ボリュームゲートウェイユーザーガイド

AWS Storage Gateway

API バージョン 2013-06-30

AWS Storage Gateway: ボリュームゲートウェイユーザーガイド

Table of Contents

Amazon S3 File Gateway のドキュメントは、「What is Amazon S3 File Gateway?」に移動しました。

Amazon FSx File Gateway のドキュメントが「Amazon FSx File Gateway とは」に移動されました。

テープゲートウェイのドキュメントは、「What is Tape Gateway?」に移動しました。

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。

ボリュームゲートウェイについて

AWS Storage Gateway は、オンプレミスのソフトウェアアプライアンスをクラウドベースのストレージに接続し、オンプレミスの IT 環境と AWS ストレージインフラストラクチャ間のデータセキュリティ機能とシームレスに統合します。このサービスを通じて、Amazon Web Services のクラウドにデータを保存し、データのセキュリティを維持するために役立つ、スケーラブルでコスト効率の高いストレージを利用できます。

AWS Storage Gateway は、ファイルベースのファイルゲートウェイ (Amazon S3 ファイルと Amazon FSx ファイル)、ボリュームベース (キャッシュ型と保存型)、およびテープベースのストレージソリューションを提供します。

トピック

ボリュームゲートウェイ

ボリュームゲートウェイ – ボリュームゲートウェイは、オンプレミスアプリケーションサーバーからインターネットスモールコンピュータシステムインターフェイス (iSCSI) デバイスとしてマウントできるクラウドベースのストレージボリュームを提供します。

ボリュームゲートウェイは、、、または Microsoft Hyper-V ハイパーバイザーで実行されている VM VMware アプライアンスとしてオンプレミスでKVMデプロイすることも、ハードウェアアプライアンスとしてデプロイすることも、Amazon ESXiEC2インスタンスとして に AWS デプロイすることもできます。

サポートするボリューム構成は以下のとおりです。

- キャッシュ型ボリューム – データを Amazon Simple Storage Service (Amazon S3) に保存し、頻繁にアクセスするデータのサブセットのコピーはローカルに保持します。プライマリストレージのコストを大幅に削減し、ストレージをオンプレミスで拡張する必要を最小限に抑えます。また、頻繁にアクセスするデータへのアクセスを低レイテンシーに保つことができます。

- 保管型ボリューム – データセット全体への低レイテンシーアクセスが必要な設定は、すべてのデータをローカルに保存するように、最初にオンプレミスのゲートウェイを設定します。次に、このデータの point-in-time スナップショットを Amazon S3 に非同期的にバックアップします。この設定では、ローカルデータセンターまたは Amazon Elastic Compute Cloud (Amazon) に復元できる、耐久性が高く安価なオフサイトバックアップが提供されますEC2。例えば、ディザスタリカバリに代替容量が必要な場合は、バックアップを Amazon に復元できますEC2。

ドキュメント: ボリュームゲートウェイのドキュメントについては、「ボリュームゲートウェイの作成」を参照してください。

Storage Gateway を初めてお使いになる方向けの情報

次のドキュメントには、すべてのゲートウェイに共通の設定情報を示す使用開始セクションと、ゲートウェイ固有の設定セクションがあります。使用開始セクションでは、ゲートウェイのストレージをデプロイ、アクティブ化、設定する方法を示しています。マネジメント セクションでは、ゲートウェイとリソースを管理する方法を示します。

- 「ボリュームゲートウェイの作成」では、ボリュームゲートウェイを作成して使用する方法について説明しています。ボリュームにストレージボリュームとバックアップデータを作成する方法が示されています。

- 「ゲートウェイを管理する」では、ゲートウェイおよびそのリソースに対する管理タスクの実行方法について説明しています。

このガイドでは、主に AWS Management Consoleを使用したゲートウェイ操作の方法について参照できます。これらのオペレーションをプログラムで実行する場合は、「 AWS Storage Gateway API リファレンス」を参照してください。

ボリュームゲートウェイの仕組み (アーキテクチャ)

以降では、ボリュームゲートウェイソリューションのアーキテクチャの概要を説明します。

ボリュームゲートウェイ

ボリュームゲートウェイの場合、キャッシュ型ボリュームまたは保管型ボリュームのどちらかを使用できます。

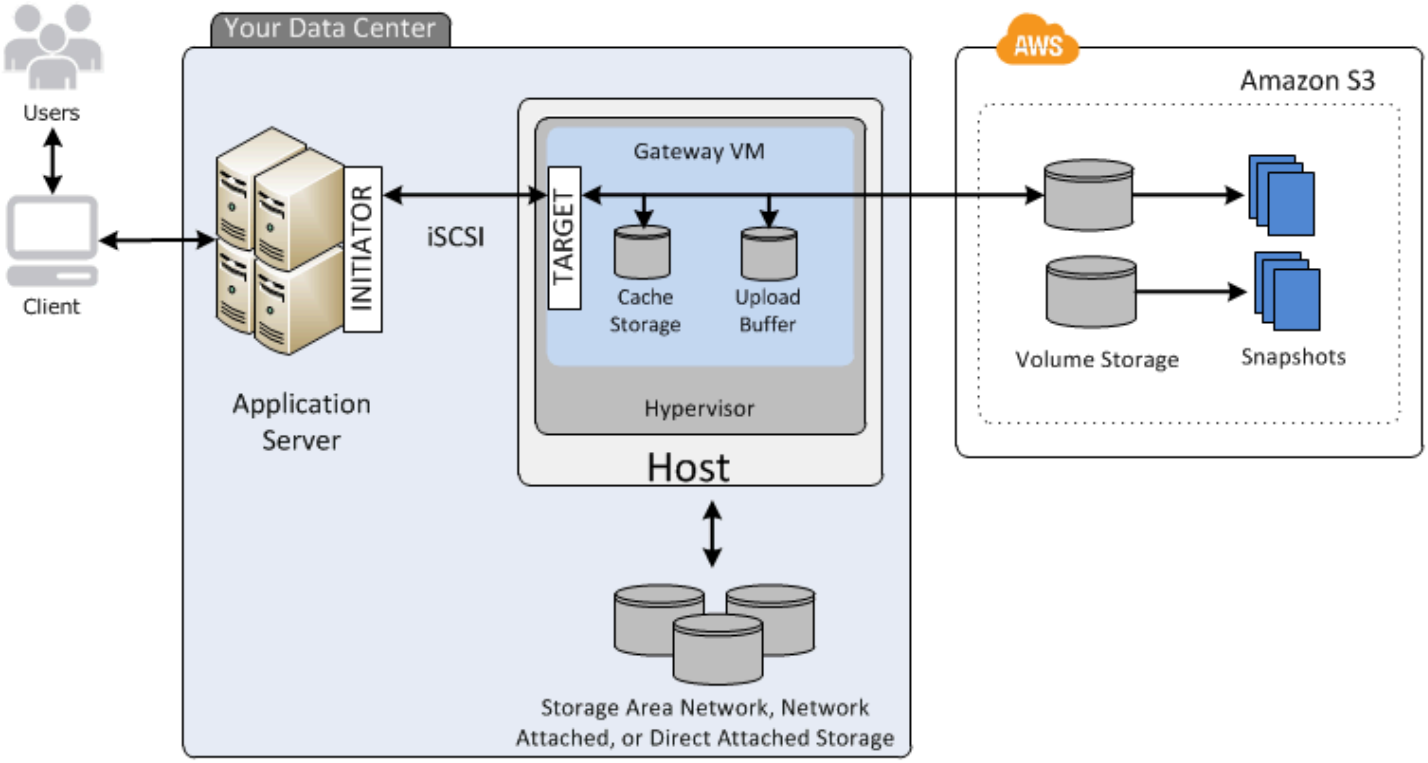
トピック

キャッシュ型ボリュームのアーキテクチャ

キャッシュ型ボリュームを使用することで、アクセス頻度の高いデータはローカルのストレージゲートウェイに保持しながら、Amazon S3 をプライマリデータストレージとして使用できます。キャッシュ型ボリュームは、オンプレミスのストレージインフラストラクチャをスケールする必要性を最小限に抑えます。同時に、アプリケーションからは引き続き、頻繁にアクセスするデータへの低レイテンシーなアクセスが可能になります。最大 32 TiB のサイズのストレージボリュームを作成し、オンプレミスアプリケーションサーバーから iSCSI デバイスとしてアタッチできます。ゲートウェイは、これらのボリュームに書き込まれたデータを Amazon S3 に保存し、最近読み込まれたデータはオンプレミスのストレージゲートウェイのキャッシュとアップロードバッファストレージに保持します。

キャッシュ型ボリュームの容量は 1 GiB ~ 32 TiB の範囲で設定できますが、1 GiB 未満の端数は切り上げとなります。キャッシュ型ボリュームに対して設定されているゲートウェイごとに最大 32 個のボリュームがサポートされ、合計ストレージボリュームは最大 1,024 TiB (1 PiB) です。

キャッシュ型ボリュームによるソリューションでは、Storage Gateway により、すべてのオンプレミスのアプリケーションデータは Amazon S3 のストレージボリュームに保存されます。下の図は、キャッシュ型ボリュームデプロイメントの概要を示しています。



VM である Storage Gateway ソフトウェアアプライアンスをデータセンターのホストにインストールしてアクティブ化したら、 を使用して Amazon S3 でバックアップされたストレージボリューム AWS Management Console をプロビジョニングします。Storage Gateway APIまたはライブラリを使用して、プログラムでストレージボリュームを AWS SDKプロビジョニングすることもできます。次に、これらのストレージボリュームをオンプレミスのアプリケーションサーバーに iSCSI デバイスとしてマウントします。

さらにオンプレミスのディスクも VM に割り当てます。ここで割り当てたオンプレミスのディスクは、以下の役割を果たします。

- ゲートウェイがキャッシュストレージとして使用するディスク – アプリケーションが のストレージボリュームにデータを書き込むと AWS、ゲートウェイはまずキャッシュストレージに使用されるオンプレミスディスクにデータを保存します。その上で、ゲートウェイはデータを Amazon S3 にアップロードします。キャッシュストレージは、オンプレミスで耐久性の高い保存場所として機能し、アップロードバッファから Amazon S3 へのアップロードを待機しているデータを保存します。

  また、キャッシュストレージはアプリケーションが最近アクセスしたデータをオンプレミスに保存し、低レイテンシーでアクセスできるようにもします。アプリケーションがデータをリクエス

トすると、ゲートウェイはまずキャッシュストレージでそのデータを検索し、見つからなければ Amazon S3 内を検索します。

キャッシュストレージに割り当てるディスク容量を決定するには、次のガイドラインを使用できます。通常、既存のファイルストアサイズの少なくとも 20% をキャッシュストレージとして割り当てる必要があります。また、キャッシュストレージの容量はアップロードバッファより大きくする必要があります。このガイドラインは、アップロードバッファ内で Amazon S3 へのアップロードが完了していないすべてのデータを永続的に保持できる、十分なキャッシュストレージを確保するために有効です。

- ゲートウェイがアップロードバッファとして使用するディスク – ゲートウェイは、受け取ったデータを Amazon S3 にアップロードする前に、アップロードバッファと呼ばれるステージングエリアに保存します。ゲートウェイは、暗号化された Secure Sockets Layer (SSL) 接続を介してこのバッファデータを にアップロードします。 AWSこのバッファデータは Amazon S3 に暗号化されて保存されます。

Amazon S3 のストレージボリュームからは、スナップショットと呼ばれる増分バックアップを作成することができます。これらの point-in-time スナップショットは Amazon S3 にも Amazon EBSスナップショットとして保存されます。新たにスナップショットをとる際には、前回のスナップショット以降に変更されたデータのみが保存されます。スナップショットが作成されると、ゲートウェイはスナップショットポイントまで変更をアップロードし、Amazon を使用して新しいスナップショットを作成しますEBS。スナップショットは、スケジュールに基づいて、または 1 回のみ実行可能です。1 つのボリュームで複数のスナップショットを連続してキューに入れることができますが、各スナップショットの作成が完了しないと、次のスナップショットは作成されません。スナップショットを削除する場合、他のスナップショットが必要ないデータのみが削除されます。Amazon EBSスナップショットの詳細については、「Amazon EBSスナップショット」を参照してください。

データのバックアップを復元する必要がある場合は、Amazon EBSスナップショットをゲートウェイストレージボリュームに復元できます。または、最大 16 TiB のサイズのスナップショットの場合、スナップショットを新しい Amazon EBSボリュームの開始点として使用できます。その後、この新しい Amazon EBSボリュームを Amazon EC2インスタンスにアタッチできます。

キャッシュされたボリュームのすべてのゲートウェイデータとスナップショットデータは Amazon S3 に保存され、サーバー側の暗号化 () を使用して保管時に暗号化されますSSE。ただし、Amazon S3 または Amazon SAmazon S3 マネジメントコンソールなどの他のツールでは、このデータにアクセスできません。 API

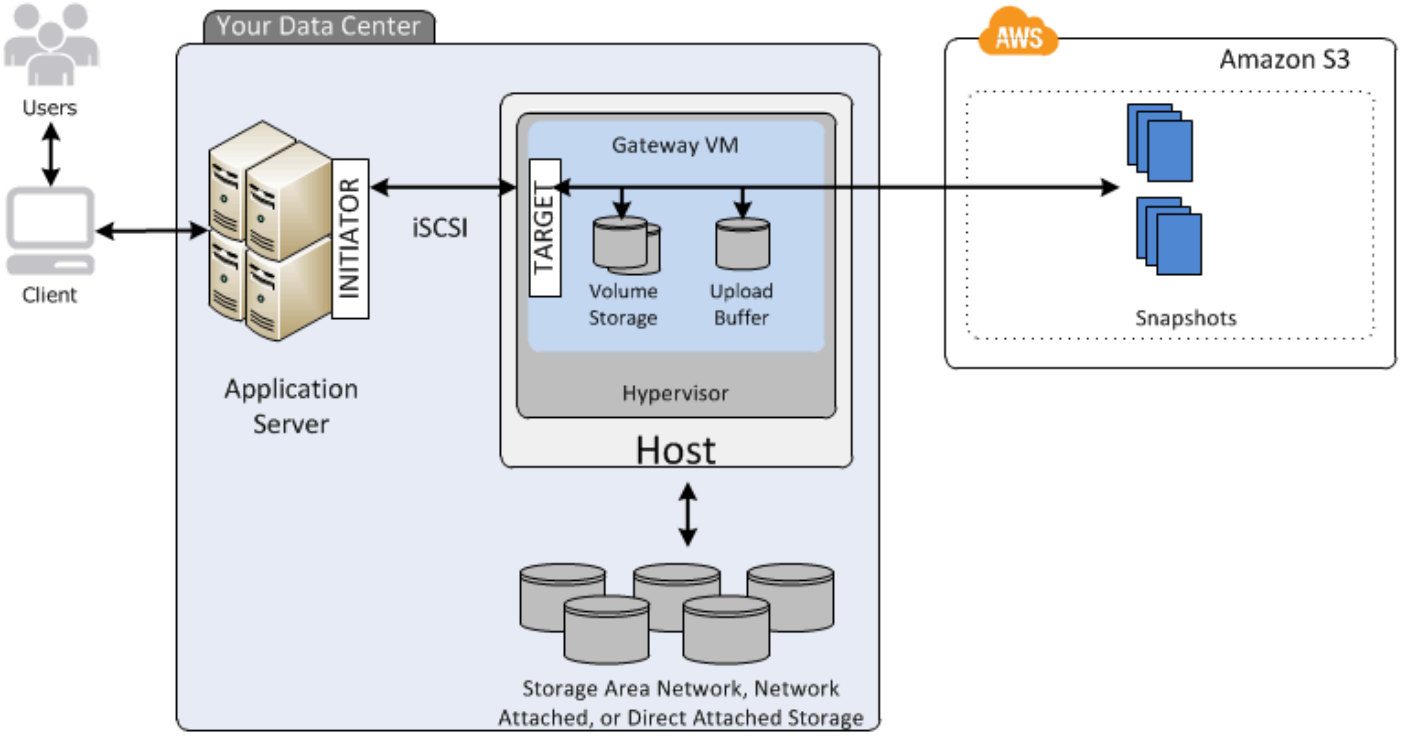
保管型ボリュームのアーキテクチャ

ストアドボリュームを使用すると、プライマリデータをローカルに保存しながら、そのデータを に非同期的にバックアップできます AWS。保管型ボリュームを使用することにより、オンプレミスのアプリケーションがそのデータセット全体に低レイテンシーでアクセスできます。同時に、耐久性のあるオフサイトのバックアップが提供されます。ストレージボリュームを作成し、オンプレミスのアプリケーションサーバーから iSCSI デバイスとしてマウントできます。保管型ボリュームに書き込まれたデータは、オンプレミスのストレージハードウェアに保管されます。このデータは、Amazon Elastic Block Store (Amazon) スナップショットとして Amazon S3 に非同期的にバックアップされます。 EBS

保管型ボリュームの容量は 1 GiB ~ 32 TiB の範囲で設定できますが、1 GiB 未満の端数は切り上げとなります。保管型ボリュームに対して設定されるゲートウェイごとに、最大 32 個のボリュームがサポートされ、合計ボリュームストレージは最大 512 TiB (0.5 PiB) です。

保管型ボリュームでは、ボリュームストレージをオンプレミスのデータセンターに維持します。つまり、アプリケーションデータはすべてオンプレミスのストレージハードウェアに保存されます。その後、ゲートウェイはデータセキュリティを維持するための機能を使用して Amazon Web Services のクラウドにデータをアップロードし、コスト効率の高いバックアップと迅速な障害復旧に利用します。すべてのデータに低レイテンシーでアクセスするために、データをローカルのオンプレミスに保持する必要があるものの、バックアップは AWSに置いておきたいという場合には、これが最適なソリューションとなります。

下の図は、保管型ボリュームのデプロイの概要を示しています。



Storage Gateway のソフトウェアアプライアンス (VM) をデータセンターのホストにインストールして起動したら、ゲートウェイのストレージボリュームを作成できます。次に、オンプレミスの直接接続ストレージ (DAS) またはストレージエリアネットワーク (SAN) ディスクにマッピングします。起動は、新規ディスクからでも、すでにデータを保持しているディスクからでも行えます。その後、これらのストレージボリュームを iSCSI デバイスとしてオンプレミスのアプリケーションサーバーにマウントできます。オンプレミスのアプリケーションがゲートウェイのストレージボリュームに対してデータの読み書きを行う時、そのデータはボリュームに割り当てられたディスクに保存され、読み込まれます。

データを Amazon S3 にアップロードする前に、ゲートウェイは受け取ったデータを、アップロードバッファと呼ばれるステージングエリアにいったん保存します。オンプレミスDASまたはSANディスクを作業ストレージに使用できます。ゲートウェイは、暗号化された Secure Sockets Layer (SSL) 接続を介してアップロードバッファから Amazon Web Services クラウドで実行されている Storage Gateway サービスにデータをアップロードします。このデータは暗号化された形で Amazon S3 に保存されます。

ストレージボリュームは、増分バックアップ (スナップショットと呼びます) をとることができます。ゲートウェイは、これらのスナップショットを Amazon S3 に Amazon EBSスナップショットとして保存します。新たにスナップショットをとる際には、前回のスナップショット以降に変更されたデータのみが保存されます。スナップショットが作成されると、ゲートウェイはスナップショットポ

イントまで変更をアップロードし、Amazon を使用して新しいスナップショットを作成しますEBS。スナップショットは、スケジュールに基づいて、または 1 回のみ実行可能です。1 つのボリュームで複数のスナップショットを連続してキューに入れることができますが、各スナップショットの作成が完了しないと、次のスナップショットは作成されません。スナップショットを削除する場合、他のスナップショットが必要ないデータのみが削除されます。

データのバックアップを復元する必要がある場合は、Amazon EBSスナップショットをオンプレミスゲートウェイストレージボリュームに復元できます。スナップショットを新しい Amazon EBSボリュームの開始点として使用し、Amazon EC2インスタンスにアタッチすることもできます。

Storage Gateway の料金

料金に関する最新情報については、 AWS Storage Gateway 詳細ページの「料金表」を参照してください。

Storage Gateway のデプロイを計画する

Storage Gateway ソフトウェアアプライアンスを使用すると、既存のオンプレミスアプリケーションインフラストラクチャを、データセキュリティ機能を提供するスケーラブルで費用対効果の高い AWS クラウドストレージに接続できます。

Storage Gateway をデプロイするには、まず次の 2 点を決定しておく必要があります。

1. ご使用のゲートウェイタイプ — このガイドでは、以下のゲートウェイタイプについて説明します。
   - ボリュームゲートウェイ – ボリュームゲートウェイを使用すると、Amazon Web Services のクラウド内にストレージボリュームを作成できます。オンプレミスアプリケーションは、これらに Internet Small Computer System Interface (iSCSI) ターゲットとしてアクセスできます。キャッシュ型および保管型という 2 つのオプションがあります。
     - キャッシュ型ボリュームでは、ボリュームデータを に保存し AWS、最近アクセスしたデータのごく一部をオンプレミスのキャッシュに保存します。この方法では、アクセス頻度が高いデータセットに低レイテンシーでアクセスできるようになります。また、 に保存されているデータセット全体にシームレスにアクセスできます AWS。キャッシュボリュームを使用すれば、ストレージリソースを拡張するためにハードウェアを追加調達する必要はありません。
     - 保存ボリュームでは、ボリュームデータのセット全体をオンプレミスに保存し、定期的な point-in-time バックアップ (スナップショット) を に保存します AWS。このモデルでは、オ

ンプレミスストレージがプライマリであり、データセット全体への低レイテンシーアクセスを提供します。 AWS ストレージは、データセンターで災害が発生した場合に復元できるバックアップです。

キャッシュ型ボリュームと保存型ボリュームの両方で、Amazon point-in-time スナップショットの形式でボリュームゲートウェイボリュームのEBSスナップショットを作成できます。ボリュームのスナップショットを新しい Amazon EBSボリュームの開始点として使用し、Amazon EC2インスタンスにアタッチできます。このアプローチを使用すると、データ処理に追加のオンデマンドコンピューティング容量やディザスタリカバリの代替容量EC2が必要な場合は、オンプレミスアプリケーションから Amazon で実行されているアプリケーションにデータを提供できます。データ保護、復旧、移行、その他のさまざまなデータ転送ニーズに対応するために、ボリュームのバージョン管理されたコピーを容量効率に優れた方法で用意できます。

Amazon EBSスナップショットに基づいてボリュームを作成する方法については、「ボリュームの作成」を参照してください。

ボリュームゲートウェイのアーキテクチャの概要については、「キャッシュ型ボリュームのアーキテクチャ」と「保管型ボリュームのアーキテクチャ」を参照してください。

2. ホスティングオプション – Storage Gateway は、オンプレミスで VM アプライアンスまたはハードウェアアプライアンスとして、または で Amazon EC2インスタンス AWS として実行できます。詳細については、「Volume Gateway の設定要件」を参照してください。データセンターがオフラインになり、使用可能なホストがない場合は、EC2インスタンスにゲートウェイをデプロイできます。Storage Gateway は、ゲートウェイ VM イメージを含む Amazon マシンイメージ (AMI) を提供します。

また、ゲートウェイソフトウェアアプライアンスのデプロイ先となるホストを構成する際には、ゲートウェイ VM に充分なストレージを割り当てる必要があります。

次のステップに進む前に、以下が完了していることを確認してください。

- オンプレミスでデプロイされたゲートウェイの場合、VM ホストのタイプを選択してセットアップします。オプションは、VMwareESXiハイパーバイザー、Microsoft Hyper-V、Linux カーネルベースの仮想マシン () ですKVM。ファイアウォールの内側にゲートウェイをデプロイする場合は、ポートからゲートウェイ VM にアクセスできるようにしておく必要があります。詳細については、「Volume Gateway の設定要件」を参照してください。

の開始方法 AWS Storage Gateway

このセクションでは、Storage Gateway の使用を開始する際の手順を説明します。開始するには、まず にサインアップします AWS。初めて使用する方には、リージョンと要件のセクションを読むことをお勧めします。

トピック

にサインアップする AWS Storage Gateway

Storage Gateway を使用するには、すべての AWS リソース、フォーラム、サポート、使用状況レポートにアクセスするための Amazon Web Services のアカウントが必要です。サービスを使用するまで、料金は発生しません。Amazon Web Services のアカウントを既にお持ちの場合は、このステップを省略できます。

Amazon Web Services のアカウントにサインアップするには

1. https://portal.aws.amazon.com/billing/サインアップ を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

   にサインアップすると AWS アカウント、 AWS アカウントのルートユーザーが作成されます。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があります。セキュリティのベストプラクティスとして、ユーザーに管理アクセスを割り当て、ルートユーザーのみを使用してルートユーザーアクセスが必要なタスクを実行してください。

料金については、Storage Gateway 詳細ページの「料金表」を参照してください。

AWS リージョン Storage Gateway をサポートする

Storage Gateway は、ゲートウェイがアクティブ化されている AWS リージョンにボリューム、スナップショット、テープ、およびファイルデータを保存します。ファイルデータは、Amazon S3 バケットがある AWS リージョンに保存されます。ゲートウェイのデプロイを開始する前に、Storage Gateway マネジメントコンソールの右上にある AWS リージョンを選択します。

- Storage Gateway — サポートされている AWS リージョンと Storage Gateway で使用できる AWS サービスエンドポイントのリストについては、「」のAWS Storage Gateway 「エンドポイントとクォータ」を参照してくださいAWS 全般のリファレンス。 Storage Gateway
- Storage Gateway ハードウェアアプライアンス — ハードウェアアプライアンスで使用できるサポートされている AWS リージョンについては、「」のAWS Storage Gateway 「ハードウェアアプライアンスのリージョン」を参照してくださいAWS 全般のリファレンス。

Volume Gateway の設定要件

以下に挙げる要件は、特記がない限り、すべてのゲートウェイ構成に共通です。

トピック

ハードウェアとストレージの要件

このセクションでは、ゲートウェイの最小ハードウェアと設定、および必要なストレージに割り当てる最小ディスク容量について説明します。

のハードウェア要件 VMs

ゲートウェイをデプロイする前に必ず、ゲートウェイ VM をデプロイする基盤となるハードウェアで、以下の最小リソースを専有できることを確認してください。

- VM に割り当てられた仮想プロセッサ 4 個。
- ボリュームゲートウェイの場合、ハードウェアは次の量の 専用である必要がありますRAM。

  - 最大 16 GiBのキャッシュサイズを持つゲートウェイRAM用に予約された 16 TiB
  - キャッシュサイズが 16 GiBのゲートウェイRAM用に予約された 32 TiB TiB
  - キャッシュサイズが 32 GiBのゲートウェイRAM用に予約された 48 TiB TiB
- ディスクの空き容量 80 GiB (VM イメージとシステムデータのインストール用)。

詳細については、「ゲートウェイのパフォーマンスの最適化」を参照してください。ハードウェアがゲートウェイ VM のパフォーマンスにどのように影響を与えるかについては、「AWS Storage Gateway クォータ」を参照してください。

Amazon EC2インスタンスタイプの要件

Amazon Elastic Compute Cloud (Amazon EC2) にゲートウェイをデプロイする場合、ゲートウェイが機能するには、インスタンスサイズが xlarge 以上である必要があります。ただし、コンピューティング最適化インスタンスファミリーの場合は、サイズとして少なくとも 2xlarge が必要です

ボリュームゲートウェイ、Amazon EC2インスタンスはゲートウェイに使用する予定のキャッシュサイズRAMに応じて、次の量の を専用にする必要があります。

- 最大 16 GiBのキャッシュサイズを持つゲートウェイRAM用に予約された 16 TiB
- キャッシュサイズが 16 GiBのゲートウェイRAM用に予約された 32 TiB TiB
- キャッシュサイズが 32 GiBのゲートウェイRAM用に予約された 48 TiB TiB

ゲートウェイの種類に応じて次のインスタンスタイプのうち 1 つを使用することをお勧めします。

キャッシュボリュームおよびテープゲートウェイの種類に応じた推奨事項

- 汎用インスタンスファミリー – m4、m5、または m6 インスタンスタイプ。

> **Note**
>
> m4.16xlarge インスタンスタイプの使用はお勧めしません。

- コンピューティング最適化インスタンスファミリー — c4、c5、または c6 インスタンスタイプ 2xlarge インスタンスサイズ以上を選択して、必要なRAM要件を満たします。
- メモリ最適化インスタンスファミリー – r3、r5、または r6 インスタンスタイプ。
- ストレージ最適化インスタンスファミリー – i3 または i4 インスタンスタイプ。

ストレージの要件

ゲートウェイには VM 用の 80 GiB 以外にもディスク領域が必要になります。

次の表は、デプロイされるゲートウェイのローカルディスクストレージの推奨サイズを示しています。

ゲートウェイタイプ	キャッシュ (最小)	キャッシュ (最大)	アップロードバッファ (最小)	アップロードバッファ (最大)	その他の必要なローカルディスク
キャッシュ型ボリュームゲートウェイ	150 GiB	64 TiB	150 GiB	2 TiB	—
保管型ボリュームゲートウェイ	—	—	150 GiB	2 TiB	1 つまたは複数の保管されたボリューム

> **Note**
>
> キャッシュおよびアップロードバッファ用として、1 つ以上のローカルドライブを、最大容量まで構成することができます。
> 既存のゲートウェイにキャッシュまたはアップロードバッファを追加するときは、ホスト (ハイパーバイザーまたは Amazon EC2インスタンス) に新しいディスクを作成することが重要です。ディスクがキャッシュやアップロードバッファとして割り当て済みである場合は、既存のディスクサイズを変更しないでください。

ゲートウェイクォータの詳細については、「AWS Storage Gateway クォータ」を参照してください。

ネットワークとファイアウォールの要件

ゲートウェイは、インターネット、ローカルネットワーク、ドメインネームサービス (DNS) サーバー、ファイアウォール、ルーターなどにアクセスする必要があります。以下は、必要なポートと、ファイアウォールとルーターを経由してアクセスを許可する方法についての情報です。

> **Note**
>
> 場合によっては、Storage Gateway を Amazon にデプロイEC2したり、 AWS IP アドレス範囲を制限するネットワークセキュリティポリシーで他のタイプのデプロイ (オンプレミスを含む) を使用したりすることがあります。このような場合、 AWS IP 範囲の値が変更されると、ゲートウェイでサービス接続の問題が発生する可能性があります。使用する必要がある AWS IP アドレス範囲の値は、ゲートウェイをアクティブ化する AWS リージョンの Amazon サービスサブセットにあります。現在の IP 範囲値については、「AWS 全般のリファレンス」の「AWS IP アドレスの範囲」を参照してください。

> **Note**
>
> ネットワーク帯域幅の要件は、ゲートウェイによってアップロードおよびダウンロードされるデータの量によって異なります。ゲートウェイのダウンロード、アクティブ化、および更新を正常に行うには、最低 100 Mbps が必要です。データ転送のパターンによって、ワークロードのサポートに必要な帯域幅が決まります。場合によっては、Storage Gateway を Amazon にデプロイEC2したり、他のタイプのデプロイを使用したりすることがあります。

トピック

ポート要件

Storage Gateway の使用には、特定のポートへのアクセス許可が必要です。次の図は、各ゲートウェイの種類に対して許可する必要がある、必須のポートを示しています。すべてのゲートウェイの種類で必要なポートと、特定のゲートウェイの種類で必要なポートがあります。ポートの要件の詳細については、「ボリュームゲートウェイのネットワークポート要件」を参照してください。

すべてのゲートウェイの種類に共通のポート

以下のポートは、すべてのゲートウェイタイプに共通で、すべてのゲートウェイタイプで必要です。

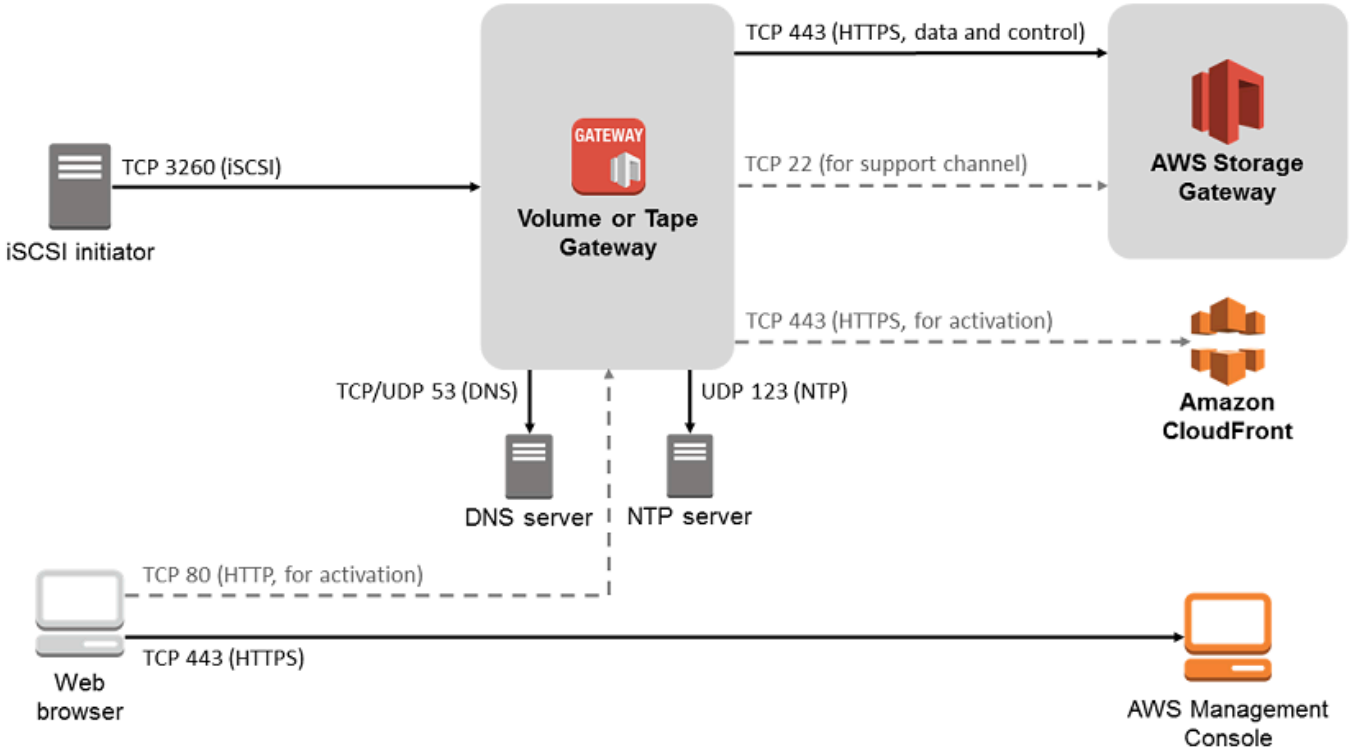
[プロトコル]	[ポート]	[Direction] (方向)	ソース	デスティネーション	用途
TCP	443 (HTTPS)	アウトバウンド	Storage Gateway	AWS	Storage Gateway から AWS サービスエンドポイントへの通信用。サービスエンドポイントの詳細については、「ファイアウォールとルーターを介した AWS Storage Gateway アクセスの許可」を参照してください。
TCP	80 (HTTP)	インバウンド	AWS マネジメントコンソールに接続するホスト。	Storage Gateway	Storage Gateway のアクティベーションキーは、ローカルシステムにより取得されます。ポート 80 は Storage Gateway アプライアンスのアクティベーション時

[プロトコル]	[ポート]	[Direction] (方向)	ソース	デスティネーション	用途
					にのみ使用されます。 Storage Gateway では、ポート 80 をパブリックアクセスが可能なように設定する必要はありません。ポート 80 へのアクセスに必要なレベルはネットワークの設定によって決まります。Storage Gateway マネジメントコンソールからゲートウェイをアクティブ化する場合、コンソールに接続するホストには、ゲートウェイのポート 80 に対するアクセス権限が必要です。

[プロトコル]	[ポート]	[Direction] (方向)	ソース	デスティネーション	用途
TCP/UDP	53 (DNS)	アウトバウンド	Storage Gateway	ドメインネームサービス (DNS) サーバー	Storage Gateway と DNSサーバー間の通信用。
TCP	22 (サポートチャネル)	アウトバウンド	Storage Gateway	AWS Support	AWS Support ゲートウェイの問題のトラブルシューティングに役立つゲートウェイへのアクセスを に許可します。このポートは、ゲートウェイの通常のオペレーションでは開いておく必要はありませんが、トラブルシューティングでは必要です。
UDP	123 (NTP)	アウトバウンド	NTP クライアント	NTP サーバー	VM 時間をホスト時間に同期するためにローカルシステムで使用されます。

ボリュームゲートウェイとテープゲートウェイのポート

次の図は、ボリュームゲートウェイに対して開くポートを示しています。



共通ポートに加えて、ボリュームゲートウェイには次のポートが必要です。

[プロトコル]	[ポート]	[Direction] (方向)	ソース	デスティネーション	用途
TCP	3260 (iSCSI)	インバウンド	iSCSI イニシエーター	Storage Gateway	ゲートウェイによって公開される iSCSI ターゲットに接続するためのローカルシステム。

ポートの要件の詳細については、「Additional Storage Gateway resources」セクションの「ボリュームゲートウェイのネットワークポート要件」を参照してください。

Storage Gateway ハードウェアアプライアンスのネットワークとファイアウォールに関する要件

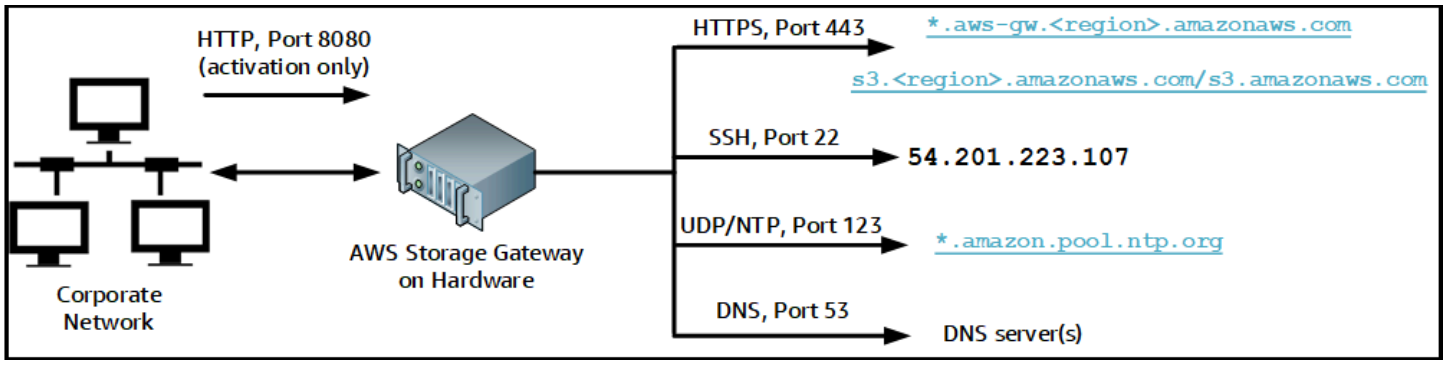
それぞれの Storage Gateway ハードウェアアプライアンスには、以下のネットワークサービスが必要です。

- インターネットアクセス – サーバー上の任意のネットワークインターフェイスを介した、インターネットへの常時接続のネットワーク接続。
- DNS サービス — ハードウェアアプライアンスとDNSサーバー間の通信のためのDNSサービス。
- 時間同期 — 自動的に設定された Amazon NTPタイムサービスに到達できる必要があります。
- IP アドレス – 割り当てられた DHCPまたは静的IPv4アドレス。アドレスを割り当てることはできませんIPv6。

Dell PowerEdge R640 サーバーの背面には 5 つの物理ネットワークポートがあります。これらのポートは、サーバーの背面から見て左から右に、次のとおりです。

1. iDRAC
2. em1
3. em2
4. em3
5. em4

リモートサーバー管理には iDRAC ポートを使用できます。



ハードウェアアプライアンスでは、以下のポートの操作が必要です。

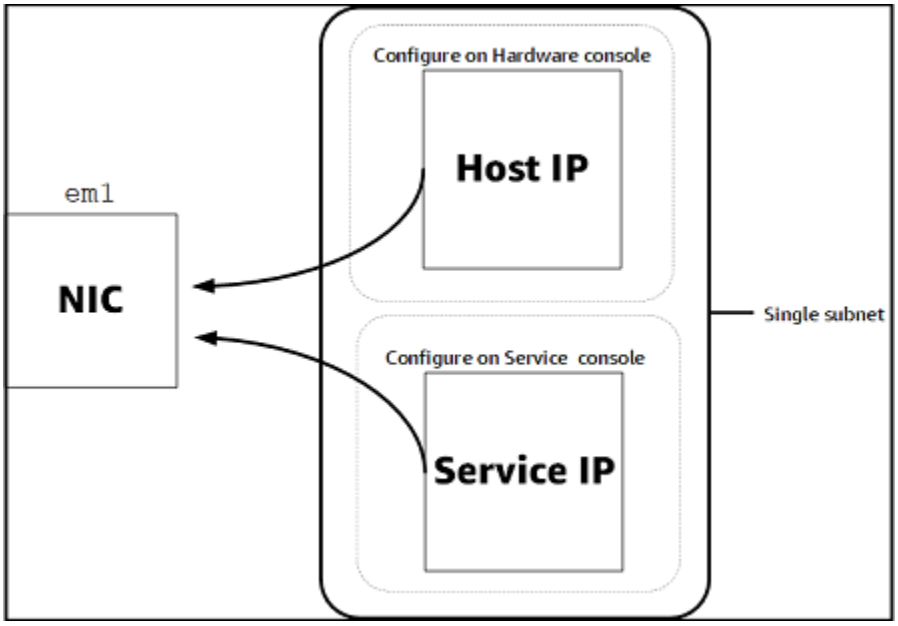
[プロトコル]	[ポート]	[Direction] (方向)	ソース	デスティネーション	用途
SSH	22	アウトバウンド	ハードウェアアプライアンス	54.201.223.107	サポートチャネル
DNS	53	アウトバウンド	ハードウェアアプライアンス	DNS サーバー	名前解決
UDP/NTP	123	アウトバウンド	ハードウェアアプライアンス	*.amazon.pool.ntp.org	時刻同期
HTTPS	443	アウトバウンド	ハードウェアアプライアンス	*.amazonaws.com	データ転送
HTTP	8080	インバウンド	AWS	ハードウェアアプライアンス	アクティベーション (短時間のみ)

ハードウェアアプライアンスでは、設計どおりに機能するためには、次のようなネットワークとファイアウォールの設定が必要です。

- 接続されているすべてのネットワークインターフェイスをハードウェアコンソールで設定します。
- 各ネットワークインターフェイスが一意のサブネット上にあることを確認します。
- 接続されているすべてのネットワークインターフェースに、前の図に示されているエンドポイントへのアウトバウンドアクセスを提供します。
- ハードウェアアプライアンスをサポートするためには、少なくとも 1 つのネットワークインターフェイスを設定します。詳細については、「ネットワークパラメータの設定」を参照してください。

> **Note**
>
> サーバーの背面とポートを示す図については、「ハードウェアアプライアンスの物理的なインストール」を参照してください。

ゲートウェイまたはホストのいずれであっても、同じネットワークインターフェイス (NIC) 上のすべての IP アドレスは、同じサブネット上にある必要があります。次の図は、アドレス割り当てスキームを示しています。



ハードウェアアプライアンスのアクティベーションと設定の詳細については、Storage Gateway ハードウェアアプライアンスの使用 を参照してください。

ファイアウォールとルーターを介した AWS Storage Gateway アクセスの許可

ゲートウェイが と通信するには、次のサービスエンドポイントにアクセスする必要がありますAWS。ファイアウォールまたはルーターを使用してネットワークトラフィックをフィルタリングまたは制限する場合は、これらのサービスエンドポイントに対し AWSへのアウトバウンド通信を許可するように、対象のファイアウォールおよびルーターを設定する必要があります。

> **Note**
>
> Storage Gateway のプライベートVPCエンドポイントを設定して、 との接続とデータ転送に使用する場合 AWS、ゲートウェイはパブリックインターネットにアクセスする必要はあり

ません。詳細については、「仮想プライベートクラウドでのゲートウェイのアクティブ化」を参照してください。

> **Important**
>
> ゲートウェイの AWS リージョンに応じて、*region* 正しいリージョン文字列を持つサービスエンドポイント内の 。

head-bucket オペレーションには、すべてのゲートウェイで以下のサービスエンドポイントが必要です。

```
s3.amazonaws.com:443
```

以下のサービスエンドポイントは、コントロールパス (anon-cp、client-cp、proxy-app) とデータパス (dp-1) オペレーションのためにすべてのゲートウェイに必要です。

```
anon-cp.storagegateway.region.amazonaws.com:443
client-cp.storagegateway.region.amazonaws.com:443
proxy-app.storagegateway.region.amazonaws.com:443
dp-1.storagegateway.region.amazonaws.com:443
```

API 呼び出しを行うには、次のゲートウェイサービスエンドポイントが必要です。

```
storagegateway.region.amazonaws.com:443
```

次に、米国西部 (オレゴン) リージョン (us-west-2) にあるゲートウェイサービスエンドポイントの例を示します。

```
storagegateway.us-west-2.amazonaws.com:443
```

以下に示す Amazon S3 サービスエンドポイントは、ファイルゲートウェイのみで使用されます。ファイルゲートウェイでは、ファイル共有のマッピング先の S3 バケットにアクセスするために、このエンドポイントが必要です。

```
bucketname.s3.region.amazonaws.com
```

次に、米国東部 (オハイオ) リージョン (us-east-2) にある S3 サービスエンドポイントの例を示します

```
s3.us-east-2.amazonaws.com
```

> **Note**
>
> ゲートウェイが S3 バケットがある AWS リージョンを特定できない場合、このサービスエンドポイントはデフォルトで になりますs3.us-east-1.amazonaws.com。ゲートウェイがアクティブ化されて S3 バケットが配置されている AWS リージョンに加えて、米国東部 (バージニア北部) リージョン (us-east-1) へのアクセスを許可しておくことをお勧めします。

以下は、 AWS GovCloud (US) リージョンの S3 サービスエンドポイントです。

```
s3-fips.us-gov-west-1.amazonaws.com (AWS GovCloud (US-West) Region (FIPS))
s3-fips.us-gov-east-1.amazonaws.com (AWS GovCloud (US-East) Region (FIPS))
s3.us-gov-west-1.amazonaws.com (AWS GovCloud (US-West) Region (Standard))
s3.us-gov-east-1.amazonaws.com (AWS GovCloud (US-East) Region (Standard))
```

次の例は、 AWS GovCloud （ 米国西部) リージョンの S3 バケットFIPSのサービスエンドポイントです。

```
bucket-name.s3-fips.us-gov-west-1.amazonaws.com
```

Storage Gateway VM は、次のNTPサーバーを使用するように設定されています。

```
0.amazon.pool.ntp.org
1.amazon.pool.ntp.org
2.amazon.pool.ntp.org
3.amazon.pool.ntp.org
```

- Storage Gateway — サポートされている AWS リージョンと Storage Gateway で使用できる AWS サービスエンドポイントのリストについては、「」のAWS Storage Gateway 「 エンドポイントとクォータ」を参照してくださいAWS 全般のリファレンス。 Storage Gateway

