0.269	• Microsoft の Azure 環境のサポートが追加されました

AWS SMS のドキュメント履歴

次の表では、AWS SMSのリリースを説明しています。

update-history-change	update-history-description	update-history-date
コンソールの非推奨 (p. 57)	ドキュメントのサポートを削除AWS SMSコンソールが並んでいますAWS SMSコンソールの非推奨. -AWS SMSAPI は 2023 年 3 月 31 日までサポートされます。	2022 年 4 月 1 日
アプリケーションの検証 (p. 57)	アプリケーションを起動する前にアプリケーションを検証するためのサポートが追加されました。アプリケーションの検証では、AWS Systems Manager を使用して EC2 インスタンス上で検証スクリプトを実行します。インスタンスの検証では、Amazon EC2 ユーザーデータを使用して、EC2 インスタンスが最初に起動したときに設定スクリプトを実行できます。	2020 年 8 月 10 日
Azure のサポート (p. 57)	Microsoft Azure のサポートが追加されました	2019 年 4 月 18 日
AWS Migration Hub との統合 (p. 57)	Migration Hub によって検出されたアプリケーションのインポートと移行のサポートが追加されました。	2019 年 2 月 22 日
アプリケーションの移行 (p. 57)	CloudFormation を使用して起動する自動化アプリケーション、さらにアプリケーションとして編成されたサーバーのグループの移行を新たにサポート。	2018 年 12 月 5 日
より大きなディスクサイズのサポート (p. 57)	S3 マニフェスト機能を使用して 4 TB を超えるディスクサイズの VM を新たにサポート。	2018 年 6 月 11 日
単一のコネクタでの複数サーバーの移行 (p. 57)	単一のコネクタでの複数の Hyper-V サーバーから複数の VM の移行のサポートが追加されました。	2018 年 4 月 25 日
Hyper-V のサポート (p. 57)	Microsoft の Hyper-V 環境のサポートが追加されました。	2017 年 14 月 12 日
アップロードのレジリエンス (p. 57)	ディスクアップロード時のレジリエンスの向上。	2017 年 11 月 8 日
向上したアップロード速度 (p. 57)	VM ディスクのアップロード速度の向上。	2017 年 8 月 29 日

vCenter 5.1、1 回限りの移行、エラーメッセージ、セキュリティ (p. 57)	vCenter 5.1 のサポートが追加されました 1 回のみの移行のサポート。エラーメッセージの見直しとセキュリティ関連のバグの修正。	2017 年 5 月 5 日
初回リリース (p. 57)	VMware環境用の Server Migration Connector 仮想アプライアンス。グラフィカルインターフェイスを使用して VM の移行タスクと SMS のレプリケーションタスクを管理するための AWS Server Migration Service コンソール。AWS Server Migration Serviceコマンドラインを使用して VM の移行タスクと SMS のレプリケーションタスクを管理する CLI。	2016 年 11 月 3 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。