- Storage Gateway ハードウェアアプライアンス - ハードウェアアプライアンスで使用できるサポートされている AWS リージョンについては、「」のStorage Gateway ハードウェアアプライアンスのリージョン」を参照してくださいAWS 全般のリファレンス。

Amazon EC2ゲートウェイインスタンスのセキュリティグループの設定

セキュリティグループは、Amazon EC2ゲートウェイインスタンスへのトラフィックを制御します。セキュリティグループを設定するときは、次のことを推奨します。

- セキュリティグループで、外部のインターネットからの着信接続は許可しないでください。ゲートウェイのセキュリティグループ内のインスタンスのみがゲートウェイと通信できるようにします。インスタンスがセキュリティグループ外からゲートウェイに接続できるようにする必要がある場合は、ポート 3260 (iSCSI 接続の場合) と 80 (アクティベーションの場合) でのみ接続を許可することをお勧めします。
- ゲートウェイセキュリティグループ外の Amazon EC2ホストからゲートウェイをアクティブ化する場合は、そのホストの IP アドレスからのポート 80 での受信接続を許可します。アクティブ化するホストの IP アドレスがわからない場合、ポート 80 を開き、ゲートウェイをアクティブ化して、アクティブ化の完了後、ポート 80 のアクセスを閉じることができます。
- トラブルシューティング AWS Support の目的で を使用している場合のみ、ポート 22 アクセスを許可します。詳細については、「EC2 ゲートウェイ AWS Support のトラブルシューティングを支援したい」を参照してください。

場合によっては、Amazon EC2インスタンスをイニシエータとして使用する (つまり、Amazon にデプロイしたゲートウェイ上の iSCSI ターゲットに接続する) ことがありますEC2。このような場合は、2 つのステップを実行するアプローチをお勧めします。

1. ゲートウェイと同じセキュリティグループのイニシエータインスタンスを起動してください。
2. アクセスを設定すると、イニシエータはゲートウェイと通信できます。

ゲートウェイで開くポートについては、「ボリュームゲートウェイのネットワークポート要件」を参照してください。

サポートされているハイパーバイザーとホストの要件

Storage Gateway は、オンプレミスで仮想マシン (VM) アプライアンス、物理ハードウェアアプライアンス、または で Amazon EC2インスタンス AWS として実行できます。

> **Note**
>
> 製造元がハイパーバイザーバージョンの全般サポートを終了した場合は、Storage Gateway でも該当するハイパーバイザーバージョンのサポートを終了します。特定のバージョンのハイパーバイザーのサポートについて詳しくは、製造元のドキュメントを参照してください。

Storage Gateway では、以下のハイパーバイザーのバージョンとホストがサポートされます。

- VMware ESXi ハイパーバイザー (バージョン 7.0 または 8.0) – この設定では、ホストに接続するためのVMware vSphere クライアントも必要です。
- Microsoft Hyper-V Hypervisor (バージョン 2012 R2、2016、2019、または 2022) – Hyper-V の無料スタンドアロン版を Microsoft Download Center から入手できます。このセットアップでは、ホストに接続する Microsoft Windows クライアントコンピュータには Microsoft Hyper-V Manager が必要になります。
- Linux カーネルベースの仮想マシン (KVM) – 無料のオープンソース仮想化テクノロジー。KVM は、Linux バージョン 2.6.20 以降のすべてのバージョンに含まれています。Storage Gateway は、CentOS /RHEL 7.7、Ubuntu 16.04LTS、および Ubuntu 18.04 LTSディストリビューションでテストおよびサポートされています。他の最新の Linux ディストリビューションは動作しますが、機能やパフォーマンスは保証されません。このオプションは、すでにKVM環境が稼働していて、KVMの仕組みに慣れている場合にお勧めします。
- Amazon EC2インスタンス – Storage Gateway は、ゲートウェイ VM イメージを含む Amazon マシンイメージ (AMI) を提供します。Amazon にデプロイできるのは、ファイル、キャッシュ型ボリューム、テープゲートウェイタイプのみですEC2。Amazon にゲートウェイをデプロイする方法については、EC2「」を参照してくださいAmazon EC2インスタンスをデプロイしてボリュームゲートウェイをホストする。
- Storage Gateway ハードウェアアプライアンス – Storage Gateway では、仮想マシンによるインフラストラクチャが制限されている場所のためのオンプレミス用デプロイオプションとして、物理ハードウェアアプライアンスが提供されています。

> **Note**
>
> Storage Gateway は、別のゲートウェイ VM のスナップショットまたはクローンから作成された VM、または Amazon EC2 からのゲートウェイの復旧をサポートしていませんAMI。ゲートウェイ VM が正しく機能しない場合は、新しいゲートウェイをアクティブ化し、デー

タをそのゲートウェイに復旧します。詳細については、「予期しない仮想マシンのシャットダウンからの復旧」を参照してください。
Storage Gateway は動的メモリと仮想メモリのバルーニングをサポートしていません。

サポートされている iSCSI イニシエータ

キャッシュ型ボリュームまたは保存型ボリュームゲートウェイをデプロイすると、ゲートウェイに iSCSI ストレージボリュームを作成できます。

これらの iSCSI デバイスに接続するために、Storage Gateway は次の iSCSI イニシエータをサポートしています。

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows 10
- Windows 8.1
- Red Hat Enterprise Linux 5
- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 7
- VMware ESX イニシエーター。 のゲストオペレーティングシステムでイニシエーターを使用する代わりに使用できます。 VMs

Important

Storage Gateway は、Windows クライアントからの Microsoft Multipath I/O (MPIO) をサポートしていません。
Storage Gateway では、ホストが Windows Server フェイルオーバークラスタリング () を使用してアクセスを調整する場合、複数のホストを同じボリュームに接続できますWSFC。ただし、 を使用しないと、同じボリュームに複数のホストを接続することはできません (クラスター化されていない NTFS/ext4 ファイルシステムの共有など) WSFC。

アクセス AWS Storage Gateway

ゲートウェイに対する各種の設定や管理作業には、Storage Gateway マネジメントコンソールを使用します。このガイドでは、「使用開始」をはじめ、さまざまなセクションで、コンソールからゲートウェイの機能を使う方法を説明しています。

Storage Gateway コンソールへのブラウザアクセスを許可するには、ブラウザが Storage Gateway APIエンドポイントにアクセスできることを確認します。詳細については、「AWS 全般のリファレンスガイド」の「AWS Storage Gateway エンドポイントとクォータ」を参照してください。

さらに、 AWS Storage Gateway APIを使用して、ゲートウェイをプログラムで設定および管理できます。の詳細については、API「」を参照してくださいAPI Storage Gateway のリファレンス。

を使用して、 AWS SDKsStorage Gateway とやり取りするアプリケーションを開発することもできます。for AWS SDKsJava、.NET、および基盤となる Storage Gateway をPHPラップAPIして、プログラミングタスクを簡素化します。SDK ライブラリのダウンロードについては、「サンプルコードライブラリ」を参照してください。

Storage Gateway ハードウェアアプライアンスの使用

Storage Gateway ハードウェアアプライアンスは、動作確認済みのサーバー構成上に Storage Gateway ソフトウェアが事前インストールされた、物理ハードウェアアプライアンスです。ハードウェアアプライアンスは、 AWS Storage Gateway コンソールの [ハードウェアアプライアンスの概要] ページから管理できます。

ハードウェアアプライアンスは、高性能な 1U サーバであり、データセンターや、企業ファイアウォール内のオンプレミス環境でデプロイすることができます。ハードウェアアプライアンスを購入しアクティブ化すると、そのプロセス内で、対象のハードウェアアプライアンスが Amazon Web Services のアカウントと関連付けられます。アクティブ化が完了すると、そのハードウェアアプライアンスはコンソールの [ハードウェアアプライアンスの概要] ページにゲートウェイとして表示されます。ハードウェアアプライアンスは、ファイルゲートウェイ、テープゲートウェイ、またはボリュームゲートウェイの各タイプとして設定できます。ハードウェアアプライアンスでこれらのゲートウェイタイプをデプロイしてアクティベートする手順は、仮想プラットフォームでの手順と同じです。

以下のセクションでは、Storage Gateway ハードウェアアプライアンスの注文、セットアップ、設定、アクティブ化、起動、および使用の手順について説明します。

トピック

サポートされている AWS リージョン

Storage Gateway ハードウェアアプライアンスがアクティベーションと使用が可能なサポート AWS リージョン 対象 のリストについては、「」のStorage Gateway ハードウェアアプライアンスリージョン」を参照してくださいAWS 全般のリファレンス。

ハードウェアアプライアンスのセットアップ

Storage Gateway ハードウェアアプライアンスを受け取ったら、ハードウェアアプライアンスコンソールを使用して、 への常時接続を提供し、アプライアンスを AWS アクティブ化するようにネットワークを設定します。アクティベーションを行うと、そのプロセスの中で、アプライアンスが Amazon Web Services アカウントに関連付けられます。アプライアンスをアクティブ化した後は、Storage Gateway コンソールから、ファイル、ボリューム、またはテープゲートウェイを起動できます。

> **Note**
>
> ハードウェアアプライアンスのファームウェアが であることを確認するのはユーザーの責任です up-to-date。

ハードウェアアプライアンスをインストールして設定するには

1. アプライアンスをラックにマウントして、電源とネットワークに接続します。詳細については、「ハードウェアアプライアンスの物理的なインストール」を参照してください。
2. ハードウェアアプライアンス (ホストIPv4) と Storage Gateway (サービス) の両方のインターネットプロトコルバージョン 4 () アドレスを設定します。詳細については、「ネットワークパラメータの設定」を参照してください。
3. 選択した AWS リージョンのコンソールハードウェアアプライアンスの概要ページでハードウェアアプライアンスをアクティブ化します。詳細については、「ハードウェアアプライアンスのアクティブ化」を参照してください。
4. Storage Gateway をハードウェアアプライアンスにインストールします。詳細については、「ゲートウェイの設定」を参照してください。

   ハードウェアアプライアンスにゲートウェイを設定する方法は、、Microsoft Hyper-VVMwareESXi、Linux カーネルベースの仮想マシン (KVM) 、または Amazon でゲートウェイを設定する場合と同じですEC2。

使用可能なキャッシュストレージの増加

ハードウェアアプライアンスでは、使用可能なストレージを 5 TB から 12 TB に増やすことができます。これにより、 のデータへの低レイテンシーアクセスのためのより大きなキャッシュが提供されます AWS。5 TB モデルを注文した場合、1.92 TB SSDs (ソリッドステートドライブ) を 5 つ購入することで、使用可能なストレージを 12 TB に増やすことができます。

入手した SSD は、アクティブ化する前のハードウェアアプライアンスに 追加します。ハードウェアアプライアンスが既にアクティブ化されており、そのアプライアンスで使用可能なストレージを 12 TB に増やす場合には、以下の手順を実行します。

1. ハードウェアアプライアンスを工場出荷時の設定にリセットします。これを行う方法については、Amazon Web Services サポートにお問い合わせください。
2. アプライアンスSSDsに 5 つの 1.92 TB を追加します。

ネットワークインターフェイスカードのオプション

注文したアプライアンスのモデルによっては、10G-Base-T 銅線ネットワークカードまたは 10G DA/SFP+ ネットワークカードが付属している場合があります。

- 10G-Base-T NIC設定：
  - 10G の場合はCAT6ケーブルを使用し、1G の場合は CAT5(e) を使用します。
- 10G DA/SFP+ NIC設定：
  - 最長 5 メートルの、Twinax 銅線ダイレクトアタッチケーブルを使用
  - Dell/Intel 互換 SFP+ 光モジュール (SR または LR)
  - SFP1G-Base-T または 10G-Base-T 用の /SFP+ 銅トランシーバー

ハードウェアアプライアンスの物理的なインストール

Storage Gateway ハードウェアアプライアンスを開梱した後、同梱されている指示に従いサーバーをラックにマウントします。アプライアンスには 1U フォームファクターがあり、国際電気標準会議 (IEC) 準拠の 19 インチラックに収まります。

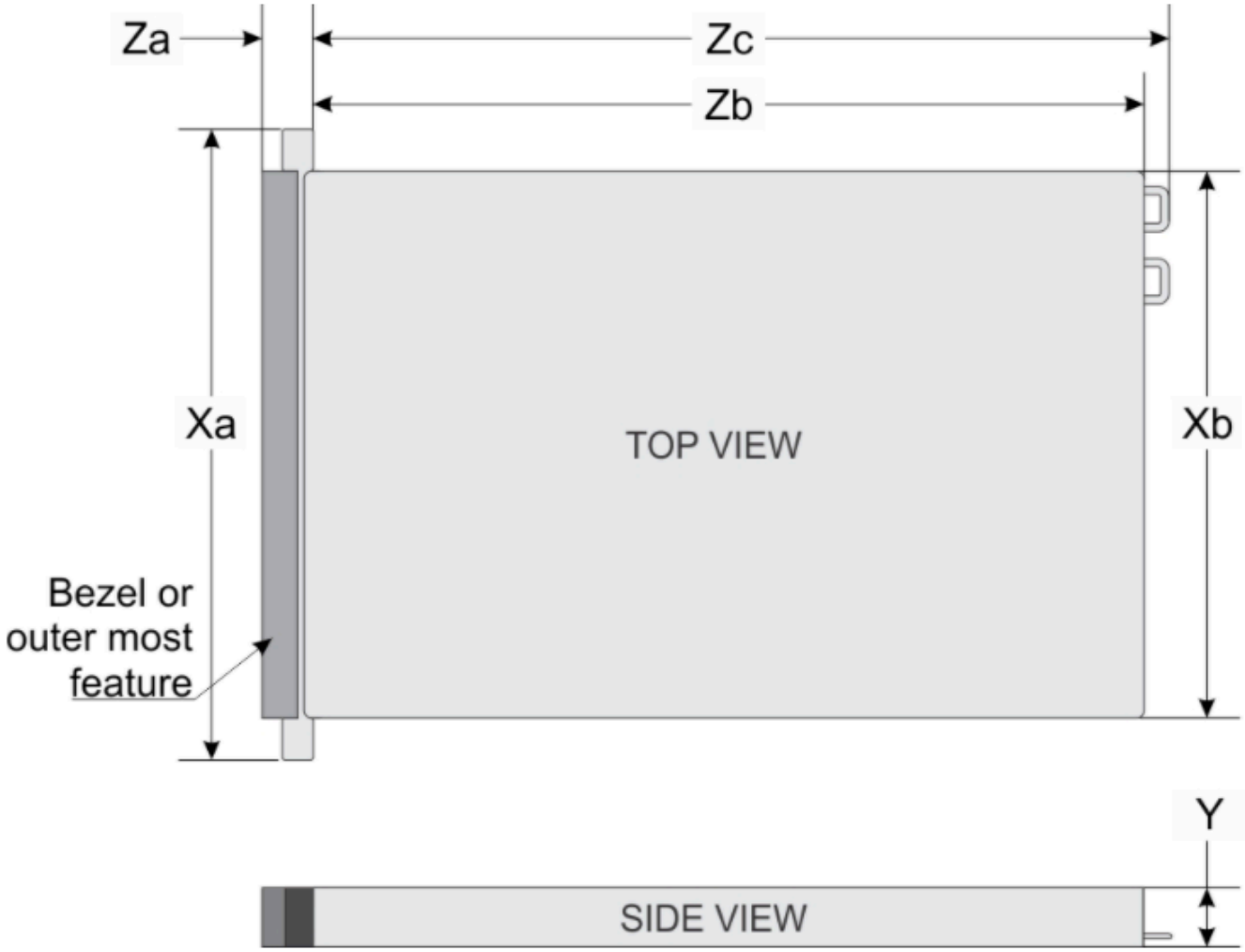
ハードウェアアプライアンスをインストールするには、次のコンポーネントが必要です。

- 電源ケーブル: 1 つは必須です。2 つを推奨します。

- サポートされているネットワークケーブル (ハードウェアアプライアンスに含まれるネットワークインターフェイスカード (NIC) によって異なります) 。二軸銅 DAC、 SFP+ 光学モジュール (Intel 互換) 、または SFP Base-T 銅トランシーバー。
- キーボードとモニター、またはキーボード、ビデオ、マウス (KVM) のスイッチソリューション。

ハードウェアアプライアンスの寸法

ハードウェアアプライアンスの寸法 (取り付けブラケットとベゼルを含む)。



System	Xa	Xb	Y	Za (with bezel)	Za (without bezel)	Zb*	Zc
10 x 2.5-inches	482.0 mm (18.97-inches)	434.0 mm (17.08-inches)	42.8 mm (1.68-inches)	35.84 mm (1.41-inches)	22.0 mm (0.87-inches)	733.82 mm (29.61-inches)	772.67 mm (30.42-inches)

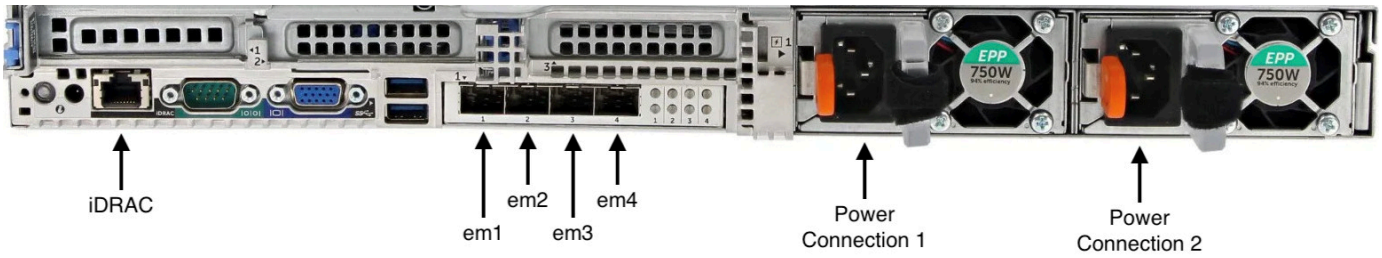
ハードウェアアプライアンスの寸法 (取り付けブラケットとベゼルを含む)。

ハードウェアアプライアンスを電源に接続するには

> **Note**
>
> 以下の手順を実行する前に、Storage Gateway ハードウェアアプライアンスのネットワークとファイアウォールに関する要件 に記載されている、Storage Gateway ハードウェアアプライアンスに関するすべての要件を満たしていることを確認します。

1. 2 つの電源装置のそれぞれに電源を接続します。1 つの電源接続のみを使用することも可能ですが、両方の電源への接続を推奨します。

   次のイメージでは、さまざまな接続を備えたハードウェアアプライアンスを示します。
   ハードウェアアプライアンスの背面。ネットワークや電源のコネクタのラベルが表示されています。

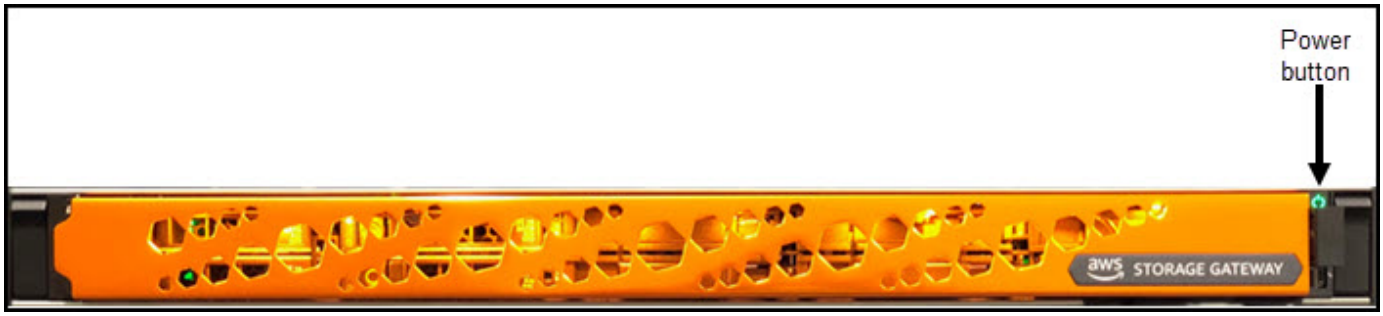
   ハードウェアアプライアンスの背面。ネットワークや電源のコネクタのラベルが表示されています。

2. イーサネットケーブルを em1 ポートに接続し、インターネットの常時接続を提供します。em1 ポートは、背面で左から右に並ぶ 4 つの物理ネットワークポートの 1 つめのポートです。

   > **Note**
   >
   > ハードウェアアプライアンスはトVLANランキングをサポートしていません。ハードウェアアプライアンスを接続するスイッチポートを非トランクVLANポートとして設定します。

3. キーボードとモニターを接続します。

4. 次のイメージに示すように、前面パネルの電源ボタンを押して、サーバーの電源をオンにします。
   ハードウェアアプライアンスの前面。電源ボタンのラベルが表示されています。



ハードウェアアプライアンスの前面。電源ボタンのラベルが表示されています。

サーバーが起動されると、ハードウェアコンソールがモニターに表示されます。ハードウェアコンソールには、初期ネットワークパラメータの設定 AWS に使用できる 固有のユーザーインターフェイスが表示されます。これらのパラメータを設定して、アプライアンスを AWS に接続し、Amazon Web Services サポートによるトラブルシューティング用のサポートチャネルを開きます。

ハードウェアコンソールを操作するには、キーボードからテキストを入力し、Up、Down、Right、Left Arrow キーを使用して、各方向に画面を移動します。Tab キーを使用して、画面上の項目を順番に進めます。一部のセットアップでは、Shift+Tab キーを使用すると、項目を逆順に移動できます。選択を保存するには、Enter キーを使用するか、または画面上のボタンを選択します。

初めてパスワードを設定するには

1. [Set Password] でパスワードを入力し、Down arrow を押します。
2. 確認のためにパスワードを再入力し、[Save Password] を選択します。

ハードウェアアプライアンスコンソールの [Save Password] ダイアログ画面。

ハードウェアアプライアンスコンソールの [Save Password] ダイアログ画面。

この時点で、ハードウェアコンソールには、以下のように表示されます。
ハードウェアアプライアンスコンソールのメインメニュー。接続状況とメニューオプションが表示されています。

ハードウェアアプライアンスコンソールのメインメニュー。接続状況とメニューオプションが表示されています。

次のステップ

ネットワークパラメータの設定

ネットワークパラメータの設定

サーバーが起動したら、ハードウェアアプライアンスの物理的なインストール に従って、ハードウェアコンソールで、最初のパスワードを入力します。

次に、ハードウェアコンソールで以下の手順を実行して、ネットワークパラメータを設定し、ハードウェアアプライアンスが AWSに接続できるようにします。

ネットワークアドレスを設定するには

1. [Configure Network] を選択して、`Enter` キーを押します。[Configure Network] 画面で、次のように表示されます。
   ハードウェアアプライアンスコンソールの [Configure Network] 画面。

ハードウェアアプライアンスコンソールの [Configure Network] 画面。

2. IP アドレス には、次のいずれかのソースから有効なIPv4アドレスを入力します。

   - Dynamic Host Configuration Protocol (DHCP) サーバーによって物理ネットワークポートに割り当てられたIPv4アドレスを使用します。

     その場合は、このIPv4アドレスを後でアクティベーションステップで使用するためにメモしておきます。

   - 静的IPv4アドレスを割り当てます。これを行うには、em1 セクションの [Static] (静的) を選択し、Enter を押して、以下のような [Configure Static IP] (静的 IP の設定) 画面を表示します。

     em1 セクションは、ポート設定グループの左上のセクションにあります。

   有効なIPv4住所を入力したら、 Down arrowまたは を押しますTab。

> **Note**
>
> この手順を使用して、冗長性のために em1 に加えて他のネットワークインターフェイスを設定できます。他のインターフェイスを設定する場合は、要件にリストされているエンドポイントへの AWS 同じ常時オン接続を提供する必要があります。
> ネットワークボンディングとリンク集約制御プロトコル (LACP) は、ハードウェアアプライアンスまたは Storage Gateway ではサポートされていません。
> サブネットに複数のネットワークインターフェイスを設定することはお勧めしません。これにより、ルーティングの問題が発生する可能性があるためです。

ハードウェアアプライアンスコンソールNICは、静的 IP 画面に設定します。

ハードウェアアプライアンスコンソールNICは、静的 IP 画面に設定します。

3. [Subnet] で有効なサブネットマスクを入力し、Down arrow キーを押します。
4. ゲートウェイ で、ネットワークゲートウェイのIPv4アドレスを入力し、 を押しますDown arrow。

5. にはDNS1、ドメインネームサービス (DNS) サーバーのIPv4アドレスを入力し、 を押しますDown arrow。
6. (オプション) に DNS22 番目のIPv4アドレスを入力し、 を押しますDown arrow。2 つ目のDNSサーバーの割り当てにより、1 つ目のDNSサーバーが使用できなくなった場合に追加の冗長性が提供されます。
7. 保存 を選択し、 Enterを押してアプライアンスの静的IPv4アドレス設定を保存します。

ハードウェアコンソールからログアウトするには

1. [Back] を選択して、メイン画面に戻ります。
2. [Logout] を選択して、ログイン画面に戻ります。

次のステップ

ハードウェアアプライアンスのアクティブ化

ハードウェアアプライアンスのアクティブ化

IP アドレスを設定したら、 AWS Storage Gateway コンソールのハードウェアページにこの IP アドレスを入力して、ハードウェアアプライアンスをアクティブ化します。アクティベーションプロセスにより、ハードウェアアプライアンスが適切なセキュリティ認証情報を備えていることを検証して、アプライアンスを AWS アカウントに登録します。

ハードウェアアプライアンスは、サポートされている任意の でアクティブ化できます AWS リージョン。サポートされている のリストについては AWS リージョン、「」のStorage Gateway ハードウェアアプライアンスリージョン」を参照してくださいAWS 全般のリファレンス。

ストレージゲートウェイハードウェアアプライアンスをアクティブ化するには

1. AWS Storage Gateway 管理コンソールを開き、ハードウェアをアクティブ化するためのアカウント認証情報を使用してサインインします。

> **Note**
>
> アクティベーションを行う場合のみは、次の条件が満たされている必要があります。
>
> - ブラウザは、ハードウェアアプライアンスと同じネットワーク上になければなりません。

- ファイアウォールは、インバウンドトラフィックのアプライアンスへのポート 8080 でのHTTPアクセスを許可する必要があります。

2. ページの左側のナビゲーションメニューから [ハードウェア] を選択します。
3. [アプライアンスをアクティブ化] を選択します。
4. [IP アドレス] には、ハードウェアアプライアンスに設定した IP アドレスを入力し、[接続] を選択します。

   IP アドレス設定の詳細については、「ネットワークパラメータの設定」を参照してください。
5. [名前] に、ハードウェアアプライアンスの名前を入力します。255 文字以内で名前を指定します。スラッシュ文字を含むことはできません。
6. [ハードウェアアプライアンスのタイムゾーン] には、ゲートウェイのほとんどのワークロードが生成されるローカルタイムゾーンを入力し、[次へ] を選択します。

   タイムゾーンは、ハードウェアの更新を行う時間を制御します。更新を実行するためのデフォルトの予定時間として、午前 2 時が使用されます。タイムゾーンが適切に設定されていれば、更新はデフォルトで現地の業務時間外に行われるのが理想的です。
7. [ハードウェアアプライアンスの詳細] セクションのアクティブ化パラメータを確認します。必要に応じて、[前へ] を選択して前に戻り、変更を行います。それ以外の場合は、[アクティブ化] を選択してアクティブ化を終了します。

[ハードウェアアプライアンスの概要] ページにバナーが表示され、ハードウェアアプライアンスが正常にアクティブ化されたことがわかります。

これで、アプライアンスはアカウントに関連付けられました。次のステップでは、新しいアプライアンスで S3 ファイルゲートウェイ、FSxファイルゲートウェイ、テープゲートウェイ、またはボリュームゲートウェイを設定して起動します。

次のステップ

ゲートウェイの作成

ゲートウェイの作成

ハードウェアアプライアンスで S3 ファイルゲートウェイ、FSxファイルゲートウェイ、テープゲートウェイ、またはボリュームゲートウェイを作成できます。

ハードウェアアプライアンスでゲートウェイを作成するには

1. にサインイン AWS Management Console し、ホーム で Storage Gateway https://console.aws.amazon.com/storagegateway/コンソールを開きます。
2. [ハードウェア] を選択します。
3. ゲートウェイを作成したいアクティブ化済みのハードウェアアプライアンスを選択し、[ゲートウェイの作成] を選択します。
4. 「ゲートウェイを作成する」で説明されている手順に従って、選択したゲートウェイタイプをセットアップ、接続、設定します。

Storage Gateway コンソールでゲートウェイを作成し終わると、ハードウェアアプライアンスへの Storage Gateway ソフトウェアのインストールが自動的に開始します。ゲートウェイが、コンソール上で [オンライン] と表示されるまで、5 ~ 10 分かかることがあります。

インストールされたゲートウェイに静的 IP アドレスを割り当てるためには、この次に、ゲートウェイのネットワークインターフェイスを設定して、それをアプリケーションが使用できるようにします。

次のステップ

ゲートウェイの IP アドレスの設定

ゲートウェイの IP アドレスの設定

ハードウェアアプライアンスをアクティブ化する前に、その物理ネットワークインターフェイスに IP アドレスを割り当てました。アプライアンスをアクティブ化し、そのアプライアンス上で Storage Gateway を起動したら、今度は、そのハードウェアアプライアンス上で実行される Storage Gateway 仮想マシンに別の IP アドレスを割り当てる必要があります。ハードウェアアプライアンスにインストールされたゲートウェイに静的 IP アドレスを割り当てるには、そのゲートウェイのローカルコンソールから IP アドレスを設定します。アプリケーション (NFSやSMBクライアント、iSCSI イニシエータなど) はこの IP アドレスに接続します。ハードウェアアプライアンスのコンソールから、ゲートウェイのローカルコンソールにアクセスできます。

アプライアンスの IP アドレスを設定してアプリケーションで動作するようにするには

1. ハードウェアコンソールで、[Open Service Console] を選択し、ゲートウェイのローカルコンソールのログイン画面を開きます。

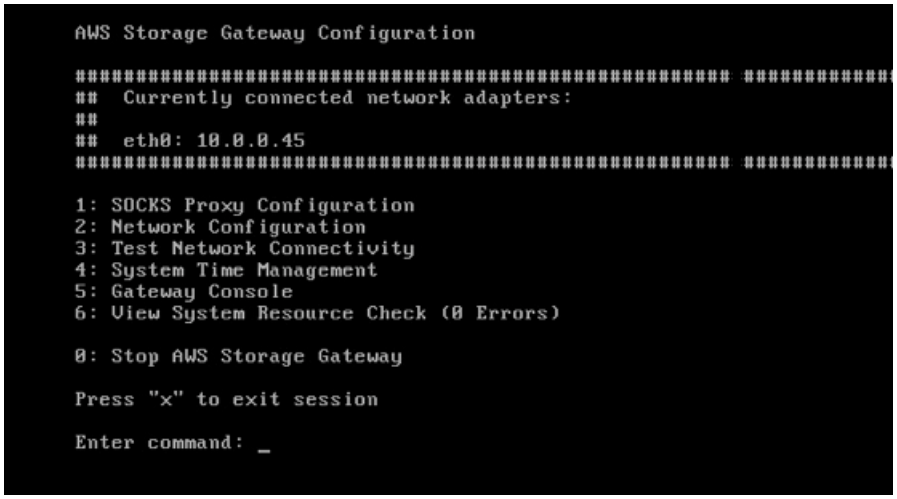
2. localhost のログインパスワードを入力し、Enter キーを押します。

   デフォルトのアカウントは admin で、デフォルトのパスワードは password です。

3. デフォルトパスワードを変更します。[Actions (アクション)]、[Set Local Password (ローカルパスワードの設定)] の順に選択し、[Set Local Password (ローカルパスワードの設定)] ダイアログボックスに、新しい認証情報を入力します。

4. (オプション) プロキシ設定の構成 手順については、「the section called “Storage Gateway コンソールからのローカルコンソールパスワードの設定”」を参照してください。

5. 次に示すように、ゲートウェイのローカルコンソールの [Network Settings] ページに移動します。
   ゲートウェイのローカルコンソールの設定ページ。ネットワーク設定などのオプションが表示されています。



   ゲートウェイのローカルコンソールの設定ページ。ネットワーク設定などのオプションが表示されています。

6. 2 と入力すると、次に示すように [Network Configuration] ページに移動します。
   DHCP および静的 IP オプションを含むゲートウェイローカルコンソールのネットワーク設定ページ。

DHCP および静的 IP オプションを含むゲートウェイローカルコンソールのネットワーク設定ページ。

7. アプリケーション用のファイル、ボリューム、テープゲートウェイを表示するように、ハードウェアアプライアンスのネットワークポートの静的アドレスまたは DHCP IP アドレスを設定します。この IP アドレスは、ハードウェアアプライアンスのアクティベーション中に使用された IP アドレスと同じサブネット上になければなりません。

ゲートウェイのローカルコンソールを終了するには

- `Crtl+]` (括弧閉) のキーストロークを入力します。ハードウェアコンソールが表示されます。

> **Note**
>
> このキーストロークは、ゲートウェイのローカルコンソールを終了する唯一の方法です。

次のステップ

ゲートウェイの設定

ゲートウェイの設定

ハードウェアアプライアンスのアクティベーションと設定が行われると、アプライアンスがコンソールに表示されます。次に、必要なタイプのゲートウェイを作成できます。該当するゲートウェイタイプの [ゲートウェイを設定] ページでインストールを続行します。手順については、「ボリュームゲートウェイを設定する」を参照してください。

ハードウェアアプライアンスからのゲートウェイの削除

ハードウェアアプライアンスからゲートウェイソフトウェアを削除するには、次の手順を実行します。これを実行すると、ハードウェアアプライアンスからゲートウェイソフトウェアがアンインストールされます。

ハードウェアアプライアンスからゲートウェイを削除するには

1. Storage Gateway コンソールの [ハードウェア] ページで、削除対象のハードウェアアプライアンスを選択します。

2. [アクション] で [ゲートウェイの削除] を選択します。確認のダイアログボックスが表示されます。
3. 指定したハードウェアアプライアンスからゲートウェイソフトウェアを削除することを確認し、確認ボックスに「remove」と入力して [削除] を選択します。

> **Note**
>
> ゲートウェイソフトウェアを削除した後で、その操作を元に戻すことはできません。特定のゲートウェイタイプでは、削除されたデータ、特にキャッシュされたデータが失われる場合があります。ゲートウェイの削除の詳細については、「ゲートウェイの削除と関連リソースの削除」を参照してください。

ゲートウェイを削除しても、ハードウェアアプライアンスはコンソールから削除されません。ハードウェアアプライアンスは、今後のゲートウェイのデプロイに使用できます。

ハードウェアアプライアンスの削除

既にアクティブ化した Storage Gateway ハードウェアアプライアンスが不要になった場合は、 AWS アカウントからアプライアンスを完全に削除できます。

> **Note**
>
> アプライアンスを別の AWS アカウントまたは に移動するには AWS リージョン、まず次の手順を使用してアプライアンスを削除し、ゲートウェイのサポートチャネルを開き、 AWS Support に連絡してソフトリセットを実行する必要があります。詳細については、ホストされているゲートウェイのトラブルシューティングに役立つ AWS Support アクセスを有効にする」を参照してください。

ハードウェアアプライアンスを削除するには

1. ゲートウェイをハードウェアアプライアンスにインストールしている場合は、アプライアンスを削除する前に、まずゲートウェイを削除する必要があります。ハードウェアアプライアンスからゲートウェイを削除する方法については、「ハードウェアアプライアンスからのゲートウェイの削除」を参照してください。
2. Storage Gateway コンソールの [ハードウェア] ページで、削除対象のハードウェアアプライアンスを選択します。

3. [アクション] で、[アプライアンスの削除] を選択します。確認のダイアログボックスが表示されます。
4. 指定したハードウェアアプライアンスを削除することを確認し、確認ボックスに「delete」と入力して [削除] を選択します。

   ハードウェアアプライアンスを削除すると、そのアプライアンスにインストールされているゲートウェイに関連付けられているリソースもすべて削除されますが、ハードウェアアプライアンス自体のデータは削除されません。

ゲートウェイを作成する

このページの概要トピックでは、Storage Gateway の作成プロセスについて概説しています。Storage Gateway コンソールを使用して特定のタイプのゲートウェイを作成する step-by-step 手順については、「Creating a Volume Gateway」を参照してください。

概要 - ゲートウェイのアクティブ化

ゲートウェイのアクティベーションには、ゲートウェイのセットアップ、 への接続 AWS、設定の確認、アクティブ化が含まれます。

ゲートウェイをセットアップする

Storage Gateway をセットアップするには、まず、作成するゲートウェイのタイプと、ゲートウェイ仮想アプライアンスを実行するホストプラットフォームを選択します。次に、選択したプラットフォーム用のゲートウェイ仮想アプライアンステンプレートをダウンロードし、オンプレミス環境にデプロイします。Storage Gateway は、優先リセラーに注文する物理ハードウェアアプライアンスとして、または AWS クラウド環境の Amazon EC2インスタンスとしてデプロイすることもできます。ゲートウェイアプライアンスをデプロイするときは、仮想ホストにローカルの物理ディスク容量を割り当てます。

に接続する AWS

次のステップでは、ゲートウェイを AWSに接続します。これを行うには、まずゲートウェイ仮想アプライアンスとクラウド内のサービス間の通信に使用する AWS サービスエンドポイントのタイプを選択します。このエンドポイントには、パブリックインターネットからVPC、またはネットワークセキュリティ設定を完全に制御できる Amazon 内からのみアクセスできます。次に、ゲートウェイの IP アドレスまたはアクティベーションキーを指定します。これらは、ゲートウェイアプライアンスのローカルコンソールに接続することで取得できます。

確認してアクティブ化する

この時点で、選択したゲートウェイと接続のオプションを確認し、必要に応じて変更することができます。すべてが意図したとおりにセットアップされたら、ゲートウェイをアクティブ化できます。アクティブ化したゲートウェイを使い始める前に、いくつかの追加設定を行い、ストレージリソースを作成する必要があります。

概要 - ゲートウェイの設定

Storage Gateway をアクティブ化したら、追加の設定をいくつか行う必要があります。このステップでは、ゲートウェイホストプラットフォームでプロビジョニングした物理ストレージを、ゲートウェイアプライアンスがキャッシュまたはアップロードバッファとして使用するように割り当てます。次に、Amazon CloudWatch Logs と CloudWatch アラームを使用してゲートウェイの状態をモニタリングできるように設定し、必要に応じてゲートウェイを識別するためのタグを追加します。アクティブ化と設定が済んだゲートウェイを使い始める前に、ストレージリソースを作成する必要があります。

概要 - ストレージリソース

Storage Gateway をアクティブ化して設定したら、そのゲートウェイで使用するクラウドストレージリソースを作成する必要があります。作成したゲートウェイのタイプに応じて、Storage Gateway コンソールを使用して、ボリューム、テープ、Amazon S3 または Amazon FSx ファイル共有を作成して関連付けます。各ゲートウェイタイプは、それぞれのリソースを使用して、関連するタイプのネットワークストレージインフラストラクチャをエミュレートし、書き込まれたデータを AWS クラウドに転送します。

ボリュームゲートウェイの作成

このセクションでは、ボリュームゲートウェイを作成し、使用する手順を説明します。

トピック

- ゲートウェイの作成
- ボリュームの作成
- ボリュームの使用
- ボリュームのバックアップ

ゲートウェイの作成

このセクションでは、ボリュームゲートウェイをダウンロード、デプロイ、およびアクティブ化する手順を説明します。

トピック

- ボリュームゲートウェイをセットアップする

- ボリュームゲートウェイを AWSに接続する
- 設定を確認してボリュームゲートウェイをアクティブ化する
- ボリュームゲートウェイを設定する

ボリュームゲートウェイをセットアップする

新しいボリュームゲートウェイをセットアップするには

1. https://console.aws.amazon.com/storagegateway/home/ AWS Management Console で を開き、ゲートウェイを作成する AWS リージョン を選択します。
2. [ゲートウェイの作成] を選択して、[ゲートウェイのセットアップ] ページを開きます。
3. [ゲートウェイの設定] セクションで、次の操作を行います。

   a. [ゲートウェイ名] に、ゲートウェイの名前を入力します。この名前を検索して、Storage Gateway コンソールのリストページでゲートウェイを見つけることができます。

   b. [ゲートウェイのタイムゾーン] では、ゲートウェイをデプロイしたい地域のローカルタイムゾーンを選択します。
4. [ゲートウェイのオプション] セクションの [ゲートウェイタイプ] で [ボリュームゲートウェイ] を選択し、ゲートウェイが使用するボリュームタイプを選択します。次のオプションから選択できます。

   - キャッシュボリューム - プライマリデータを Amazon S3 に保存し、アクセス頻度の高いデータは、すぐにアクセスできるようにローカルのキャッシュに保持しておきます。
   - 保管型ボリューム - データをすべてローカルに保存し、Amazon S3 にも非同期でバックアップします。このボリュームタイプを使用するゲートウェイは、Amazon EC2 にデプロイできません。
5. [プラットフォームオプション] セクションで、次の操作を行います。

   a. [ホストプラットフォーム] では、ゲートウェイをデプロイするプラットフォームを選択し、Storage Gateway コンソールページに表示されるプラットフォーム固有の指示に従ってホストプラットフォームを設定します。次のオプションから選択できます。

      - VMware ESXi - VMware ESXi を使用して、ゲートウェイ仮想マシンをダウンロード、デプロイ、設定します。
      - Microsoft Hyper-V - Microsoft Hyper-V を使用して、ゲートウェイ仮想マシンをダウンロード、デプロイ、設定します。

- Linux KVM - Linux KVM を使用して、ゲートウェイ仮想マシンをダウンロード、デプロイ、設定します。
- Amazon EC2 - ゲートウェイをホストするように Amazon EC2 インスタンスを設定し、起動します。このオプションは、[保管型ボリューム] のゲートウェイでは使用できません。
- ハードウェアアプライアンス - ゲートウェイをホスト AWS するために、 から専用の物理ハードウェアアプライアンスを注文します。

b. [ゲートウェイのセットアップの確認] で、選択したホストプラットフォームのデプロイ手順を実行したことを確認するチェックボックスを選択します。この手順は、[ハードウェアアプライアンス] ホストプラットフォームには適用されません。

6. [Next] (次へ) をクリックして先に進みます。

ゲートウェイがセットアップされたので、接続方法と との通信方法を選択する必要がありますAWS。手順については、「ボリュームゲートウェイを に接続する AWS」を参照してください。

ボリュームゲートウェイを AWSに接続する

新しいボリュームゲートウェイを に接続するには AWS

1. 「ボリュームゲートウェイをセットアップする」で説明されている手順をまだ実行していない場合は、実行します。終了したら、[次へ] を選択して、Storage Gateway コンソールの [AWSに接続] ページを開きます。
2. 「エンドポイントオプション」セクションの「サービスエンドポイント」で、ゲートウェイがとの通信に使用するエンドポイントのタイプを選択します AWS。次のオプションから選択できます。

   - パブリックアクセス可能 - ゲートウェイはパブリックインターネット AWS 経由で と通信します。このオプションを選択する場合は、[FIPS が有効なエンドポイント] チェックボックスを使用して、接続が連邦情報処理規格 (FIPS) に準拠する必要があるかどうかを指定します。

     > **Note**
     >
     > コマンドラインインターフェイスまたは API AWS を介して 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 準拠のエンドポイントを使用します。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。

FIPS のサービスエンドポイントは、一部の AWS リージョンでのみ使用できます。詳細については、「AWS 全般のリファレンス」の「Storage Gateway エンドポイントとクォータ」を参照してください。

- ホストされた VPC - ゲートウェイは VPC とのプライベート接続を介して AWS と通信するため、ネットワーク設定を制御できます。このオプションを選択する場合は、ドロップダウンメニューから VPC エンドポイント ID を選択するか、VPC エンドポイントの DNS 名または IP アドレスを指定して、既存の VPC エンドポイントを指定する必要があります。

3. [ゲートウェイ接続オプション] セクションの [接続オプション] で、 AWSに対してゲートウェイを識別する方法を選択します。次のオプションから選択できます。

   - IP アドレス - ゲートウェイの IP アドレスを、対応するフィールドに入力します。この IP アドレスは、公開アドレス、または現在のネットワーク内からアクセス可能なアドレスにする必要があります。また、ウェブブラウザから接続できる必要があります。

     ゲートウェイの IP アドレスは、ハイパーバイザークライアントからゲートウェイのローカルコンソールにログインするか、Amazon EC2 インスタンスの詳細ページからコピーすることで取得できます。

   - アクティベーションキー - ゲートウェイのアクティベーションキーを、対応するフィールドに入力します。アクティベーションキーは、ゲートウェイのローカルコンソールを使用して生成できます。ゲートウェイの IP アドレスを使用できない場合は、このオプションを選択してください。

4. [Next] (次へ) をクリックして先に進みます。

ゲートウェイを に接続する方法を選択したら AWS、ゲートウェイをアクティブ化する必要があります。手順については、「設定を確認してボリュームゲートウェイをアクティブ化する」を参照してください。

設定を確認してボリュームゲートウェイをアクティブ化する

新しいボリュームゲートウェイをアクティブ化するには

1. 次のトピックで説明されている手順をまだ実行していない場合は、実行します。

   - ボリュームゲートウェイをセットアップする
   - ボリュームゲートウェイを に接続する AWS

終了したら、[次へ] を選択して、Storage Gateway コンソールの [確認およびアクティブ化] ページを開きます。

2. ページの各セクションで、初期ゲートウェイの詳細を確認します。
3. セクションにエラーがある場合は、[編集] を選択して、対応する設定ページに戻って適宜変更します。

> **Note**
>
> ゲートウェイを作成した後で、ゲートウェイオプションや接続設定を変更することはできません。

4. [アクティブゲートウェイ] を選択して、先に進みます。

ゲートウェイのアクティブ化はこれで完了です。次は、初回設定を行い、ローカルストレージディスクを割り当て、ログ記録を設定する必要があります。手順については、「ボリュームゲートウェイを設定する」を参照してください。

ボリュームゲートウェイを設定する

新しいボリュームゲートウェイで初回の設定を行うには

1. 次のトピックで説明されている手順をまだ実行していない場合は、実行します。

   - ボリュームゲートウェイをセットアップする
   - ボリュームゲートウェイを に接続する AWS
   - 設定を確認してボリュームゲートウェイをアクティブ化する

   終了したら、[次へ] を選択して、Storage Gateway コンソールの [ゲートウェイの設定] ページを開きます。

2. [ストレージの設定] セクションで、ドロップダウンメニューを使用して、容量が 165 GiB 以上のディスクを少なくとも 1 つキャッシュストレージに割り当て、容量が 150 GiB 以上のディスクを少なくとも 1 つアップロードバッファに割り当てます。このセクションに表示されるローカルディスクは、ホストプラットフォームでプロビジョニングされている物理ストレージに対応しています。

3. CloudWatch ロググループセクションで、ゲートウェイの状態をモニタリングするように Amazon CloudWatch Logs を設定する方法を選択します。次のオプションから選択できます。

   - 新しいロググループの作成 - ゲートウェイをモニタリングするための新しいロググループを設定します。
   - 既存のロググループの使用 - 対応するドロップダウンメニューから既存のロググループを選択します。
   - ログ記録の無効化 - Amazon CloudWatch Logs を使用してゲートウェイをモニタリングしないでください。

   > **Note**
   >
   > Storage Gateway のヘルスログを受信するには、ロググループリソースポリシーに次のアクセス許可が存在する必要があります。*############*を、デプロイの特定のロググループ resourceArn 情報に置き換えます。
   >
   > ```
   > "Sid": "AWSLogDeliveryWrite20150319",
   >       "Effect": "Allow",
   >       "Principal": {
   >         "Service": [
   >           "delivery.logs.amazonaws.com"
   >         ]
   >       },
   >       "Action": [
   >         "logs:CreateLogStream",
   >         "logs:PutLogEvents"
   >       ],
   >       "Resource": "arn:aws:logs:eu-west-1:1234567890:log-group:/foo/bar:log-stream:*"
   > ```
   >
   > 「リソース」要素は、アクセス許可を個々のロググループに明示的に適用する場合にのみ必要です。

4. CloudWatch アラームセクションで、ゲートウェイメトリクスが定義された制限から逸脱したときに通知するように Amazon CloudWatch アラームを設定する方法を選択します。次のオプションから選択できます。

- Storage Gateway の推奨アラームを作成する – ゲートウェイの作成時に、すべての推奨 CloudWatch アラームを自動的に作成します。推奨されるアラームの詳細については、「アラームについて CloudWatch 」を参照してください。

  > **Note**
  >
  > この機能には、事前設定された Storage Gateway フルアクセス CloudWatch ポリシーの一部として自動的に付与されないポリシー許可が必要です。推奨 CloudWatch アラームを作成する前に、セキュリティポリシーで次のアクセス許可が付与されていることを確認してください。
  >
  > - `cloudwatch:PutMetricAlarm` - アラームを作成する
  > - `cloudwatch:DisableAlarmActions` - アラームアクションをオフにする
  > - `cloudwatch:EnableAlarmActions` - アラームアクションをオンにする
  > - `cloudwatch:DeleteAlarms` - アラームを削除する

- カスタムアラームの作成 – ゲートウェイのメトリクスを通知する新しい CloudWatch アラームを設定します。アラームの作成 を選択してメトリクスを定義し、Amazon CloudWatch コンソールでアラームアクションを指定します。手順については、「Amazon ユーザーガイド」の「Amazon CloudWatch アラームの使用」を参照してください。 CloudWatch
- アラームなし – ゲートウェイのメトリクスに関する通知は受信 CloudWatchしません。

5. (オプション) [タグ] セクションで [新しいタグを追加] を選択し、Storage Gateway ゲートウェイコンソールのリストページでゲートウェイを検索およびフィルタリングしやすくするためのキーと値のペアを入力します。大文字と小文字は区別されます。この手順を繰り返し、必要な数だけタグを追加します。
6. [設定] を選択して、ゲートウェイの作成を完了します。

   新しいゲートウェイのステータスを確認するには、Storage Gateway の [ゲートウェイの概要] ページでゲートウェイを検索してください。

ゲートウェイの作成はこれで完了です。次は、ゲートウェイで使用するボリュームを作成する必要があります。手順については、「ボリュームの作成」を参照してください。

ボリュームの作成

これまでは、VM のキャッシュストレージとアップロードバッファに追加したローカルディスクが割り当てられました。ここでは、アプリケーションがデータを読み書きするストレージボリュームを作成します。ゲートウェイでは、キャッシュストレージ内で最近ローカルにアクセスされたボリュームのデータ、および Amazon S3 に非同期で転送されたデータが保持されます。保管型ボリュームの場合、VM アップロードバッファとアプリケーションのデータに追加したローカルディスクが割り当てられました。

> **Note**
>
> AWS Key Management Service （ AWS KMS) を使用して、Amazon S3 に保存されているキャッシュ型ボリュームに書き込まれたデータを暗号化できます。現在、この暗号化には AWS Storage Gateway API リファレンス を使用できます。詳細については、「CreateCachediSCSIVolume」または「」を参照してくださいcreate-cached-iscsi-volume。

ボリュームを作成するには

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. Storage Gateway コンソールで、[Create volume] (ボリュームの作成) を選択します。
3. [ボリュームの作成] ダイアログボックスで、[ゲートウェイ] 用のゲートウェイを選択します。
4. キャッシュ型ボリュームの場合、[Capacity] (キャパシティー) にキャパシティーを入力します。

   保管型ボリュームの場合、リストから [ディスク ID] 値を選択します。
5. [Volume content] (ボリュームの内容) は、ボリュームを作成しているゲートウェイの種類に応じて選択します。

   キャッシュ型ボリュームの場合、次のオプションがあります:

   - 新しい空のボリュームを作成します。
   - Amazon EBS スナップショットに基づいてボリュームを作成します。このオプションを選択する場合は、[EBS スナップショット ID] の値を指定します。

> **Note**
>
> Storage Gateway では、 AWS Marketplace ボリュームのスナップショットから キャッシュ型ボリュームを作成することはできません。

- 最後のボリューム復元ポイントからのクローン。このオプションを選択するときは、[ソースボリューム] のボリューム ID を選択します。リージョンにボリュームがない場合、このオプションは表示されません。

保管型ボリュームの場合、次のオプションがあります。

- 新しい空のボリュームを作成します。
- スナップショットに基づいたボリュームを作成します。このオプションを選択する場合は、[EBS スナップショット ID] の値を指定します。
- ディスクに既存データを保持

6. [iSCSI target name] (iSCSI ターゲット名) に名前を入力します。

   ターゲット名には、小文字、数字、ピリオド (.) およびハイフン (-) を含めることができます。このターゲット名は検出後、[iSCSI Microsoft initiator] UI の [Targets] タブに、[iSCSI target node] として表示されます。たとえば、名前 `target1` は `iqn.1007-05.com.amazon:target1` のように表示されます。そのターゲット名がストレージエリアネットワーク (SAN) 内でグローバルに一意であることを確認します。

7. [ネットワークインターフェイス] 設定の IP アドレスが選択済みであることを確認します。または [ネットワークインターフェイス] の IP アドレスを選択します。[ネットワークインターフェイス] で、1 つの IP アドレスが、ゲートウェイ VM に対して設定された各アダプタに対して表示されます。ゲートウェイ VM が 1 つのネットワークアダプタにのみ設定されている場合、存在する IP アドレスは 1 つのみであるため、この [ネットワークインターフェイス] リストは表示されません。

   iSCSI ターゲットが選択したネットワークアダプタで使用できるようになります。

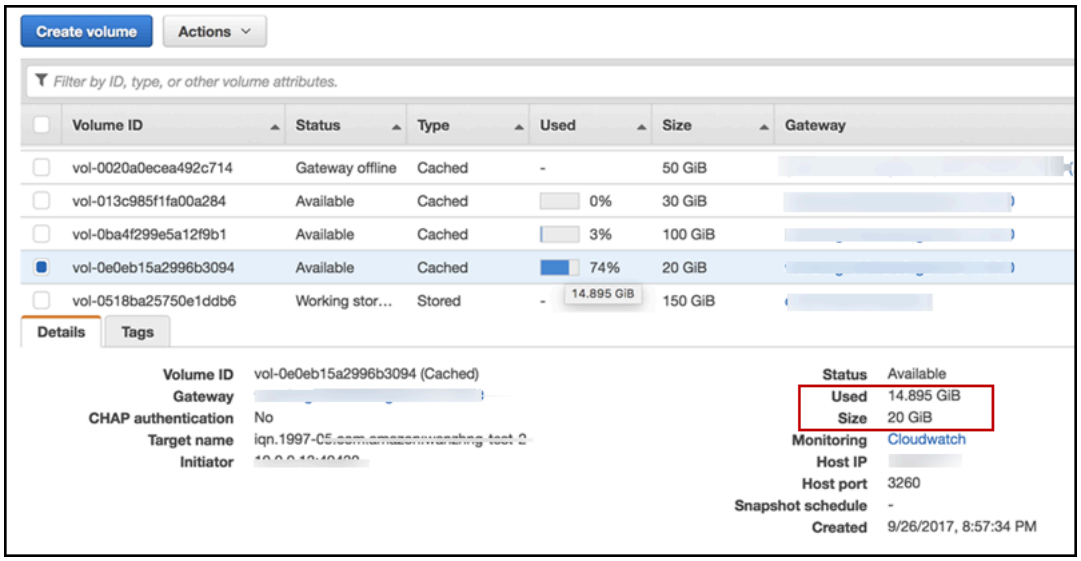
   複数のネットワークアダプタを使用するようにゲートウェイを定義した場合、ボリュームにアクセスするためにストレージアプリケーションが使用する IP アドレスを選択します。複数のネットワークアダプタを設定する方法の詳細については、「ゲートウェイを複数の に設定する NICs」を参照してください。

> **Note**
>
> ネットワークアダプタを選択した後、この設定を変更することはできません。

8. (オプション) [タグ] で、キーと値を入力して、ボリュームにタグを追加します。タグは、ボリュームの管理、フィルタリング、検索に便利な、大文字と小文字の区別があるキーと値のペアです。
9. [Create volume] (ボリュームの作成) を選択します。

   このリージョンで以前に作成したボリュームがある場合は、Storage Gateway コンソールに表示されます。

   [CHAP 認証の設定] ダイアログボックスが表示されます。この時点でボリュームにチャレンジハンドシェイク認証プロトコル (CHAP) を設定できますが、[Cancel] (キャンセル) を選択して、後で設定することもできます。CHAP の設定についての詳細は、「ボリューム用の CHAP 認証の設定」を参照してください。



CHAP を設定しない場合は、ボリュームの使用を開始します。詳細については、「ボリュームの使用」を参照してください。

ボリューム用の CHAP 認証の設定

CHAP は、ストレージボリュームターゲットへのアクセスが試みられる際に認証を要求することによって、プレイバック攻撃に対する保護を提供します。[CHAP 認証の設定] ダイアログボックスで、ボリュームに対して CHAP を設定するための情報を指定します。

CHAP を設定するには

1. CHAP を設定するボリュームを選択します。
2. [アクション] メニューで、[CHAP 認証の設定] を選択します。
3. [Initiator Name] (イニシエータ名) に、イニシエータの名前を入力します。
4. [Initiator secret] (イニシエータのシークレット) で、iSCSI イニシエータの認証に使用した秘密のフレーズを入力します。
5. [Target secret] (ターゲットのシークレット) で、相互 CHAP のターゲットの認証に使用した秘密のフレーズを入力します。
6. [Save] を選択してエントリを保存します。

   CHAP の認証の設定の詳細については、「iSCSI ターゲットのCHAP認証の設定」を参照してください。

次のステップ

ボリュームの使用

ボリュームの使用

ボリュームを使用する方法に関する手順を以下で確認できます。ボリュームを使用するには、まず iSCSI ターゲットとしてクライアントに接続してから、初期化してフォーマットします。

トピック

クライアントへのボリュームの接続

クライアントで iSCSI イニシエータを使用してボリュームに接続します。以下の手順の最後に、ボリュームが クライアントのローカルデバイスとして使用可能になります。

> **Important**
>
> Storage Gateway では、ホストが Windows Server フェイルオーバークラスタリング () を使用してアクセスを調整する場合、複数のホストを同じボリュームに接続できますWSFC。クラスター化されていない NTFS/ext4 ファイルシステムを共有するなどWSFC、 を使用せずに複数のホストを同じボリュームに接続することはできません。

トピック

- Microsoft Windows クライアントへの接続
- Red Hat Enterprise Linux クライアントへの接続

Microsoft Windows クライアントへの接続

以下の手順は、Windows クライアントに接続するために従うステップの概要を示しています。詳細については、「iSCSI イニシエーターの接続」を参照してください。

Windows クライアントに接続するには

1. iscsicpl.exe を開始します。
2. iSCSI Initiator Properties ダイアログボックスで、Discovery タブを選択し、Discovery Portal を選択します。
3. 「ターゲットポータルの検出」ダイアログボックスで、IP アドレスまたはDNS名前に iSCSI ターゲットの IP アドレスを入力します。
4. ゲートウェイのストレージボリュームターゲットに新しいターゲットポータルを接続します。
5. ターゲットを選択し、[接続] を選択します。
6. [ターゲット] タブで、ターゲットのステータスが、ターゲットが接続されていることを示す値 [Connected (接続済み)] であることを確認し、[OK] を選択します。

Red Hat Enterprise Linux クライアントへの接続

次の手順は、Red Hat Enterprise Linux (RHEL) クライアントに接続するために実行する手順の概要を示しています。詳細については、「iSCSI イニシエーターの接続」を参照してください。

Linux クライアントを iSCSI ターゲットに接続するには

1. iscsi-initiator-utils RPM パッケージをインストールします。

パッケージをインストールするには、以下のコマンドを使用できます。

```
sudo yum install iscsi-initiator-utils
```

2. iSCSI デーモンが実行されていることを確認します。

   5 RHEL または 6 の場合は、次のコマンドを使用します。

   ```
   sudo /etc/init.d/iscsi status
   ```

   7 RHEL の場合は、次のコマンドを使用します。

   ```
   sudo service iscsid status
   ```

3. ゲートウェイに定義されているボリュームまたはVTLデバイスターゲットを検出します。次の検出コマンドを使用します。

   ```
   sudo /sbin/iscsiadm --mode discovery --type sendtargets --portal [GATEWAY_IP]:3260
   ```

   discovery コマンドの出力は、次の出力例のようになります。

   ボリュームゲートウェイの場合: *[GATEWAY_IP]*:3260, 1
   iqn.1997-05.com.amazon:myvolume

   テープゲートウェイの場合: iqn.1997-05.com.amazon:*[GATEWAY_IP]*-tapedrive-01

4. ターゲットに接続します。

   必ず正しい を指定してください。*[GATEWAY_IP]* connect コマンドIQNの および 。

   以下のコマンドを使用します。

   ```
   sudo /sbin/iscsiadm --mode node --targetname
    iqn.1997-05.com.amazon:[ISCSI_TARGET_NAME] --portal [GATEWAY_IP]:3260,1 --login
   ```

5. ボリュームがクライアントマシン (イニシエータ) にアタッチされていることを確認します。そのためには、次のコマンドを使用します。

   ```
   ls -l /dev/disk/by-path
   ```

コマンドの出力は、次の出力例のようになります。

```
lrwxrwxrwx. 1 root root 9 Apr 16 19:31 ip-[GATEWAY_IP]:3260-iscsi-
iqn.1997-05.com.amazon:myvolume-lun-0 -> ../../sda
```

イニシエータをセットアップした後、「」で説明されているように iSCSI 設定をカスタマイズすることを強くお勧めしますLinux iSCSI 設定のカスタマイズ。

ボリュームの初期化とフォーマット

クライアントで iSCSI イニシエータを使用してボリュームに接続したら、ボリュームを初期化してフォーマットします。

トピック

- Microsoft Windows でのボリュームの初期化とフォーマット
- Red Hat Enterprise Linux でのボリュームの初期化とフォーマット

Microsoft Windows でのボリュームの初期化とフォーマット

Windows でボリュームを初期化してフォーマットするには、次の手順を使用します。

ストレージボリュームを初期化してフォーマットするには

1. **diskmgmt.msc** を起動し、[Disk Management] コンソールを開きます。
2. ディスクの初期化ダイアログボックスで、ボリュームを MBR (マスターブートレコード) パーティションとして初期化します。パーティションの形式を選択する場合、接続先のボリュームのタイプ (キャッシュ型または保管型) を、次の表のように考慮する必要があります。

パーティションの形式	次の条件を使用します。
MBR (マスターブートレコード)	• ゲートウェイが保管型ボリュームで、ストレージボリュームのサイズが 1 TiB に制限されている場合。 • ゲートウェイがキャッシュ型ボリュームで、ストレージボリュームのサイズが 2 TiB 未満である場合。

パーティションの形式	次の条件を使用します。
GPT (GUID パーティションテーブル)	ゲートウェイのストレージボリュームのサイズが 2 TiB 以上ある場合。

3. シンプルボリュームの作成

   a. ボリュームをオンラインにして初期化します。使用可能なボリュームがすべて、ディスク管理コンソールに表示されます。

   b. ディスクのコンテキスト (右クリック) メニューを開き、[New Simple Volume] を選択します。

   > **Important**
   >
   > 間違ったディスクをフォーマットしないように注意してください。フォーマットするディスクのサイズが、ゲートウェイ VM に割り当てたローカルディスクのサイズと一致すること、およびそのディスクのステータスが [Unallocated] であることを確認します。

   c. 最大ディスクサイズを指定します。

   d. ドライブ文字またはパスをボリュームに割り当て、[クリックフォーマットする] を選択してボリュームをフォーマットします。

   > **Important**
   >
   > キャッシュボリュームには [クリックフォーマットする] を使用することを強くお勧めします。これにより、初期化 I/O と初期スナップショットサイズが小さくなり、使用可能なボリュームへの時間が最も高速になります。また、キャッシュボリュームスペースを使用したフルフォーマット処理を回避できます。

   > **Note**
   >
   > ボリュームのフォーマットにかかる時間は、ボリュームサイズによって異なります。このプロセスは完了までに数分かかることがあります。

Red Hat Enterprise Linux でのボリュームの初期化とフォーマット

Red Hat Enterprise Linux () でボリュームを初期化およびフォーマットするには、次の手順に従いますRHEL。

ストレージボリュームを初期化してフォーマットするには

1. ディレクトリを /dev フォルダに変更します。
2. sudo cfdisk コマンドを実行します。
3. 次のコマンドを使用して新しいボリュームを確認します。新しいボリュームを見つけるには、ボリュームのパーティションのレイアウトをリストします。

   ```
   $ lsblk
   ```

   新しい未使用のボリュームについて、「認識されないボリュームラベル」というエラーが表示されます。
4. 新しいボリュームを初期化します。パーティションの形式を選択する場合、接続先のボリュームのサイズと種類 (キャッシュ型またはゲートウェイ保管型) を、次の表のように考慮する必要があります。

パーティションの形式	次の条件を使用します。
MBR (マスターブートレコード)	• ゲートウェイが保管型ボリュームで、ストレージボリュームのサイズが 1 TiB に制限されている場合。 • ゲートウェイがキャッシュ型ボリュームで、ストレージボリュームのサイズが 2 TiB 未満である場合。
GPT (GUID パーティションテーブル)	ゲートウェイのストレージボリュームのサイズが 2 TiB 以上ある場合。

MBR パーティションの場合は、次のコマンドを使用します。 sudo parted /dev/*your volume* mklabel msdos

GPT パーティションの場合は、次のコマンドを使用します。 sudo parted /dev/*your volume* mklabel gpt

5. パーティションを作成するには、次のコマンドを使用します。

   ```
   sudo parted -a opt /dev/your volume mkpart primary file system 0% 100%
   ```

6. 次のコマンドを使用して、ドライブ文字をパーティションに割り当てて、ファイルシステムを作成します。

   ```
   sudo mkfs -L datapartition /dev/your volume
   ```

7. 次のコマンドを使用して、ファイルシステムをマウントします。

   ```
   sudo mount -o defaults /dev/your volume /mnt/your directory
   ```

ゲートウェイのテスト

次のタスクを実行して、ボリュームゲートウェイの設定をテストします。

1. ボリュームにデータを書き込む。
2. スナップショットを取得する。
3. スナップショットを別ボリュームに復元する。

ゲートウェイのセットアップを確認するには、ボリュームのスナップショットバックアップを作成し、スナップショットを に保存します AWS。次に、新しいボリュームに対してスナップショットを復元できます。ゲートウェイは、 の指定されたスナップショットから新しいボリューム AWS にデータをコピーします。

> **Note**
>
> 暗号化された Amazon Elastic Block Store (Amazon EBS) ボリュームからのデータの復元はサポートされていません。

Microsoft Windows でストレージボリュームの Amazon EBSスナップショットを作成するには

1. Windows コンピュータで、いくつかのデータをマッピングされたストレージボリュームにコピーします。

   この演習では、コピーするデータ量は問題ではありません。小さなファイルで十分に復元を確認することができます。

2. Storage Gateway コンソールのナビゲーションペインで、[Volumes] (ボリューム) を選択します。
3. ゲートウェイ用に作成したストレージボリュームを選択します。

   このゲートウェイは 1 個のストレージボリュームのみを備えている必要があります。ボリュームを選択すると、ボリュームのプロパティが表示されます。
4. アクション で、EBSスナップショットの作成 を選択してボリュームのスナップショットを作成します。

   ディスク上のデータ量およびアップロード帯域幅によっては、スナップショットが完了するのに数秒かかる場合があります。スナップショットを作成するボリュームの ID をメモします。スナップショットを見つけるには ID を使用します。
5. EBS 「スナップショットの作成」ダイアログボックスで、スナップショットの説明を入力します。
6. (オプション) [タグ] で、キーと値を入力して、スナップショットにタグを追加します。タグは、スナップショットの管理、フィルタリング、検索に便利な、大文字と小文字の区別があるキーと値のペアです。
7. [スナップショットの作成] を選択します。スナップショットは Amazon EBSスナップショットとして保存されます。スナップショット ID を書き留めます。ボリューム用に作成されたスナップショットの数はスナップショット列に表示されます。
8. EBS スナップショット列で、スナップショットを作成したボリュームのリンクを選択して、Amazon EC2コンソールでEBSスナップショットを表示します。

スナップショットを別ボリュームに復元するには

ボリュームの作成 を参照してください。

次のステップ

前のセクションでは、ゲートウェイの作成とプロビジョニングを行い、ホストをゲートウェイのストレージボリュームに接続しました。ゲートウェイの iSCSI ボリュームにデータを追加し、ボリュームのスナップショットを作成し、それを新しいボリュームに復元して、新しいボリュームに接続し、データがそれに表示されることを確認しました。

演習を終了したら、以下の点を考慮します。

- ゲートウェイを引き続き使用するのであれば、実際のワークロードに合わせてアップロードバッファのサイズを設定します。詳細については、「実際のワークロードに対する、ボリュームゲートウェイストレージのサイズ設定」を参照してください。
- ゲートウェイを引き続き使用する予定がないのであれば、料金が発生しないようにするために、ゲートウェイを削除することを検討します。詳細については、「不要なリソースのクリーンアップ」を参照してください。

本ガイドのその他のセクションには、以下の方法に関する情報が記載されています。

- ストレージボリュームとその管理方法の詳細については、「ゲートウェイを管理する」を参照してください。
- ゲートウェイの問題をトラブルシューティングする方法については、「ゲートウェイのトラブルシューティング」を参照してください。
- ゲートウェイを最適化するには、「ゲートウェイのパフォーマンスの最適化」を参照してください。
- Storage Gateway メトリクスの概要と、ゲートウェイの動作のモニタリング方法については、「Storage Gateway のモニタリング」を参照してください。
- データを保存するようにゲートウェイの iSCSI ターゲットを設定する方法の詳細については、「」を参照してくださいボリュームの Windows クライアントへの接続。

実際のワークロードに合わせたボリュームゲートウェイのストレージのサイズ設定と、不要なリソースのクリーンアップの詳細については、以下のセクションを参照してください。

実際のワークロードに対する、ボリュームゲートウェイストレージのサイズ設定

この時点では、シンプルな設定でゲートウェイが動作しています。ただし、このゲートウェイを作成するために使用した前提は、実際の作業負荷に適しているわけではありません。このゲートウェイを実際の作業負荷で使用する場合は、次の 2 つの操作を行う必要があります。

1. アップロードバッファのサイズを適切に指定します。
2. まだ行っていない場合は、アップロードバッファの監視をセットアップします。

両方のタスクを実行する方法を以下で確認できます。キャッシュ型ボリュームに対してゲートウェイをアクティブ化した場合、実際の作業負荷用にキャッシュストレージのサイズも設定する必要もあります。

ゲートウェイキャッシュ型のセットアップ用に、アップロードバッファとキャッシュストレージのサイズを設定するには

- アップロードバッファのサイズ設定では、「割り当てるアップロードバッファのサイズの決定」に示している式を使用します。アップロードバッファには、少なくとも 150 GiB を割り当てることを強くお勧めします。アップロードバッファの式で得られる値が 150 GiB 未満だったとしても、アップロードバッファには 150 GiB を割り当ててください。

  アップロードバッファ式では、アプリケーションからゲートウェイへのスループットとゲートウェイから へのスループットの差が考慮され AWS、データを書き込む期間を乗算されます。例えば、1 日 12 時間、1 秒当たり 40 MB の速度でアプリケーションがゲートウェイにテキストデータを書き込み、ネットワークのスループットが 1 秒当たり 12 MB であるとします。テキストデータに対する圧縮係数が 2:1 と仮定すると、アップロードバッファ容量には約 675 GiB を割り当てる必要があるということが式からわかります。

保管型のセットアップに対して、アップロードバッファのサイズを設定するには

- 割り当てるアップロードバッファのサイズの決定 で検討した式を使用します。アップロードバッファには、少なくとも 150 GiB を割り当てることを強くお勧めします。アップロードバッファの式で得られる値が 150 GiB 未満だったとしても、アップロードバッファには 150 GiB を割り当ててください。

  アップロードバッファ式では、アプリケーションからゲートウェイへのスループットとゲートウェイから へのスループットの差が考慮され AWS、データを書き込む期間を乗算されます。例えば、1 日 12 時間、1 秒当たり 40 MB の速度でアプリケーションがゲートウェイにテキストデータを書き込み、ネットワークのスループットが 1 秒当たり 12 MB であるとします。テキストデータに対する圧縮係数が 2:1 と仮定すると、アップロードバッファ容量には約 675 GiB を割り当てる必要があるということが式からわかります。

アップロードバッファを監視するには

1. ホーム で Storage Gateway https://console.aws.amazon.com/storagegateway/コンソールを開きます。
2. [ゲートウェイ] タブ、[詳細] タブの順に選択し、[Upload Buffer Used (使用中のアップロードバッファ)] フィールドを見つけて、ゲートウェイの現在のアップロードバッファを表示します。
3. アップロードバッファの使用について通知する 1 つ以上のアラームを設定します。

Amazon CloudWatch コンソールで 1 つ以上のアップロードバッファアラームを作成することを強くお勧めします。たとえば、警告を受ける使用レベルのアラームや、超えた場合にアクションの対象となる使用レベルのアラームを設定できます。アクションにより、さらにアップロードバッファ容量が追加される場合があります。詳細については、「ゲートウェイのアップロードバッファの上限アラームを設定するには」を参照してください。

不要なリソースのクリーンアップ

サンプル演習またはテストとしてゲートウェイを作成した場合は、予期しない結果や不必要な料金が発生するのを避けるため、クリーンアップを検討します。

不要なリソースをクリーンアップする

1. スナップショットを削除します。手順については、「スナップショットの削除」を参照してください。
2. ゲートウェイを引き続き使用する予定がなければ、削除します。詳細については、「ゲートウェイの削除と関連リソースの削除」を参照してください。
3. オンプレミスホストから Storage Gateway VM を削除します。Amazon EC2インスタンスでゲートウェイを作成した場合は、インスタンスを終了します。

ボリュームのバックアップ

Storage Gateway を使用することで、クラウドベースのストレージで Storage Gateway ボリュームを使用するオンプレミスのビジネスアプリケーションを保護することができます。Storage Gateway のネイティブスナップショットスケジューラまたは AWS Backupを使用して、オンプレミスの Storage Gateway ボリュームをバックアップできます。どちらの場合でも、Storage Gateway ボリュームのバックアップは Amazon EBS スナップショットとして Amazon Web Services で保存されます。

トピック

- Storage Gateway を使用してボリュームをバックアップする
- AWS Backup を使用してボリュームをバックアップする

Storage Gateway を使用してボリュームをバックアップする

Storage Gateway マネジメントコンソールを使用して、Amazon EBS スナップショットを作成し、Amazon Web Services で保存して、ボリュームをバックアップできます。1 回限りのスナップショットを作成することも、スナップショットのスケジュールを設定して Storage Gateway で管理することもできます。Storage Gateway コンソールを使用して、後で新しいボリュームにスナップショットを復元できます。バックアップの実行方法および Storage Gateway でバックアップを管理する方法の詳細については、次のトピックを参照してください。

- ゲートウェイのテスト
- 1 回限りのスナップショットの作成
- ボリュームをクローンする

AWS Backup を使用してボリュームをバックアップする

AWS Backup は、Amazon Web Services クラウドとオンプレミスの両方のサービス間でアプリケーションデータを簡単かつ費用対効果の高い方法でバックアップできるようにする、一元化されたバックアップ AWS サービスです。これにより、ビジネスおよび規制バックアップ AWS Backup のコンプライアンス要件を満たすことができます。 は、以下を実行できる一元的な場所を提供することで、 AWS ストレージボリューム、データベース、ファイルシステムの保護を簡単にします。

- バックアップする AWS リソースを設定して監査します。
- バックアップのスケジューリングの自動化。
- 保持ポリシーの設定。
- 最近のすべてのバックアップと復元アクティビティのモニタリング。

Storage Gateway は と統合されているため AWS Backup、 を使用して、クラウドベースのストレージに Storage Gateway ボリュームを使用するオンプレミスのビジネスアプリケーションを AWS Backup バックアップできます。 は、キャッシュ型ボリュームと保管型ボリュームの両方のバックアップと復元 AWS Backup をサポートします。の詳細については AWS Backup、「 AWS Backup ドキュメント」を参照してください。の詳細については AWS Backup、「 AWS Backup ユーザーガイド」の「 とは AWS Backup」を参照してください。

Storage Gateway ボリュームのバックアップおよびリカバリオペレーションは、 を使用して AWS Backup 管理できるため、カスタムスクリプトの作成や point-in-time バックアップの手動管理が不要になります。では AWS Backup、単一の AWS Backup ダッシュボードからクラウド内の AWS リソースと一緒にオンプレミスボリュームのバックアップをモニタリングすることもできます。を使用

して AWS Backup 、1 回限りのオンデマンドバックアップを作成するか、 で管理されるバックアッププランを定義できます AWS Backup。

から取得した Storage Gateway ボリュームのバックアップ AWS Backup は、Amazon EBS スナップショットとして Amazon S3 に保存されます。Storage Gateway ボリュームのバックアップは、AWS Backup コンソールまたは Amazon EBS コンソールから確認できます。

で管理されている Storage Gateway ボリュームは、任意のオンプレミスゲートウェイまたはクラウド内ゲートウェイ AWS Backup に簡単に復元できます。また、このようなボリュームを Amazon EC2 インスタンスで使用できる Amazon EBS ボリュームに復元することもできます。

を使用して Storage Gateway ボリューム AWS Backup をバックアップする利点

を使用して Storage Gateway ボリューム AWS Backup をバックアップする利点は、コンプライアンス要件を満たし、運用上の負担を回避し、バックアップ管理を一元化できることです。 AWS Backup では、次のことを実行できます。

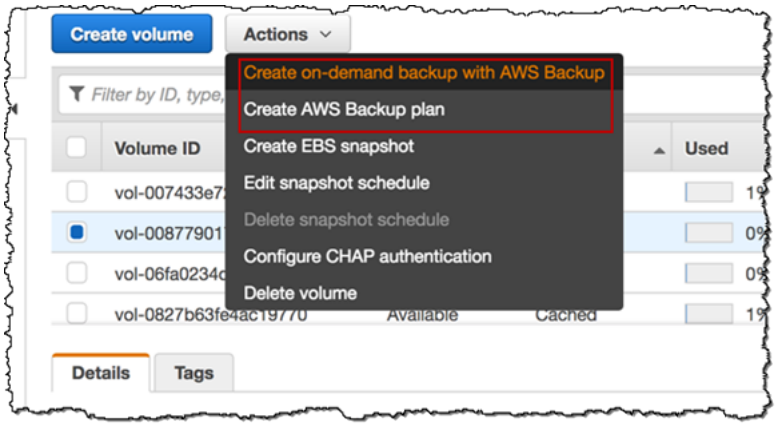
- バックアップ要件を満たすカスタマイズ可能なバックアップポリシーのスケジュールを設定します。
- カスタムスクリプトを開発したり、ボリュームの point-in-time バックアップを手動で管理したりする必要がないように、バックアップ保持と有効期限を設定します。
- 複数のゲートウェイやその他の AWS リソースにわたるバックアップを一元的に管理およびモニタリングできます。

AWS Backup を使用してボリュームのバックアップを作成するには

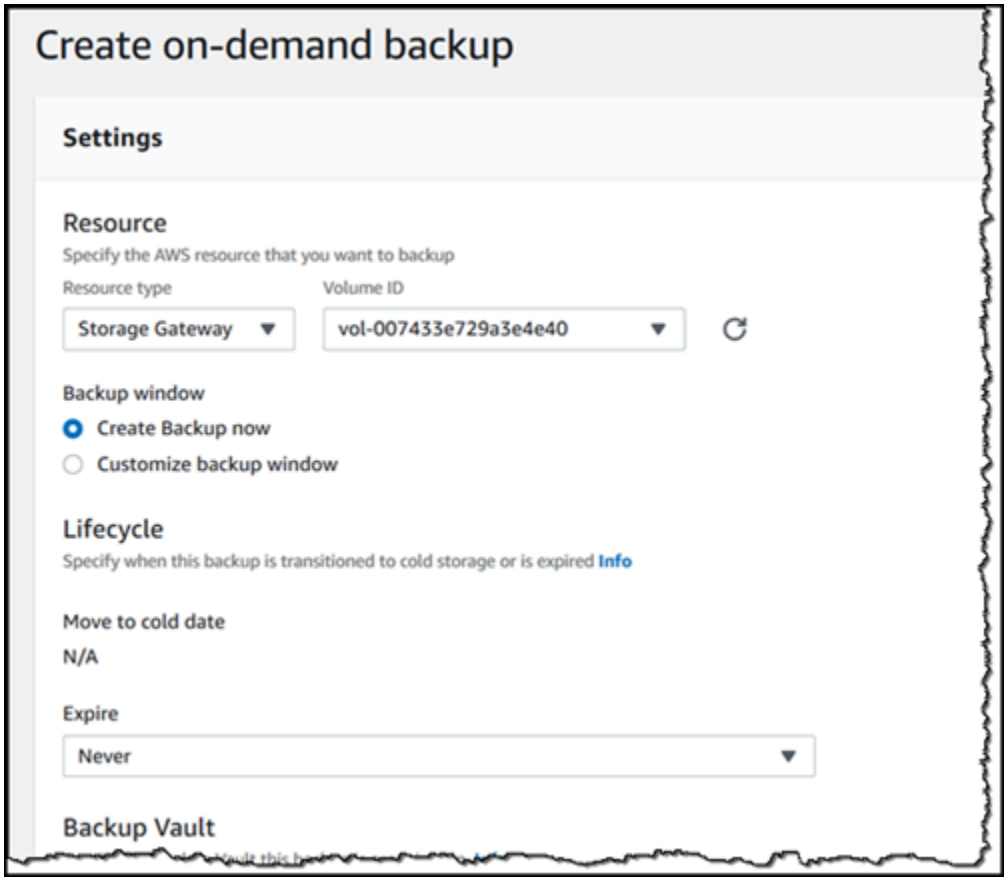
> **Note**
>
> AWS Backup では、 が AWS Backup 使用する AWS Identity and Access Management (IAM) ロールを選択する必要があります。このロールは、 AWS Backup によって自動的に作成されないため、作成する必要があります。また、 AWS Backup とこの IAM ロールの間に信頼関係を作成する必要があります。これを行う方法については、AWS Backup ユーザーガイドを参照してください。これを行う方法については、AWS Backup ユーザーガイドの「Creating a Backup Plan」を参照してください。

1. Storage Gateway コンソールを開き、左のナビゲーションペインから [Volumes] (ボリューム) を選択します。

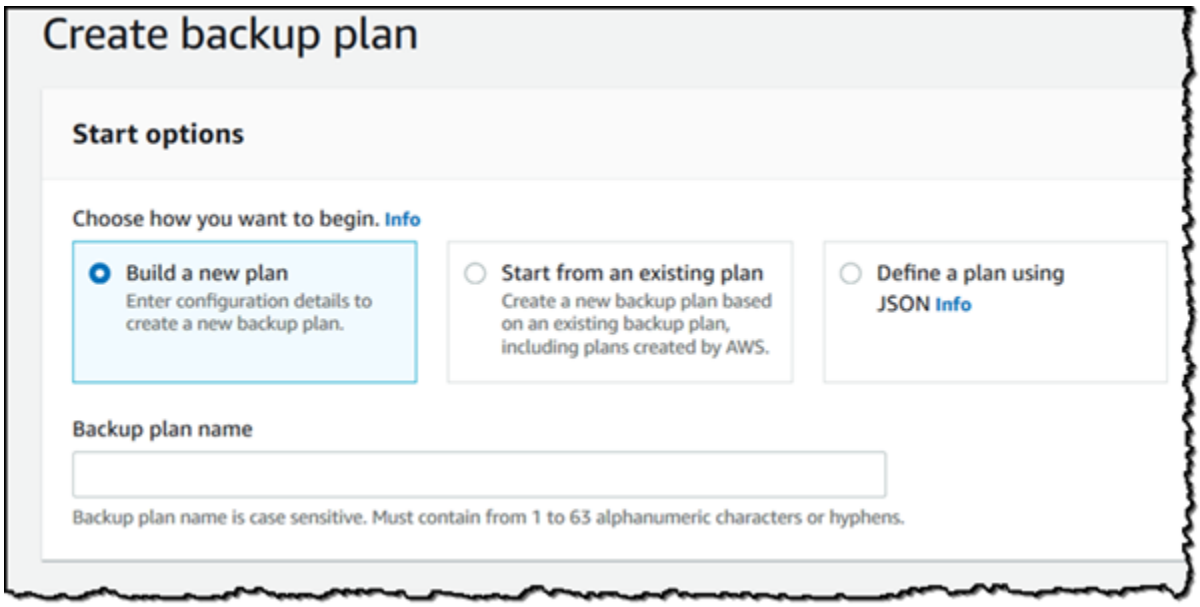
2. 「アクション」で「 でオンデマンドバックアップを作成する AWS Backup 」または AWS 「バックアッププランを作成する」を選択します。



Storage Gateway ボリュームのオンデマンドバックアップを作成する場合は、 を使用してオンデマンドバックアップを作成する AWS Backupを選択します。 AWS Backup コンソールが表示されます。



新しい AWS Backup プランを作成する場合は、 AWS バックアッププランの作成を選択します。 AWS Backup コンソールに移動します。



AWS Backup コンソールでは、バックアッププランの作成、バックアッププランへの Storage Gateway ボリュームの割り当て、バックアップの作成を行うことができます。また、継続的なバックアップマネジメントタスクも実行できます。

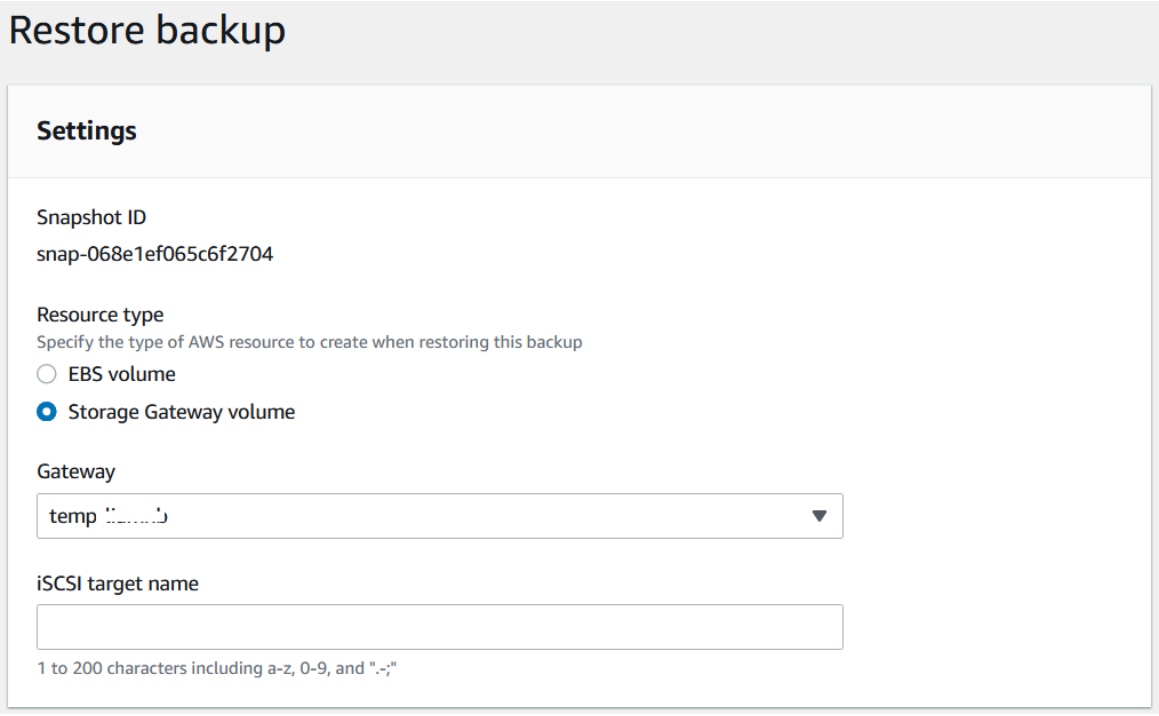
AWS Backupからボリュームを検索して復元する

AWS Backup コンソールからバックアップ Storage Gateway ボリュームを検索して復元できます。詳細については、『AWS Backup ユーザーガイド』を参照してください。詳細については、AWS Backup ユーザーガイドの「Recovery Points」を参照してください。

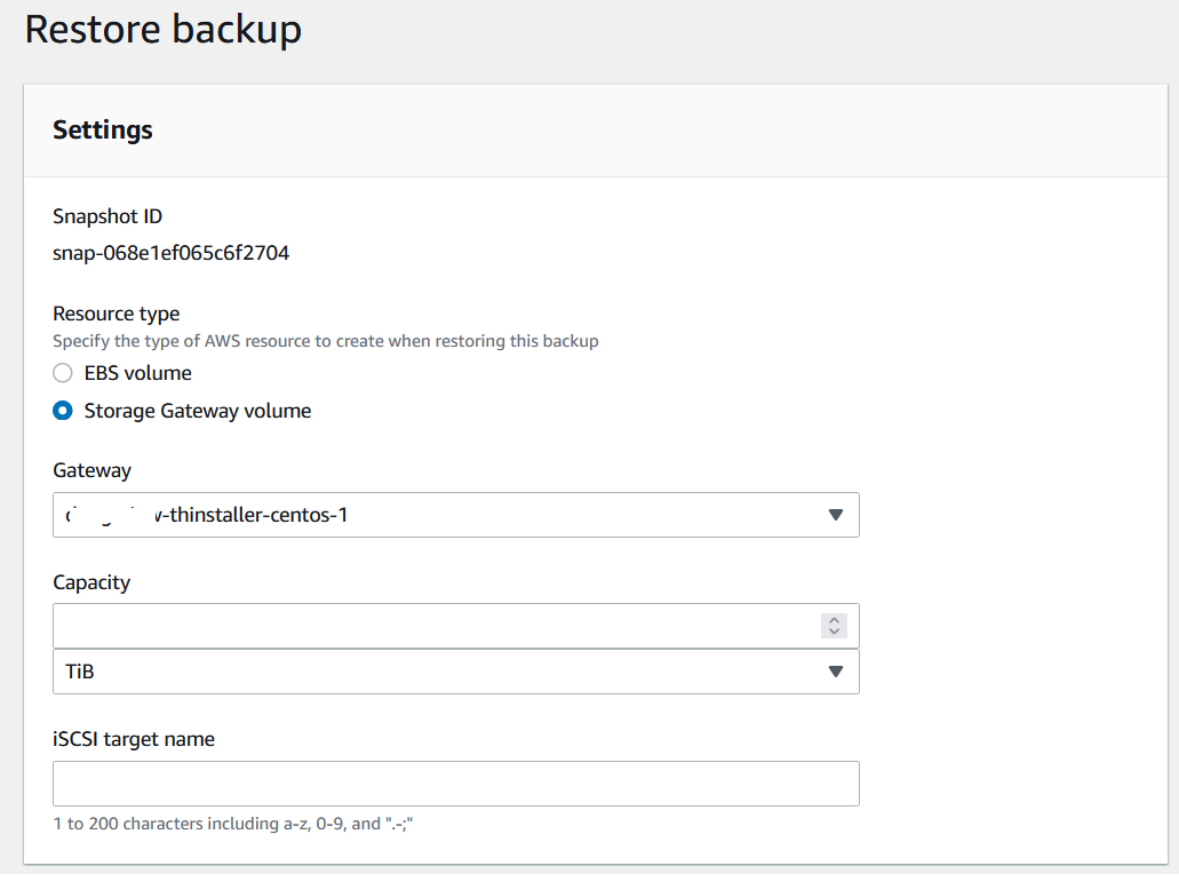
ボリュームを見つけて復元するには

1. AWS Backup コンソールを開き、復元する Storage Gateway ボリュームのバックアップを見つけます。Storage Gateway ボリュームのバックアップは、Amazon EBS ボリュームまたは Storage Gateway ボリュームに復元できます。復元要件に適したオプションを選択します。
2. [Restore type] (復元の種類) で、保存済みあるいはキャッシュ済みの Storage Gateway ボリュームを復元し、必要な情報を入力します。

   - 保存済みのボリュームでは、[ゲートウェイ名]、[ディスク ID]、[iSCSI ターゲット名] に関する情報を入力します。



- キャッシュ済みのボリュームでは、[ゲートウェイ名]、[容量]、[iSCSI ターゲット名] に関する情報を入力します。



3. [Restore resource (リソースの復元)] を選択してボリュームを復元します。

> **Note**
>
> Amazon EBS コンソールを使用して、 によって作成されたスナップショットを削除することはできません AWS Backup。

仮想プライベートクラウドでのゲートウェイのアクティブ化

オンプレミスのゲートウェイアプライアンスとクラウドベースのストレージインフラストラクチャの間にプライベート接続を確立できます。この接続を使用してゲートウェイをアクティブ化し、パブリックインターネット経由で通信せずにデータを AWS ストレージサービスに転送できます。Amazon VPCサービスを使用すると、カスタム仮想プライベートクラウド () でプライベートネットワークインターフェイスエンドポイントを含む AWS リソースを起動できますVPC。VPC を使用すると、IP アドレス範囲、サブネット、ルートテーブル、ネットワークゲートウェイなどのネットワーク設定を制御できます。の詳細についてはVPCs、「Amazon ユーザーガイド」の「Amazon VPCとは」を参照してください。 VPC

でゲートウェイをアクティブ化するにはVPC、Amazon VPCコンソールを使用して Storage Gateway のVPCエンドポイントを作成し、VPCエンドポイント ID を取得し、ゲートウェイを作成してアクティブ化するときにこのVPCエンドポイント ID を指定します。詳細については、ボリュームゲートウェイを に接続する AWS」を参照してください。

> **Note**
>
> Storage Gateway のVPCStorage Gatewayをアクティブ化する必要があります

トピック

- Storage Gateway 用のVPCエンドポイントの作成

Storage Gateway 用のVPCエンドポイントの作成

VPC エンドポイントを作成するには、次の手順に従います。Storage Gateway 用のVPCエンドポイントが既にある場合は、それを使用してゲートウェイをアクティブ化できます。

Storage Gateway のVPCエンドポイントを作成するには

1. にサインイン AWS Management Console し、 で Amazon VPCコンソールを開きますhttps://console.aws.amazon.com/vpc/。
2. ナビゲーションペインで [エンドポイント] を選択し、[Create endpoint (エンドポイントの作成)] を選択します。
3. [エンドポイントの作成] ページで、[サービスカテゴリ] の [AWS サービス] を選択します。
4. [Service Name] (サービス名)には `com.amazonaws.region.storagegateway` を選択します。例えば、 ですcom.amazonaws.us-east-2.storagegateway。
5. にはVPC、 を選択しVPC、そのアベイラビリティーゾーンとサブネットを書き留めます。
6. プライベートDNS名の有効化が選択されていないことを確認します。
7. セキュリティグループ で、 に使用するセキュリティグループを選択しますVPC。デフォルトのセキュリティグループを使用できます。セキュリティグループで次のTCPポートがすべて許可されていることを確認します。

   - TCP 443
   - TCP 1026
   - TCP 1027
   - TCP 1028
   - TCP 1031
   - TCP 2222
8. [エンドポイントの作成] を選択します。エンドポイントの初期状態は [pending (保留中)] です。エンドポイントが作成されたら、先ほど作成したVPCエンドポイントの ID を書き留めます。
9. エンドポイントが作成されたら、エンドポイント を選択し、新しいVPCエンドポイントを選択します。
10. 選択したストレージゲートウェイエンドポイントの詳細タブの名前 DNS で、アベイラビリティーゾーンを指定しないDNS名前を使用します。DNS 名前は次のようになります。 `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

これでVPCエンドポイントが作成され、ゲートウェイを作成できます。詳細については、「ゲートウェイを作成する」を参照してください。

ゲートウェイを管理する

ゲートウェイの管理に関するタスクには、キャッシュストレージとアップロードバッファ領域の設定、ボリュームや仮想テープの操作、および一般的なメンテナンスの実行が含まれます。ゲートウェイをまだ作成していない場合は、「の開始方法 AWS Storage Gateway」を参照してください。

ゲートウェイのソフトウェアリリースには、検証済みのオペレーティングシステムの更新とセキュリティパッチが定期的に含まれています。これらの更新は、スケジュールされたメンテナンス期間中の通常のゲートウェイ更新プロセスの一環として適用され、通常 6 か月ごとにリリースされます。注: Storage Gateway アプライアンスは、マネージド型の仮想マシンとして扱い、Storage Gateway アプライアンスインスタンスへのアクセスや変更を試みるべきではありません。通常のゲートウェイ更新メカニズム以外の方法 (例: または Hypervisor ツール) を使用してソフトウェアパッケージをインストールSSMまたは更新しようとすると、ゲートウェイが適切に機能しなくなる可能性があります。

トピック

- ボリュームゲートウェイの管理
- 新しいゲートウェイへのデータの移動

ボリュームゲートウェイの管理

以下は、ボリュームゲートウェイリソースを管理する方法についての情報です。

キャッシュ型ボリュームは、Amazon Simple Storage Service (Amazon S3) 内のボリュームで、アプリケーションデータを保存できる iSCSI ターゲットとして公開されます。このセクションでは、キャッシュ型セットアップのボリュームを追加および削除する方法について説明します。Amazon EC2ゲートウェイで Amazon Elastic Block Store (Amazon EBS) ボリュームを追加および削除する方法についても説明します。

トピック

- 基本的なゲートウェイ情報の編集
- ボリュームの追加
- ボリュームサイズの拡大
- ボリュームをクローンする
- ボリュームの使用量の表示

- ボリュームで課金されるストレージを削減する
- ボリュームの削除
- 別のゲートウェイにボリュームを移動する
- 1 回限りのスナップショットの作成
- スナップショットスケジュールの編集
- スナップショットの削除
- ボリュームステータスと移行について

> **Important**
>
> Amazon S3 にプライマリデータを保存するキャッシュ型ボリュームの場合、ボリューム全体にあるすべてのデータを読み書きするようなプロセスは回避する必要があります。たとえば、キャッシュ型ボリューム全体をスキャンするウイルススキャンソフトウェアは使用しないことをお勧めします。このようなスキャンでは、オンデマンド型かスケジュール型かにかかわらず、Amazon S3 に保存されているすべてのデータがローカルにダウンロードされスキャンされるので、より大きな帯域幅を専有することになります。このディスク全体のスキャンの代わりに、リアルタイムでウイルススキャンが行えます。つまり、キャッシュ型ボリュームとの間で読み書きが実行された時点で、そのデータをスキャンできます。

ボリュームのサイズを変更することはできません。ボリュームのサイズを変更するには、ボリュームのスナップショットを作成し、そのスナップショットから新しいキャッシュ型ボリュームを作成します。新しいボリュームは、スナップショットを作成したボリュームよりも大きくすることができます。ボリュームを削除する方法については、「ボリュームを削除するには」を参照してください。ボリュームを追加し、既存のデータを保持する方法については、「ボリュームの削除」を参照してください。

キャッシュされたボリュームデータとスナップショットデータはすべて Amazon S3 に保存され、サーバー側の暗号化 () を使用して保管時に暗号化されますSSE。ただし、Amazon S3 または Amazon SAmazon S3 マネジメントコンソールなどの他のツールを使用してこのデータにアクセスすることはできません。 API

基本的なゲートウェイ情報の編集

Storage Gateway コンソールを使用して、ゲートウェイ名、タイムゾーン、 CloudWatch ロググループなど、既存のゲートウェイの基本情報を編集できます。

既存のゲートウェイの基本情報を編集するには

1. ホーム で Storage Gateway https://console.aws.amazon.com/storagegateway/コンソールを開きます。
2. [ゲートウェイ] を選択し、基本情報を編集するゲートウェイを選択します。
3. [アクション] ドロップダウンメニューから [ゲートウェイ情報の編集] を選択します。
4. 目的の設定を適宜変更して、[変更を保存] を選択します。

> **Note**
>
> ゲートウェイの名前を変更すると、ゲートウェイをモニタリングするように設定された CloudWatch アラームが切断されます。アラームを再接続するには、 CloudWatch コンソールで各アラームGatewayNameの を更新します。

ボリュームの追加

アプリケーションのニーズが増えたため、ボリュームをゲートウェイに追加する必要がある場合があります。ボリュームを追加するとき、ゲートウェイに割り当てたキャッシュストレージとアップロードバッファのサイズを考慮する必要があります。ゲートウェイには、新しいボリュームに十分なバッファとキャッシュスペースが必要です。詳細については、「割り当てるアップロードバッファのサイズの決定」を参照してください。

ボリュームは、Storage Gateway コンソールまたは Storage Gateway API を使用して追加できます。Storage Gateway API を使用してボリュームを追加する方法については、「CreateCachediSCSIVolume」を参照してください。Storage Gateway コンソールを使用して、ボリュームを追加する方法については、「ボリュームの作成」を参照してください。

ボリュームサイズの拡大

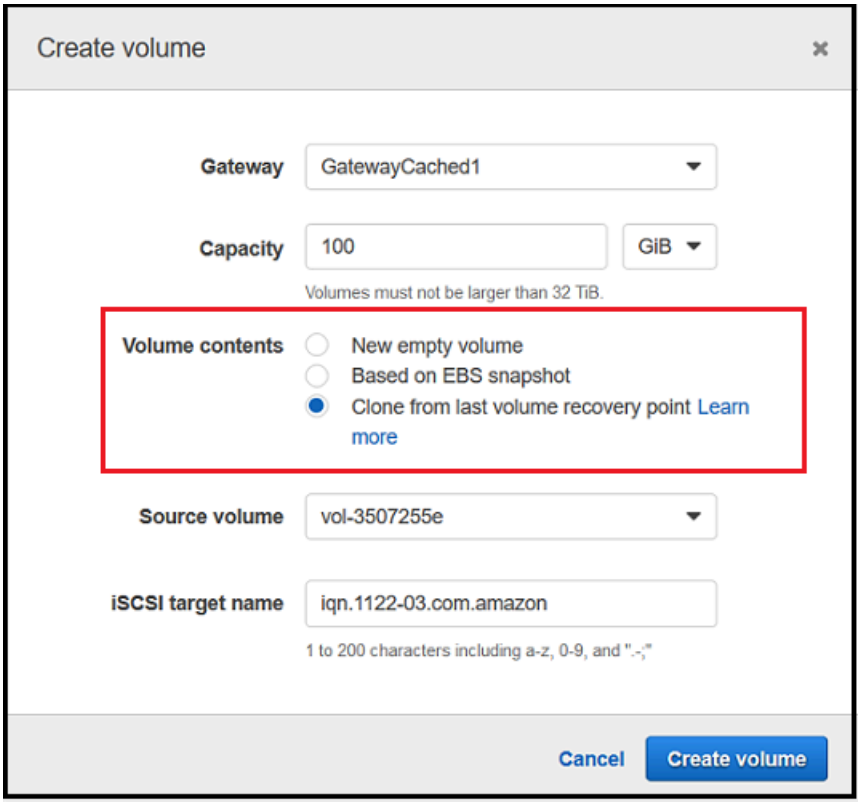
アプリケーションのニーズが増えるにつれて、ゲートウェイにボリュームを追加する代わりにボリュームを拡大したい場合があります。この場合は、以下のいずれか方法があります。

- 拡大するボリュームのスナップショットを作成し、そのスナップショットを使用して、より大きいサイズの新しいボリュームを作成します。スナップショットの作成方法については、「1 回限りのスナップショットの作成」を参照してください。スナップショットを使用した新しいボリュームの作成方法については、「ボリュームの作成」を参照してください。

- 拡大するキャッシュ型ボリュームを使用して、より大きいサイズの新しいボリュームのクローンを作成します。ボリュームのクローン方法については、「ボリュームをクローンする」を参照してください。ボリュームを作成する方法については、「ボリュームの作成」を参照してください。

ボリュームをクローンする

同じ AWS リージョン内の既存のキャッシュ型ボリュームから新しいボリュームを作成できます。新しいボリュームは選択されたボリュームの最新の復旧ポイントから作成されます。ボリューム復旧ポイントは、ボリュームのすべてのデータに整合性がある時点です。ボリュームのクローンを作成するには、[Create volume] (ボリュームの作成) ダイアログ・ボックスの[Clone from last recovery point] (最後のリカバリポイントからクローンを作成する) オプションで、ソースとして使用するボリュームを選択します。次のスクリーンショットは、[ボリュームの作成] ダイアログボックスを示しています。



既存のボリュームからのクローンは、Amazon EBS スナップショットを作成するより短時間で完了でき、コスト効率にも優れています。クローン作成では、ソースボリュームからの最新のリカバリポイントを使用して、ソースボリュームから新しいボリュームにデータ byte-to-byte のコピーが実行されます。Storage Gateway は、キャッシュ型ボリュームのためにリカバリポイントを自動的に作成します。最後のリカバリポイントが作成された日時を確認するには、Amazon の `TimeSinceLastRecoveryPoint`メトリクスを確認します CloudWatch。

クローンされたボリュームはソースボリュームから独立しています。つまり、クローン後にいずれかのボリュームに行われた変更は、他方には影響はありません。たとえば、ソースボリュームを削除しても、クローンされたボリュームには影響しません。イニシエータが接続されて、有効に使用されているときに、ソースボリュームをクローンできます。そうすることでソースボリュームのパフォーマンスには影響しません。ボリュームのクローン方法については、「ボリュームの作成」を参照してください。

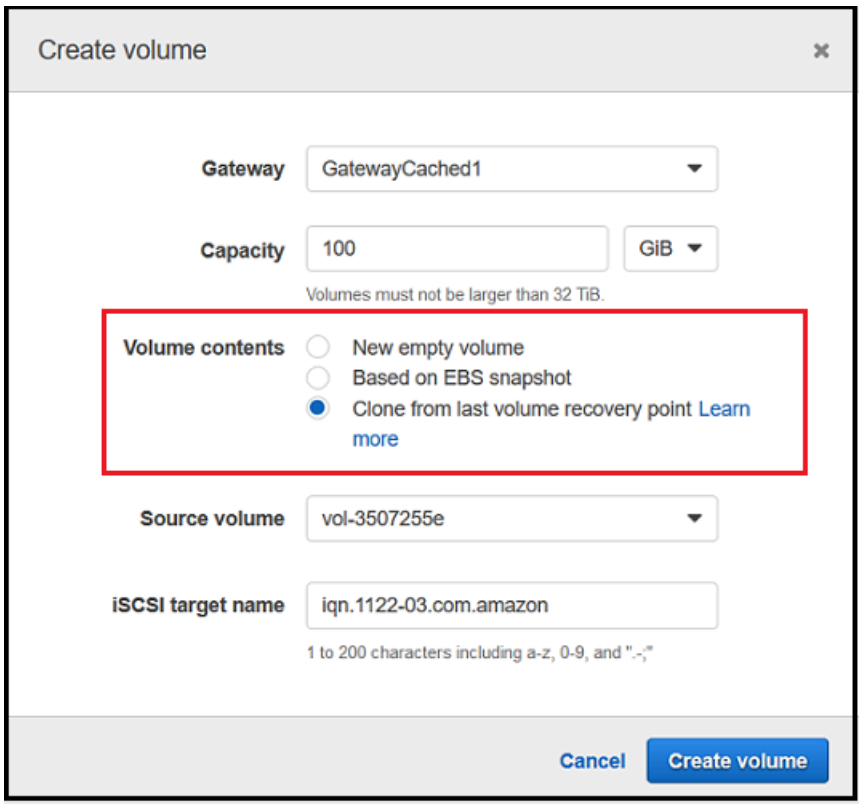
また復旧シナリオでクローンプロセスを使用できます。詳細については、「ゲートウェイキャッシュ型が到達不可能なためデータを復旧する場合」を参照してください。

ボリューム復旧ポイントからのクローン

次の手順は、ボリューム復旧ポイントからボリュームをクローンする方法と、そのボリュームの使用方法を示しています。

到達不可能なゲートウェイからボリュームをクローンして使用する

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. Storage Gateway コンソールで、[Create volume] (ボリュームの作成) を選択します。
3. [ボリュームの作成] ダイアログボックスで、[ゲートウェイ] 用のゲートウェイを選択します。
4. [容量] にボリュームの容量を入力します。容量はソースボリュームと同じサイズ以上でなければなりません。
5. [Clone from last recovery point] を選び、[Source volume] のボリューム ID を選択します。ソースボリュームは、選択した AWS リージョン内の任意のキャッシュ型ボリュームにすることができます。



6. [iSCSI ターゲット名] に名前を入力します。

   ターゲット名には、小文字、数字、ピリオド (.) およびハイフン (-) を含めることができます。このターゲット名は検出後、[iSCSI Microsoft initiator] UI の [Targets] タブに、[iSCSI target node] として表示されます。たとえば、名前 `target1` は `iqn.1007-05.com.amazon:target1` のように表示されます。そのターゲット名がストレージエリアネットワーク (SAN) 内でグローバルに一意であることを確認します。

7. [ネットワークインターフェイス] 設定の IP アドレスがゲートウェイであることを確認します。または [ネットワークインターフェイス] の IP アドレスを選択します。

   複数のネットワークアダプタを使用するようにゲートウェイを定義した場合、ボリュームにアクセスするために保管アプリケーションが使用する IP アドレスを選択します。ゲートウェイに対して定義された各ネットワークアダプタは、選択できる 1 つの IP アドレスを表します。

   ゲートウェイ VM が 1 つ以上のネットワークアダプタ用に設定されている場合には、[ボリュームの作成] ダイアログボックスに [ネットワークインターフェイス] のリストが表示されます。このリストには、ゲートウェイ VM に設定された各アダプタに対して 1 つの IP アドレスが示されます。ゲートウェイ VM が 1 つのネットワークアダプタにのみ設定されている場合、存在する IP アドレスは 1 つのみであるため、リストは表示されません。

8. [Create volume] (ボリュームの作成) を選択します。[CHAP 認証の設定] ダイアログボックスが表示されます。後で CHAP を設定できます。詳細については、iSCSI ターゲットのCHAP認証の設定 を参照してください。

次のステップはボリュームをクライアントに接続することです。詳細については、「クライアントへのボリュームの接続」を参照してください。

復旧スナップショットの作成

次の手順は、ボリューム復旧ポイントからスナップショットを作成する方法と、そのスナップショットの使用方法を示しています。1 回限りの一時的なスナップショットを取得したり、ボリュームのスナップショットスケジュールをセットアップしたりできます。

到達不可能なゲートウェイからボリュームの復旧スナップショットを作成し、使用するには

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. ナビゲーションペインで、[Gateways] を選択します。
3. 到達不可能なゲートウェイを選択し、[Details] タブを選択します。

   復旧スナップショットのメッセージはタブに表示されます。

4. [Create recovery snapshot] を選択して、[Create recovery snapshot] ダイアログボックスを開きます。
5. 表示されるボリュームのリストから、復元するボリュームを選択し、[Create snapshots] を選択します。

   Storage Gateway はスナップショットに関する処理を開始します。
6. スナップショットを見つけて復元します。

ボリュームの使用量の表示

データをボリュームに書き込む際には、Storage Gateway マネジメントコンソールを使用してボリュームに保存済みとなったデータ量を表示できます。各ボリュームの [Details] タブに、ボリューム使用状況の情報が表示されます。

ボリュームに書き込まれるデータ量を表示するには

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. ナビゲーションペインで [Volumes] を選択し、対象のボリュームを選択します。
3. [詳細] タブを選択します。

   以下のフィールドには、ボリュームに関する情報が示されます。

   - [Size:] 選択したボリュームの全容量。
   - [Used:] ボリュームに保存されているデータのサイズ。

   > **Note**
   >
   > これらの値は、ボリュームにデータを保存するまで、2015 年 5 月 13 日よ以前に作成されたボリュームに対しては利用できません。

ボリュームで課金されるストレージを削減する

ファイルシステムからファイルを削除しても、必ずしも基になるブロックデバイスからデータが作成されたり、ボリュームに保存されているデータの量が減るわけではありません。ボリュームにおいて課金されるストレージの量を減らす必要がある場合、ファイルをゼロで上書きすることお勧めします。これにより、実際のストレージの量を無視できる程度の規模に圧縮できます。Storage Gateway は、圧縮されたストレージに基づいてボリュームの利用に課金を行います。

> **Note**
>
> ボリュームのデータをランダムデータで上書きする削除ツールを使用する場合には、使用量は削減しません。これは、ランダムデータが圧縮不可能であるためです。

ボリュームの削除

アプリケーションのニーズが変化した際に、ボリュームの削除が必要となることがあります。例えば、より大きなストレージボリュームを使用するために、アプリケーションを移行する場合などです。ボリュームを削除する前に、現在ボリュームに書き込みを行っているアプリケーションがないことを確認します。また、ボリュームのスナップショットを作成中ではないことも確認します。ボリュームでスナップショットのスケジュールが定義されているかどうかは、Storage Gateway コンソールの [Snapshot Schedules] (スナップショットスケジュール) タブで確認します。詳細については、「スナップショットスケジュールの編集」を参照してください。

Storage Gateway コンソールまたは Storage Gateway を使用してボリュームを削除できます API。Storage Gateway を使用してボリュームAPIを削除する方法については、「ボリュームの削除」を参照してください。以下の手順は、コンソールの使い方を示しています。

ボリュームを削除する前に、データのバックアップまたは重要なデータのスナップショットを作成します。保管型ボリュームの場合、ローカルディスクは消去されません。ボリューム削除後に復元することはできません。

ボリュームを削除するには

1. ホーム で Storage Gateway https://console.aws.amazon.com/storagegateway/コンソールを開きます。
2. [ボリューム] を選択し、削除対象のボリュームを 1 つ以上選択します。
3. [アクション] で [ボリュームの削除] を選択します。確認のダイアログボックスが表示されます。
4. 指定したボリュームを削除することを確認し、確認ボックスに 「delete」と入力して [削除] を選択します。

別のゲートウェイにボリュームを移動する

データとパフォーマンスのニーズが高まるに従い、ボリュームを別のボリュームゲートウェイに移動したくなる場合があります。これを行うには、Storage Gateway コンソールあるいは API を使用して、ボリュームをデタッチおよびアタッチします。

ボリュームのデタッチおよびアタッチすると、以下を実行できます。

- より最適なホストプラットフォームあるいは最新の Amazon EC2 インスタンスにボリュームを移動すること。
- サーバーで基盤となるハードウェアを更新すること。

- ハイパーバイザータイプ間でボリュームを移動すること。

ボリュームのデタッチを行うと、ゲートウェイは AWSの Storage Gateway サービスに対し、そのボリュームのデータおよびメタデータをアップロードして保存します。デタッチされたボリュームは、サポートされている任意のホストプラットフォームのゲートウェイにその後簡単にアタッチできます。

> **Note**
>
> デタッチしたボリュームは、削除するまで、標準のボリュームストレージとして課金されます。請求額を削減する方法については、「ボリュームで課金されるストレージを削減する」を参照してください。

> **Note**
>
> ボリュームのアタッチおよびデタッチにはいくつかの制限があります。
>
> - ボリュームのデタッチには長い時間がかかる場合があります。ボリュームをデタッチすると、ゲートウェイはボリューム上のすべてのデータを にアップロード AWS してから、ボリュームをデタッチします。アップロードが完了するまでにかかる時間は、アップロードする必要のあるデータ量と AWSへのネットワーク接続によって異なります。
> - キャッシュ済みのボリュームをデタッチする場合、これを保存済みのボリュームとして再アタッチすることはできません。
> - 保存済みのボリュームをデタッチする場合、これをキャッシュ済みのボリュームとして再アタッチすることはできません。
> - デタッチされたボリュームは、これがゲートウェイにアタッチされるまで使用することはできません。
> - 保存済みのボリュームをアタッチする場合、ゲートウェイにアタッチする前に完全に復元する必要があります。
> - ボリュームのアタッチあるいはデタッチを開始したら、ボリュームを使用する前にオペレーションが完了するまで待機する必要があります。
> - 現在のところ、ボリュームの強制的な削除は API のみでサポートされています。
> - ゲートウェイからボリュームをデタッチしている間にこのゲートウェイを削除すると、データは喪失されます。ゲートウェイを削除する前に、ボリュームのデタッチオペレーションが完了するまで待ってください。

- 保存済みのゲートウェイが復元状態にある場合、このゲートウェイからボリュームをデタッチすることはできません。

以下のステップに、Storage Gateway コンソールを使用してボリュームのデタッチとアタッチを行う方法を示します。API を使用してこれを行う方法の詳細については、 API リファレンスのDetachVolume「」またはAttachVolume「」を参照してください。 AWS Storage Gateway

ゲートウェイからボリュームをデタッチするには

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. [ボリューム] を選択し、デタッチ対象のボリュームを 1 つ以上選択します。
3. [アクション] で [ボリュームのデタッチ] を選択します。確認のダイアログボックスが表示されます。
4. 指定したボリュームをデタッチすることを確認し、確認ボックスに「detach」と入力して [デタッチ] を選択します。

> **Note**
>
> デタッチするボリュームに大量のデータがある場合、このボリュームはすべてのデータのアップロードが完了するまで [アタッチ済み] から [デタッチ中] ステータスに移行します。その後、ステータスは [デタッチ済み] に変更します。少量のデータにおいては、[デタッチ中] ステータスが表示されない場合があります。ボリュームにデータがない場合、ステータスは [アタッチ済み] から [デタッチ済み] に変わります。

別のゲートウェイにボリュームをアタッチできるようになりました。

ゲートウェイにボリュームをアタッチするには

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. ナビゲーションペインで [ボリューム] を選択します。デタッチした各ボリュームのステータスは [デタッチ済み] と示されます。
3. デタッチ済みのボリュームのリストから、アタッチするボリュームを選択します。一度にアタッチできるボリュームは 1 つのみです。

4. [アクション] で [ボリュームのアタッチ] を選択します。
5. [ボリュームのアタッチ] ダイアログボックスで、ボリュームをアタッチするゲートウェイを選択し、ボリュームを接続する iSCSI ターゲットを入力します。

   保存済みのボリュームをアタッチする場合には、[ディスク ID] にそのディスク識別子を入力します。
6. [ボリュームのアタッチ] を選択します。アタッチするボリューム上に大量のデータがある場合は、`AttachVolume` オペレーションが成功した時点で、この表示が [Detached] (デタッチ済み) から [Attached] (アタッチ済み) に移行します。
7. CHAP 認証設定ウィザードが表示されたら、[イニシエータ名]、[イニシエータのシークレット]、[ターゲットのシークレット] を選択し、[Save (保存)] を選択します。チャレンジハンドシェイク認証プロトコル (CHAP) 認証を操作する詳細については、「iSCSI ターゲットのCHAP 認証の設定」を参照してください。

1 回限りのスナップショットの作成

スケジュールされたスナップショットの他に、ボリュームゲートウェイでは 1 回限りの臨時のスナップショットを作成できます。これを作成すると、スケジュールされている次のスナップショットを待たずに、すぐにストレージボリュームをバックアップできます。

ストレージボリュームの 1 回限りのスナップショットを作成するには

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. ナビゲーションペインで [Volumes] を選択し、スナップショットを作成するボリュームを選択します。
3. [アクション] で [スナップショットを作成] を選択します。
4. [Create snapshot] ダイアログボックスで、スナップショットの説明を入力し、[Create snapshot] を選択します。

   スナップショットがコンソールを使用して作成されたことを確認できます。

スナップショットはボリュームと同じ行の [Snapshots] に表示されます。

スナップショットスケジュールの編集

保管型ボリュームの場合、 は 1 日 1 回というデフォルトのスナップショットスケジュール AWS Storage Gateway を作成します。

> **Note**
>
> デフォルトのスナップショットスケジュールを削除することはできません。保管型ボリュームには少なくとも 1 つのスナップショットスケジュールが必要です。ただし、毎日のスナップショットが発生する時間か、頻度 (1、2、4、8、12、または 24 時間ごと) か、またはその両方を指定して、スナップショットスケジュールを変更できます。

キャッシュ型ボリューム AWS Storage Gateway の場合、デフォルトのスナップショットスケジュールは作成しません。データは Amazon S3 に保存されるため、デフォルトのスケジュールは作成されません。このため、災害対策を目的としたスナップショットやスナップショットスケジュールは必要ありません。ただし、必要に応じていつでもスナップショットスケジュールを設定できます。キャッシュ型ボリュームのスナップショットを作成することは、必要時のデータ復元のためのもう 1 つの方法となります。

ボリュームのスナップショットスケジュールを編集するには、次の手順に従います。

ボリュームのスナップショットスケジュールを編集するには

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. ナビゲーションペインで [Volumes] を選択し、スナップショットが作成されたボリュームを選択します。
3. [Actions (アクション)] で、[Edit snapshot schedule (スナップショットスケジュールの編集)] を選択します。
4. [Edit snapshot schedule] ダイアログボックスで、スケジュールを変更し、[Save] を選択します。

スナップショットの削除

ストレージボリュームのスナップショットを削除できます。たとえば、長期間に渡ってストレージボリュームの多数のスナップショットを作成し、古いスナップショットが不要になった場合などは、こ

れを実行できます。スナップショットは増分バックアップなので、スナップショットを削除すると、他のスナップショットで必要とされていないデータのみが削除されます。

トピック

- AWS SDK for Java を使用したスナップショットの削除
- AWS SDK for .NET を使用したスナップショットの削除
- AWS Tools for Windows PowerShellを使用したスナップショットの削除

Amazon EBS コンソールで、スナップショットを一度に 1 つずつ削除できます。Amazon EBS コンソールを使用してスナップショットを削除する方法については、Amazon EC2 ユーザーガイドの「Amazon EBS スナップショットの削除」を参照してください。

一度に複数のスナップショットを削除するには、Storage Gateway オペレーションをサポートするAWS SDKsのいずれかを使用できます。例については、「AWS SDK for Java を使用したスナップショットの削除」、「AWS SDK for .NET を使用したスナップショットの削除」、および「AWS Tools for Windows PowerShellを使用したスナップショットの削除」を参照してください。

AWS SDK for Java を使用したスナップショットの削除

ボリュームに関連付けられている多数のスナップショットを削除するには、プログラム的な方法を使用します。次の例で、 AWS SDK for Java を使用してスナップショットを削除する方法を示します。サンプルコードを使用するには、Java コンソールアプリケーションの実行について理解している必要があります。手順については、AWS SDK for Java デベロッパーガイドの「Getting Started」を参照してください。いくつかのスナップショットだけを削除する必要がある場合は、スナップショットの削除 で説明されているように、コンソールを使用します。

Example : AWS SDK for Java を使用したスナップショットの削除

次の Java コード例では、ゲートウェイの各ボリュームのスナップショットと、スナップショットの開始時間が指定した日付の前か後かをリストに表示します。Storage Gateway と Amazon EC2 には AWS SDK for Java API を使用します。Amazon EC2 API には、スナップショットを操作するためのオペレーションが含まれています。

サービスエンドポイント、ゲートウェイの Amazon リソースネーム (ARN) およびスナップショットを保存する日数を提供するコードを更新します。スナップショットは、この期限が削除される前に取得されます。また、`viewOnly` というブール値も指定する必要があります。この値は、削除されるスナップショットを表示するかどうかや、実際に削除を行うかどうかを示します。まずは、表示オプションだけで (つまり、`viewOnly` を `true` に設定して) コードを実行して、コードによって何が削

除されるかを確認します。Storage Gateway で使用できる AWS サービスエンドポイントのリストについては、AWS Storage Gateway 「」の「 エンドポイントとクォータ」を参照してくださいAWS 全般のリファレンス。 Storage Gateway

```
import java.io.IOException;
import java.util.ArrayList;
import java.util.Calendar;
import java.util.Collection;
import java.util.Date;
import java.util.GregorianCalendar;
import java.util.List;

import com.amazonaws.auth.PropertiesCredentials;
import com.amazonaws.services.ec2.AmazonEC2Client;
import com.amazonaws.services.ec2.model.DeleteSnapshotRequest;
import com.amazonaws.services.ec2.model.DescribeSnapshotsRequest;
import com.amazonaws.services.ec2.model.DescribeSnapshotsResult;
import com.amazonaws.services.ec2.model.Filter;
import com.amazonaws.services.ec2.model.Snapshot;
import com.amazonaws.services.storagegateway.AWSStorageGatewayClient;
import com.amazonaws.services.storagegateway.model.ListVolumesRequest;
import com.amazonaws.services.storagegateway.model.ListVolumesResult;
import com.amazonaws.services.storagegateway.model.VolumeInfo;

public class ListDeleteVolumeSnapshotsExample {

    public static AWSStorageGatewayClient sgClient;
    public static AmazonEC2Client ec2Client;
    static String serviceURLSG = "https://storagegateway.us-east-1.amazonaws.com";
    static String serviceURLEC2 = "https://ec2.us-east-1.amazonaws.com";

    // The gatewayARN
    public static String gatewayARN = "*** provide gateway ARN ***";

    // The number of days back you want to save snapshots. Snapshots before this cutoff
 are deleted
    // if viewOnly = false.
    public static int daysBack = 10;

    // true = show what will be deleted; false = actually delete snapshots that meet
 the daysBack criteria
    public static boolean viewOnly = true;
```

```
    public static void main(String[] args) throws IOException {

        // Create a Storage Gateway and amazon ec2 client
        sgClient = new AWSStorageGatewayClient(new PropertiesCredentials(

ListDeleteVolumeSnapshotsExample.class.getResourceAsStream("AwsCredentials.properties")));

        sgClient.setEndpoint(serviceURLSG);

        ec2Client = new AmazonEC2Client(new PropertiesCredentials(

ListDeleteVolumeSnapshotsExample.class.getResourceAsStream("AwsCredentials.properties")));
        ec2Client.setEndpoint(serviceURLEC2);

        List<VolumeInfo> volumes = ListVolumesForGateway();
        DeleteSnapshotsForVolumes(volumes, daysBack);

    }
    public static List<VolumeInfo> ListVolumesForGateway()
    {
        List<VolumeInfo> volumes = new ArrayList<VolumeInfo>();

        String marker = null;
        do {
            ListVolumesRequest request = new
ListVolumesRequest().withGatewayARN(gatewayARN);
            ListVolumesResult result = sgClient.listVolumes(request);
            marker = result.getMarker();

            for (VolumeInfo vi : result.getVolumeInfos())
            {
                volumes.add(vi);
                System.out.println(OutputVolumeInfo(vi));
            }
        } while (marker != null);

        return volumes;
    }
    private static void DeleteSnapshotsForVolumes(List<VolumeInfo> volumes,
            int daysBack2) {

        // Find snapshots and delete for each volume
        for (VolumeInfo vi : volumes) {
```

```
            String volumeARN = vi.getVolumeARN();
            String volumeId =
 volumeARN.substring(volumeARN.lastIndexOf("/")+1).toLowerCase();
            Collection<Filter> filters = new ArrayList<Filter>();
            Filter filter = new Filter().withName("volume-id").withValues(volumeId);
            filters.add(filter);

            DescribeSnapshotsRequest describeSnapshotsRequest =
                new DescribeSnapshotsRequest().withFilters(filters);
            DescribeSnapshotsResult describeSnapshotsResult =
                ec2Client.describeSnapshots(describeSnapshotsRequest);

            List<Snapshot> snapshots = describeSnapshotsResult.getSnapshots();
            System.out.println("volume-id = " + volumeId);
            for (Snapshot s : snapshots){
                StringBuilder sb = new StringBuilder();
                boolean meetsCriteria = !CompareDates(daysBack, s.getStartTime());
                sb.append(s.getSnapshotId() + ", " + s.getStartTime().toString());

                sb.append(", meets criteria for delete? " + meetsCriteria);
                sb.append(", deleted? ");
                if (!viewOnly & meetsCriteria) {
                    sb.append("yes");
                    DeleteSnapshotRequest deleteSnapshotRequest =
                        new DeleteSnapshotRequest().withSnapshotId(s.getSnapshotId());
                    ec2Client.deleteSnapshot(deleteSnapshotRequest);
                }
                else {
                    sb.append("no");
                }
                System.out.println(sb.toString());
            }
        }
    }

    private static String OutputVolumeInfo(VolumeInfo vi) {

        String volumeInfo = String.format(
                 "Volume Info:\n" +
                 "  ARN: %s\n" +
                 "  Type: %s\n",
                 vi.getVolumeARN(),
                 vi.getVolumeType());
        return volumeInfo;
```

```
     }

    // Returns the date in two formats as a list
    public static boolean CompareDates(int daysBack, Date snapshotDate) {
        Date today = new Date();
        Calendar cal = new GregorianCalendar();
        cal.setTime(today);
        cal.add(Calendar.DAY_OF_MONTH, -daysBack);
        Date cutoffDate = cal.getTime();
        return (snapshotDate.compareTo(cutoffDate) > 0) ? true : false;
    }

}
```

AWS SDK for .NET を使用したスナップショットの削除

ボリュームに関連付けられている多数のスナップショットを削除するには、プログラム的な方法を使用します。次に、 AWS SDK for .NET バージョン 2 および 3 を使用してスナップショットを削除する方法の例を示します。サンプルコードを使用するには、.NET コンソールアプリケーションの実行について理解している必要があります。詳細については、「AWS SDK for .NET デベロッパーガイド」の「Getting Started」を参照してください。いくつかのスナップショットだけを削除する必要がある場合は、スナップショットの削除 で説明されているように、コンソールを使用します。

Example : AWS SDK for .NET を使用したスナップショットの削除

次の C# コード例では、 AWS Identity and Access Management ユーザーはゲートウェイの各ボリュームのスナップショットを一覧表示できます。ユーザーは、スナップショットの開始時間が指定日 (保持期間) 前あるいは後であるかを決定し、保持期間を過ぎたスナップショットを削除できます。この例では、Storage Gateway および Amazon EC2 用の AWS SDK for .NET API を使用しています。Amazon EC2 API には、スナップショットを操作するためのオペレーションが含まれています。

次のコード例では、 AWS SDK for .NET バージョン 2 および 3 を使用しています。以前のバージョンの .NET を新しいバージョンに移行できます。詳細については、AWS 「コードを SDK for .NET の最新バージョンに移行する」を参照してください。

サービスエンドポイント、ゲートウェイの Amazon リソースネーム (ARN) およびスナップショットを保存する日数を提供するコードを更新します。スナップショットは、この期限が削除される前に取得されます。また、`viewOnly` というブール値も指定する必要があります。この値は、削除されるスナップショットを表示するかどうかや、実際に削除を行うかどうかを示します。まずは、表示オプションだけで (つまり、`viewOnly` を `true` に設定して) コードを実行して、コードによって何が削

除されるかを確認します。Storage Gateway で使用できる AWS サービスエンドポイントのリストについては、AWS Storage Gateway 「」の「 エンドポイントとクォータ」を参照してくださいAWS 全般のリファレンス。 Storage Gateway

まず、ユーザーを作成し、最小限の IAM ポリシーをそのユーザーにアタッチします。次に、ゲートウェイの自動スナップショットをスケジュールします。

次のコードでは、ユーザーによるスナップショットの削除を許可する最小限のポリシーを作成します。この例では、ポリシーの名前は **sgw-delete-snapshot** です。

```
{
      "Version": "2012-10-17",
      "Statement": [
          {
              "Sid": "StmtEC2Snapshots",
              "Effect": "Allow",
              "Action": [
                  "ec2:DeleteSnapshot",
                  "ec2:DescribeSnapshots"
              ],
              "Resource": [
                  "*"
              ]
          },
          {
              "Sid": "StmtSgwListVolumes",
              "Effect": "Allow",
              "Action": [
                  "storagegateway:ListVolumes"
              ],
              "Resource": [
                  "*"
              ]
          }
      ]
  }
```

次の C# コードでは、指定されたゲートウェイで、ボリュームと指定されたカットオフ期間が一致するすべてのスナップショットを検出し、削除します。

```
using System;
using System.Collections.Generic;
```

```
using System.Text;
using Amazon.EC2;
using Amazon.EC2.Model;
using Amazon.StorageGateway.Model;
using Amazon.StorageGateway;

namespace DeleteStorageGatewaySnapshotNS
{
    class Program
    {
        /*
         * Replace the variables below to match your environment.
         */

         /* IAM AccessKey */
        static String AwsAccessKey = "AKIA...............";

        /* IAM SecretKey */
        static String AwsSecretKey = "******************************";

        /* Account number, 12 digits, no hyphen */
        static String OwnerID = "123456789012";

        /* Your Gateway ARN. Use a Storage Gateway ID, sgw-XXXXXXXX* */
        static String GatewayARN = "arn:aws:storagegateway:ap-
southeast-2:123456789012:gateway/sgw-XXXXXXXX";

        /* Snapshot status: "completed", "pending", "error" */

        static String SnapshotStatus = "completed";

        /* Region where your gateway is activated */
        static String AwsRegion = "ap-southeast-2";

        /* Minimum age of snapshots before they are deleted (retention policy) */
        static int daysBack = 30;

        /*
         * Do not modify the four lines below.
         */
        static AmazonEC2Config ec2Config;
        static AmazonEC2Client ec2Client;
        static AmazonStorageGatewayClient sgClient;
        static AmazonStorageGatewayConfig sgConfig;
```

```
        static void Main(string[] args)
        {
            // Create an EC2 client.
            ec2Config = new AmazonEC2Config();
            ec2Config.ServiceURL = "https://ec2." + AwsRegion + ".amazonaws.com";
            ec2Client = new AmazonEC2Client(AwsAccessKey, AwsSecretKey, ec2Config);

            // Create a Storage Gateway client.
            sgConfig = new AmazonStorageGatewayConfig();
            sgConfig.ServiceURL = "https://storagegateway." + AwsRegion +
".amazonaws.com";
            sgClient = new AmazonStorageGatewayClient(AwsAccessKey, AwsSecretKey,
sgConfig);

            List<VolumeInfo> StorageGatewayVolumes = ListVolumesForGateway();
            List<Snapshot> StorageGatewaySnapshots =
ListSnapshotsForVolumes(StorageGatewayVolumes,
                                                    daysBack);
            DeleteSnapshots(StorageGatewaySnapshots);
        }

        /*
         * List all volumes for your gateway
         * returns: A list of VolumeInfos, or null.
         */
        private static List<VolumeInfo> ListVolumesForGateway()
        {
            ListVolumesResponse response = new ListVolumesResponse();
            try
            {
                ListVolumesRequest request = new ListVolumesRequest();
                request.GatewayARN = GatewayARN;
                response = sgClient.ListVolumes(request);

                foreach (VolumeInfo vi in response.VolumeInfos)
                {
                    Console.WriteLine(OutputVolumeInfo(vi));
                }
            }
            catch (AmazonStorageGatewayException ex)
            {
                Console.WriteLine(ex.Message);
            }
```

```
            return response.VolumeInfos;
        }

        /*
         * Gets the list of snapshots that match the requested volumes
         * and cutoff period.
         */
        private static List<Snapshot> ListSnapshotsForVolumes(List<VolumeInfo> volumes,
int snapshotAge)
        {
            List<Snapshot> SelectedSnapshots = new List<Snapshot>();
            try
            {
                foreach (VolumeInfo vi in volumes)
                {
                    String volumeARN = vi.VolumeARN;
                    String volumeID = volumeARN.Substring(volumeARN.LastIndexOf("/") +
1).ToLower();

                    DescribeSnapshotsRequest describeSnapshotsRequest = new
DescribeSnapshotsRequest();

                    Filter ownerFilter = new Filter();
                    List<String> ownerValues = new List<String>();
                    ownerValues.Add(OwnerID);
                    ownerFilter.Name = "owner-id";
                    ownerFilter.Values = ownerValues;
                    describeSnapshotsRequest.Filters.Add(ownerFilter);

                    Filter statusFilter = new Filter();
                    List<String> statusValues = new List<String>();
                    statusValues.Add(SnapshotStatus);
                    statusFilter.Name = "status";
                    statusFilter.Values = statusValues;
                    describeSnapshotsRequest.Filters.Add(statusFilter);

                    Filter volumeFilter = new Filter();
                    List<String> volumeValues = new List<String>();
                    volumeValues.Add(volumeID);
                    volumeFilter.Name = "volume-id";
                    volumeFilter.Values = volumeValues;
                    describeSnapshotsRequest.Filters.Add(volumeFilter);

                    DescribeSnapshotsResponse describeSnapshotsResponse =
```

```
                    ec2Client.DescribeSnapshots(describeSnapshotsRequest);

                List<Snapshot> snapshots = describeSnapshotsResponse.Snapshots;
                Console.WriteLine("volume-id = " + volumeID);
                foreach (Snapshot s in snapshots)
                {
                    if (IsSnapshotPastRetentionPeriod(snapshotAge, s.StartTime))
                    {
                        Console.WriteLine(s.SnapshotId + ", " + s.VolumeId + ",
                           " + s.StartTime + ", " + s.Description);
                        SelectedSnapshots.Add(s);
                    }
                }
            }
        }
        catch (AmazonEC2Exception ex)
        {
            Console.WriteLine(ex.Message);
        }
        return SelectedSnapshots;
    }

    /*
     * Deletes a list of snapshots.
     */
    private static void DeleteSnapshots(List<Snapshot> snapshots)
    {
        try
        {
            foreach (Snapshot s in snapshots)
            {

                DeleteSnapshotRequest deleteSnapshotRequest = new
DeleteSnapshotRequest(s.SnapshotId);
                DeleteSnapshotResponse response =
ec2Client.DeleteSnapshot(deleteSnapshotRequest);
                Console.WriteLine("Volume: " +
                          s.VolumeId +
                          " => Snapshot: " +
                          s.SnapshotId +
                          " Response: "
                          + response.HttpStatusCode.ToString());
            }
        }
```

```
            catch (AmazonEC2Exception ex)
            {
                Console.WriteLine(ex.Message);
            }
        }

        /*
         * Checks if the snapshot creation date is past the retention period.
         */
        private static Boolean IsSnapshotPastRetentionPeriod(int daysBack, DateTime
 snapshotDate)
        {
            DateTime cutoffDate = DateTime.Now.Add(new TimeSpan(-daysBack, 0, 0, 0));
            return (DateTime.Compare(snapshotDate, cutoffDate) < 0) ? true : false;
        }

        /*
         * Displays information related to a volume.
         */
        private static String OutputVolumeInfo(VolumeInfo vi)
        {
            String volumeInfo = String.Format(
                "Volume Info:\n" +
                "  ARN: {0}\n" +
                "  Type: {1}\n",
                vi.VolumeARN,
                vi.VolumeType);
            return volumeInfo;
        }
    }
}
```

AWS Tools for Windows PowerShellを使用したスナップショットの削除

ボリュームに関連付けられている多数のスナップショットを削除するには、プログラム的な方法を使用します。次に、 AWS Tools for Windows PowerShellを使用してスナップショットを削除する方法の例を示します。サンプルスクリプトを使用するには、PowerShell スクリプトの実行に慣れている必要があります。詳細については、https://docs.aws.amazon.com/powershell/latest/userguide/pstools-getting-started.html の「AWS Tools for Windows PowerShellご利用開始にあたって」を参照してください。いくつかのスナップショットだけを削除する必要がある場合は、スナップショットの削除 の説明に従ってコンソールを使用します。

Example : を使用したスナップショットの削除 AWS Tools for Windows PowerShell

次の PowerShell スクリプト例では、ゲートウェイの各ボリュームのスナップショットと、スナップショットの開始時刻が指定した日付より前か後かを示します。Storage Gateway と Amazon EC2 の AWS Tools for Windows PowerShell コマンドレットを使用します。Amazon EC2 API には、スナップショットを操作するためのオペレーションが含まれています。

スクリプトを更新し、ゲートウェイの Amazon リソースネーム (ARN) およびスナップショットを保存する日数を提供する必要があります。スナップショットは、この期限が削除される前に取得されます。また、viewOnly というブール値も指定する必要があります。この値は、削除されるスナップショットを表示するかどうかや、実際に削除を行うかどうかを示します。まずは、表示オプションだけで (つまり、viewOnly を true に設定して) コードを実行して、コードによって何が削除されるかを確認します。

```
<#
.DESCRIPTION
    Delete snapshots of a specified volume that match given criteria.

.NOTES
    PREREQUISITES:
    1) AWS Tools for Windows PowerShell from https://aws.amazon.com/powershell/
    2) Credentials and AWS Region stored in session using Initialize-AWSDefault.
    For more info see, https://docs.aws.amazon.com/powershell/latest/userguide/
specifying-your-aws-credentials.html

.EXAMPLE
    powershell.exe .\SG_DeleteSnapshots.ps1
#>

# Criteria to use to filter the results returned.
$daysBack = 18
$gatewayARN = "*** provide gateway ARN ***"
$viewOnly = $true;

#ListVolumes
$volumesResult = Get-SGVolume -GatewayARN $gatewayARN
$volumes = $volumesResult.VolumeInfos
Write-Output("`nVolume List")
foreach ($volumes in $volumesResult)
  { Write-Output("`nVolume Info:")
    Write-Output("ARN:  " + $volumes.VolumeARN)
    write-Output("Type: " + $volumes.VolumeType)
```

```
  }

Write-Output("`nWhich snapshots meet the criteria?")
foreach ($volume in $volumesResult)
  {
    $volumeARN = $volume.VolumeARN

    $volumeId = ($volumeARN-split"/")[3].ToLower()

    $filter = New-Object Amazon.EC2.Model.Filter
    $filter.Name = "volume-id"
    $filter.Value.Add($volumeId)

    $snapshots = get-EC2Snapshot -Filter $filter
    Write-Output("`nFor volume-id = " + $volumeId)
    foreach ($s in $snapshots)
    {
       $d = ([DateTime]::Now).AddDays(-$daysBack)
       $meetsCriteria = $false
       if ([DateTime]::Compare($d, $s.StartTime) -gt 0)
       {
            $meetsCriteria = $true
       }

       $sb = $s.SnapshotId + ", " + $s.StartTime + ", meets criteria for delete? " +
 $meetsCriteria
       if (!$viewOnly -AND $meetsCriteria)
       {
           $resp = Remove-EC2Snapshot -SnapshotId $s.SnapshotId
           #Can get RequestId from response for troubleshooting.
           $sb = $sb + ", deleted? yes"
       }
       else {
           $sb = $sb + ", deleted? no"
       }
       Write-Output($sb)
    }
  }
```

ボリュームステータスと移行について

各ボリュームには、ボリュームの状態をわかりやすく示すステータスが関連付けられています。ほぼ常に、ステータスは、ボリュームが正常に機能しており、ユーザーによる対応は不要であることを示

しています。まれに、ボリュームで問題が発生していることをステータスが示すことがあり、ユーザーによる対応が必要かどうかは問題によって異なります。このセクションでは、ユーザーによる対応が必要かどうかを判断するために役立つ情報を示します。ボリュームのステータスは、Storage Gateway コンソールで確認できます。または、 DescribeCachediSCSIVolumesや などの Storage Gateway APIオペレーションのいずれかを使用して確認できますDescribeStorediSCSIVolumes。

トピック

ボリュームのステータスについて

次の表に、Storage Gateway コンソールに表示されるボリュームステータスを示します。ボリュームステータスは、ゲートウェイの各ストレージボリュームの [Status] 列に表示されます。通常どおり機能しているボリュームのステータスは [Available (使用可能)] となっています。

次の表では、各ストレージボリュームのステータスについての説明と、各ステータスごとの対応のタイミングおよびその必要性についてを示しています。[Available (使用可能)] ステータスは、ボリュームの正常な状態を示すステータスです。ボリュームの使用中は常に、またはほとんどの場合にこのステータスである必要があります。

ステータス	意味
[使用可能]	ボリュームは使用できます。このステータスは、ボリュームが正常に実行中であることを示すステータスです。 [ブートストラッピング] フェーズが完了すると、ボリュームは [Available (使用可能)] ステータスに戻ります。つまり、ゲートウェイは最初に [Pass Through (パススルー)] ステータスになってからボリュームに生じたすべての変更を同期します。
ブートストラッピング	ゲートウェイは、 に保存されているデータのコピーとローカルでデータを同期しています AWS。ほとんどの場合、ストレージボリュームのステータスは自動的に [Available (使用可能)] になるため、通常このステータスに対しては何もする必要はありません。

ステータス	意味
	ボリュームのステータスが [ブートストラッピング] の場合、以下のシナリオが考えられます。 • ゲートウェイが予期せずシャットダウンした。 • ゲートウェイのアップロードバッファの容量を超えた。このシナリオでは、ボリュームのステータスが [Pass Through (パススルー)] で、アップロードバッファの空き容量が十分に増設されたときに、ブートストラップが発生します。アップロードバッファの空き領域の割合を増やす 1 つの方法として、追加のアップロードバッファ領域を用意できます。特にこのシナリオでは、ストレージボリュームのステータスが [Pass Through (パススルー)] から [ブートストラッピング] に変わってから、[Available (使用可能)] に変わります。ブートストラップの間もこのボリュームを使い続けることができます。ただし、この時点でボリュームのスナップショットを作成することはできません。 • 保管型ボリュームゲートウェイを作成していて、既存のローカルディスクデータを保存しています。このシナリオでは、ゲートウェイはすべてのデータを にアップロードし始めます AWS。ボリュームは、ローカルディスクのすべてのデータが にコピーされるまで、ブートストラップステータスになります AWS。ブートストラップの間もボリュームを使用できます。ただし、この時点でボリュームのスナップショットを作成することはできません。
[作成中]	ボリュームは現在作成中であり、使用準備ができていません。[Creating (作成中)] は過渡的なステータスです。アクションは必要ありません。
[Deleting] (削除中)	ボリュームは削除中です。[Deleting (削除中)] ステータスは過渡的なものです。アクションは必要ありません。
回復不可能	エラーが発生し、ボリュームは回復できません。この場合の操作については、「ボリュームの問題のトラブルシューティング」を参照してください。

ステータス	意味
パススルー	ローカルに保持されているデータは、 に保存されているデータと同期しません AWS。ボリュームが [パススルー] ステータスにあるときに書き込まれたデータは、ボリュームのステータスが [ブートストラッピング] になるまでキャッシュに残ります。このデータは、ブートストラップステータスが開始され AWS ると、 にアップロードされ始めます。 [パススルー] ステータスになる理由にはいくつかあり、以下のような理由が考えられます。 • ゲートウェイでアップロードバッファ領域が不足した場合、[パススルー] ステータスになります。ボリュームのステータスが [パススルー] である間、アプリケーションでストレージボリュームからのデータの読み込み、および書き込みを続けることができます。ただし、ゲートウェイではそのアップロードバッファにボリュームデータを書き込むことも、このデータを AWSにアップロードすることもしていません。 ゲートウェイでは、ボリュームのステータスが [パススルー] になるまで、ボリュームに書き込まれたデータのアップロードが続行されます。ボリュームのステータスが [パススルー] である間は、保留中またはスケジュールされたストレージボリュームのスナップショットは作成できません。アップロードバッファの超過が原因でストレージボリュームのステータスが [パススルー] である場合に行う操作については、「ボリュームの問題のトラブルシューティング」を参照してください。 ACTIVE ステータスに戻るには、パススルーのボリュームがブートストラップフェーズを完了する必要があります。ブートストラップ中、ボリュームは 内で同期を再確立し AWS、ボリュームへの変更のレコード (ログ) を再開してCreateSnapshot 機能をアクティブ化できるようにします。[ブートストラッピング] 実行中、ボリュームへの書き込みはアップロードバッファに記録されます。 • 複数のストレージボリュームで同時にブートストラップが発生したときは、[パススルー] ステータスになります。1 度に 1 つのゲートウェ

ステータス	意味
	イストレージのみがブートストラップを行うことができます。たとえば、2 つのストレージボリュームを作成し、両方で既存データの保存を選択するとします。この場合、2 番目のストレージボリュームは、最初のストレージボリュームがブートストラップを終了するまで、[パススルー] ステータスとなります。このシナリオでは、必要となる動作はありません。各ストレージボリュームは、作成が完了すると自動的に [Available (使用可能)] ステータスに移行します。ストレージボリュームのステータスが [パススルー] または [ブートストラッピング] の間は、ストレージボリュームの読み込みおよび書き込みができます。 • まれに、[パススルー] ステータスが、アップロードバッファの使用に割り当てられているディスクでエラーが発生したことを示していることがあります。このシナリオで行う操作については、ボリュームの問題のトラブルシューティング を参照してください。 • [パススルー] ステータスは、ボリュームが [アクティブ] または [ブートストラッピング] ステータスのときに発生することがあります。この場合、ボリュームは書き込みを受信しますが、アップロードされたバッファにはその書き込みを記録 (ログ) するための十分な容量がありません。 • [パススルー] ステータスは、ボリュームが任意の状態にあり、ゲートウェイが正常にシャットダウンされていない場合に発生します。この種類のシャットダウンは、ソフトウェアがクラッシュした、あるいは VM の電源が切れている場合に生じます。この場合、ボリュームのすべてのステータスは [パススルー] ステータスに変更します。

ステータス	意味
[Restoring] (復元中)	ボリュームは既存のスナップショットから復元中です。このステータスは、保管型ボリュームにのみ適用されます。詳細については、「ボリュームゲートウェイの仕組み (アーキテクチャ)」を参照してください。 同時に 2 つのストレージボリュームを復元する場合、両方のストレージボリュームのステータスが [リストア中] になります。各ストレージボリュームは、作成が完了すると自動的に [Available (使用可能)] ステータスに移行します。[リストア中] ステータスの間は、ストレージボリュームの読み込みと書き込み、およびスナップショットの作成ができます。
パススルーのリストア中	既存のスナップショットから復元中のボリュームで、アップロードバッファの問題が発生しました。このステータスは、保管型ボリュームにのみ適用されます。詳細については、「ボリュームゲートウェイの仕組み (アーキテクチャ)」を参照してください。 [パススルーのリストア中] ステータスになる原因の 1 つは、ゲートウェイでアップロードバッファ領域が不足した場合です。ステータスが [パススルーのリストア中] である間、アプリケーションでストレージボリュームのデータの読み込み、および書き込みを続けることができます。ただし、ステータスが [パススルーのリストア中] に、ストレージボリュームのスナップショットを作成することはできません。アップロードバッファ容量の超過が原因でストレージボリュームのステータスが [パススルーのリストア中] になっている場合に行うアクションについては、「ボリュームの問題のトラブルシューティング」を参照してください。 まれに、[パススルーのリストア中] ステータスが、アップロードバッファ用に割り当てられているディスクでエラーが発生したことを示していることがあります。このシナリオで行う操作については、ボリュームの問題のトラブルシューティング を参照してください。

ステータス	意味
アップロードバッファ設定なし	ゲートウェイでアップロードバッファが構成されていないため、ボリュームの作成あるいは使用はできません。キャッシュ型ボリューム設定でボリュームにアップロードバッファ容量を追加する方法については、「割り当てるアップロードバッファのサイズの決定」を参照してください。保管型ボリューム設定でボリュームにアップロードバッファ容量を追加する方法については、「割り当てるアップロードバッファのサイズの決定」を参照してください。

アタッチメントステータスについて

Storage Gateway コンソールまたは を使用して、ボリュームをゲートウェイからデタッチしたり、ゲートウェイにアタッチしたりできますAPI。次の表に、Storage Gateway コンソールに表示される、ボリュームアタッチメントのステータスを示します。ボリュームアタッチメントのステータスは、ゲートウェイの各ストレージボリュームの [アタッチメントのステータス] 列に表示されます。たとえば、ゲートウェイからデタッチされたボリュームには [デタッチ済み] のステータスがあります。ボリュームのデタッチとアタッチ方法については、「別のゲートウェイにボリュームを移動する」を参照してください。

ステータス	意味
アタッチ済み	ボリュームはゲートウェイにアタッチされます。
デタッチ済み	ボリュームはゲートウェイからデタッチされます。
デタッチ中	ボリュームはゲートウェイからデタッチされています。ボリュームをデタッチするときにこのボリュームにデータがない場合、このステータスが表示されないことがあります。

キャッシュ型ボリュームステータスの遷移を理解する

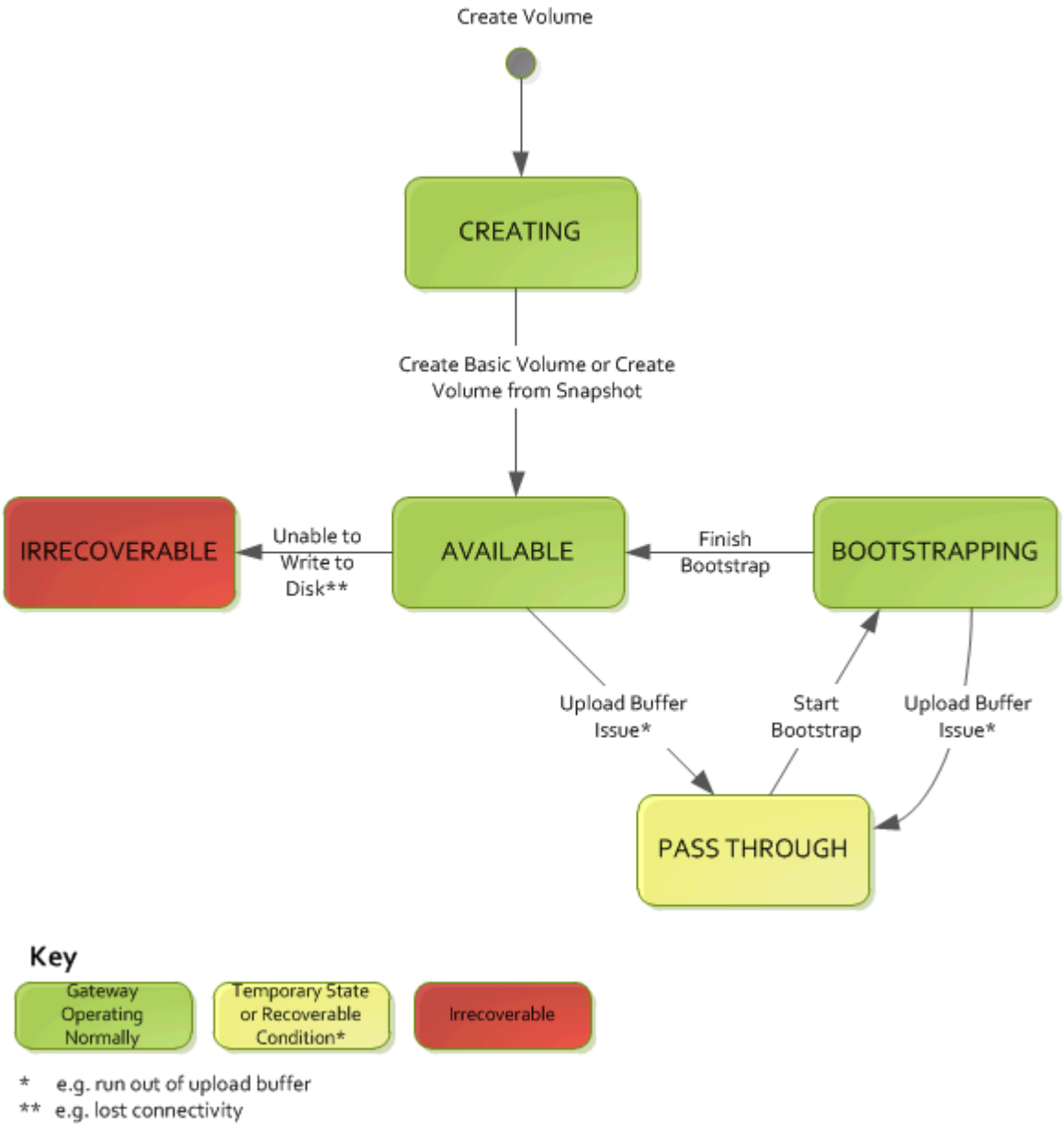
次の図を使用して、キャッシュ型ゲートウェイのボリュームでよく発生するステータス間の遷移を理解します。ゲートウェイを効果的に使用するために、この図を詳しく理解する必要はありません。むしろ、ボリュームゲートウェイの仕組みについて、この図で詳しく知ることができます。

この図には、[アップロードバッファ設定なし] ステータスや [Deleting (削除中)] ステータスは含まれていません。図では、ボリュームのステータスを緑、黄、赤のボックスで表しています。各色は次に説明するように理解します。

色	ボリュームのステータス
グリーン	ゲートウェイは正常に動作しています。ボリュームのステータスは [Available (使用可能)] であるか、またはやがて [Available (使用可能)] になります。
黄色	ボリュームのステータスが [パススルー] です。これは、ストレージボリュームに潜在的な問題があることを示しています。アップロードバッファ領域が満たされているためにこのステータスが表示される場合、バッファ領域が再び利用可能になることがあります。その時点で、ストレージボリュームは [Available (使用可能)] ステータスに自己修正されます。それ以外の場合は、アップロードバッファ領域をゲートウェイに追加して、ストレージボリュームのステータスを [Available (使用可能)] にする必要があります。アップロードバッファ容量が超過した場合にトラブルシューティングする方法については、「ボリュームの問題のトラブルシューティング」を参照してください。アップロードバッファ容量を追加する方法については、「割り当てるアップロードバッファのサイズの決定」を参照してください。
レッド	ストレージボリュームのステータスが [回復不可能] です。この場合、ボリュームを削除する必要があります。これを行う方法については、「ボリュームを削除するには」を参照してください。

図では、2 つのステータスの間の遷移はラベル付きの線で表されます。たとえば、[Creating (作成中)] ステータスから [Available (使用可能)] ステータスへの遷移には、Create Basic Volume (ベーシックボリュームの作成) or Create Volume from Snapshot (ベーシックボリューム作成あるいはスナップ

ショットからのボリュームの作成) というラベルが付きます。この移行はキャッシュ型ボリュームの作成を表しています。ストレージボリュームの作成方法については、「ボリュームの追加」を参照してください。



> **Note**
>
> ボリュームの [パススルー] ステータスは、黄色でこの図に表示されます。またこの色は、Storage Gateway コンソールの [Status] (ステータス) ボックスに表示される、同じステータスアイコンの色とは異なります。

保管型ボリュームステータスの遷移を理解する

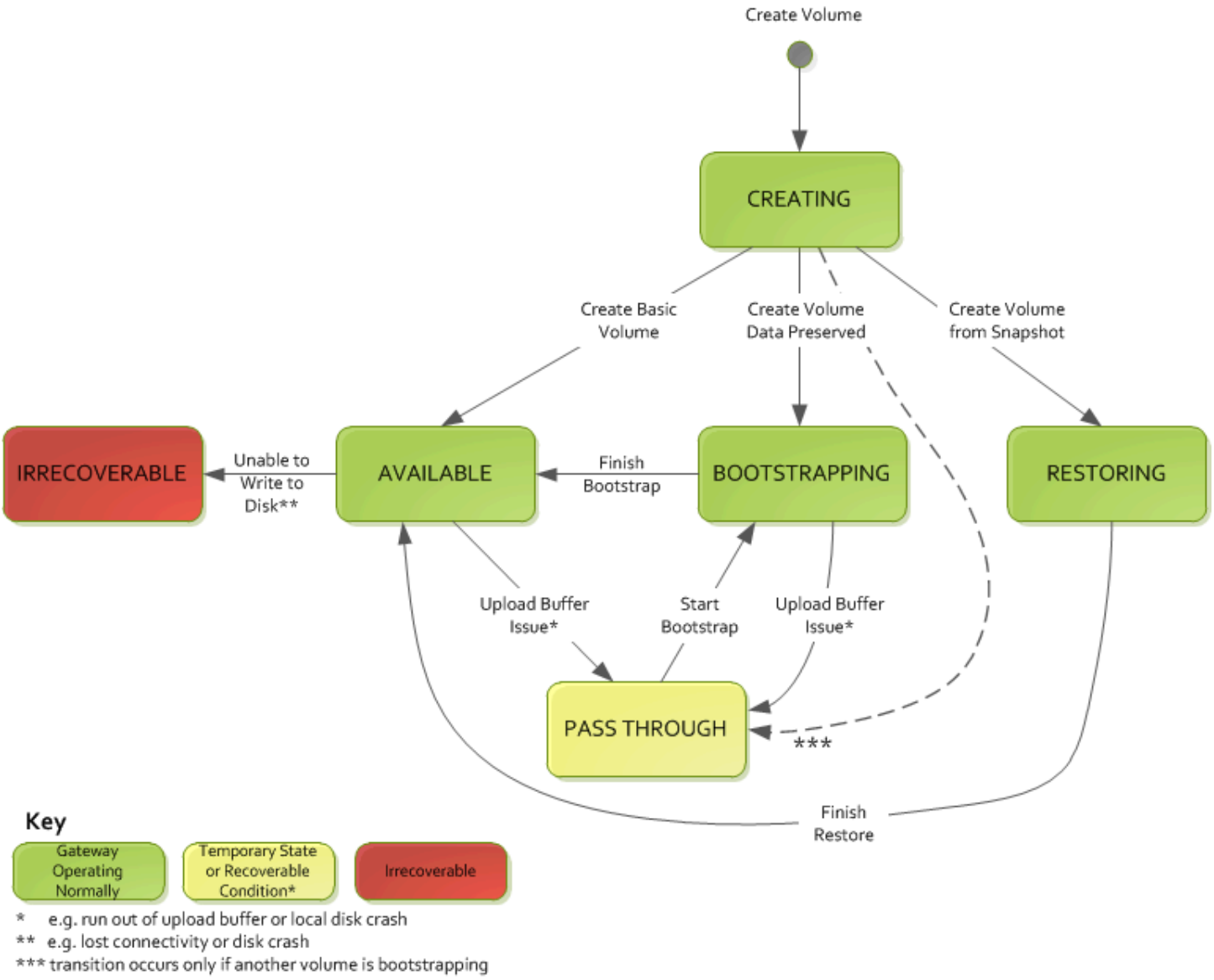
次の図を使用して、保管型ゲートウェイのボリュームでよく発生するステータス間の遷移を理解します。ゲートウェイを効果的に使用するために、この図を詳しく理解する必要はありません。むしろ、ボリュームゲートウェイの仕組みについて、この図で詳しく知ることができます。

この図には、[アップロードバッファ設定なし] ステータスや [Deleting (削除中)] ステータスは含まれていません。図では、ボリュームのステータスを緑、黄、赤のボックスで表しています。各色は次に説明するように理解します。

色	ボリュームのステータス
グリーン	ゲートウェイは正常に動作しています。ボリュームのステータスは [Available (使用可能)] であるか、またはやがて [Available (使用可能)] になります。
黄色	ストレージボリュームの作成中やデータの保存中に、他のボリュームがブートストラップ中の場合、ステータスは [作成中] から [パススルー] に変わります。この場合、[パススルー] ステータスのボリュームは、[ブートストラッピング] ステータスになり、最初のボリュームのブートストラップが終了すると、[Available (使用可能)] ステータスになります。特定のシナリオがある場合を除き、黄色 ([パススルー] ステータス) は、ストレージボリュームに潜在的な問題があることを示します。最も多いのはアップロードバッファの問題です。アップロードバッファ容量が超過している場合、バッファ領域が再び利用可能になることがあります。その時点で、ストレージボリュームは [Available (使用可能)] ステータスに自己修正されます。それ以外の場合は、アップロードバッファ容量をゲートウェイに追加して、ストレージボリュームのステータスを [Available (使用可能)] に戻す必要があります。アップロードバッファ容量が超過した場合にトラブルシューティングする方法については、「ボリュームの問題のトラブ

色	ボリュームのステータス
	ルシューティング」を参照してください。アップロードバッファ容量を追加する方法については、「割り当てるアップロードバッファのサイズの決定」を参照してください。
レッド	ストレージボリュームのステータスが [回復不可能] です。この場合、ボリュームを削除する必要があります。これを行う方法については、「ボリュームの削除」を参照してください。

次の図では、2 つのステータスの間の遷移はラベル付きの線で表されます。たとえば、[Creating (作成中)] ステータスから [Available (使用可能)] ステータスへの遷移には、Create Basic Volume (ベーシックボリュームの作成) というラベルが付きます。この移行は、データ保存なしでのストレージボリュームの作成、あるいはスナップショットからのボリュームの作成を表しています。



> **Note**
>
> ボリュームの [パススルー] ステータスは、黄色でこの図に表示されます。またこの色は、Storage Gateway コンソールの [Status] (ステータス) ボックスに表示される、同じステータスアイコンの色とは異なります。

新しいゲートウェイへのデータの移動

データやパフォーマンスのニーズが大きくなるにつれて、またはゲートウェイを移行する AWS 通知を受け取った場合は、ゲートウェイ間でデータを移動できます。以下に、この目的の例をいくつか示します。

- データをより良いホストプラットフォームまたは新しい Amazon EC2インスタンスに移動します。
- サーバーで基盤となるハードウェアを更新すること。

新しいゲートウェイにデータを移動するためのステップは、使用しているゲートウェイのタイプによって異なります。

> **Note**
>
> データは、同じゲートウェイタイプ間でのみ移動できます。

保管型ボリュームの新しい保管型ボリュームゲートウェイへの移動

保管型ボリュームを新しい保管型ボリュームゲートウェイに移動するには

1. 古い保管型ボリュームゲートウェイに書き込みを行っているアプリケーションをすべて停止します。
2. 以下のステップによりボリュームのスナップショットを作成した後、そのスナップショットの完了まで待機します。

    a. ホーム で Storage Gateway https://console.aws.amazon.com/storagegateway/コンソールを開きます。

    b. ナビゲーションペインで [Volumes] (ボリューム) をクリックした後に、スナップショットの作成元となるボリュームを選択します。

    c. [アクション] で [スナップショットを作成] を選択します。

    d. [Create snapshot] (スナップショットの作成) ダイアログボックスで、スナップショットの説明を入力し、[Create snapshot] (スナップショットを作成) をクリックします。

    スナップショットがコンソールを使用して作成されたことを確認できます。依然としてデータがボリュームにアップロード中である場合は、アップロードが完了するのを待ってから、

次のステップに進みます。保留中のスナップショットがなくなったことを、そのステータスにより確認するには、対象のボリュームのスナップショットへのリンクを選択します。

3. 次の手順に従って、古い保管型ボリュームゲートウェイを停止します。

   a. ナビゲーションペインで [ゲートウェイ] をクリックしてから、停止する古い保管型ボリュームゲートウェイを選択します。ゲートウェイのステータスは [実行中] です。

   b. [Actions] (アクション) で [Stop gateway] (ゲートウェイを停止) をクリックします。このダイアログボックスでゲートウェイの ID を確認した上で、[Stop gateway] (ゲートウェイを停止) をクリックします。

      ゲートウェイが停止中、ゲートウェイのステータスを示すメッセージが表示されることがあります。ゲートウェイをシャットダウンすると、[Details] (詳細) タブにはメッセージと、[Start gateway] (ゲートウェイの起動) ボタンが表示されます。ゲートウェイがシャットダウンした後は、ゲートウェイのステータスが[Shutdown] (シャットダウン) に遷移します。

   c. ハイパーバイザーコントロールを使用して VM をシャットダウンします。

   ゲートウェイを停止する方法については、「ボリュームゲートウェイを起動および停止する」を参照してください。

4. 保管型ボリュームに関連付けられているストレージディスクを、ゲートウェイの VM からデタッチします。これにより、VM のルートディスクは除外されます。

5. Storage Gateway コンソールからhttps://console.aws.amazon.com/storagegateway/ホーム で利用可能な新しいハイパーバイザー VM イメージを使用して、新しい保存済みボリュームStorage Gatewayをアクティブ化します。

6. ステップ 5 で古い保管型ボリュームゲートウェイ VM からデタッチした物理ストレージディスクをアタッチします。

7. ディスク上の既存のデータを保持するには、以下のステップに従って保管型ボリュームを作成します。

   a. Storage Gateway コンソールで、[Create volume] (ボリュームの作成) を選択します。

   b. [ボリュームの作成] ダイアログボックスで、ステップ 5 で作成した保管型ボリュームゲートウェイを選択します。

   c. リストから [Disk ID] (ディスク ID) の値を選択します。

   d. [Volume content] (ボリュームの内容) で、[Preserve existing data on the disk] (ディスクに既存データを保持) オプションを選択します。

ボリュームの作成方法については、「ボリュームの作成」を参照してください。

8. (オプション) 表示されるCHAP認証の設定ウィザードで、イニシエーター名 、イニシエーターシークレット 、およびターゲットシークレット を入力し、保存 を選択します。

   Challenge-Handshake Authentication Protocol (CHAP) 認証の使用の詳細については、「」を参照してくださいiSCSI ターゲットのCHAP認証の設定。

9. 保存したボリュームに書き込むアプリケーションを起動します。

10. 新しい保管型ボリュームゲートウェイが正常に動作していることを確認したら、古い保管型ボリュームゲートウェイを削除できます。

> **Important**
>
> 削除を行う前に、対象のゲートウェイのボリュームに現在書き込んでいるアプリケーションがないことを確認してください。使用中のゲートウェイを削除すると、データが失われる場合があります。

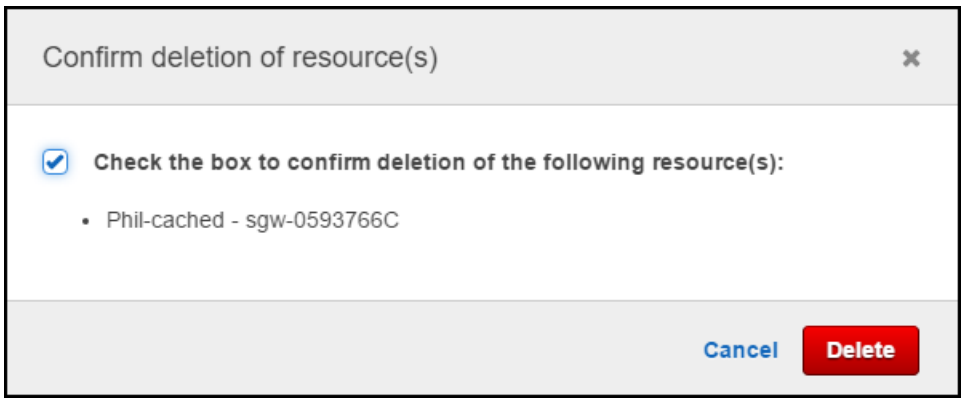
次のステップに従って、古い保管型ボリュームゲートウェイを削除します。

> **Warning**
>
> 削除したゲートウェイを復元することはできません。

a. ナビゲーションペインで [ゲートウェイ] をクリックし、削除対象の古い保管型ボリュームゲートウェイを選択します。

b. [Actions (アクション)] の [Delete gateway (ゲートウェイを削除)] を選択します。

c. 表示される確認ダイアログボックスで、削除を確認するチェックボックスを選択します。リスト内のゲートウェイ ID により、削除対象の古い保管型ボリュームゲートウェイが指定されていることを確認し、[削除] をクリックします。



11. 古いゲートウェイ VM を削除します。VM を削除する方法については、お使いのハイパーバイザーの情報でご確認ください。

キャッシュ型ボリュームを新しいキャッシュ型ボリュームゲートウェイの仮想マシンに移動する

キャッシュ型ボリュームを新しいキャッシュ型ボリュームゲートウェイの仮想マシン (VM) に移動するには

1. 古いキャッシュ型ボリュームゲートウェイに書き込んでいるアプリケーションをすべて停止します。
2. i ボリュームを使用しているクライアントから iSCSI ボリュームをアンマウントまたは切断します。これにより、クライアントがそれらのボリュームでデータの変更や追加を行なくなるので、ボリューム上のデータの整合性を維持できます。
3. 以下のステップによりボリュームのスナップショットを作成した後、そのスナップショットの完了まで待機します。

    a. ホーム で Storage Gateway https://console.aws.amazon.com/storagegateway/コンソールを開きます。

    b. ナビゲーションペインで [Volumes] (ボリューム) をクリックした後に、スナップショットの作成元となるボリュームを選択します。

    c. [アクション] で [スナップショットを作成] を選択します。

    d. [Create snapshot] (スナップショットの作成) ダイアログボックスで、スナップショットの説明を入力し、[Create snapshot] (スナップショットを作成) をクリックします。

    スナップショットがコンソールを使用して作成されたことを確認できます。依然としてデータがボリュームにアップロード中である場合は、アップロードが完了するのを待ってから、

次のステップに進みます。保留中のスナップショットがなくなったことを、そのステータスにより確認するには、対象のボリュームのスナップショットへのリンクを選択します。

コンソールでのボリュームステータスの確認については、「ボリュームステータスと移行について」を参照してください。キャッシュ型ボリュームのステータスについては、「キャッシュ型ボリュームステータスの遷移を理解する」を参照してください。

4. 古いキャッシュ型ボリュームゲートウェイを停止するには、以下のステップに従います。

   a. ナビゲーションペインで [ゲートウェイ] をクリックし、停止する古いキャッシュ型ボリュームゲートウェイを選択します。ゲートウェイのステータスは [実行中] です。

   b. [Actions] (アクション) で [Stop gateway] (ゲートウェイを停止) をクリックします。このダイアログボックスでゲートウェイの ID を確認した上で、[Stop gateway] (ゲートウェイを停止) をクリックします。後のステップで必要になるので、ゲートウェイ ID を書き留めておきます。

      古いゲートウェイの停止処理中、ゲートウェイのステータスを示すメッセージが表示されることがあります。古いゲートウェイがシャットダウンされると、メッセージと [Start gateway] (ゲートウェイの起動) ボタンが、[Details] (詳細) タブに表示されます。ゲートウェイがシャットダウンした後は、ゲートウェイのステータスが[Shutdown] (シャットダウン) に遷移します。

   c. ハイパーバイザーコントロールを使用して古い VM をシャットダウンします。Amazon EC2 インスタンスのシャットダウンの詳細については、「Amazon ユーザーガイド」の「インスタンスの停止と起動」を参照してください。 EC2 KVM、、VMwareまたは Hyper-V VM のシャットダウンの詳細については、ハイパーバイザーのドキュメントを参照してください。

   ゲートウェイを停止する方法については、「ボリュームゲートウェイを起動および停止する」を参照してください。

5. ルートディスク、キャッシュディスク、アップロードバッファディスクを含むすべてのディスクを、古いゲートウェイ VM からデタッチします。

> **Note**
>
> ルートディスクのボリューム ID と、そのルートディスクに関連付けられているゲートウェイ ID を書き留めます。このディスクは、後のステップで新しい Storage Gateway ハイパーバイザーからデタッチします。(ステップ 11 を参照してください。)

キャッシュされたボリュームゲートウェイの VM として Amazon EC2インスタンスを使用している場合は、「Amazon ユーザーガイド」の「Linux インスタンスから Amazon EBSボリュームをデタッチ」する」を参照してください。 EC2 KVM、、VMwareまたは Hyper-V VM からディスクをデタッチする方法については、ハイパーバイザーのドキュメントを参照してください。

6. 新しい Storage Gateway ハイパーバイザー VM インスタンスを作成しますが、ゲートウェイとしてアクティブ化しないでください。新しい Storage Gateway ハイパーバイザー VM の作成方法については、「ボリュームゲートウェイをセットアップする」を参照してください。この新しいゲートウェイは、古いゲートウェイの ID を引き受けます。

   > **Note**
   >
   > 新しい VM には、キャッシュ用のディスクやアップロードバッファを追加しないでください。新しい VM は、古い VM で使用されていたのと同じキャッシュディスクとアップロードバッファディスクを使用します。

7. 新しい Storage Gateway ハイパーバイザー VM インスタンスでも、古い VM と同じネットワーク構成を使用する必要があります。ゲートウェイのデフォルトのネットワーク設定は、Dynamic Host Configuration Protocol () ですDHCP。ではDHCP、ゲートウェイに IP アドレスが自動的に割り当てられます。

   新しい VM の静的 IP アドレスを手動で設定する必要がある場合は、「ゲートウェイのネットワークの設定」を参照して詳細をご確認ください。ゲートウェイが Socket Secure バージョン 5 (SOCKS5) プロキシを使用してインターネットに接続する必要がある場合は、オンプレミスのゲートウェイでのプロキシ経由のルーティング「」で詳細を確認してください。

8. 新しい VM を起動します。

9. ステップ 5 で古いキャッシュ型ボリュームゲートウェイ VM からデタッチしたディスクを、新しいキャッシュ型ボリュームゲートウェイにアタッチします。古いゲートウェイ VM の場合と同じ順序で、これらを新しいゲートウェイ VM にアタッチします。

   すべてのディスクを変更なしで移行する必要があります。ボリュームサイズを変更しないでください。変更するとメタデータの整合性がなくなります。

10. 次の形式を使用する で新しい VM に接続してURL、ゲートウェイ移行プロセスを開始します。

```
http://your-VM-IP-address/migrate?gatewayId=your-gateway-ID
```

新しいゲートウェイ VM には、古いゲートウェイ VM で使用したのと同じ IP アドレスを再使用できます。URL は次の例のようになります。

```
http://198.51.100.123/migrate?gatewayId=sgw-12345678
```

これをブラウザURLから、または を使用してコマンドラインから使用してcurl、移行プロセスを開始します。

ゲートウェイ移行プロセスが正常に開始されると、次のメッセージが表示されます。

```
Successfully imported Storage Gateway information. Please refer to
Storage Gateway documentation to perform the next steps to complete the
migration.
```

11. ステップ 5 でメモしたボリューム ID の、古いゲートウェイのルートディスクをデタッチします。
12. ゲートウェイを起動します。

    新しいキャッシュ型ボリュームゲートウェイを起動するには、次のステップに従います。

    a. ホーム で Storage Gateway https://console.aws.amazon.com/storagegateway/コンソールを開きます。
    b. ナビゲーションペインで [Gateways] (ゲートウェイ) をクリックしてから、起動する新しいゲートウェイを選択します。ゲートウェイのステータスは [シャットダウン] です。
    c. [Details] (詳細) 、[Start gateway] (ゲートウェイの起動) の順にクリックします。

    ゲートウェイの起動の詳細については、「ボリュームゲートウェイを起動および停止する」を参照してください。
13. これでボリュームが、新しいゲートウェイ VM の IP アドレスでアプリケーションを使用できるようになります。
14. ボリュームが使用可能であることを確認し、古いゲートウェイ VM を削除します。VM を削除する方法については、お使いのハイパーバイザーの情報でご確認ください。

Storage Gateway のモニタリング

このセクションでは、Amazon を使用して、ゲートウェイに関連付けられたリソースのモニタリングなど、ゲートウェイをモニタリングする方法について説明します CloudWatch。ゲートウェイのアップロードバッファとキャッシュストレージをモニタリングできます。Storage Gateway コンソールを使用してゲートウェイのメトリクスとアラームを表示します。例えば、読み取り/書き込みオペレーションで使用されたバイト数、読み取り/書き込みオペレーションにかかった時間、および Amazon Web Services クラウドからデータを取得するためにかかった時間を表示できます。メトリックスを使用することにより、ゲートウェイの状態を追跡して、1 つ以上のメトリックスが定義されているしきい値を超えると通知を受け取るようにアラームをセットアップできます。

Storage Gateway は、追加料金なしで CloudWatch メトリクスを提供します。Storage Gateway メトリクスは 2 週間記録されます。これらのメトリクスを使用することにより、履歴情報にアクセスして、ゲートウェイとボリュームのパフォーマンスをより的確に把握できます。Storage Gateway は、高解像度 CloudWatch アラームを除くアラームも追加料金なしで提供します。 CloudWatch 料金の詳細については、「Amazon CloudWatch の料金」を参照してください。の詳細については CloudWatch、「Amazon ユーザーガイド CloudWatch 」を参照してください。

トピック

- ゲートウェイメトリクスについて
- Storage Gateway メトリクスのディメンション
- アップロードバッファのモニタリング
- キャッシュストレージのモニタリング
- CloudWatch アラームについて
- ゲートウェイの推奨 CloudWatch アラームの作成
- ゲートウェイのカスタム CloudWatch アラームの作成
- ボリュームゲートウェイのモニタリング

ゲートウェイメトリクスについて

このトピックの説明では、ゲートウェイメトリクスを、ゲートウェイの範囲内にあるメトリクス、つまり、ゲートウェイに関する何かを測定するメトリクスと定義しています。ゲートウェイには 1 つ以上のボリュームが含まれているので、ゲートウェイ固有のメトリクスは、ゲートウェイにあるすべてのボリュームの代表です。たとえば、`CloudBytesUploaded` メトリクスは、レポート期間中に

ゲートウェイがクラウドに送信した総バイト数です。このメトリクスには、ゲートウェイのすべてのボリュームのアクティビティが含まれます。

ゲートウェイメトリクスデータを使用するとき、メトリクスを表示するゲートウェイの一意の ID を指定します。これを行うには、GatewayId 値と GatewayName 値の両方を指定します。ゲートウェイのメトリクスを使用する場合は、メトリクスの名前空間でゲートウェイのディメンションを指定して、ゲートウェイ固有のメトリクスをボリューム固有のメトリクスと区別します。詳細については、「Amazon CloudWatch メトリクスの使用」を参照してください。

> **Note**
>
> 一部のメトリクスは、直近のモニタリング期間中に新しいデータが生成された場合にのみデータポイントを返します。

メトリクス	説明
AvailabilityNotifications	ゲートウェイによって生成された可用性関連のヘルス通知の数。 このメトリクスを Sum 統計とともに使用して、ゲートウェイで可用性関連のイベントが発生しているかどうかを調べます。イベントの詳細については、設定した CloudWatch ロググループを確認してください。 単位: 数値
CacheHitPercent	キャッシュから提供されたアプリケーション読み取りの割合。サンプリングは、レポート期間の最後に行われます。 単位: パーセント

メトリクス	説明	
CacheUsed	ゲートウェイのキャッシュストレージで使用されている総バイト数。サンプリングは、レポート期間の最後に行われます。 単位: バイト	
IoWaitPercent	ゲートウェイがローカルディスクからの応答を待機している時間の割合。 単位: パーセント	
MemTotalBytes	ゲートウェイ VM にRAMプロビジョニングされる のバイト数。 単位: バイト	
MemUsedBytes	ゲートウェイ VM がRAM現在使用している のバイト数。 単位: バイト	
QueuedWrites	への書き込みを待機しているバイト数。ゲートウェイ内のすべてのボリュームについてAWS、レポート期間の終了時にサンプリングされます。このバイト数はゲートウェイの作業ストレージに保存されます。 単位: バイト	

メトリクス	説明
ReadBytes	ゲートウェイにあるすべてのボリュームを対象としたレポートの期間中に内部設置型のアプリケーションから読み取られた総バイト数。 このメトリクスを Sum 統計で使用してスループットを測定し、 Samples 統計で を測定しますIOPS。 単位: バイト
ReadTime	ゲートウェイにあるすべてのボリュームを対象としたレポートの期間中にオンプレミスのアプリケーションからの読み込みオペレーションにかかった合計時間 (ミリ秒)。 このメトリクスを Average 統計と共に使用してレイテンシーを測定します。 単位: ミリ秒
TimeSinceLastRecoveryPoint	使用可能な最新の復旧ポイントからの時間。詳細については、「ゲートウェイキャッシュ型が到達不可能なためデータを復旧する場合」を参照してください。 単位: 秒

メトリクス	説明	
TotalCacheSize	キャッシュの総バイト数。サンプリングは、レポート期間の最後に行われます。 単位: バイト	
UploadBufferPercentUsed	ゲートウェイのアップロードバッファの使用率。サンプリングは、レポート期間の最後に行われます。 単位: パーセント	
UploadBufferUsed	ゲートウェイのアップロードバッファで使用されている総バイト数。サンプリングは、レポート期間の最後に行われます。 単位: バイト	
UserCpuPercent	ゲートウェイ処理に費やされたCPU時間の割合。すべてのコアで平均化されます。 単位: パーセント	
WorkingStorageFree	ゲートウェイの作業ストレージの未使用領域の量。サンプリングは、レポート期間の最後に行われます。 単位: バイト	

メトリクス	説明
WorkingStoragePercentUsed	ゲートウェイのアップロードバッファの使用率。サンプリングは、レポート期間の最後に行われます。 単位: パーセント
WorkingStorageUsed	ゲートウェイのアップロードバッファで使用されている総バイト数。サンプリングは、レポート期間の最後に行われます。 単位: バイト
WriteBytes	ゲートウェイにあるすべてのボリュームを対象としたレポートの期間中に内部設置型のアプリケーションに書き込まれた総バイト数。 このメトリクスを Sum 統計で使用してスループットを測定し、 Samples 統計で を測定しますIOPS。 単位: バイト

メトリクス	説明	
WriteTime	ゲートウェイにあるすべてのボリュームを対象としたレポートの期間中にオンプレミスのアプリケーションからの書き込みオペレーションにかかった合計時間 (ミリ秒)。 このメトリクスを Average 統計と共に使用してレイテンシーを測定します。 単位: ミリ秒	

Storage Gateway メトリクスのディメンション

Storage Gateway サービス CloudWatch の名前空間は ですAWS/StorageGateway。データは自動的に 5 分間無料で取得できます。

ディメンション	説明
GatewayId , GatewayName	このディメンションを指定すると、リクエストしたデータがフィルタリングされて、ゲートウェイ固有のメトリクスのものだけになります。対象となるゲートウェイは、GatewayId または GatewayName の値で特定できます。メトリクスの表示に関連した時間範囲でゲートウェイの名前が異なる場合は、GatewayId を使用します。 ゲートウェイのスループットとレイテンシーデータは、ゲートウェイの全ボリュームによって変動します。ゲートウェイメトリクスの操作については、「ゲートウェイと 間のパフォーマンスの測定 AWS」を参照してください。
VolumeId	このディメンションを指定すると、リクエストしたデータがフィルタリングされて、ボリュームに固有のメトリクスのものだけになります。VolumeId の値によって、使用するストレー

ディメンション	説明
	ジボリュームを特定します。ボリュームメトリクスの使用の詳細については、「アプリケーションとゲートウェイの間のパフォーマンスの測定」を参照してください。

アップロードバッファのモニタリング

このセクションでは、ゲートウェイのアップロードバッファをモニタリングする方法と、バッファが特定のしきい値を超えると通知を受け取るようにアラームを作成する方法について説明します。これにより、バッファが完全に消費され、ストレージアプリケーションが AWSへのバックアップを停止する前に、ゲートウェイにバッファストレージを追加できます。

アップロードバッファのモニタリング方法は、キャッシュ型ボリュームおよびテープゲートウェイの両方のアーキテクチャで同じです。詳細については、「ボリュームゲートウェイの仕組み (アーキテクチャ)」を参照してください。

> **Note**
>
> `WorkingStoragePercentUsed`、`WorkingStorageUsed`、および `WorkingStorageFree` メトリクスは、Storage Gateway のキャッシュ型ボリューム機能がリリースされる前にのみ、保存されたボリュームのアップロードバッファについて表していました。現在は、同等のアップロードバッファメトリクスとして `UploadBufferPercentUsed`、`UploadBufferUsed`、および `UploadBufferFree` を使用します。これらのメトリクスは、両方のゲートウェイアーキテクチャに適用されます。

対象となる項目	測定方法
アップロードバッファの使用量	`UploadBufferPercentUsed` 、`UploadBufferUsed` 、および `UploadBufferFree` メトリクスを `Average` 統計と共に使用します。例えば、期間中のストレージ使用量を分析するには、`UploadBufferUsed` を `Average` 統計と共に使用します。

使用されるアップロードバッファの割合を測定するには

1. で CloudWatch コンソールを開きますhttps://console.aws.amazon.com/cloudwatch/。
2. StorageGateway: Gateway Metrics ディメンションを選択し、使用するゲートウェイを見つけます。
3. `UploadBufferPercentUsed` メトリクスを選択します。
4. [Time Range] で値を選択します。
5. `Average` 統計を選択します。
6. [Period] で、デフォルトのレポート時間に合わせて 5 分を選択します。

表示された時系列のデータポイントのセットには、アップロードバッファの使用率が含まれています。

次の手順を使用して、 CloudWatch コンソールを使用してアラームを作成できます。アラームとしきい値の詳細については、「Amazon CloudWatch ユーザーガイド」の CloudWatch 「アラームの作成」を参照してください。

ゲートウェイのアップロードバッファの上限アラームを設定するには

1. で CloudWatch コンソールを開きますhttps://console.aws.amazon.com/cloudwatch/。
2. [Create Alarm (アラームの作成)] を選択して、アラームの作成ウィザードを起動します。
3. アラームのメトリクスを指定します。
   a. アラームの作成ウィザードのメトリクスの選択ページで、AWS/StorageGateway : GatewayId、GatewayNameディメンションを選択し、使用するゲートウェイを見つけます。
   b. `UploadBufferPercentUsed` メトリクスを選択します。`Average` 統計および 5 分の期間を使用します。
   c. [Continue] (続行) を選択します。
4. アラームの名前、説明、しきい値を定義します。
   a. Create Alarm Wizard の [Define Alarm (アラームの定義)] ページで、[Name (名前)] ボックスにアラームの名前を、[Description (説明)] ボックスにアラームの説明を入力して、アラームを指定します。
   b. アラームのしきい値を定義します。
   c. [Continue] (続行) を選択します。

5. アラームの E メールアクションを設定します。

   a. Create Alarm Wizard の [Configure Actions (アクションの設定)] ページで、[Alarm State (アラームの状態)] として [Alarm (アラーム)] を選択します。

   b. [Topic] (トピック) で [Choose or create email topic] (E メールトピックの選択または作成) を選択します。

      E メールトピックを作成するには、Amazon SNSトピックを設定することを意味します。Amazon の詳細についてはSNS、「Amazon ユーザーガイド」の「Amazon のセットアップSNS CloudWatch 」を参照してください。

   c. [トピック] に、トピックを示すわかりやすい名前を入力します。

   d. [Add Action] (アクションの追加) を選択します。

   e. [Continue] (続行) を選択します。

6. アラーム設定を確認してアラームを作成します。

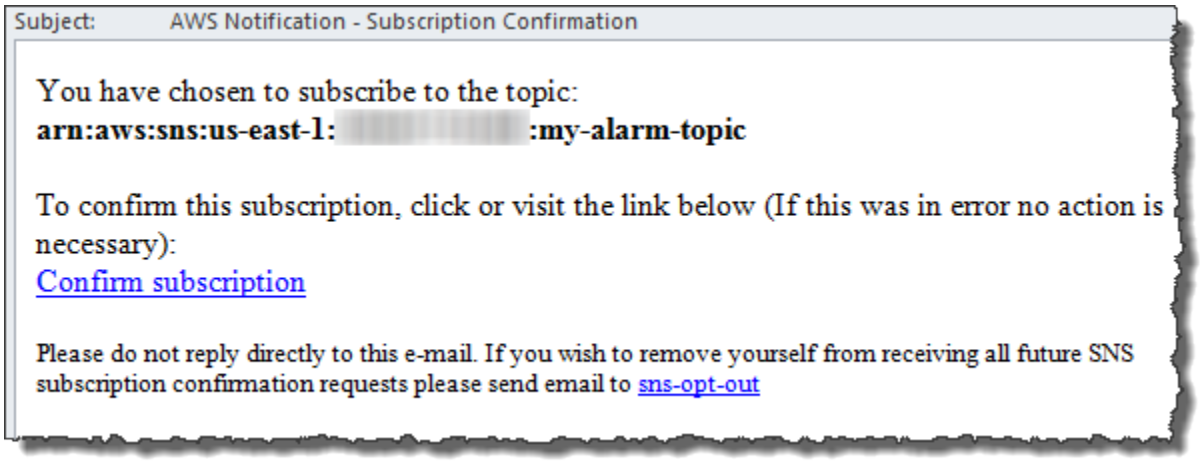
   a. Create Alarm Wizard の [Review (レビュー)] ページで、アラーム定義、メトリクス、および実行する関連アクション (E メール通知の送信など) を確認します。

   b. アラームの要約を確認したら、[Save Alarm] を選択します。

7. アラームトピックの受信登録を確認します。

   a. トピックの作成時に指定した SNS E メールアドレスに送信された Amazon E メールを開きます。

      次の図は、一般的な E メール通知を示しています。



   b. メール内のリンクをクリックして、受信登録を確認します。

サブスクリプションの確認が表示されます。

キャッシュストレージのモニタリング

このセクションでは、ゲートウェイのキャッシュストレージをモニタリングする方法と、キャッシュのパラメーターが特定のしきい値を超えると通知を受け取るようにアラームを作成する方法について説明します。このアラームを使用すると、ゲートウェイにキャッシュストレージを追加するタイミングがわかります。

キャッシュストレージのモニタリングは、キャッシュ型ボリュームのアーキテクチャのみで行われます。詳細については、「ボリュームゲートウェイの仕組み (アーキテクチャ)」を参照してください。

対象となる項目	測定方法
キャッシュの総使用量	CachePercentUsed および TotalCacheSize メトリクスを Average 統計と共に使用します。たとえば、期間中のストレージのキャッシュ使用状況を分析するには、CachePercentUsed を Average 統計と共に使用します。 TotalCacheSize メトリクスは、ゲートウェイにキャッシュを追加した場合にのみ変化します。
キャッシュから提供された読み取りリクエストの割合	CacheHitPercent メトリクスと共に Average 統計を使用します。 通常、CacheHitPercent は高いままであることが適切です。
ダーティキャッシュの割合 - にアップロードされていないコンテンツが含まれています AWS	CachePercentDirty メトリクスと共に Average 統計を使用します。 通常は、CachePercentDirty は低いままにします。

ゲートウェイとそのすべてのボリュームに対してダーティなキャッシュの割合を測定するには

1. で CloudWatch コンソールを開きますhttps://console.aws.amazon.com/cloudwatch/。

2. StorageGateway: Gateway Metrics ディメンションを選択し、使用するゲートウェイを見つけます。
3. `CachePercentDirty` メトリクスを選択します。
4. [Time Range] で値を選択します。
5. `Average` 統計を選択します。
6. [Period] で、デフォルトのレポート時間に合わせて 5 分を選択します。

表示された時系列のデータポイントのセットには、5 分間のダーティなキャッシュの割合が含まれています。

ボリュームのダーティなキャッシュの割合を測定するには

1. で CloudWatch コンソールを開きますhttps://console.aws.amazon.com/cloudwatch/。
2. StorageGateway: ボリュームメトリクスディメンションを選択し、操作するボリュームを見つけます。
3. `CachePercentDirty` メトリクスを選択します。
4. [Time Range] で値を選択します。
5. `Average` 統計を選択します。
6. [Period] で、デフォルトのレポート時間に合わせて 5 分を選択します。

表示された時系列のデータポイントのセットには、5 分間のダーティなキャッシュの割合が含まれています。

CloudWatch アラームについて

CloudWatch アラームは、メトリクスと式に基づいてゲートウェイに関する情報をモニタリングします。ゲートウェイに CloudWatch アラームを追加し、Storage Gateway コンソールでそのステータスを表示できます。ボリュームゲートウェイのモニタリングに使用されるメトリクスの詳細については、「ゲートウェイメトリクスについて」および「ボリュームメトリクスについて」を参照してください。アラームごとに、そのALARM状態を開始する条件を指定します。Storage Gateway コンソールのアラームステータスインジケータは、 ALARM状態のときに赤に変わるため、ステータスをプロアクティブにモニタリングしやすくなります。状態の継続的な変化に応じて自動的にアクションを呼び出すようにアラームを設定できます。 CloudWatch アラームの詳細については、「Amazon CloudWatch ユーザーガイド」の「Amazon アラームの使用 CloudWatch 」を参照してください。

> **Note**
>
> を表示するアクセス許可がない場合は CloudWatch、アラームを表示できません。

アクティブ化されたゲートウェイごとに、次の CloudWatchアラームを作成することをお勧めします。

- 高い IO 待機率: `IoWaitpercent` >= 20、3 つのデータポイント、15 分以内
- キャッシュのダーティ率: `CachePercentDirty` > 80、4 つのデータポイント、20 分以内
- ヘルス通知: `HealthNotifications` >= 1、1 つのデータポイント、5 分以内 このアラームを設定するときは、欠損データ処理を に設定しますnotBreaching。

> **Note**
>
> ヘルス通知アラームは、ゲートウェイが で以前のヘルス通知を持っていた場合にのみ設定できます CloudWatch。

HA モードが有効なVMwareホストプラットフォーム上のゲートウェイの場合、次の追加の CloudWatch アラームもお勧めします。

- 可用性通知: `AvailabilityNotifications` >= 1、1 つのデータポイント、5 分以内 このアラームを設定するときは、欠損データ処理を に設定しますnotBreaching。

次の表に、アラームの状態を示します。

状態	説明
OK	メトリクスや式は、定義されているしきい値の範囲内です。
アラーム	メトリクスまたは式が、定義されているしきい値を超えています。
不十分なデータ	アラームが開始直後であるか、メトリクスが利用できないか、メトリクス用のデータが不足し

状態	説明
	ているため、アラームの状態を判定できません。
なし	ゲートウェイのアラームが作成されていません。新しいアラームを作成する方法については、「ゲートウェイのカスタム CloudWatch アラームの作成」を参照してください。
使用不可	アラームの状態が不明です。[Monitoring] (モニタリング) タブでエラー情報を表示するには、[Unavailable] (使用不可) を選択します。

ゲートウェイの推奨 CloudWatch アラームの作成

Storage Gateway コンソールを使用して新しいゲートウェイを作成する場合、初期設定プロセスの一環として、すべての推奨 CloudWatch アラームを自動的に作成することを選択できます。詳細については、「ボリュームゲートウェイを設定する」を参照してください。既存のゲートウェイの推奨 CloudWatch アラームを追加または更新する場合は、次の手順を使用します。

既存のゲートウェイの推奨 CloudWatch アラームを追加または更新するには

> **Note**
>
> この機能には、事前設定された Storage Gateway フルアクセス CloudWatch ポリシーの一部として自動的に付与されないポリシー許可が必要です。推奨 CloudWatch アラームを作成する前に、セキュリティポリシーで次のアクセス許可が付与されていることを確認してください。
>
> - `cloudwatch:PutMetricAlarm` - アラームを作成する
> - `cloudwatch:DisableAlarmActions` - アラームアクションをオフにする
> - `cloudwatch:EnableAlarmActions` - アラームアクションをオンにする
> - `cloudwatch:DeleteAlarms` - アラームを削除する

1. https://console.aws.amazon.com/storagegateway/home/ で Storage Gateway コンソールを開きます。
2. ナビゲーションペインで、ゲートウェイ を選択し、推奨 CloudWatch アラームを作成するゲートウェイを選択します。
3. ゲートウェイの詳細ページで、[モニタリング] タブを選択します。
4. [アラーム] で [推奨アラームを作成] を選択します。推奨アラームが自動的に作成されます。

   アラームセクションには、特定のゲートウェイのすべての CloudWatch アラームが一覧表示されます。ここから、1 つ以上のアラームを選択して削除したり、アラームアクションをオンまたはオフにしたり、新しいアラームを作成したりできます。

ゲートウェイのカスタム CloudWatch アラームの作成

CloudWatch は、Amazon Simple Notification Service (Amazon SNS) を使用して、アラームの状態が変更されたときにアラーム通知を送信します。アラームは、指定期間にわたって単一のメトリクスを監視し、指定したしきい値に対応したメトリクスの値に基づいて、期間数にわたって 1 つ以上のアクションを実行します。アクションは、Amazon SNSトピックに送信される通知です。CloudWatch アラームを作成するときに Amazon SNSトピックを作成できます。Amazon の詳細についてはSNS、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNSとは」を参照してください。

Storage Gateway コンソールで CloudWatch アラームを作成するには

1. https://console.aws.amazon.com/storagegateway/home/ で Storage Gateway コンソールを開きます。
2. ナビゲーションペインで [ゲートウェイ] を選択してから、アラームを作成するゲートウェイを選択します。
3. ゲートウェイの詳細ページで、[モニタリング] タブを選択します。
4. アラーム で、アラームの作成 を選択して CloudWatch コンソールを開きます。
5. CloudWatch コンソールを使用して、必要なアラームのタイプを作成します。以下のタイプのアラームを作成できます。

   - 静的しきい値アラーム: 指定のメトリクスに応じて設定されたしきい値に基づくアラーム。アラームは、メトリクスが指定された評価期間数のしきい値を超えたときに ALARM状態になります。

静的しきい値アラームを作成するには、「Amazon ユーザーガイド」の「静的しきい値に基づく CloudWatch アラームの作成」を参照してください。 CloudWatch

- 異常検出アラーム: 異常検出では、過去のメトリクスデータのマイニングにより、想定値のモデルが作成されます。異常検出のしきい値を設定すると、 はこのしきい値をモデルとともに CloudWatch 使用して、メトリクスの値の「正常」範囲を決定します。しきい値を高くするほど、「正常」な値の範囲が広がります。アラームがトリガーされるのが、メトリクスの値が想定値の範囲を上回る場合、下回る場合、または上回るか下回った場合のいずれかを選択できます。

  異常検出アラームを作成するには、「Amazon CloudWatch ユーザーガイド」の「異常検出に基づく CloudWatch アラームの作成」を参照してください。
- メトリクス数式アラーム: 1 つ以上のメトリクスを使用した数式に基づくアラーム。式、しきい値、および評価期間を指定します。

  メトリクス数式アラームを作成するには、「Amazon CloudWatch ユーザーガイド」の「メトリクス数式に基づく CloudWatch アラームの作成」を参照してください。
- 複合アラーム: 他のアラームのアラーム状態を監視してアラーム状態を決定するアラーム。複合アラームは、アラームノイズの低減に役立ちます。

  複合アラームを作成するには、「Amazon ユーザーガイド」の「複合アラームの作成」を参照してください。 CloudWatch

6. CloudWatch コンソールでアラームを作成したら、Storage Gateway コンソールに戻ります。アラームを表示するには、次のいずれかを行います。

   - ナビゲーションペインで [ゲートウェイ] を選択してから、アラームを表示するゲートウェイを選択します。詳細タブのアラーム で、CloudWatch アラーム を選択します。
   - ナビゲーションペインで [ゲートウェイ] を選択し、アラームを表示したいゲートウェイを選択して、[モニタリング] タブを選択します。

     アラームセクションには、特定のゲートウェイのすべての CloudWatch アラームが一覧表示されます。ここから、1 つ以上のアラームを選択して削除したり、アラームアクションをオンまたはオフにしたり、新しいアラームを作成したりできます。
   - ナビゲーションペインで [ゲートウェイ] を選択し、アラームを表示したいゲートウェイのアラーム状態を選択します。

アラームを編集または削除する方法の詳細については、CloudWatch「アラームの編集または削除」を参照してください。

> **Note**
>
> Storage Gateway コンソールを使用してゲートウェイを削除すると、ゲートウェイに関連付けられているすべての CloudWatch アラームも自動的に削除されます。

ボリュームゲートウェイのモニタリング

このセクションでは、キャッシュ型ボリュームまたは保管型ボリュームのセットアップのゲートウェイをモニタリングする方法について説明します。これには、ゲートウェイに関連付けられているボリュームのモニタリングとアップロードバッファのモニタリングが含まれます。ゲートウェイのメトリクスを表示するには AWS Management Console 、 を使用します。例えば、読み取り/書き込みオペレーションで使用されたバイト数、読み取り/書き込みオペレーションにかかった時間、および Amazon Web Services クラウドからデータを取得するためにかかった時間を表示できます。メトリックスを使用することにより、ゲートウェイの状態を追跡して、1 つ以上のメトリックスが定義されているしきい値を超えると通知を受け取るようにアラームをセットアップできます。

Storage Gateway は、追加料金なしで CloudWatch メトリクスを提供します。Storage Gateway メトリクスは 2 週間記録されます。これらのメトリクスを使用することにより、履歴情報にアクセスして、ゲートウェイとボリュームのパフォーマンスをより的確に把握できます。の詳細については CloudWatch、「Amazon CloudWatch ユーザーガイド」を参照してください。

トピック

- Amazon Logs を使用したボリュームゲートウェイヘルス CloudWatch ログの取得
- Amazon CloudWatch メトリクスの使用
- アプリケーションとゲートウェイの間のパフォーマンスの測定
- ゲートウェイと AWSの間のパフォーマンスの測定
- ボリュームメトリクスについて

Amazon Logs を使用したボリュームゲートウェイヘルス CloudWatch ログの取得

Amazon CloudWatch Logs を使用して、ボリュームゲートウェイと関連リソースのヘルスに関する情報を取得できます。これらのログを使用して、ゲートウェイで発生するエラーをモニタリングできます。さらに、Amazon CloudWatch サブスクリプションフィルターを使用して、ログ情報のリアルタイム処理を自動化できます。詳細については、「Amazon ユーザーガイド」の「サブスクリプションによるログデータのリアルタイム処理」を参照してください。 CloudWatch

例えば、VMware High Availability (HA) が有効なクラスターにゲートウェイがデプロイされ、エラーについて把握する必要があるとします。ゲートウェイをモニタリングし、ゲートウェイでエラーが発生したときに通知を受け取るように CloudWatch ロググループを設定できます。このグループの設定は、ゲートウェイをアクティブ化するときか、ゲートウェイをアクティブ化して実行した後に可能です。ゲートウェイをアクティブ化するときに CloudWatch ロググループを設定する方法については、「」を参照してくださいボリュームゲートウェイを設定する。 CloudWatch ロググループに関する一般的な情報については、「Amazon ユーザーガイド」の「ロググループとログストリームの使用」を参照してください。 CloudWatch

これらのタイプのエラーをトラブルシューティングおよび修正する方法については、「ボリュームの問題のトラブルシューティング」を参照してください。

次の手順は、ゲートウェイがアクティブ化された後に CloudWatch ロググループを設定する方法を示しています。

ゲートウェイで動作するように CloudWatch ロググループを設定するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/storagegateway/home で Storage Gateway コンソールを開きます。
2. 左側のナビゲーションペインで、ゲートウェイ を選択し、 CloudWatch ロググループを設定するゲートウェイを選択します。
3. アクション で、ゲートウェイ情報の編集 を選択するか、詳細 タブのヘルスログ および 非有効化 で、ロググループの設定 を選択して 編集 ***CustomerGatewayName*** ダイアログボックスを開きます。
4. [Gateway health log group] (ゲートウェイヘルスロググループ) で、次のいずれかを選択します。

   - ロググループを使用してゲートウェイをモニタリングしない場合は、 CloudWatch ログ記録を無効にします。

- 新しいロググループを作成して、新しい CloudWatch ロググループを作成します。
- 既存のロググループを使用して、既存の CloudWatch ロググループを使用します。[Existing log group list] (既存のロググループのリスト) から、ロググループを選択します。

5. [変更の保存] をクリックします。
6. ゲートウェイのヘルスログを表示するには、次の操作を行います。

   1. 左側のナビゲーションペインで、ゲートウェイ を選択し、 CloudWatch ロググループを設定したゲートウェイを選択します。
   2. 詳細 タブを選択し、ヘルスログ で CloudWatch ログ を選択します。ロググループの詳細ページが Amazon CloudWatch コンソールで開きます。

Amazon CloudWatch メトリクスの使用

AWS Management Console または CloudWatch API を使用して、ゲートウェイのモニタリングデータを取得できます。コンソールには、 CloudWatch API の未加工データに基づいて一連のグラフが表示されます。 CloudWatch API は、 AWS Software Development Kits (SDKsまたは Amazon CloudWatch API ツールのいずれかを使用して使用することもできます。必要に応じて、コンソールに表示されるグラフまたは API から取得したグラフを使用できます。

メトリクスを操作する際に使用するメソッドに関係なく、次の情報を指定する必要があります。

- 使用するメトリクスディメンション。ディメンションは、メトリクスを一意に識別するための名前と値のペアです。Storage Gateway のディメンションは `GatewayId`、`GatewayName`、および `VolumeId` です。 CloudWatch コンソールでは、 `Gateway Metrics`および `Volume Metrics`ビューを使用して、ゲートウェイ固有およびボリューム固有のディメンションを簡単に選択できます。ディメンションの詳細については、「Amazon CloudWatch ユーザーガイド」の「ディメンション」を参照してください。
- メトリクス名 (`ReadBytes` など)。

次の表は、使用できる Storage Gateway メトリクスデータのタイプをまとめたものです。

CloudWatch 名前空間	ディメンション	説明
`AWS/StorageGateway`	`GatewayId` , `GatewayName`	これらのディメンションを指定すると、ゲートウェイの各側面を示すメトリックスデータがフィルタリングされ

CloudWatch 名前空間	ディメンション	説明
		ます。GatewayId ディメンションと GatewayName ディメンションの両方を指定することで、使用するゲートウェイを特定できます。 ゲートウェイのスループットおよびレイテンシーデータは、ゲートウェイのすべてのボリュームに基づいています。 データは自動的に 5 分間無料で取得できます。
	VolumeId	このディメンションは、ボリューム固有のメトリクスデータをフィルタリングします。VolumeId ディメンションによって、使用するボリュームを特定します。 データは自動的に 5 分間無料で取得できます。

ゲートウェイおよびボリュームメトリクスの使用は、その他のサービスメトリクスの使用と似ています。以下に示す CloudWatch ドキュメントには、最も一般的なメトリクスタスクに関する説明が記載されています。

- 利用可能なメトリクスの表示
- メトリクスの統計の取得
- CloudWatch アラームの作成

アプリケーションとゲートウェイの間のパフォーマンスの測定

ゲートウェイを使用しているアプリケーションストレージのパフォーマンスを把握するために使用できる測定値は、データスループット、データレイテンシー、および 1 秒あたりのオペレーション数です。正しい集計統計を使用すると、Storage Gateway メトリクスを使用して、これらの値を測定できます。

統計とは、指定した期間を対象としたメトリックスの集計を意味します。でメトリクスの値を表示するときは CloudWatch、データレイテンシー (ミリ秒) に Average 統計を使用し、データスループット (バイト/秒) に Sum 統計を使用し、1 秒あたりの入出力オペレーション数 (IOPS) に Samples 統

計を使用します。詳細については、「Amazon ユーザーガイド」の「統計」を参照してください。CloudWatch

次の表は、アプリケーションとゲートウェイの間のスループット、レイテンシー、および IOPS の測定に使用できるメトリクスと対応する統計をまとめたものです。

対象となる項目	測定方法
スループット	`ReadBytes` および `WriteBytes` メトリクスを Sum CloudWatch 統計と共に使用します。たとえば、5 分間のサンプル期間に対する `ReadBytes` メトリックスの Sum 値を 300 秒で割ると、スループット（バイト/秒）がわかります。
レイテンシー	`ReadTime` および `WriteTime` メトリクスを `Average` CloudWatch 統計と共に使用します。たとえば、`ReadTime` メトリックスの `Average` 値を使用すると、サンプル期間に対するオペレーションあたりのレイテンシーがわかります。
IOPS	`ReadBytes` および `WriteBytes` メトリクスを `Samples` CloudWatch 統計と共に使用します。たとえば、5 分間のサンプル期間の `ReadBytes` メトリックスの `Samples` 値を 300 秒で割ると、IOPS がわかります。

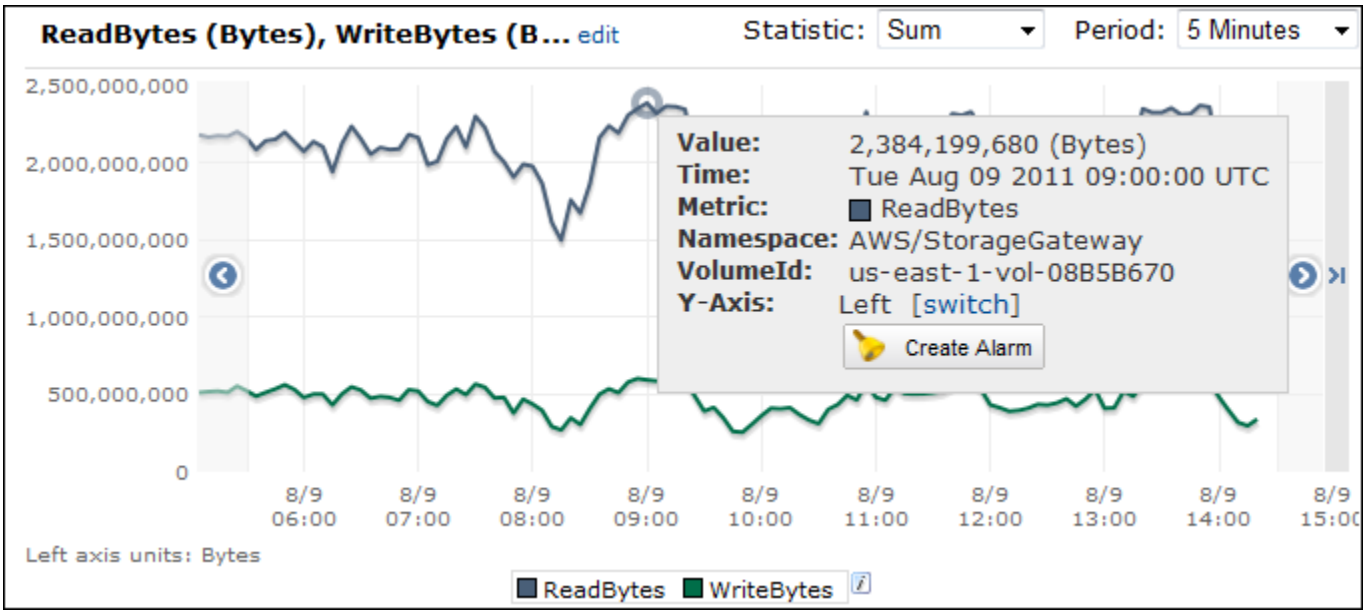
平均レイテンシーグラフおよび平均サイズグラフでは、期間中に完了したオペレーション (読み込みまたは書き込みのうち、いずれかグラフに該当する方) の合計数に基づいて平均が計算されます。

アプリケーションからボリュームへのデータスループットを測定するには

1. https://console.aws.amazon.com/cloudwatch/ で CloudWatch コンソールを開きます。
2. [Metrics] を選択し、[All metrics] タブを選択して、[Storage Gateway] を選択します。
3. [Volume metrics] ディメンションを選択し、対象のボリュームを見つけます。
4. `ReadBytes` および `WriteBytes` メトリクスを選択します。
5. [Time Range] で値を選択します。
6. `Sum` 統計を選択します。
7. [Period] で 5 分以上の値を選択します。

8. 表示された時系列のデータポイントのセット (ReadBytes のポイントと WriteBytes のポイント) で、各データポイントを期間 (秒) で割ると、サンプルポイントのスループットがわかります。総スループットとは、スループットの合計です。

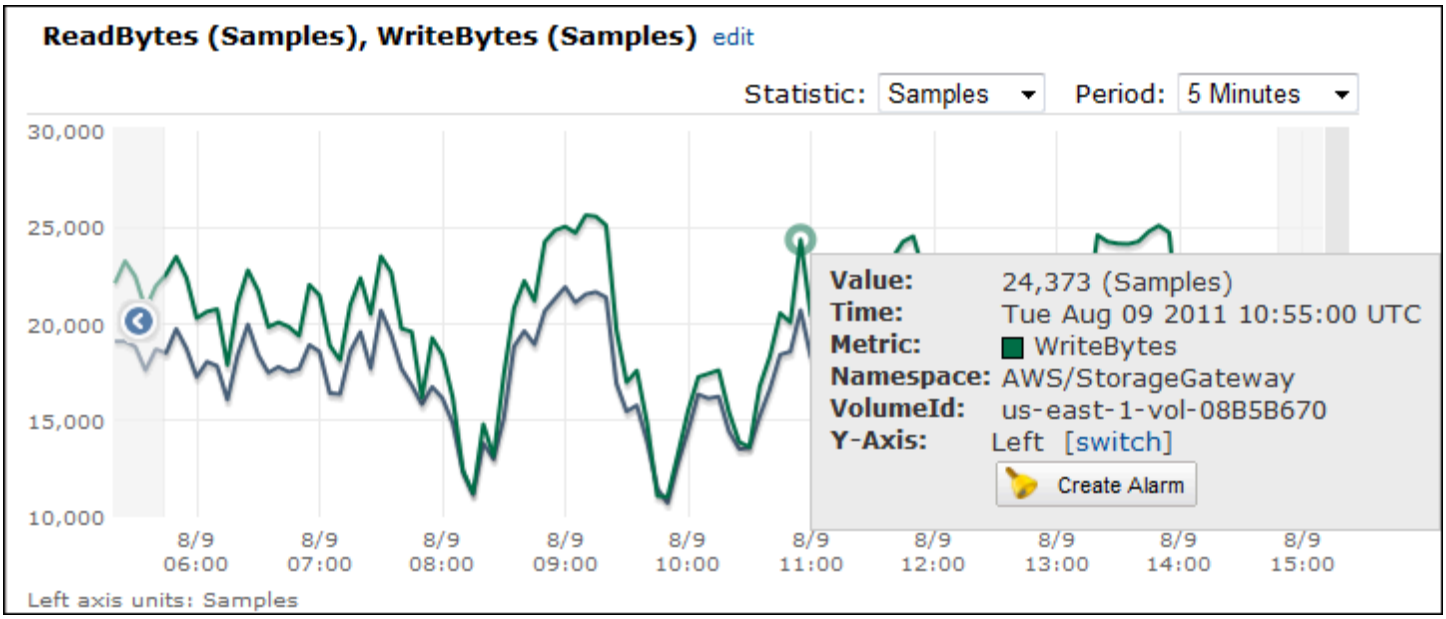
次の図は、ReadBytes 統計を使用したボリュームの WriteBytes メトリクスと Sum メトリクスを示しています。この図では、データポイントにカーソルを合わせると、そのデータポイントに関する情報 (データポイントの値やバイト数など) が表示されます。バイト数の値を [Period] の値 (5 分) で割ると、そのサンプルポイントのデータスループットがわかります。強調表示されたポイントでは、読み込みスループットは 2,384,199,680 バイトで、300 秒で割ると 7.6 メガバイト/秒になります。



アプリケーションからボリュームへの 1 秒あたりのデータ入力/出力オペレーションの数を測定するには

1. https://console.aws.amazon.com/cloudwatch/ で CloudWatch コンソールを開きます。
2. [Metrics] を選択し、[All metrics] タブを選択して、[Storage Gateway] を選択します。
3. [Volume metrics] ディメンションを選択し、対象のボリュームを見つけます。
4. ReadBytes および WriteBytes メトリクスを選択します。
5. [Time Range] で値を選択します。
6. Samples 統計を選択します。
7. [Period] で 5 分以上の値を選択します。
8. 表示された時系列のデータポイントのセット (ReadBytes のポイントと WriteBytes のポイント) で、各データポイントを期間 (秒) で割ると IOPS がわかります。

次の図は、ReadBytes 統計を使用したストレージボリュームの WriteBytes および Samples メトリクスを示しています。この図では、データポイントにカーソルを合わせると、そのデータポイントに関する情報 (データポイントの値やサンプル数など) が表示されます。サンプル数の値を [Period] の値 (5 分) で割ると、そのサンプルポイントの 1 秒あたりのオペレーションの数がわかります。強調表示されたポイントでは、書き込みオペレーションは 24,373 バイトで、300 秒で割ると 1 秒あたりの書き込みオペレーションは 81 となります。



ゲートウェイと AWSの間のパフォーマンスの測定

データスループット、データレイテンシー、および 1 秒あたりのオペレーション数は、Storage Gateway を使用しているアプリケーションストレージのパフォーマンスを把握するために使用できる 3 つの測定値です。正しい集計統計を使用すると、用意されている Storage Gateway メトリクスを使用して、これらの 3 つの値を測定できます。次の表は、ゲートウェイと AWSの間のスループット、レイテンシー、および 1 秒あたりの入力/出力オペレーション数 (IOPS) を測定するのに使用できるメトリクスおよび対応する統計をまとめたものです。

対象となる項目	測定方法
スループット	ReadBytes および WriteBytes メトリクスを Sum CloudWatch 統計と共に使用します。たとえば、5 分間のサンプル期間に対する ReadBytes メトリックスの Sum 値を 300 秒で割ると、スループット (バイト/秒) がわかります。

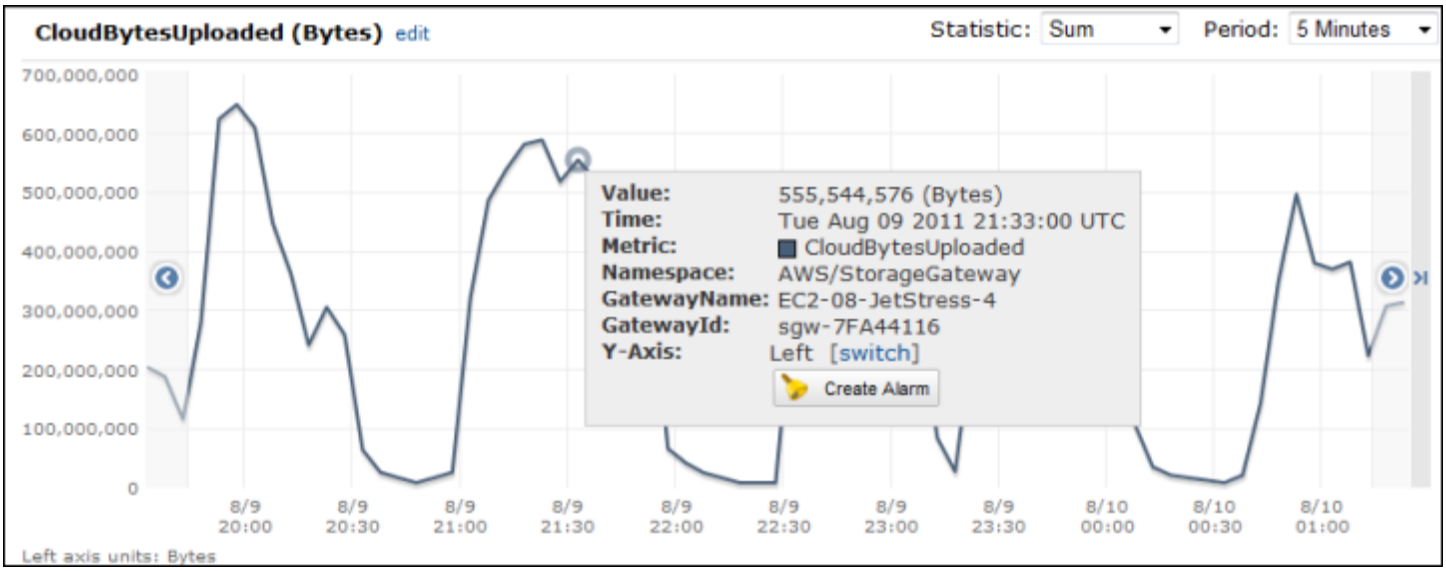
対象となる項目	測定方法
レイテンシー	ReadTime および WriteTime メトリクスを Average CloudWatch 統計と共に使用します。たとえば、ReadTime メトリックスの Average 値を使用すると、サンプル期間に対するオペレーションあたりのレイテンシーがわかります。
IOPS	ReadBytes および WriteBytes メトリクスを Samples CloudWatch 統計と共に使用します。たとえば、5 分間のサンプル期間の ReadBytes メトリックスの Samples 値を 300 秒で割ると、IOPS がわかります。
へのスループット AWS	CloudWatch 統計で CloudBytesDownloaded および Sum CloudBytesUploaded メトリクスを使用します。例えば、5 分間のサンプル期間における CloudBytesDownloaded メトリクスのSum値を 300 秒で割ると、 からゲートウェイ AWS へのスループットがバイト/秒として得られます。
へのデータのレイテンシー AWS	CloudDownloadLatency メトリクスと共に Average 統計を使用します。例えば、CloudDownloadLatency メトリックスの Average 統計を使用すると、オペレーションあたりのレイテンシーがわかります。

ゲートウェイから へのアップロードデータのスループットを測定するには AWS

1. https://console.aws.amazon.com/cloudwatch/ で CloudWatch コンソールを開きます。
2. [Metrics] を選択し、[All metrics] タブを選択して、[Storage Gateway] を選択します。
3. [Gateway metrics] ディメンションを選択し、対象のボリュームを見つけます。
4. CloudBytesUploaded メトリクスを選択します。
5. [Time Range] で値を選択します。
6. Sum 統計を選択します。
7. [Period] で 5 分以上の値を選択します。
8. 表示された時系列のデータポイントのセットで、各データポイントを期間 (秒) で割ると、そのサンプル期間中のスループットがわかります。

次の図は、CloudBytesUploaded 統計を使用したゲートウェイボリュームの Sum メトリクスを示しています。この図では、データポイントにカーソルを合わせると、そのデータポイントに関する情

報 (データポイントの値やアップロードしたバイト数など) が表示されます。この値を [Period] の値 (5 分) で割ると、そのサンプルポイントのスループットがわかります。強調表示されたポイントでは、ゲートウェイから へのスループット AWS は 555,544,576 バイトを 300 秒で割ったもので、1.7 メガバイト/秒です。



ゲートウェイのオペレーションあたりのレイテンシーを測定するには

1. https://console.aws.amazon.com/cloudwatch/ で CloudWatch コンソールを開きます。
2. [Metrics] を選択し、[All metrics] タブを選択して、[Storage Gateway] を選択します。
3. [Gateway metrics] ディメンションを選択し、対象のボリュームを見つけます。
4. `ReadTime` および `WriteTime` メトリクスを選択します。
5. [Time Range] で値を選択します。
6. `Average` 統計を選択します。
7. [Period] で、デフォルトのレポート時間に合わせて 5 分を選択します。
8. 表示された時系列のポイントのセット (`ReadTime` のポイントと `WriteTime` のポイント) で、同じ時間サンプルにデータポイントを追加すると、総合的なレイテンシー (ミリ秒) がわかります。

ゲートウェイから へのデータレイテンシーを測定するには AWS

1. https://console.aws.amazon.com/cloudwatch/ で CloudWatch コンソールを開きます。
2. [Metrics] を選択し、[All metrics] タブを選択して、[Storage Gateway] を選択します。
3. [Gateway metrics] ディメンションを選択し、対象のボリュームを見つけます。

4. CloudDownloadLatency メトリクスを選択します。
5. [Time Range] で値を選択します。
6. Average 統計を選択します。
7. [Period] で、デフォルトのレポート時間に合わせて 5 分を選択します。

表示された時系列のデータポイントのセットには、レイテンシー (ミリ秒) が含まれます。

へのゲートウェイのスループットの上限アラームを設定するには AWS

1. https://console.aws.amazon.com/cloudwatch/ で CloudWatch コンソールを開きます。
2. [Alarms] を選択します。
3. [Create Alarm (アラームの作成)] を選択して、アラームの作成ウィザードを起動します。
4. [Storage Gateway] ディメンションを選択し、対象のゲートウェイを見つけます。
5. CloudBytesUploaded メトリクスを選択します。
6. アラームを定義するには、CloudBytesUploaded メトリクスが指定した期間中に指定した値以上になった場合のアラーム状態を定義します。例えば、CloudBytesUploaded メトリクスが 60 分間 10 MB 以上になった場合のアラーム状態を定義することができます。
7. そのアラーム状態に対して実行するアクションを設定します。たとえば、E メール通知を送信するように設定できます。
8. [アラームの作成] を選択します。

からデータを読み取るための上限アラームを設定するには AWS

1. https://console.aws.amazon.com/cloudwatch/ で CloudWatch コンソールを開きます。
2. [Create Alarm (アラームの作成)] を選択して、アラームの作成ウィザードを起動します。
3. StorageGateway: Gateway Metrics ディメンションを選択し、使用するゲートウェイを見つけます。
4. CloudDownloadLatency メトリクスを選択します。
5. CloudDownloadLatency メトリクスが指定した期間中に指定した値以上になった場合のアラーム状態を定義して、アラームを定義します。例えば、CloudDownloadLatency が 2 時間以上、60,000 ミリ秒以上になった場合のアラーム状態を定義することができます。
6. そのアラーム状態に対して実行するアクションを設定します。たとえば、E メール通知を送信するように設定できます。
7. [アラームの作成] を選択します。

ボリュームメトリクスについて

以下では、ゲートウェイのボリュームを対象とする Storage Gateway メトリクスについて説明します。ゲートウェイの各ボリュームには、メトリクスのセットが関連付けられています。

一部のボリューム固有のメトリクスには、ゲートウェイ固有のメトリクスと同じ名前が付けられています。これらのメトリクスは、同じ種類の測定を表していますが、ゲートウェイの代わりにボリュームがスコープとなっています。作業を開始する前に、ゲートウェイメトリクスとボリュームメトリクスのどちらを使用するかを指定します。具体的には、ボリュームメトリクスを操作する場合は、メトリクスを表示するストレージボリュームの ID を指定します。詳細については、「Amazon CloudWatch メトリクスの使用」を参照してください。

> **Note**
>
> 一部のメトリクスは、直近のモニタリング期間中に新しいデータが生成された場合にのみデータポイントを返します。

次の表は、ストレージボリュームに関する情報を入手するために使用できる Storage Gateway メトリクスを示しています。

メトリクス	説明	キャッシュボリューム	保管型ボリューム
`AvailabilityNotification`	ボリュームから送信された可用性の通知の数。 単位: 数	はい	はい
`CacheHitPercent`	キャッシュから提供されるボリュームからのアプリケーション読み込みオペレーションの割合。サンプリングは、レポート期間の最後に行われます。	はい	いいえ

メトリクス	説明	キャッシュボリューム	保管型ボリューム
	ボリュームからのアプリケーション読み込みオペレーションがない割合、このメトリックにより 100 パーセントが報告されます。 単位: パーセント		
CachePercentDirty	AWSに保持されていないゲートウェイのキャッシュの割合全体に対するボリュームの割合。サンプリングは、レポート期間の最後に行われます。 ゲートウェイの CachePercentDirty メトリクスを使用して、AWSに保持されていないゲートウェイのキャッシュの割合全体を表示します。詳細については、「ゲートウェイメトリクスについて」を参照してください。 単位: パーセント	はい	はい

メトリクス	説明	キャッシュボリューム	保管型ボリューム
CachePercentUsed	ゲートウェイのキャッシュストレージの総使用率に対するボリュームの割合。サンプリングは、レポート期間の最後に行われます。 ゲートウェイの CachePercentUsed メトリクスを使用して、ゲートウェイのキャッシュストレージの総使用率を表示します。詳細については、「ゲートウェイメトリクスについて」を参照してください。 単位: パーセント	はい	いいえ
CloudBytesDownloaded	クラウドからボリュームにダウンロードされたバイト数。 単位: バイト	はい	はい
CloudBytesUploaded	クラウドからボリュームにアップロードされたバイト数。 単位: バイト	はい	はい

メトリクス	説明	キャッシュボリューム	保管型ボリューム
HealthNotification	ボリュームから送信されたヘルス通知の数。 単位: 数	はい	はい
IoWaitPercent	ボリュームで現在使用されている IoWaitPercent ユニットの割合。 単位: パーセント	はい	はい
MemTotalBytes	ボリュームで現在使用されているメモリが総メモリに占める割合。 単位: パーセント	はい	いいえ
MemoryUsage	ボリュームで現在使用されているメモリの割合。 単位: パーセント	はい	いいえ

メトリクス	説明	キャッシュボリューム	保管型ボリューム
ReadBytes	レポートの期間中にオンプレミスのアプリケーションから読み取られた総バイト数。 このメトリクスを Sum 統計と共に使用してスループットを測定し、Samples 統計と共に使用して IOPS を測定します。 単位: バイト	はい	はい
ReadTime	レポートの期間中にオンプレミスのアプリケーションからの読み込みオペレーションにかかった合計時間 (ミリ秒)。 このメトリクスを Average 統計と共に使用してレイテンシーを測定します。 単位: ミリ秒	はい	はい

メトリクス	説明	キャッシュボリューム	保管型ボリューム
UserCpuPercent	ボリュームで現在使用されている、割り当てられた CPU コンピューティングユニットの割合。 単位: パーセント	はい	はい
WriteBytes	レポートの期間中にオンプレミスのアプリケーションに書き込まれた総バイト数。 このメトリクスを Sum 統計と共に使用してスループットを測定し、Samples 統計と共に使用して IOPS を測定します。 単位: バイト	はい	はい

メトリクス	説明	キャッシュボリューム	保管型ボリューム
WriteTime	レポートの期間中にオンプレミスのアプリケーションからの書き込みオペレーションにかかった合計時間 (ミリ秒)。 このメトリクスを Average 統計と共に使用してレイテンシーを測定します。 単位: ミリ秒	はい	はい
QueuedWrites	レポート期間の終了時にサンプリングされた AWS、 への書き込みを待機しているバイト数。 単位: バイト	はい	はい

ゲートウェイの維持

ゲートウェイの維持には、キャッシュストレージとアップロードバッファ領域の設定などのタスク、およびゲートウェイのパフォーマンスの一般的なメンテナンスが含まれます。これらのタスクは、すべてのゲートウェイの種類に共通です。ゲートウェイをまだ作成していない場合は、「ゲートウェイを作成する」を参照してください。

トピック

- ゲートウェイ VM のシャットダウン
- Storage Gateway のローカルディスクの管理
- ボリュームゲートウェイの帯域幅管理
- ゲートウェイの更新の管理
- ローカルコンソールを使用したメンテナンスタスクの実行
- ゲートウェイの削除と関連リソースの削除

ゲートウェイ VM のシャットダウン

ハイパーバイザーにパッチを適用するときなど、メンテナンスのために VM をシャットダウンまたは再起動する必要がある場合があります。VM をシャットダウンする前に、まずゲートウェイを停止する必要があります。ファイルゲートウェイの場合、VM をシャットダウンするだけです。このセクションでは、Storage Gateway マネジメントコンソールを使用してゲートウェイを起動および停止することに重点を置いていますが、VM ローカルコンソールまたは Storage Gateway を使用してゲートウェイを起動および停止することもできますAPI。VM の電源をオンにするときは、必ずゲートウェイを再起動します。

> **Important**
>
> エフェメラルストレージを使用する Amazon EC2ゲートウェイを停止して起動すると、ゲートウェイは完全にオフラインになります。これは、物理ストレージディスクが置き換えられたために発生します。この問題の回避策はありません。唯一の解決策は、ゲートウェイを削除し、新しいEC2インスタンスで新しいゲートウェイをアクティブ化することです。

> **Note**
>
> バックアップソフトウェアがテープへの書き込み、またはテープからの読み取りを行っているときに、ゲートウェイを停止すると、書き込みまたは読み取りは失敗する可能性があります。ゲートウェイを停止する前に、進行中のタスクがないかどうか、バックアップソフトウェアとバックアップスケジュールを確認する必要があります。

- Gateway VM ローカルコンソール – 「デフォルトの認証情報を使用したローカルコンソールへのログイン」を参照してください。
- Storage Gateway API- 「」を参照してください。 ShutdownGateway

ファイルゲートウェイの場合、VM をシャットダウンするだけです。ゲートウェイはシャットダウンしません。

ボリュームゲートウェイを起動および停止する

ボリュームゲートウェイを停止するには

1. ホーム で Storage Gateway https://console.aws.amazon.com/storagegateway/コンソールを開きます。
2. ナビゲーションペインで [Gateways] を選択してから、停止するゲートウェイを選択します。ゲートウェイのステータスは [実行中] です。
3. [Actions (アクション)] で [Stop gateway (ゲートウェイの停止)] を選択し、ダイアログボックスでゲートウェイの ID を確認してから [Stop gateway (ゲートウェイの停止)] を選択します。

   ゲートウェイが停止中、ゲートウェイのステータスを示すメッセージが表示されることがあります。ゲートウェイをシャットダウンすると、メッセージおよび [Start gateway] ボタンが、[Details] タブに表示されます。

ゲートウェイを停止すると、ストレージのリソースには、ストレージが開始されるまでアクセスすることはできません。ゲートウェイの停止時にデータをアップロードしている場合、ゲートウェイを起動するとアップロードが再開されます。

ボリュームゲートウェイを起動するには

1. ホーム で Storage Gateway https://console.aws.amazon.com/storagegateway/コンソールを開きます。
2. ナビゲーションペインで [Gateways] を選択してから、起動するゲートウェイを選択します。ゲートウェイのステータスは [シャットダウン] です。
3. [詳細] を選択します。それから、[ゲートウェイの起動] を選択します。

Storage Gateway のローカルディスクの管理

ゲートウェイ仮想マシン (VM) は、バッファリングおよびストレージ用としてオンプレミスで割り当てるローカルディスクを使用します。Amazon EC2インスタンスで作成されたゲートウェイは、Amazon EBSボリュームをローカルディスクとして使用します。

トピック

- ローカルディスクストレージの容量の決定
- 割り当てるアップロードバッファのサイズの決定
- 割り当てるキャッシュストレージのサイズの決定
- 追加のアップロードバッファとキャッシュストレージの設定

ローカルディスクストレージの容量の決定

ゲートウェイに割り当てるディスクの数とサイズは、ユーザーが決定できます。デプロイするストレージソリューションに応じて (「Storage Gateway のデプロイを計画する」を参照)、ゲートウェイには次の追加のストレージが必要になります。

- ボリュームゲートウェイ:
  - 保管型ゲートウェイには、アップロードバッファとして使用するディスクが 1 つ以上必要です。
  - ゲートウェイキャッシュ型には、ディスクが 2 つ以上必要です。1 つはキャッシュとして使用し、1 つはアップロードバッファとして使用します。

次の表は、デプロイされるゲートウェイのローカルディスクストレージの推奨サイズを示しています。ゲートウェイをセットアップした後で、ワークロードの需要増に応じてローカルストレージを追加できます。

ローカルストレージ	説明	
アップロードバッファ	ゲートウェイによってデータが Amazon S3 にアップロードされる前に、アップロードバッファにデータのステージングエリアが用意されます。ゲートウェイは、暗号化された Secure Sockets Layer (SSL) 接続を介してこのバッファデータを にアップロードします AWS。	
キャッシュストレージ	キャッシュストレージは、オンプレミスで恒久的な保存場所として、アップロードバッファから Amazon S3 にアップロードされるのを保留中のデータを保存する働きをします。アプリケーションがボリュームまたはテープで I/O を実行すると、ゲートウェイは、低レイテンシーのアクセスを実現するために、データをキャッシュストレージに保存します。アプリケーションがボリュームまたはテープに対してデータを要求すると、ゲートウェイは、 AWSからデータをダウンロードする前に、まずキャッシュストレージにデータがあるかどうかをチェックします。	

> **Note**
>
> ディスクをプロビジョニングするとき、同じ物理リソース (同じディスク) を使用しているアップロードバッファとキャッシュストレージのローカルディスクはプロビジョニングしないことを強くお勧めします。基盤となる物理ストレージリソースは、 のデータストアとして

表されますVMware。ゲートウェイ VM をデプロイする場合は、VM ファイルを保存するデータストアを選択します。たとえば、キャッシュストレージまたはアップロードバッファとして使用するなど、ローカルディスクをプロビジョニングする場合は、VM と同じデータストアまたは別のデータストアに仮想ディスクを保存することもできます。
複数のデータストアがある場合は、キャッシュストレージ用とアップロードバッファ用でデータストアの場所を分けることを強くお勧めします。基になる物理ディスクが 1 つのみのデータストアを、キャッシュストレージとアップロードバッファの両方に使用すると、パフォーマンスが低下する場合があります。これは、バックアップが などのパフォーマンスの低いRAID設定である場合にも当てはまりますRAID1。

ゲートウェイの初回の設定およびデプロイ後、アップロードバッファのディスクを追加または削除して、ローカルストレージを調整できます。キャッシュストレージのディスクを追加することもできます。

割り当てるアップロードバッファのサイズの決定

割り当てるアップロードバッファのサイズを決めるには、アップロードバッファの計算式を使用します。少なくとも 150 GiB のアップロードバッファを割り当てることを強く推奨します。計算式の結果が 150 GiB 未満の値を返す場合は、アップロードバッファに割り当てる容量には 150 GiB を使用します。各ゲートウェイのアップロードバッファに設定できる最大容量は 2 TiB です。

> **Note**
>
> ボリュームゲートウェイの場合、アップロードバッファが容量に達すると、ボリュームはPASSTHROUGHステータスになります。このステータスでは、アプリケーションが書き込む新しいデータはローカルに保持されますが、 AWS すぐには にアップロードされません。そのため、新しいスナップショットは作成できません。アップロードバッファ容量が解放されると、ボリュームは BOOTSTRAPPINGステータスになります。このステータスでは、ローカルに保持された新しいデータは にアップロードされます AWS。最後に、ボリュームは ACTIVEステータスに戻ります。その後、Storage Gateway はローカルに保存されているデータと に保存されているコピーとの通常の同期を再開し AWS、新しいスナップショットの作成を開始できます。ボリュームステータスの詳細については、「ボリュームステータスと移行について」を参照してください。

割り当てるアップロードバッファの量を見積もるには、予想される送受信データレートを計算し、これらのレートを以下の計算式に当てはめます。

受信データレート

これはアプリケーションスループットです。つまり、オンプレミスアプリケーションが一定期間にゲートウェイにデータを書き込むレートです。

送信データレート

これはネットワークスループットです。つまり、ゲートウェイが AWSにデータをアップロードできるレートです。このレートは、ネットワークの速度、利用状況、帯域幅スロットリングの設定により変化します。圧縮には、このレートを調整する必要があります。データを にアップロードすると AWS、ゲートウェイは可能な限りデータ圧縮を適用します。たとえば、アプリケーションデータがテキストのみである場合、効果的な圧縮率はおよそ 2:1 です。ただし、動画を書き込む場合、ゲートウェイはデータ圧縮を行えないことがあります。データ圧縮を行うには、ゲートウェイのアップロードバッファを増やす必要があります。

以下のいずれかに該当する場合は、150 GiB 以上のアップロードバッファ領域を割り当てることを強くお勧めします。

- 着信レートは発信レートよりも高くなっています。
- この数式は、150 GiB 未満の値を返します。

$$\left(\text{Application Throughput (MB/s)} - \text{Network Throughput to AWS (MB/s)} \times \text{Compression Factor}\right) \times \text{Duration of writes (s)} = \text{Upload Buffer (MB)}$$

たとえば、1 日 12 時間、40 MB/秒 の速度でビジネスアプリケーションがゲートウェイにテキストデータを書き込み、ネットワークのスループットが 12 MB/秒 であるとします。テキストデータの圧縮係数が 2:1 とすると、約 690 GiB のスペースをアップロードバッファに割り当てることになります。

Example

```
((40 MB/sec) - (12 MB/sec * 2)) * (12 hours * 3600 seconds/hour) = 691200 megabytes
```

最初にこの概算値を使うことで、アップロードバッファ容量としてゲートウェイに割り当てるディスクサイズを判断できます。必要に応じて、Storage Gateway コンソールを使用してアップロードバッファ領域を追加します。また、Amazon の CloudWatch 運用メトリクスを使用して、アップロード

バッファの使用状況をモニタリングし、追加のストレージ要件を決定することもできます。メトリックとアラームの設定については、アップロードバッファのモニタリング を参照してください。

割り当てるキャッシュストレージのサイズの決定

ゲートウェイは、そのキャッシュストレージを使用して、最近アクセスされたデータに低レイテンシーでアクセスします。キャッシュストレージは、オンプレミスで恒久的な保存場所として、アップロードバッファから Amazon S3 にアップロードされるのを保留中のデータを保存する働きをします。通常、キャッシュストレージにはアップロードバッファの 1.1 倍のサイズを設定します。キャッシュストレージサイズを予測する方法の詳細については、「割り当てるアップロードバッファのサイズの決定」を参照してください。

キャッシュストレージ用のディスクをプロビジョニングするには、最初に、この概算値を使うことができます。その後、Amazon CloudWatch の運用メトリクスを使用してキャッシュストレージの使用状況をモニタリングし、コンソールを使用して必要に応じてより多くのストレージをプロビジョニングできます。メトリクスの使用とアラームの設定の詳細については、「キャッシュストレージのモニタリング」を参照してください。

追加のアップロードバッファとキャッシュストレージの設定

アプリケーションのニーズの変化に応じて、ゲートウェイのアップロードバッファやキャッシュストレージの容量を増やすことができます。機能を中断したりダウンタイムを発生させたりすることなく、ゲートウェイにストレージ容量を追加できます。容量を追加する場合は、ゲートウェイ VM を有効にした状態で行います。

> **Important**
>
> 既存のゲートウェイにキャッシュまたはアップロードバッファを追加する場合は、ゲートウェイホストハイパーバイザーまたは Amazon EC2インスタンスに新しいディスクを作成する必要があります。キャッシュまたはアップロードバッファとしてすでに割り当てられている既存のディスクを削除したり、そのサイズを変更したりしないでください。

ゲートウェイ用のアップロードアップロードバッファまたはキャッシュストレージを追加して設定するには

1. ゲートウェイホストハイパーバイザーまたは Amazon EC2インスタンスに 1 つ以上の新しいディスクをプロビジョニングします。ハイパーバイザーでディスクをプロビジョニングする方

法については、ハイパーバイザーのドキュメントを参照してください。Amazon EC2インスタンスの Amazon EBSボリュームのプロビジョニングの詳細については、Linux インスタンス用 Amazon Elastic Compute Cloud ユーザーガイドの「Amazon EBSボリューム」を参照してください。 次の手順では、このディスクをアップロードバッファまたはキャッシュストレージとして設定します。

2. ホーム で Storage Gateway https://console.aws.amazon.com/storagegateway/コンソールを開きます。
3. ナビゲーションペインで、[Gateways] を選択します。
4. ゲートウェイを検索し、リストから選択します。
5. [アクション] メニューから [ストレージの設定] を選択します。
6. [ストレージの設定] セクションで、プロビジョニングしたディスクを特定します。ディスクが表示されない場合は、更新アイコンを選択してリストを更新します。ディスクごとに、割り当て先CACHESTORAGEからドロップダウンメニューから UPLOADBUFFERまたは を選択します。

   > **Note**
   >
   > UPLOAD BUFFER は、ストアドボリュームゲートウェイにディスクを割り当てるために使用できる唯一のオプションです。

7. [変更を保存] を選択して設定を保存します。

ボリュームゲートウェイの帯域幅管理

ゲートウェイから へのアップロードスループット AWS 、または からゲートウェイ AWS へのダウンロードスループットを制限 (またはスロットリング) できます。帯域幅のスロットル機能は、ゲートウェイによるネットワーク帯域幅の使用量の制御に役立ちます。デフォルトでは、アクティブ化されたゲートウェイのレート制限は、アップロードまたはダウンロード時には設定されていません。

レート制限は、 を使用するか AWS Management Console、Storage Gateway API (「」を参照UpdateBandwidthRateLimit) または AWS Software Development Kit () を使用してプログラムで指定できますSDK。帯域幅をプログラムでスロットリングすることで (例えば、帯域幅を変更するようにタスクをスケジュールすることで)、制限を 1 日を通して自動的に変更することができます。

スケジュールベースでゲートウェイの帯域幅スロットリングを定義することもできます。帯域幅スロットリングをスケジュールするには、1 つ以上の bandwidth-rate-limit 間隔を定義します。詳細に

ついては、「Storage Gateway コンソールを使用したスケジュールベースの帯域幅スロットリング」を参照してください。

帯域幅スロットリングの単一設定を構成することは、毎日 に設定された単一 bandwidth-rate-limit 間隔のスケジュールを定義00:00し、開始時刻を 、終了時刻を にすることと同じ機能です23:59。

> **Note**
>
> このセクションの情報は、テープゲートウェイとボリュームゲートウェイに固有の情報です。Amazon S3 ファイルゲートウェイの帯域幅を管理するには、「Managing Bandwidth for Your Amazon S3 File Gateway」を参照してください。帯域幅レートの制限は現在、Amazon FSx File Gateway ではサポートされていません。

トピック

- Storage Gateway コンソールを使用して帯域幅スロットリングを変更する
- Storage Gateway コンソールを使用したスケジュールベースの帯域幅スロットリング
- を使用したゲートウェイ帯域幅レート制限の更新 AWS SDK for Java
- を使用したゲートウェイ帯域幅レート制限の更新 AWS SDK for .NET
- を使用したゲートウェイ帯域幅レート制限の更新 AWS Tools for Windows PowerShell

Storage Gateway コンソールを使用して帯域幅スロットリングを変更する

次の手順は、Storage Gateway コンソールを使用してゲートウェイの帯域幅スロットリングを変更する方法を示しています。

コンソールを使用してゲートウェイの帯域幅スロットルを変更するには

1. ホーム で Storage Gateway https://console.aws.amazon.com/storagegateway/コンソールを開きます。
2. 左側のナビゲーションペインで [ゲートウェイ] を選択してから、管理対象のゲートウェイを選択します。
3. [アクション] で、[帯域幅レート制限の編集] を選択します。
4. [速度制限の編集] ダイアログボックスで、新しい制限値を入力し、[保存] をクリックします。変更はゲートウェイの [Details] タブに表示されます。

Storage Gateway コンソールを使用したスケジュールベースの帯域幅スロットリング

次の手順は、Storage Gateway コンソールを使用してゲートウェイの帯域幅スロットリングのスケジュールを変更する方法を示しています。

ゲートウェイ帯域幅スロットリングのスケジュールを追加または変更するには

1. ホーム で Storage Gateway https://console.aws.amazon.com/storagegateway/コンソールを開きます。
2. 左側のナビゲーションペインで [ゲートウェイ] を選択してから、管理対象のゲートウェイを選択します。
3. [Actions] (アクション) で、[Edit bandwidth rate limit schedule] (帯域幅レート制限スケジュールの編集) を選択します。

   ゲートウェイ bandwidth-rate-limit のスケジュールは、帯域幅レート制限スケジュールの編集ダイアログボックスに表示されます。デフォルトでは、新しいゲートウェイ bandwidth-rate-limit スケジュールは空です。
4. 「帯域幅レート制限スケジュールの編集」ダイアログボックスで、「新しい項目を追加」を選択して新しい bandwidth-rate-limit間隔を追加します。間隔 bandwidth-rate-limitごとに次の情報を入力します。

   - 曜日 – bandwidth-rate-limit 間隔は、平日 (月曜日から金曜日)、週末 (土曜日と日曜日)、曜日ごと、または 1 つ以上の特定の曜日に対して作成できます。
   - [開始時刻] – ゲートウェイのローカルタイムゾーンを使用して、帯域幅期間の開始時刻を HH:MM 形式で入力します。

     > **Note**
     >
     > bandwidth-rate-limit 間隔は、ここで指定した分の開始から始まります。

   - 終了時刻 – HH:MM 形式を使用して、ゲートウェイのローカルタイムゾーンの bandwidth-rate-limit 間隔の終了時刻を入力します。

     > **Important**
     >
     > bandwidth-rate-limit 間隔は、ここで指定した分の最後に終了します。1 時間の終わりに終了する期間をスケジュールするには、「**59**」と入力します。

連続する期間を続けてスケジュールする際に、1 時間の開始時に移行し、期間の間に中断がないようにするには、最初の期間の終了時間を「**59**」分と入力します。後の期間の開始時間は、「**00**」分と入力します。

- [ダウンロード速度] – ダウンロードのレート制限をキロビット/秒 (Kbps) で入力するか、[無制限] を選択して、ダウンロードの帯域幅スロットリングを無効にします。ダウンロード速度の最小値は 100 Kbps です。
- [アップロード速度] – アップロードのレート制限をキロビット/秒 (Kbps) で入力するか、[無制限] を選択して、アップロードの帯域幅スロットリングを無効にします。アップロード速度の最小値は 50 Kbps です。

bandwidth-rate-limit 間隔を変更するには、間隔パラメータに変更された値を入力します。

bandwidth-rate-limit 間隔を削除するには、削除する間隔の右側にある削除を選択します。

変更が完了したら、[保存] をクリックします。

5. 新しい項目を追加を選択し、日付、開始時刻と終了時刻、ダウンロード速度とアップロード速度の制限を入力して、 bandwidth-rate-limit 間隔を追加し続けます。

> **Important**
>
> B andwidth-rate-limit 間隔は重複できません。期間の開始時間は、前の期間の終了時間より後、かつ、次の区間の開始時間より前である必要があります。

6. すべての bandwidth-rate-limit 間隔を入力したら、変更を保存を選択して bandwidth-rate-limit スケジュールを保存します。

bandwidth-rate-limit スケジュールが正常に更新されると、ゲートウェイの詳細パネルに現在のダウンロードとアップロードのレート制限が表示されます。

を使用したゲートウェイ帯域幅レート制限の更新 AWS SDK for Java

帯域幅レート制限をプログラムで更新することで (例えば、スケジュールされたタスクを使用することで)、一定期間にわたって制限を自動的に調整できます。次の例は、 AWS SDK for Javaを使用して、ゲートウェイの帯域幅レート制限を更新する方法を示しています。サンプルコードを使用するには、Java コンソールアプリケーションの実行について理解している必要があります。詳細については、AWS SDK for Java デベロッパーガイドの「Getting Started」を参照してください。

Example : を使用したゲートウェイ帯域幅レート制限の更新 AWS SDK for Java

次の Java コードの例では、ゲートウェイの帯域幅レート制限を更新します。このサンプルコードを使用するには、サービスエンドポイント、ゲートウェイ Amazon リソースネーム (ARN) 、およびアップロードとダウンロードの制限を指定する必要があります。Storage Gateway で使用できる AWS サービスエンドポイントのリストについては、AWS Storage Gateway 「」の「エンドポイントとクォータ」を参照してくださいAWS 全般のリファレンス。 Storage Gateway

```
import java.io.IOException;

import com.amazonaws.AmazonClientException;
import com.amazonaws.auth.PropertiesCredentials;
import com.amazonaws.services.storagegateway.AWSStorageGatewayClient;
import com.amazonaws.services.storagegateway.model.UpdateBandwidthRateLimitRequest;
import com.amazonaws.services.storagegateway.model.UpdateBandwidthRateLimitResult;


public class UpdateBandwidthExample {

    public static AWSStorageGatewayClient sgClient;

    // The gatewayARN
    public static String gatewayARN = "*** provide gateway ARN ***";

    // The endpoint
    static String serviceURL = "https://storagegateway.us-east-1.amazonaws.com";

    // Rates
    static long uploadRate = 51200;  // Bits per second, minimum 51200
    static long downloadRate = 102400;   // Bits per second, minimum 102400

    public static void main(String[] args) throws IOException {

        // Create a Storage Gateway client
        sgClient = new AWSStorageGatewayClient(new PropertiesCredentials(

 UpdateBandwidthExample.class.getResourceAsStream("AwsCredentials.properties")));
        sgClient.setEndpoint(serviceURL);

        UpdateBandwidth(gatewayARN, uploadRate, downloadRate);

    }
```

```
    private static void UpdateBandwidth(String gatewayARN2, long uploadRate2,
            long downloadRate2) {
        try
        {
            UpdateBandwidthRateLimitRequest updateBandwidthRateLimitRequest =
                new UpdateBandwidthRateLimitRequest()
                .withGatewayARN(gatewayARN)
                .withAverageDownloadRateLimitInBitsPerSec(downloadRate)
                .withAverageUploadRateLimitInBitsPerSec(uploadRate);

            UpdateBandwidthRateLimitResult updateBandwidthRateLimitResult =
 sgClient.updateBandwidthRateLimit(updateBandwidthRateLimitRequest);
            String returnGatewayARN = updateBandwidthRateLimitResult.getGatewayARN();
            System.out.println("Updated the bandwidth rate limits of " +
 returnGatewayARN);
            System.out.println("Upload bandwidth limit = " + uploadRate + " bits per
 second");
            System.out.println("Download bandwidth limit = " + downloadRate + " bits
 per second");
        }
        catch (AmazonClientException ex)
        {
            System.err.println("Error updating gateway bandwith.\n" + ex.toString());
        }
    }
}
```

を使用したゲートウェイ帯域幅レート制限の更新 AWS SDK for .NET

帯域幅レート制限をプログラムで更新することで (例えば、スケジュールされたタスクを使用することで)、一定期間にわたって制限を自動的に調整できます。次の例は、 AWS SDK for .NETを使用して、ゲートウェイの帯域幅レート制限を更新する方法を示しています。サンプルコードを使用するには、 NETコンソールアプリケーションの実行に精通している必要があります。詳細については、AWS SDK for .NET デベロッパーガイドの「Getting Started」を参照してください。

Example : を使用したゲートウェイ帯域幅レート制限の更新 AWS SDK for .NET

次の C# コードの例では、ゲートウェイの帯域幅レート制限を更新します。このサンプルコードを使用するには、サービスエンドポイント、ゲートウェイ Amazon リソースネーム (ARN) 、およびアップロードとダウンロードの制限を指定する必要があります。Storage Gateway で使用できる AWS サービスエンドポイントのリストについては、AWS Storage Gateway 「」の「エンドポイントとクォータ」を参照してくださいAWS 全般のリファレンス。 Storage Gateway

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using Amazon.StorageGateway;
using Amazon.StorageGateway.Model;

namespace AWSStorageGateway
{
    class UpdateBandwidthExample
    {
        static AmazonStorageGatewayClient sgClient;
        static AmazonStorageGatewayConfig sgConfig;

        // The gatewayARN
        public static String gatewayARN = "*** provide gateway ARN ***";

        // The endpoint
        static String serviceURL = "https://storagegateway.us-east-1.amazonaws.com";

        // Rates
        static long uploadRate = 51200;  // Bits per second, minimum 51200
        static long downloadRate = 102400;   // Bits per second, minimum 102400

        public static void Main(string[] args)
        {
            // Create a Storage Gateway client
            sgConfig = new AmazonStorageGatewayConfig();
            sgConfig.ServiceURL = serviceURL;
            sgClient = new AmazonStorageGatewayClient(sgConfig);

            UpdateBandwidth(gatewayARN, uploadRate, downloadRate);

            Console.WriteLine("\nTo continue, press Enter.");
            Console.Read();
        }

        public static void UpdateBandwidth(string gatewayARN, long uploadRate, long
 downloadRate)
        {
            try
            {
                UpdateBandwidthRateLimitRequest updateBandwidthRateLimitRequest =
```

```
                    new UpdateBandwidthRateLimitRequest()
                    .WithGatewayARN(gatewayARN)
                    .WithAverageDownloadRateLimitInBitsPerSec(downloadRate)
                    .WithAverageUploadRateLimitInBitsPerSec(uploadRate);

                UpdateBandwidthRateLimitResponse updateBandwidthRateLimitResponse =
 sgClient.UpdateBandwidthRateLimit(updateBandwidthRateLimitRequest);
                String returnGatewayARN =
 updateBandwidthRateLimitResponse.UpdateBandwidthRateLimitResult.GatewayARN;
                Console.WriteLine("Updated the bandwidth rate limits of " +
 returnGatewayARN);
                Console.WriteLine("Upload bandwidth limit = " + uploadRate + " bits per
 second");
                Console.WriteLine("Download bandwidth limit = " + downloadRate + " bits
 per second");
            }
            catch (AmazonStorageGatewayException ex)
            {
                Console.WriteLine("Error updating gateway bandwith.\n" +
 ex.ToString());
            }
        }
    }
}
```

を使用したゲートウェイ帯域幅レート制限の更新 AWS Tools for Windows PowerShell

帯域幅レート制限をプログラムで更新することで (例えば、スケジュールされたタスクを使用することで)、一定期間にわたって制限を自動的に調整できます。次の例は、 AWS Tools for Windows PowerShellを使用して、ゲートウェイの帯域幅レート制限を更新する方法を示しています。サンプルコードを使用するには、スクリプトの実行 PowerShellに精通している必要があります。詳細については、AWS Tools for Windows PowerShell ユーザーガイドの「使用開始」を参照してください。

Example : を使用したゲートウェイ帯域幅レート制限の更新 AWS Tools for Windows PowerShell

次の PowerShell スクリプト例では、ゲートウェイの帯域幅レート制限を更新します。このサンプルスクリプトを使用するには、ゲートウェイの Amazon リソースネーム (ARN) と、アップロードとダウンロードの制限を指定する必要があります。

```
<#
.DESCRIPTION
```

```
    Update Gateway bandwidth limits.

.NOTES
    PREREQUISITES:
    1) AWS Tools for PowerShell from https://aws.amazon.com/powershell/
    2) Credentials and region stored in session using Initialize-AWSDefault.
    For more info, see https://docs.aws.amazon.com/powershell/latest/userguide/
specifying-your-aws-credentials.html


.EXAMPLE
    powershell.exe .\SG_UpdateBandwidth.ps1
#>

$UploadBandwidthRate = 51200
$DownloadBandwidthRate = 102400
$gatewayARN = "*** provide gateway ARN ***"

#Update Bandwidth Rate Limits
Update-SGBandwidthRateLimit -GatewayARN $gatewayARN `
                            -AverageUploadRateLimitInBitsPerSec $UploadBandwidthRate `
                            -AverageDownloadRateLimitInBitsPerSec
 $DownloadBandwidthRate

$limits =  Get-SGBandwidthRateLimit -GatewayARN $gatewayARN

Write-Output("`nGateway: " + $gatewayARN);
Write-Output("`nNew Upload Rate: " + $limits.AverageUploadRateLimitInBitsPerSec)
Write-Output("`nNew Download Rate: " + $limits.AverageDownloadRateLimitInBitsPerSec)
```

ゲートウェイの更新の管理

Storage Gateway は、マネージド型クラウドサービスコンポーネントと、オンプレミスまたは AWS クラウド内の Amazon EC2インスタンスにデプロイするゲートウェイアプライアンスコンポーネントで構成されます。どちらのコンポーネントも定期的に更新を受け取ります。このセクションのトピックでは、これらの更新の頻度、適用方法、およびデプロイ内のゲートウェイで更新関連の設定を構成する方法について説明します。

> **Important**
>
> Storage Gateway アプライアンスは、マネージド型の仮想マシンとして扱い、インストールへのアクセスや変更を試みるべきではありません。通常の AWS ゲートウェイ更新メカニズ

ム (やハイパーバイザーツールなど) 以外の方法を使用してソフトウェアパッケージをインストールSSMまたは更新しようとすると、ゲートウェイが誤動作する可能性があります。

更新頻度と予想される動作

AWS は、デプロイされたゲートウェイを中断することなく、必要に応じてクラウドサービスコンポーネントを更新します。デプロイされたゲートウェイアプライアンスは、毎月メンテナンスの更新を受け取ります。毎月のメンテナンス更新には、オペレーティングシステムとソフトウェアのアップグレード、安定性、パフォーマンス、セキュリティに対処するための修正、新機能へのアクセスが含まれます。すべての更新は累積的であり、適用時にゲートウェイを最新バージョンにアップグレードします。各更新に含まれる特定の変更については、https://docs.aws.amazon.com/storagegateway/latest/vgw/release-notes.html」を参照してください。

毎月のメンテナンス更新により、サービスが短時間中断される場合があります。ゲートウェイの VM ホストは更新中に再起動する必要はありませんが、ゲートウェイアプライアンスの更新と再起動中はゲートウェイが短時間使用できなくなります。

ゲートウェイをデプロイしてアクティブ化すると、デフォルトの毎週のメンテナンスウィンドウスケジュールが設定されます。メンテナンスウィンドウのスケジュールはいつでも変更できます。毎月のメンテナンス更新をオフにすることもできますが、オンのままにしておくことをお勧めします。

> **Note**
>
> 緊急の更新は、定期的なメンテナンス更新がオフになっていても、メンテナンスウィンドウのスケジュールに従って適用されることがあります。

更新がゲートウェイに適用される前に、 は Storage Gateway コンソールと にメッセージで AWS 通知します AWS Health Dashboard。詳細については、「AWS Health Dashboard」を参照してください。ソフトウェア更新通知が送信される E メールアドレスを変更するには、AWS 「 アカウント管理リファレンスガイド」の「アカウントの代替連絡先の更新」を参照してください。 AWS

更新が利用可能になると、ゲートウェイの詳細タブにメンテナンスメッセージが表示されます。最後に正常に更新された日時は、詳細タブで確認できます。

メンテナンスの更新をオンまたはオフにする

メンテナンス更新を有効にすると、ゲートウェイは設定されたメンテナンスウィンドウのスケジュールに従ってこれらの更新を自動的に適用します。詳細については、」を参照してください。

メンテナンス更新がオフになっている場合、ゲートウェイはこれらの更新を自動的に適用しませんが、Storage Gateway コンソール、、APIまたは を使用していつでも手動で適用できますCLI。この設定に関係なく、設定されたメンテナンスウィンドウ中に緊急の更新が適用されることがあります。

> **Note**
>
> 次の手順では、Storage Gateway コンソールを使用してゲートウェイの更新を有効または無効にする方法について説明します。を使用してこの設定をプログラムUpdateMaintenanceStartTimeで変更するにはAPI、Storage Gateway APIリファレンスの「」を参照してください。

Storage Gateway コンソールを使用してメンテナンスの更新をオンまたはオフにするには：

1. ホーム で Storage Gateway https://console.aws.amazon.com/storagegateway/コンソールを開きます。
2. ナビゲーションペインで、ゲートウェイ を選択し、メンテナンス更新を設定するゲートウェイを選択します。
3. アクション を選択し、メンテナンス設定の編集 を選択します。
4. メンテナンス更新 で、オン またはオフ を選択します。
5. 完了したら変更を保存を選択します。

Storage Gateway コンソールの選択したゲートウェイの詳細タブで、更新された設定を確認できます。

ゲートウェイメンテナンスウィンドウのスケジュールを変更する

メンテナンス更新が有効になっている場合、ゲートウェイはメンテナンスウィンドウのスケジュールに従ってこれらの更新を自動的に適用します。緊急の更新は、メンテナンスの更新設定に関係なく、設定されたメンテナンスウィンドウ中に適用されることがあります。

> **Note**
>
> 次の手順では、Storage Gateway コンソールを使用してメンテナンスウィンドウのスケジュールを変更する方法について説明します。を使用してこの設定をプログラムUpdateMaintenanceStartTimeで変更するにはAPI、Storage Gateway APIリファレンスの「」を参照してください。

Storage Gateway コンソールを使用してメンテナンスウィンドウのスケジュールを変更するには：

1. ホーム で Storage Gateway https://console.aws.amazon.com/storagegateway/コンソールを開きます。
2. ナビゲーションペインで、ゲートウェイ を選択し、メンテナンス更新を設定するゲートウェイを選択します。
3. アクション を選択し、メンテナンス設定の編集 を選択します。
4. メンテナンスウィンドウの開始時刻 で、次の操作を行います。

   a. スケジュール で、毎週または毎月 を選択してメンテナンスウィンドウのケイデンスを設定します。

   b. 週次 を選択した場合は、曜日と時刻の値を変更して、メンテナンスウィンドウが開始される各週の特定のポイントを設定します。

      毎月 を選択した場合は、メンテナンスウィンドウが開始される各月の特定時点を設定するように、その月の日と時刻の値を変更します。

      > **Note**
      >
      > 月の中の日として設定できる最大値は 28 です。メンテナンススケジュールを 29～31 日に開始するように設定することはできません。
      > この設定中にエラーが発生した場合は、ゲートウェイソフトウェアが古くなっている可能性があります。まずゲートウェイを手動で更新してから、メンテナンスウィンドウのスケジュールを再度設定することを検討してください。

5. 完了したら変更を保存を選択します。

Storage Gateway コンソールの選択したゲートウェイの詳細タブで、更新された設定を確認できます。

ローカルコンソールを使用したメンテナンスタスクの実行

ホストのローカルコンソールを使用して次のメンテナンスタスクを実行できます。ローカルコンソールタスクは、VM ホストまたは Amazon EC2インスタンスで実行できます。多くのタスクはさまざまなホストに共通していますが、異なる点もいくつかあります。

VM ローカルコンソールでのタスクの実行

ゲートウェイがオンプレミスでデプロイされている場合は、VM ホストのローカルコンソールを使用して、以下のメンテナンスタスクを実行できます。これらのタスクはVMware、、Hyper-V、および Linux カーネルベースの仮想マシン (KVM) ホストに共通です。

トピック

- デフォルトの認証情報を使用したローカルコンソールへのログイン
- Storage Gateway コンソールからのローカルコンソールパスワードの設定
- オンプレミスのゲートウェイでのプロキシ経由のルーティング
- ゲートウェイのネットワークの設定
- ゲートウェイのインターネット接続のテスト
- ゲートウェイ VM の時刻の同期
- ローカルコンソールでの Storage Gateway コマンドの実行
- ゲートウェイシステムリソースのステータスの表示
- ゲートウェイのネットワークアダプタの設定

デフォルトの認証情報を使用したローカルコンソールへのログイン

VM にログインできるようになると、ログイン画面が表示されます。ローカルコンソールに初めてログインする場合は、デフォルトのサインイン認証情報を使用してログインします。これらのデフォルトのログイン認証情報を使用することで、ゲートウェイのネットワーク設定を構成したり、ローカルコンソールからパスワードを変更したりできるメニューにアクセスできます。Storage Gateway では、ローカル AWS Storage Gateway コンソールからパスワードを変更する代わりに、コンソールから独自のパスワードを設定できます。新しいパスワードを設定するためにデフォルトパスワードを知っている必要はありません。詳細については、「Storage Gateway コンソールからのローカルコンソールパスワードの設定」を参照してください。

ゲートウェイのローカルコンソールにログインするには

1. ローカルコンソールに初めてログインする場合は、デフォルトの認証情報を使用して VM にログインします。デフォルトのユーザー名は admin、パスワードは password です。

   初めてではない場合は、認証情報を使用してログインします。

   > **Note**
   >
   > デフォルトのパスワードは変更することを推奨します。変更するには、[AWS Appliance Activation - Configuration] メインメニューで [Gateway Console] に対応する番号を入力し、passwd コマンドを実行してください。このコマンドを実行する方法については、「ローカルコンソールでの Storage Gateway コマンドの実行」を参照してください。AWS Storage Gateway コンソールから独自のパスワードを設定することもできます。詳細については、「Storage Gateway コンソールからのローカルコンソールパスワードの設定」を参照してください。

   > **Important**
   >
   > 古いバージョンのボリュームまたはテープゲートウェイでは、ユーザー名は sguser、パスワードは sgpassword です。パスワードをリセットし、ゲートウェイが新しいバージョンに更新された場合、ユーザー名は admin に変更されますが、パスワードは維持されます。

2. ログインすると、[AWS Storage Gateway Configuration] メインメニューが表示されます。このメニューから、さまざまなタスクを実行できます。

実行するタスク	参照先のトピック
ゲートウェイのSOCKSプロキシを設定する	オンプレミスのゲートウェイでのプロキシ経由のルーティング.
ネットワークを設定する	ゲートウェイのネットワークの設定.
ネットワークの接続をテストする	ゲートウェイのインターネット接続のテスト.
VM の時刻を管理します	ゲートウェイ VM の時刻の同期.

実行するタスク	参照先のトピック
Storage Gateway コンソールコマンドを実行する	ローカルコンソールでの Storage Gateway コマンドの実行.
システムリソースチェックを表示する	ゲートウェイシステムリソースのステータスの表示.

ゲートウェイをシャットダウンするには、「**0**」と入力します。

設定セッションを終了するには、「**X**」と入力します。

Storage Gateway コンソールからのローカルコンソールパスワードの設定

ローカルコンソールに初めてログインするとき、デフォルトの認証情報 (ユーザー名 `admin` およびパスワード `password`) を使用して VM にログインします。新しいゲートウェイを作成した直後に必ず新しいパスワードを設定することをお勧めします。このパスワードは、必要に応じてローカルコンソールではなく AWS Storage Gateway コンソールから設定できます。新しいパスワードを設定するためにデフォルトパスワードを知っている必要はありません。

Storage Gateway コンソールでローカルコンソールパスワードを設定するには

1. ホーム で Storage Gateway https://console.aws.amazon.com/storagegateway/コンソールを開きます。
2. ナビゲーションペインで、[Gateways] を選択し、新しいパスワードを設定するゲートウェイを選択します。
3. [Actions] で、[Set Local Console Password] を選択します。
4. [Set Local Console Password] ダイアログボックスで、新しいパスワードを入力し、確認のためにパスワードを再入力してから、[Save] を選択します。新しいパスワードを設定すると、デフォルトのパスワードが置き換えられます。Storage Gateway にはパスワードが保存されず、VM に安全に送信されます。

> **Note**
>
> パスワードには、キーボードの任意の文字を使用することができ、長さは 1 ~ 512 文字です。

オンプレミスのゲートウェイでのプロキシ経由のルーティング

ボリュームゲートウェイとテープゲートウェイは、オンプレミスゲートウェイと 間のソケットセキュアバージョン 5 (SOCKS5) プロキシの設定をサポートします AWS。

> **Note**
>
> サポートされているプロキシ設定は のみですSOCKS5。

ゲートウェイがプロキシサーバーを使用してインターネットと通信する必要がある場合は、ゲートウェイのSOCKSプロキシ設定を構成する必要があります。そのためには、プロキシを実行しているホストの IP アドレスとポート番号を指定します。その後、Storage Gateway はすべてのトラフィックをプロキシサーバー経由でルーティングします。ゲートウェイのネットワーク要件の詳細については、ネットワークとファイアウォールの要件を参照してください。

次の手順は、ボリュームゲートウェイとテープゲートウェイのSOCKSプロキシを設定する方法を示しています。

ボリュームゲートウェイとテープゲートウェイのSOCKS5プロキシを設定するには

1. ゲートウェイのローカルコンソールにログインします。
   - VMware ESXi – 詳細については、「」を参照してくださいを使用したゲートウェイローカルコンソールへのアクセス VMware ESXi。
   - Microsoft Hyper-V – 詳細については、「Microsoft Hyper-V でゲートウェイのローカルコンソールにアクセスする」を参照してください。
   - KVM – 詳細については、「」を参照してくださいLinux を使用したゲートウェイローカルコンソールへのアクセス KVM。
2. AWS Storage Gateway - 設定のメインメニューから、対応する数字を入力してSOCKSプロキシ設定 を選択します。
3. AWS Storage Gateway SOCKSプロキシ設定メニューから、対応する数字を入力して、次のいずれかのタスクを実行します。

このタスクを実行するには	操作
SOCKS プロキシを設定する	

このタスクを実行するには	操作
	対応する数字を入力して、SOCKSプロキシの設定 を選択します。 設定を完了するには、ホスト名とポートを指定する必要があります。
現在のSOCKSプロキシ設定を表示する	対応する数字を入力して、現在のSOCKSプロキシ設定の表示 を選択します。 SOCKS プロキシが設定されていない場合は、メッセージが表示されますSOCKS Proxy not configured 。SOCKS プロキシが設定されている場合は、プロキシのホスト名とポートが表示されます。
SOCKS プロキシ設定を削除する	対応する数字を入力して、SOCKSプロキシ設定の削除 を選択します。 "SOCKS Proxy Configuration Removed " というメッセージが表示されます。

4. VM を再起動してHTTP設定を適用します。

ゲートウェイのネットワークの設定

ゲートウェイのデフォルトのネットワーク設定は、Dynamic Host Configuration Protocol () ですDHCP。ではDHCP、ゲートウェイに IP アドレスが自動的に割り当てられます。場合によっては、以下に示すように、ゲートウェイの IP を静的 IP アドレスとして手動で割り当てる必要があります。

静的 IP アドレスを使用するようにゲートウェイを設定するには

1. ゲートウェイのローカルコンソールにログインします。

   - VMware ESXi – 詳細については、「」を参照してください[を使用したゲートウェイローカルコンソールへのアクセス VMware ESXi]。

- Microsoft Hyper-V – 詳細については、「Microsoft Hyper-V でゲートウェイのローカルコンソールにアクセスする」を参照してください。
- KVM – 詳細については、「」を参照してくださいLinux を使用したゲートウェイローカルコンソールへのアクセス KVM。

2. [AWS Storage Gateway - Configuration] メインメニューから、対応する番号を入力して [Network Configuration] を選択します。
3. [AWS Storage Gateway Network Configuration] メニューから、以下のいずれかのタスクを実行します。

このタスクを実行するには	操作
ネットワークアダプタの詳細を表示する	対応する番号を入力して [Describe Adapter] を選択します。 アダプタ名のリストが表示され、「**eth0**」などのアダプタ名の入力を求めるプロンプトが表示されます。指定したアダプタが使用中の場合、アダプタに関する次の情報が表示されます。 • メディアアクセスコントロール (MAC) アドレス • IP アドレス • ネットマスク • ゲートウェイ IP アドレス • DHCP アクティブ化ステータス 静的 IP アドレスを設定したり、ゲートウェイのデフォルトアダプタを設定したりするとき

このタスクを実行するには	操作
	は、ここに記載されているアダプタ名を使用します。
設定 DHCP	対応する数字を入力して、 の設定を選択しますDHCP。 を使用するようにネットワークインターフェイスを設定するように求められますDHCP。

このタスクを実行するには	操作
ゲートウェイの静的 IP アドレスを設定する	対応する番号を入力して [Configure Static IP] を選択します。 静的 IP アドレスを設定するために、以下の情報の入力を求められます。 • ネットワークアダプタ名 • IP アドレス • ネットマスク • デフォルトゲートウェイアドレス • プライマリドメインネームサービス (DNS) アドレス • セカンダリDNSアドレス **Important** ゲートウェイが既にアクティブになっている場合、設定を有効にするには、Storage Gateway コンソールでゲートウェイをシャットダウンして再起動する必要があります。詳細については、「ゲートウェイ VM のシャットダウン」を参照してください。 ゲートウェイが複数のネットワークインターフェイスを使用している場合は、 DHCPまたは

このタスクを実行するには	操作
	静的 IP アドレスを使用するように、アクティブ化されたすべてのインターフェイスを設定する必要があります。 例えば、ゲートウェイ VM が として設定された 2 つのインターフェイスを使用しているとしますDHCP。後で 1 つのインターフェイスを静的 IP に設定すると、もう 1 つのインターフェイスは無効になります。この場合、そのインターフェイスを有効にするには、静的 IP を設定する必要があります。 両方のインターフェイスが最初に静的 IP アドレスを使用するように設定され、次にゲートウェイが を使用するように設定されている場合DHCP、両方のインターフェイスは を使用しますDHCP。

このタスクを実行するには	操作
ゲートウェイのホスト名を設定する	対応する番号を入力して [Configure Hostname] を選択します。 ゲートウェイが指定した静的ホスト名を使用するか、 DCHPまたは r を介して自動的に取得するかを選択するように求められますDNS。 静的 を選択すると、 などの静的ホスト名を指定するように求められます`testgateway.example.com` 。を入力して設定yを適用します。 **Note** ゲートウェイに静的ホスト名を設定する場合は、指定されたホスト名がゲートウェイが結合されているドメインにあることを確認します。また、ゲートウェイの IP アドレスを静的ホスト名にポイントする A レコードをDNSシステム内に作成する必要があります。

このタスクを実行するには	操作
ゲートウェイのすべてのネットワーク設定を にリセットする DHCP	対応する数字を入力して、すべて にリセットDHCPを選択します。 すべてのネットワークインターフェイスは、を使用するように設定されていますDHCP。 **Important** ゲートウェイがすでにアクティブになっている場合、設定を有効にするには、Storage Gateway コンソールでゲートウェイをシャットダウンして再起動する必要があります。詳細については、「ゲートウェイ VM のシャットダウン」を参照してください。
ゲートウェイのデフォルトルートアダプタを設定する	対応する番号を入力して [Set Default Adapter] を選択します。 ゲートウェイで使用できるアダプタが表示され、「**eth0**」など、いずれかのアダプタを選択するよう求めるプロンプトが表示されます。
ゲートウェイDNSの設定を表示する	対応する数字を入力して、DNS設定の表示 を選択します。 プライマリネームサーバーとセカンダリDNSネームサーバーの IP アドレスが表示されます。

このタスクを実行するには	操作
ルーティングテーブルを表示する	対応する番号を入力して [View Routes] を選択します。 ゲートウェイのデフォルトルートが表示されます。

ゲートウェイのインターネット接続のテスト

ゲートウェイのローカルコンソールを使用してインターネット接続をテストできます。このテストは、ゲートウェイのネットワーク問題をトラブルシューティングするときに役立ちます。

インターネットに対するゲートウェイの接続をテストするには

1. ゲートウェイのローカルコンソールにログインします。

   - VMware ESXi – 詳細については、「」を参照してください[を使用したゲートウェイローカルコンソールへのアクセス VMware ESXi](#)。
   - Microsoft Hyper-V – 詳細については、「[Microsoft Hyper-V でゲートウェイのローカルコンソールにアクセスする](#)」を参照してください。
   - KVM – 詳細については、「」を参照してください[Linux を使用したゲートウェイローカルコンソールへのアクセス KVM](#)。

2. [AWS Storage Gateway - Configuration] メインメニューから、対応する番号を入力して [Test Network Connectivity] を選択します。

   ゲートウェイがすでにアクティブ化されている場合は、接続テストがすぐに開始します。まだアクティブ化されていないゲートウェイの場合は、次の手順で説明 AWS リージョン するように、エンドポイントタイプ と を指定する必要があります。

3. ゲートウェイがまだアクティブ化されていない場合は、対応する番号を入力して、ゲートウェイのエンドポイントタイプを選択します。

4. パブリックエンドポイントタイプを選択した場合は、対応する数字を入力して、テスト AWS リージョン する を選択します。Storage Gateway でサポートされている AWS サービスエンドポイント AWS リージョン のリストについては、「」の[AWS Storage Gateway 「 エンドポイントとクォータ](#)」を参照してくださいAWS 全般のリファレンス。 Storage Gateway

テストが進むと、各エンドポイントに 〔PASSED〕 または 〔FAILED〕 が表示され、次のように接続のステータスが表示されます。

メッセージ	説明
[PASSED]	Storage Gateway がネットワークに接続されています。
[FAILED]	Storage Gateway はネットワークに接続されていません。

ゲートウェイ VM の時刻の同期

ゲートウェイをデプロイして実行した後、ゲートウェイ VM の時刻がずれることがあります。たとえば、長時間のネットワーク中断が発生し、ハイパーバイザーホストとゲートウェイの時刻が更新されない場合、ゲートウェイ VM の時刻が実際の時刻と一致しなくなります。時刻にずれがあると、スナップショットなどのオペレーションが発生した時点を示す時刻と、実際の発生時刻との間に相違が発生します。

にデプロイされたゲートウェイではVMwareESXi、ハイパーバイザーのホスト時間を設定し、VM 時間をホストに同期するだけで、時間のずれを回避できます。詳細については、「VM の時刻とホストの時刻の同期」を参照してください。

Microsoft Hyper-V にデプロイされたゲートウェイの場合は、定期的に VM の時刻を確認する必要があります。詳細については、「ゲートウェイ VM の時刻の同期」を参照してください。

ローカルコンソールでの Storage Gateway コマンドの実行

Storage Gateway の VM ローカルコンソールは、ゲートウェイの設定と問題の診断のための安全な環境を提供します。ローカルコンソールコマンドを使用して、ルーティングテーブルの保存、 への接続などのメンテナンスタスクを実行できます AWS Support。

設定または診断コマンドを実行するには

1. ゲートウェイのローカルコンソールにログインします。

   - VMware ESXi ローカルコンソールへのログインの詳細については、「」を参照してくださいを使用したゲートウェイローカルコンソールへのアクセス VMware ESXi。

- Microsoft Hyper-V ローカルコンソールへのログインの詳細については、「Microsoft Hyper-V でゲートウェイのローカルコンソールにアクセスする」を参照してください。
- KVM ローカルコンソールへのログインの詳細については、「」を参照してくださいLinux を使用したゲートウェイローカルコンソールへのアクセス KVM。

2. [AWS Appliance Activation - Configuration] メインメニューから、対応する番号を入力して「Gateway Console」を選択します。
3. ゲートウェイコンソールのコマンドプロンプトから、「**h**」と入力します。

   コンソールにAVAILABLECOMMANDSメニューが表示され、使用可能なコマンドが一覧表示されます。

Command	機能
dig	dig から出力を収集してDNSトラブルシューティングを行います。
exit	コンソール設定メニューに戻ります。
h	使用可能なコマンドリストを表示します。
ifconfig	ネットワークインターフェイスを表示または設定します。 **Note** Storage Gateway コンソールまたは専用のローカルコンソールメニューオプションを使用して、ネットワークまたは IP 設定を構成することをお勧めします。手順については、「ゲートウェイネットワークの設定」を参照してください。
ip	ルーティング、デバイス、トンネルを表示または操作します。

Command	機能
	Note Storage Gateway コンソールまたは専用のローカルコンソールメニューオプションを使用して、ネットワークまたは IP 設定を構成することをお勧めします。手順については、「ゲートウェイネットワークの設定」を参照してください。
iptables	IPv4 パケットフィルタリングと の管理ツール NAT。
ncport	ネットワーク上の特定のTCPポートへの接続をテストします。
nping	ネットワークのトラブルシューティング用に、nping からの出力を収集します。
open-support-channel	AWS サポートに接続します。
passwd	認証トークンを更新します。
save-iptables	IP テーブルを永続化します。
save-routing-table	新しく追加されたルーティングテーブルエントリーを保存します。

Command	機能
sslcheck	証明書発行者の出力を返します **Note** Storage Gateway は証明書発行者の検証を使用し、ssl 検査をサポートしていません。このコマンドが aws-appliance@amazon.com 以外の発行者を返す場合、アプリケーションが ssl 検査を実行している可能性があります。その場合は、Storage Gateway アプライアンスの ssl 検査をバイパスすることをお勧めします。
tcptraceroute	送信先へのTCPトラフィックの traceroute 出力を収集します。

4. ゲートウェイコンソールのコマンドプロンプトから、使用したい機能に対応するコマンドを入力し、指示に従います。

コマンドの詳細については、 **man** + と入力します。*command name* コマンドプロンプトの 。

ゲートウェイシステムリソースのステータスの表示

ゲートウェイの起動時に、ゲートウェイは仮想CPUコア、ルートボリュームサイズ、および を チェックしますRAM。その後、ゲートウェイが適切に機能するためにこれらのシステムリソースが十分であるかどうかが確認されます。このチェックの結果は、ゲートウェイのローカルコンソールで表示できます。

システムリソースチェックのステータスを表示するには

1. ゲートウェイのローカルコンソールにログインします。

   - VMware ESXi コンソールへのログインの詳細については、「」を参照してください[を使用したゲートウェイローカルコンソールへのアクセス VMware ESXi]。

- Microsoft Hyper-V ローカルコンソールへのログインの詳細については、「Microsoft Hyper-V でゲートウェイのローカルコンソールにアクセスする」を参照してください。
- KVM ローカルコンソールへのログインの詳細については、「」を参照してくださいLinux を使用したゲートウェイローカルコンソールへのアクセス KVM。

2. [AWS Appliance Activation - Configuration] メインメニューで、対応する番号を入力して「View System Resource Check」を選択します。

   各リソースには [OK 〕、〔WARNING〕、または 〔FAIL〕 が表示され、リソースのステータスが次のように表示されます。

メッセージ	説明
[OK]	リソースはシステムリソースチェックに合格しました。
[WARNING]	リソースは推奨される要件を満たしていませんが、ゲートウェイは引き続き機能します。Storage Gateway は、リソースチェックの結果について説明するメッセージを表示します。
[FAIL]	リソースは最小要件を満たしていません。ゲートウェイ は適切に機能していない可能性があります。Storage Gateway は、リソースチェックの結果について説明するメッセージを表示します。

   また、コンソールには、エラーと警告の数がリソースチェックメニューオプションの横に表示されます。

ゲートウェイのネットワークアダプタの設定

デフォルトでは、Storage Gateway は E1000 ネットワークアダプタタイプを使用するように設定されていますが、 VMXNET3 (10 GbE) ネットワークアダプタを使用するようにゲートウェイを再設定できます。複数の IP アドレスから Storage Gateway にアクセスできるように設定することもできます。これを行うには、複数のネットワークアダプタを使用するようにゲートウェイを設定します。

トピック

- VMXNET3 ネットワークアダプタを使用するようにゲートウェイを設定する
- ゲートウェイを複数の に設定する NICs

VMXNET3 ネットワークアダプタを使用するようにゲートウェイを設定する

Storage Gateway は、 VMwareESXiと Microsoft Hyper-V ハイパーバイザーホストの両方で E1000 ネットワークアダプタタイプをサポートします。ただし、 VMXNET3 (10 GbE) ネットワークアダプタタイプはVMwareESXiハイパーバイザーでのみサポートされています。ゲートウェイがVMwareESXiハイパーバイザーでホストされている場合は、 VMXNET3 (10 GbE) アダプタータイプを使用するようにゲートウェイを再設定できます。これらのアダプターの詳細については、Broadcom (VMware) ウェブサイトの「仮想マシンのネットワークアダプターの選択」を参照してください。

> **Important**
>
> を選択するにはVMXNET3、ゲストオペレーティングシステムタイプがその他の Linux64 である必要があります。

VMXNET3 アダプターを使用するようにゲートウェイを設定する手順は次のとおりです。

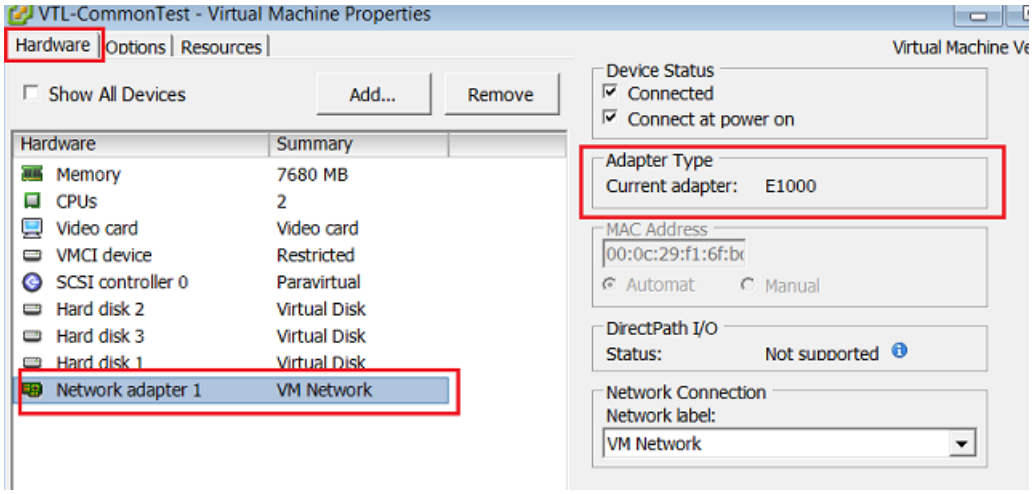
1. デフォルトの E1000 アダプタを削除します。
2. VMXNET3 アダプターを追加します。
3. ゲートウェイを再起動します。
4. ネットワークに対してアダプタを設定します。

各ステップの実行方法について説明します。

デフォルトの E1000 アダプターを削除し、VMXNET3アダプターを使用するようにゲートウェイを設定するには

1. でVMware、ゲートウェイのコンテキスト (右クリック) メニューを開き、設定の編集 を選択します。
2. [Virtual Machine Properties] ウィンドウで [Hardware] タブを選択します。

3. [Hardware] で [Network adapter] を選択します。[Adapter Type] セクションで現在のアダプタが E1000 であることを確認します。このアダプターをVMXNET3アダプターに置き換えます。



4. E1000 ネットワークアダプタを選択し、[Remove] を選択します。この例では、E1000 ネットワークアダプタは Network adapter 1 です。

> **Note**
>
> E1000 とVMXNET3ネットワークアダプタはゲートウェイで同時に実行できますが、ネットワークの問題を引き起こす可能性があるため、実行することはお勧めしません。

5. [Add] を選択して Add Hardware ウィザードを開きます。
6. [Ethernet Adapter] を選択し、[Next] を選択します。
7. ネットワークタイプウィザードで、[Adapter Type] (アダプタタイプ) に **VMXNET3** を選択してから、[Next] (次へ) をクリックします。
8. 仮想マシンのプロパティウィザードで、「アダプタータイプ」セクションで現在のアダプターがに設定されていることを確認してからVMXNET3、「OK」を選択します。
9. VMware VSphere クライアントで、ゲートウェイをシャットダウンします。
10. VMware VSphere クライアントで、ゲートウェイを再起動します。

ゲートウェイが再起動したら、インターネットへのネットワーク接続が確立されるように、追加したアダプタを再設定します。

ネットワークに対してアダプタを設定するには

1. VSphere クライアントで、コンソールタブを選択してローカルコンソールを起動します。この設定タスクでは、デフォルトのログイン認証情報を使用して、ゲートウェイのローカルコンソールにログインします。デフォルト認証情報を使用してログインする方法については、「デフォルトの認証情報を使用したローカルコンソールへのログイン」を参照してください。
2. プロンプトで、対応する番号を入力して [Network Configuration] を選択します。
3. プロンプトで、対応する数字を入力してすべて にリセットを選択しDHCP、プロンプトで **y** (はいの場合) を入力して、動的ホスト設定プロトコル () を使用するようにすべてのアダプターを設定しますDHCP。使用可能なすべてのアダプターは、 を使用するように設定されていますDHCP。

   ゲートウェイが既にアクティブになっている場合は、ゲートウェイをシャットダウンし、Storage Gateway マネジメントコンソールから再起動する必要があります。ゲートウェイが再起動したら、インターネットへのネットワーク接続をテストする必要があります。ネットワーク接続をテストする方法については、「ゲートウェイのインターネット接続のテスト」を参照してください。

ゲートウェイを複数の に設定する NICs

複数のネットワークアダプタ (NICs) を使用するようにゲートウェイを設定すると、複数の IP アドレスからゲートウェイにアクセスできます。このようにするのは、次のような場合です。

- スループットの最大化 – ネットワークアダプタがボトルネックになっている場合に、ゲートウェイへのスループットを最大にしたい場合があります。
- アプリケーションの分離 – アプリケーションがゲートウェイのボリュームに書き込む方法を分離することが必要な場合があります。たとえば、重要なストレージアプリケーションで、ゲートウェイ用に定義されている特定のアダプタが排他的に使用されるように設定することがあります。
- ネットワークの制約 — アプリケーション環境では、iSCSI ターゲットとそれらに接続するイニシエータを、ゲートウェイが と通信するネットワークとは異なる分離されたネットワークに保持する必要がある場合がありますAWS。

一般的な複数アダプタのユースケースでは、ゲートウェイが通信するルートとして 1 つのアダプタが設定されていますAWS（つまり、デフォルトゲートウェイとして）。この 1 つのアダプターを除き、イニシエータは、接続先の iSCSI ターゲットを含むアダプターと同じサブネットに存在する必要があります。そうでない場合は、意図したターゲットと通信できない可能性があります。ター

ゲットが との通信に使用されるのと同じアダプターで設定されている場合 AWS、そのターゲットの iSCSI トラフィックと AWS トラフィックは同じアダプターを経由します。

1 つのアダプタを Storage Gateway コンソールに接続するように設定し、その後 2 つ目のアダプタを追加した場合、Storage Gateway は 2 番目のアダプタを優先ルートとして使用するように自動的にルートテーブルを設定します。複数のアダプタを設定する手順については、以下のセクションを参照してください。

- VMware ESXi ホストNICs内の複数の に対するゲートウェイの設定
- Microsoft Hyper-V ホストNICsでの複数の のゲートウェイの設定

Amazon EC2 Local Console でのタスクの実行

一部のメンテナンスタスクでは、Amazon EC2インスタンスにデプロイされたゲートウェイを実行するときに、ローカルコンソールにログインする必要があります。このセクションでは、ローカルコンソールにログインして、メンテナンスタスクを実行する方法について説明します。

トピック

- Amazon EC2 Gateway ローカルコンソールへのログイン
- HTTP プロキシEC2経由で にデプロイされたゲートウェイをルーティングする
- ゲートウェイのネットワーク接続をテストする
- ゲートウェイシステムリソースのステータスの表示
- ローカルコンソールでの Storage Gateway コマンドの実行

Amazon EC2 Gateway ローカルコンソールへのログイン

Secure Shell (SSH) クライアントを使用して Amazon EC2インスタンスに接続できます。詳細については、「Amazon ユーザーガイド」の「インスタンスに接続する」を参照してください。 EC2 この方法で接続するには、インスタンスの起動時に指定したSSHキーペアが必要です。Amazon EC2 キーペアの詳細については、「Amazon ユーザーガイド」の「Amazon EC2 キーペア」を参照してください。 EC2

ゲートウェイのローカルコンソールにログインするには

1. ローカルコンソールにログインします。Windows コンピュータからEC2インスタンスに接続する場合は、管理者 としてログインします。

2. ログインすると、[AWS Storage Gateway - Configuration] メインメニューが表示されます。このメニューから、さまざまなタスクを実行できます。

実行するタスク	参照先のトピック
ゲートウェイのSOCKSプロキシを設定する	HTTP プロキシEC2経由で にデプロイされたゲートウェイをルーティングする
ネットワークの接続をテストする	ゲートウェイのネットワーク接続をテストする
Storage Gateway コンソールコマンドを実行する	ローカルコンソールでの Storage Gateway コマンドの実行
システムリソースチェックを表示する	ゲートウェイシステムリソースのステータスの表示.

ゲートウェイをシャットダウンするには、「**0**」と入力します。

設定セッションを終了するには、「**X**」と入力します。

HTTP プロキシEC2経由で にデプロイされたゲートウェイをルーティングする

Storage Gateway は、Amazon EC2と にデプロイされたゲートウェイ間の Socket Secure バージョン 5 (SOCKS5) プロキシの設定をサポートします AWS。

ゲートウェイがプロキシサーバーを使用してインターネットと通信する必要がある場合は、ゲートウェイのHTTPプロキシ設定を構成する必要があります。そのためには、プロキシを実行しているホストの IP アドレスとポート番号を指定します。その後、Storage Gateway はすべての AWS エンドポイントトラフィックをプロキシサーバー経由でルーティングします。HTTP プロキシを使用する場合でも、ゲートウェイとエンドポイント間の通信は暗号化されます。

ローカルプロキシサーバー経由でゲートウェイのインターネットトラフィックをルーティングするには

1. ゲートウェイのローカルコンソールにログインします。手順については、Amazon EC2 Gateway ローカルコンソールへのログイン を参照してください。
2. AWS アプライアンスのアクティベーション - 設定のメインメニューから、対応する数字を入力してHTTPプロキシの設定 を選択します。

3. AWS アプライアンスアクティベーションHTTPプロキシ設定メニューから、実行するタスクに対応する番号を入力します。

   - HTTP プロキシの設定 - 設定を完了するには、ホスト名とポートを指定する必要があります。
   - 現在のHTTPプロキシ設定を表示する - HTTPプロキシが設定されていない場合は、メッセージが表示されますHTTP Proxy not configured。HTTP プロキシが設定されている場合は、プロキシのホスト名とポートが表示されます。
   - HTTP プロキシ設定を削除する - メッセージHTTP Proxy Configuration Removedが表示されます。

ゲートウェイのネットワーク接続をテストする

ゲートウェイのローカルコンソールを使用して、ネットワーク接続をテストできます。このテストは、ゲートウェイのネットワーク問題をトラブルシューティングするときに役立ちます。

ゲートウェイの接続をテストするには

1. ゲートウェイのローカルコンソールにログインします。手順については、Amazon EC2 Gateway ローカルコンソールへのログイン を参照してください。
2. [AWS Appliance Activation - Configuration] メインメニューから、対応する番号を入力して [Test Network Connectivity] を選択します。

   ゲートウェイがすでにアクティブ化されている場合は、接続テストがすぐに開始します。まだアクティブ化されていないゲートウェイの場合は、次の手順で説明 AWS リージョン するように、エンドポイントタイプ と を指定する必要があります。
3. ゲートウェイがまだアクティブ化されていない場合は、対応する番号を入力して、ゲートウェイのエンドポイントタイプを選択します。
4. パブリックエンドポイントタイプを選択した場合は、対応する数字を入力して、テスト AWS リージョン する を選択します。Storage Gateway でサポートされている AWS サービスエンドポイント AWS リージョン のリストについては、「」のAWS Storage Gateway 「 エンドポイントとクォータ」を参照してくださいAWS 全般のリファレンス。 Storage Gateway

テストが進むと、各エンドポイントに 〔PASSED〕 または 〔FAILED〕 が表示され、次のように接続のステータスが表示されます。

メッセージ	説明
[PASSED]	Storage Gateway がネットワークに接続されています。
[FAILED]	Storage Gateway はネットワークに接続されていません。

ゲートウェイシステムリソースのステータスの表示

ゲートウェイの起動時に、ゲートウェイは仮想CPUコア、ルートボリュームサイズ、および を チェックしますRAM。その後、ゲートウェイが適切に機能するためにこれらのシステムリソースが十分であるかどうかが確認されます。このチェックの結果は、ゲートウェイのローカルコンソールで表示できます。

システムリソースチェックのステータスを表示するには

1. ゲートウェイのローカルコンソールにログインします。手順については、Amazon EC2 Gateway ローカルコンソールへのログイン を参照してください。
2. [AWS Appliance Activation - Configuration] メインメニューで、対応する番号を入力して「View System Resource Check」を選択します。

   各リソースには [OK 〕、〔WARNING〕、または 〔FAIL〕 が表示され、リソースのステータスが次のように表示されます。

メッセージ	説明
[OK]	リソースはシステムリソースチェックに合格しました。
[WARNING]	リソースは推奨される要件を満たしていませんが、ゲートウェイは引き続き機能します。Storage Gateway は、リソースチェックの結果について説明するメッセージを表示します。

メッセージ	説明
[FAIL]	リソースは最小要件を満たしていません。ゲートウェイ は適切に機能していない可能性があります。Storage Gateway は、リソースチェックの結果について説明するメッセージを表示します。

また、コンソールには、エラーと警告の数がリソースチェックメニューオプションの横に表示されます。

ローカルコンソールでの Storage Gateway コマンドの実行

AWS Storage Gateway コンソールは、ゲートウェイの問題を設定および診断するための安全な環境を提供するのに役立ちます。コンソールコマンドを使用して、ルーティングテーブルの保存や への接続などのメンテナンスタスクを実行できます AWS Support。

設定または診断コマンドを実行するには

1. ゲートウェイのローカルコンソールにログインします。手順については、Amazon EC2 Gateway ローカルコンソールへのログイン を参照してください。
2. [AWS Appliance Activation - Configuration] メインメニューから、対応する番号を入力して「Gateway Console」を選択します。
3. ゲートウェイコンソールのコマンドプロンプトから、「h」と入力します。

   コンソールにAVAILABLECOMMANDSメニューが表示され、使用可能なコマンドが一覧表示されます。

Command	機能
dig	dig から出力を収集してDNSトラブルシューティングを行います。
exit	コンソール設定メニューに戻ります。
h	使用可能なコマンドリストを表示します。

Command	機能
ifconfig	ネットワークインターフェイスを表示または設定します。 **Note** Storage Gateway コンソールまたは専用のローカルコンソールメニューオプションを使用して、ネットワークまたは IP 設定を構成することをお勧めします。
ip	ルーティング、デバイス、トンネルを表示または操作します。 **Note** Storage Gateway コンソールまたは専用のローカルコンソールメニューオプションを使用して、ネットワークまたは IP 設定を構成することをお勧めします。
iptables	IPv4 パケットフィルタリングと の管理ツール NAT。
ncport	ネットワーク上の特定のTCPポートへの接続をテストします。
nping	ネットワークのトラブルシューティング用に、nping からの出力を収集します。
open-support-channel	AWS サポートに接続します。
save-iptables	IP テーブルを永続化します。

Command	機能
save-routing-table	新しく追加されたルーティングテーブルエントリーを保存します。
sslcheck	ネットワークのトラブルシューティングSSLの有効性を確認します。
tcptraceroute	送信先へのTCPトラフィックの traceroute 出力を収集します。

4. ゲートウェイコンソールのコマンドプロンプトから、使用したい機能に対応するコマンドを入力し、指示に従います。

コマンドについて知るには、コマンド名の後に -h オプションを入力します (例: `sslcheck -h`)。

ゲートウェイローカルコンソールへのアクセス

VM のローカルコンソールにアクセスする方法は、ゲートウェイ VM をデプロイしたハイパーバイザーの種類によって異なります。このセクションでは、Linux カーネルベースの仮想マシン (KVM) 、ESXi、および Microsoft Hyper-V Manager を使用して VM VMware ローカルコンソールにアクセスする方法について説明します。

トピック

- Linux を使用したゲートウェイローカルコンソールへのアクセス KVM
- を使用したゲートウェイローカルコンソールへのアクセス VMware ESXi
- Microsoft Hyper-V でゲートウェイのローカルコンソールにアクセスする

Linux を使用したゲートウェイローカルコンソールへのアクセス KVM

で実行されている仮想マシンを設定するにはKVM、使用する Linux ディストリビューションに応じてさまざまな方法があります。コマンドラインからKVM設定オプションにアクセスする手順は次のとおりです。手順はKVM実装によって異なる場合があります。

を使用してゲートウェイのローカルコンソールにアクセスするには KVM

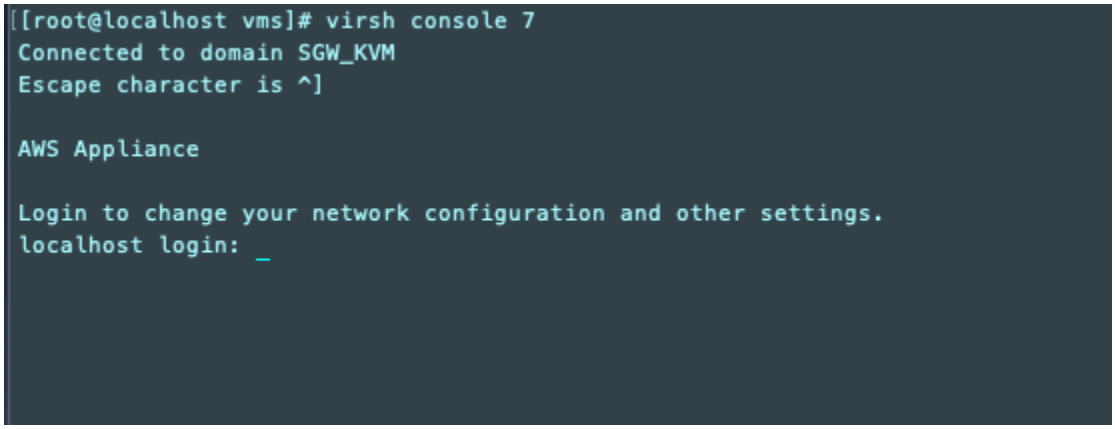
1. 次のコマンドを使用して、 でVMs現在利用可能な を一覧表示しますKVM。

```
# virsh list
```

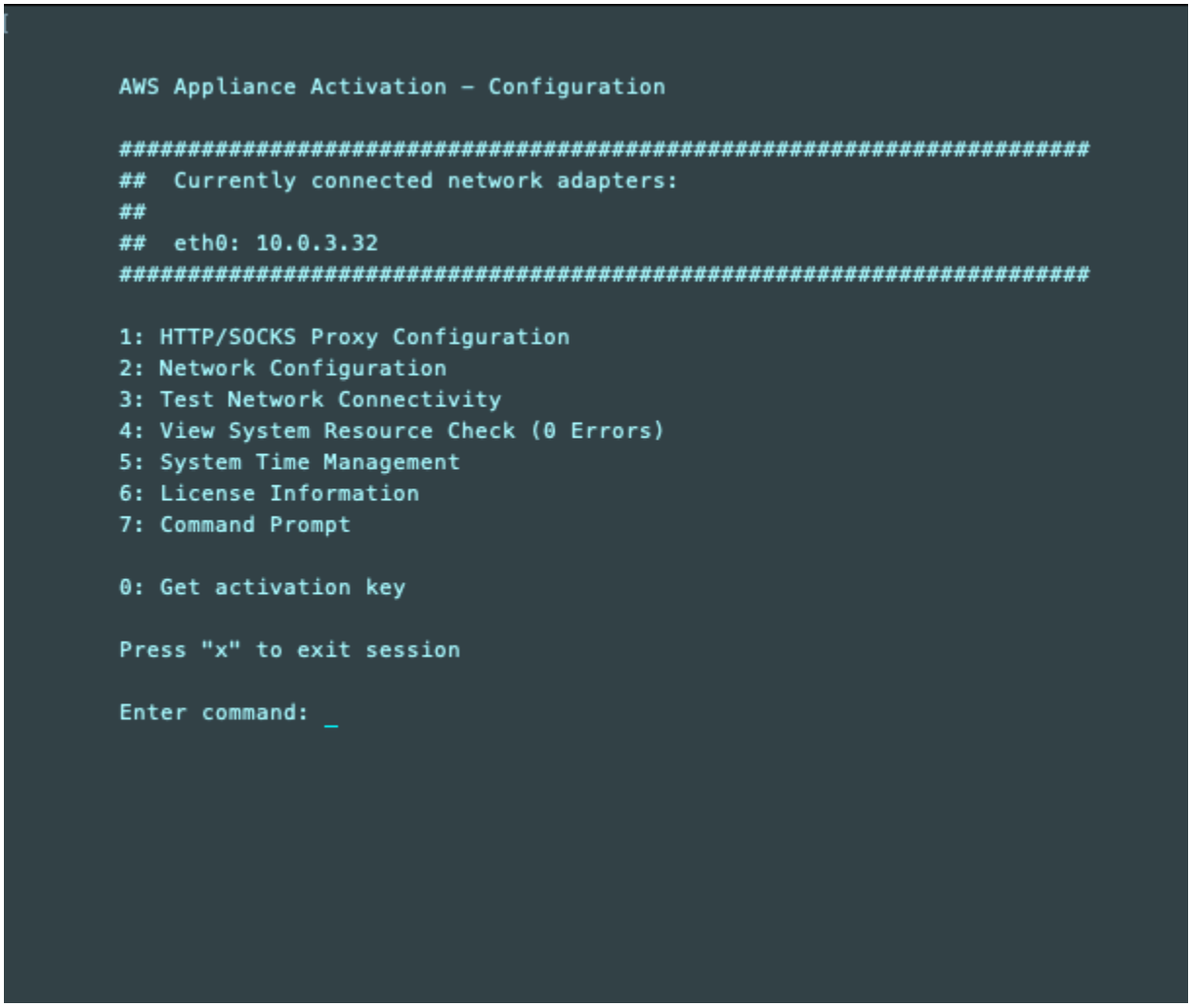
VMs で利用可能な を選択できますId。

2. ローカルコンソールにアクセスするには、次のコマンドを使用します。

```
# virsh console VM_Id
```



3. ローカルコンソールにログインするためのデフォルトの認証情報を取得するには、「デフォルトの認証情報を使用したローカルコンソールへのログイン」を参照してください。
4. ログイン後、ゲートウェイをアクティブ化して構成できます。

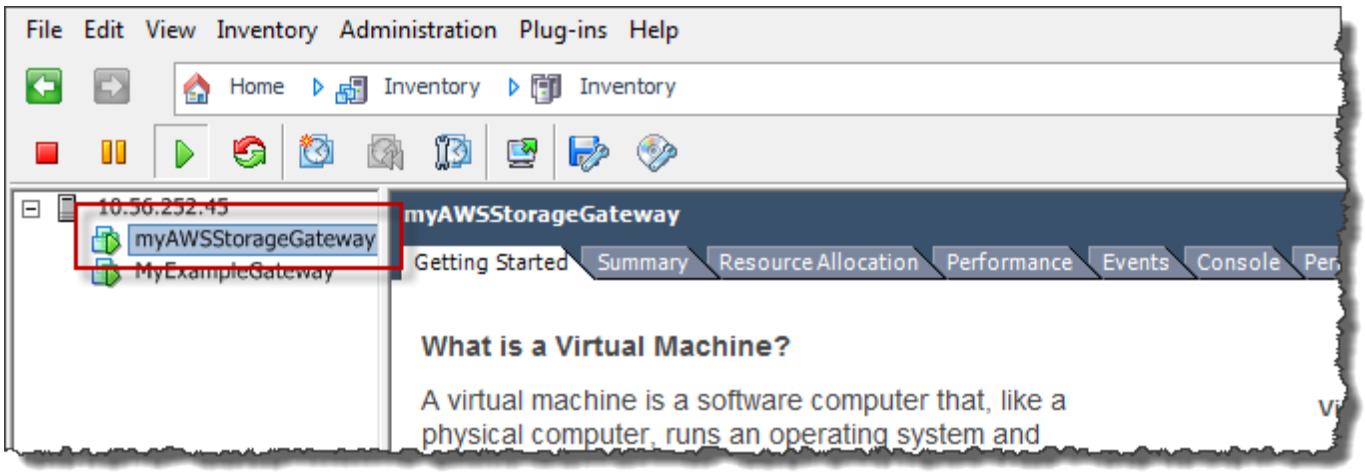


を使用したゲートウェイローカルコンソールへのアクセス VMware ESXi

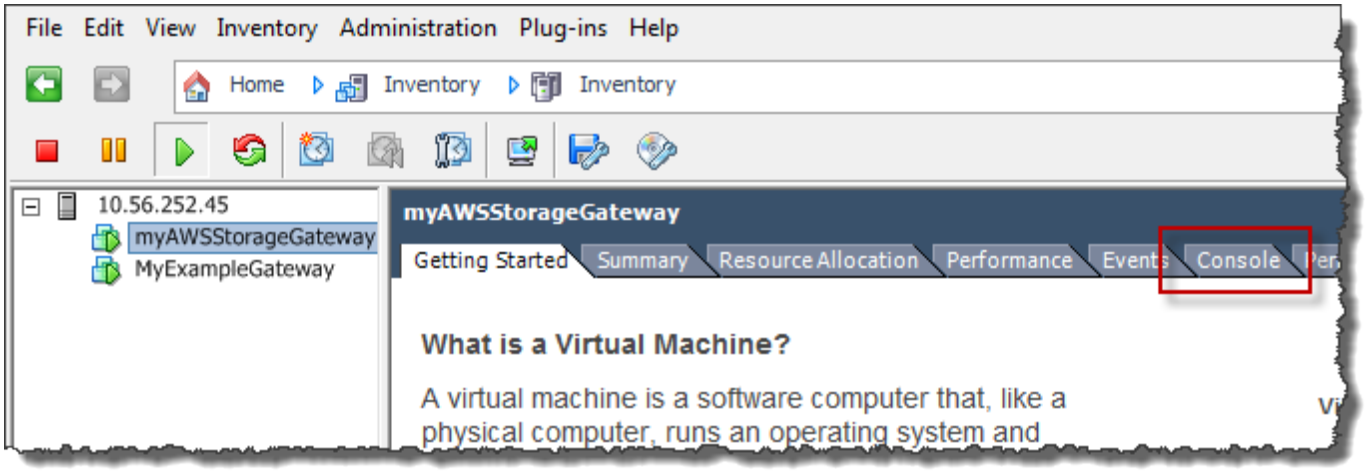
を使用してゲートウェイのローカルコンソールにアクセスするには VMware ESXi

1. VMware vSphere クライアントで、ゲートウェイ VM を選択します。
2. ゲートウェイの電源がオンになっていることを確認します。

> **Note**
>
> ゲートウェイ VM の電源が入っている場合は、次のスクリーンショットに示すように、VM アイコンと共に緑の矢印アイコンが表示されます。ゲートウェイ VM がオンになっていない場合は、[Toolbar] (ツールバー) メニュー上の緑の [Power On] (電源オン) アイコンをクリックしてオンにすることができます。

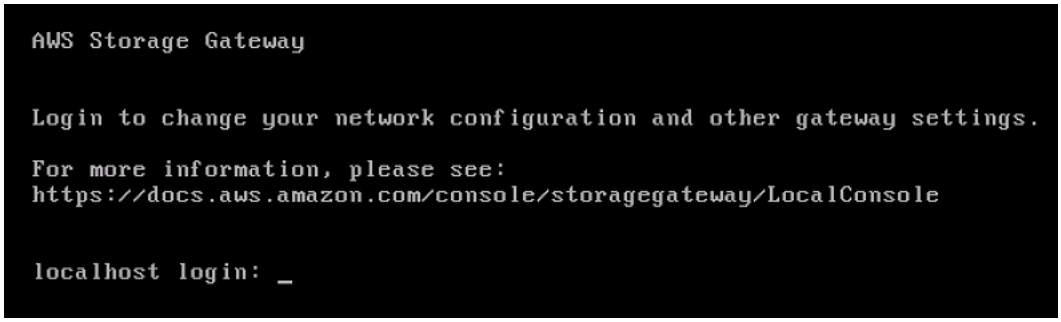


3. [Console] タブを選択します。



しばらくすると、VM にログインできる状態になります。

> **Note**
>
> コンソールウィンドウからカーソルを解放するには、Ctrl + Alt キーを押します。



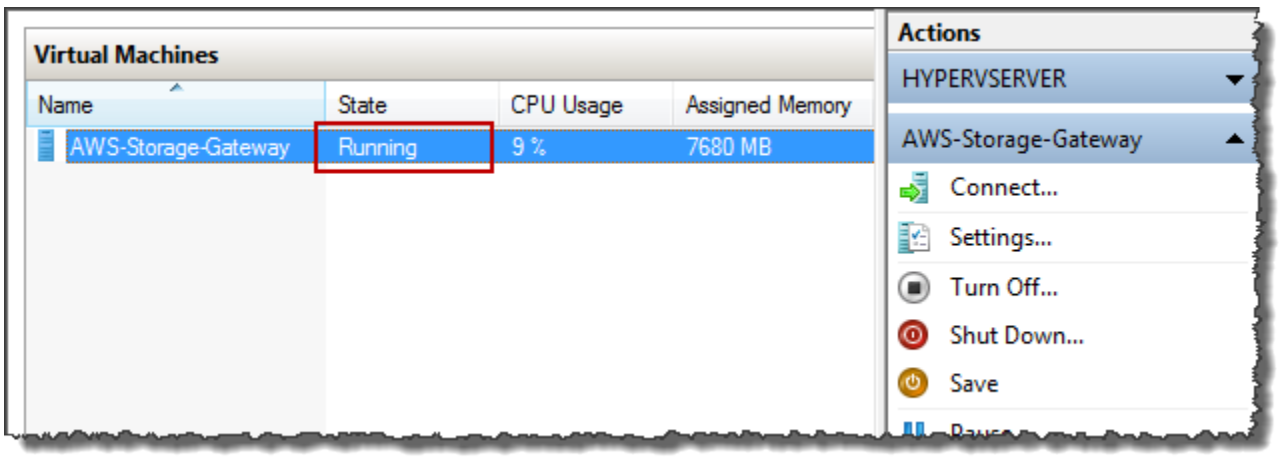
4. デフォルトの認証情報を使用してログインするには、「デフォルトの認証情報を使用したローカルコンソールへのログイン」の手順に進みます。

Microsoft Hyper-V でゲートウェイのローカルコンソールにアクセスする

ゲートウェイのローカルコンソールにアクセスするには (Microsoft Hyper-V)

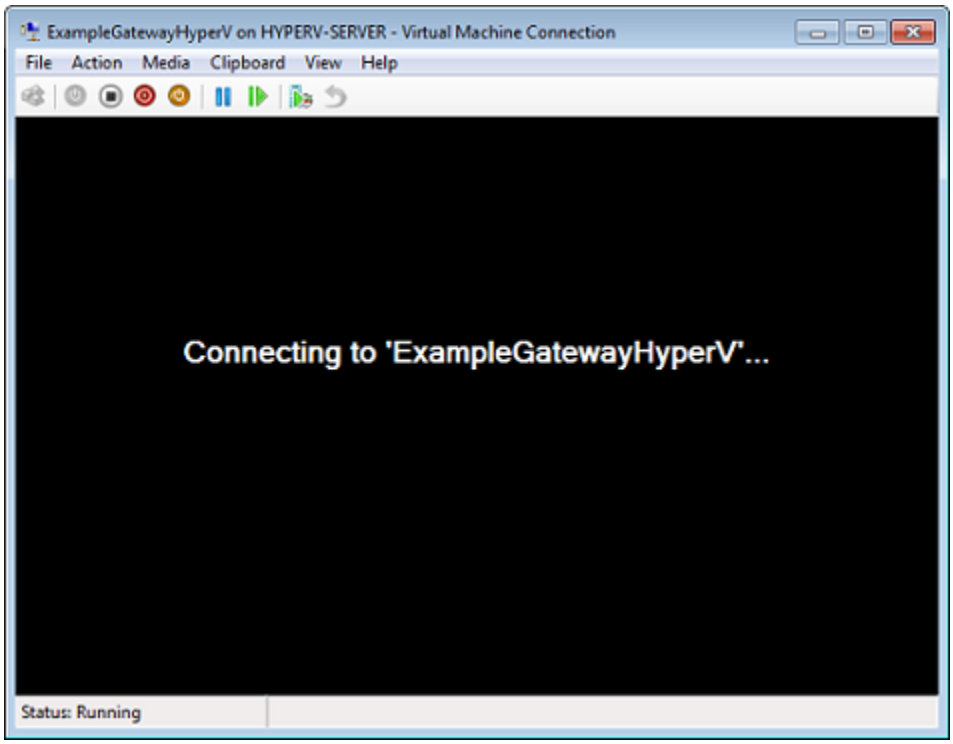
1. Microsoft Hyper-V Manager の [Virtual Machines] リストで、ゲートウェイ VM を選択します。
2. ゲートウェイの電源がオンになっていることを確認します。

> **Note**
>
> ゲートウェイ VM がオンになっていれば、次のスクリーンショットに示すように、VM の [State] (状態) として Running と表示されます。ゲートウェイ VM がオンになっていない場合は、[Actions] (アクション) ペインの [Start] (起動) を選択してオンにすることができます。



3. [Actions] ペインの [Connect] を選択します。

   [Virtual Machine Connection] ウィンドウが表示されます。認証ウィンドウが表示されたら、ハイパーバイザー管理者から提供されたサインイン認証情報を入力します。



   しばらくすると、VM にログインできる状態になります。

4. デフォルトの認証情報を使用してログインするには、「デフォルトの認証情報を使用したローカルコンソールへのログイン」の手順に進みます。

ゲートウェイのネットワークアダプタの設定

このセクションでは、ゲートウェイに複数のネットワークアダプタを設定する方法について説明します。

トピック

- VMware ESXi ホストNICs内の複数の に対するゲートウェイの設定
- Microsoft Hyper-V ホストNICsでの複数の のゲートウェイの設定

VMware ESXi ホストNICs内の複数の に対するゲートウェイの設定

次の手順では、ゲートウェイ VM にネットワークアダプタが 1 つ定義されていることを前提としており、 VMware にアダプタを追加する方法について説明しますESXi。

VMware ESXi ホストで追加のネットワークアダプタを使用するようにゲートウェイを設定するには

1. ゲートウェイをシャットダウンします。
2. VMware vSphere クライアントで、ゲートウェイ VM を選択します。

   この手順では、VM の電源は入れたままにしてかまいません。
3. クライアントでゲートウェイ VM のコンテキスト (右クリック) メニューを開き、[Edit Settings] を選択します。
4. [Virtual Machine Properties] (仮想マシンのプロパティ) ダイアログボックスの [Hardware] (ハードウェア) タブで、[Add] (追加) を選択してデバイスを追加します。
5. [Add Hardware] ウィザードに従って、ネットワークアダプタを追加します。

   a. [Device Type] ペインで [Ethernet Adapter] を選択してアダプタを追加し、[Next] を選択します。

   b. [Network Type] (ネットワークタイプ) ペインで、[Type] (タイプ) に [Connect at power on] (電源投入時に接続) が選択されていることを確認してから、[Next] (次へ) をクリックします。

      Storage Gateway でVMXNET3ネットワークアダプタを使用することをお勧めします。アダプターリストに表示されるアダプタータイプの詳細については、「」の「ネットワークアダプタータイプESXi」および vCenter 「サーバードキュメント」を参照してください。

   c. [Ready to Complete] ペインで情報を確認し、[Finish] を選択します。
6. VM の [Summary] タブを選択し、[IP Address] ボックスの横にある [View All] を選択します。[Virtual Machine IP Addresses] ウィンドウに、ゲートウェイへのアクセスに使用できるすべての IP アドレスが表示されます。2 番目の IP アドレスがゲートウェイに対して表示されることを確認します。

> **Note**
>
> アダプタの変更が有効になり、VM のサマリ情報が更新されるまでに、しばらく時間がかかる場合があります。

7. Storage Gateway コンソールでゲートウェイをオンにします。
8. Storage Gateway コンソールの [Navigation] (ナビゲーション) ペインで、[Gateways] (ゲートウェイ) を選択し、アダプタを追加したゲートウェイを選択します。2 番目の IP アドレスが [詳細] タブに表示されることを確認します。

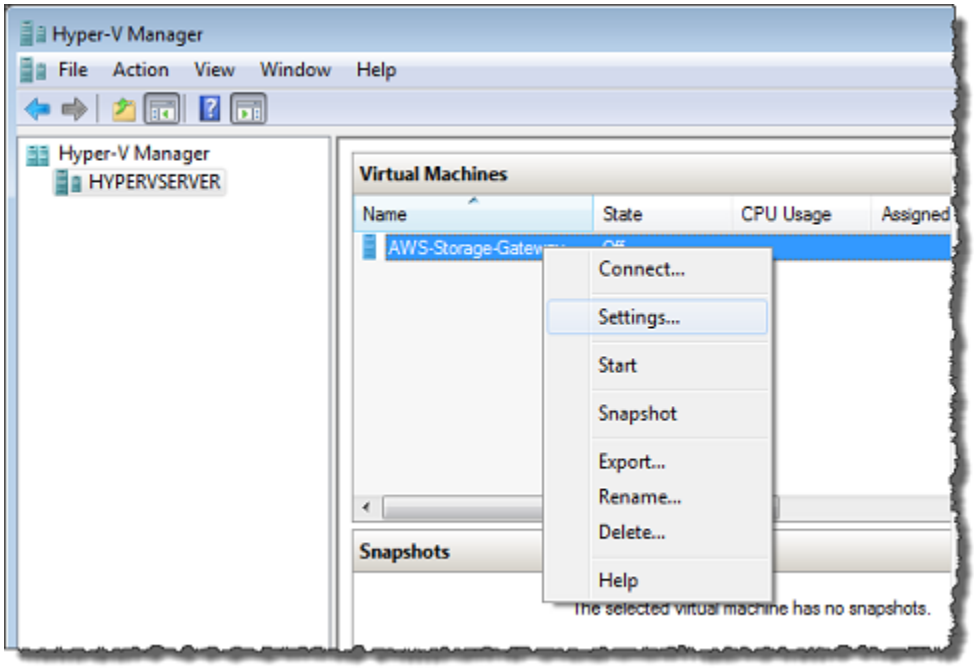
、Hyper-VVMware、およびKVMホストに共通するローカルコンソールタスクの詳細については、「」を参照してください。 VM ローカルコンソールでのタスクの実行

Microsoft Hyper-V ホストNICsでの複数の のゲートウェイの設定

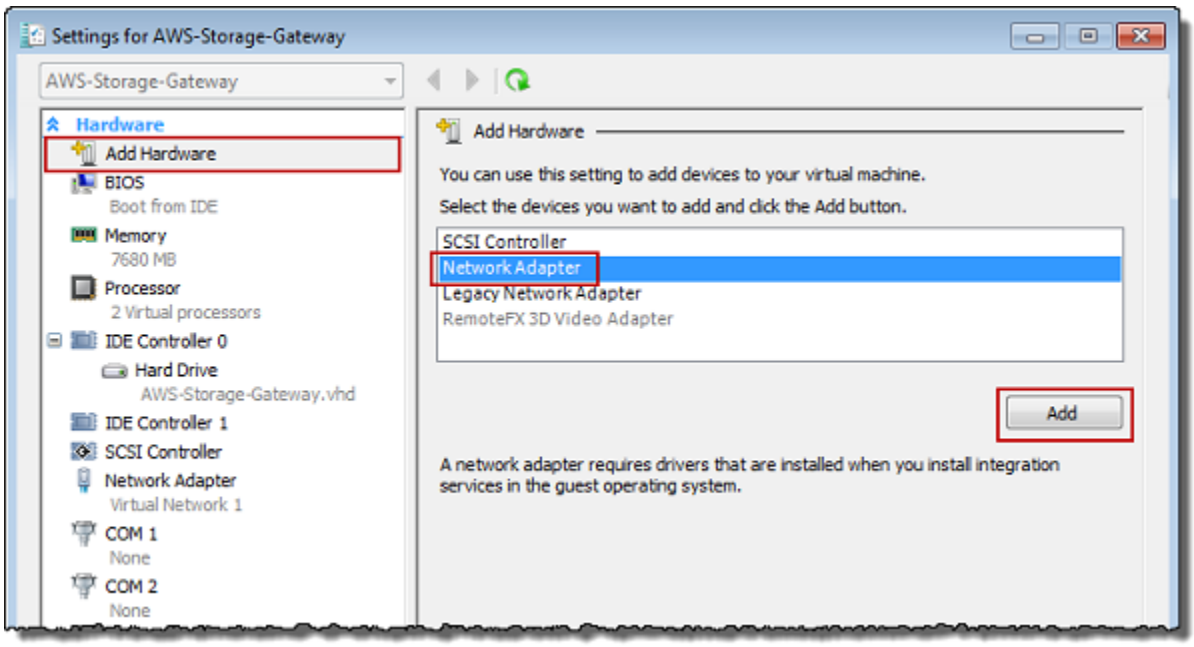
次の手順では、ゲートウェイ VM で 1 つのネットワークアダプタが定義済みで、2 番目のアダプタを設定しようとしています。この手順では、Microsoft Hyper-V ホスト用のアダプタを追加する方法を示します。

Microsoft Hyper-V で追加のネットワークアダプタを使用するようにゲートウェイを設定するには

1. Storage Gateway コンソールでゲートウェイをオフにします。手順については、ボリュームゲートウェイを停止するには を参照してください。
2. Microsoft Hyper-V Manager でゲートウェイの VM を選択します。
3. VM がオフになっていない場合は、ゲートウェイのコンテキスト (右クリック) メニューを開き、[Turn Off] を選択します。
4. クライアントでゲートウェイ VM のコンテキストメニューを開き、[Settings] を選択します。

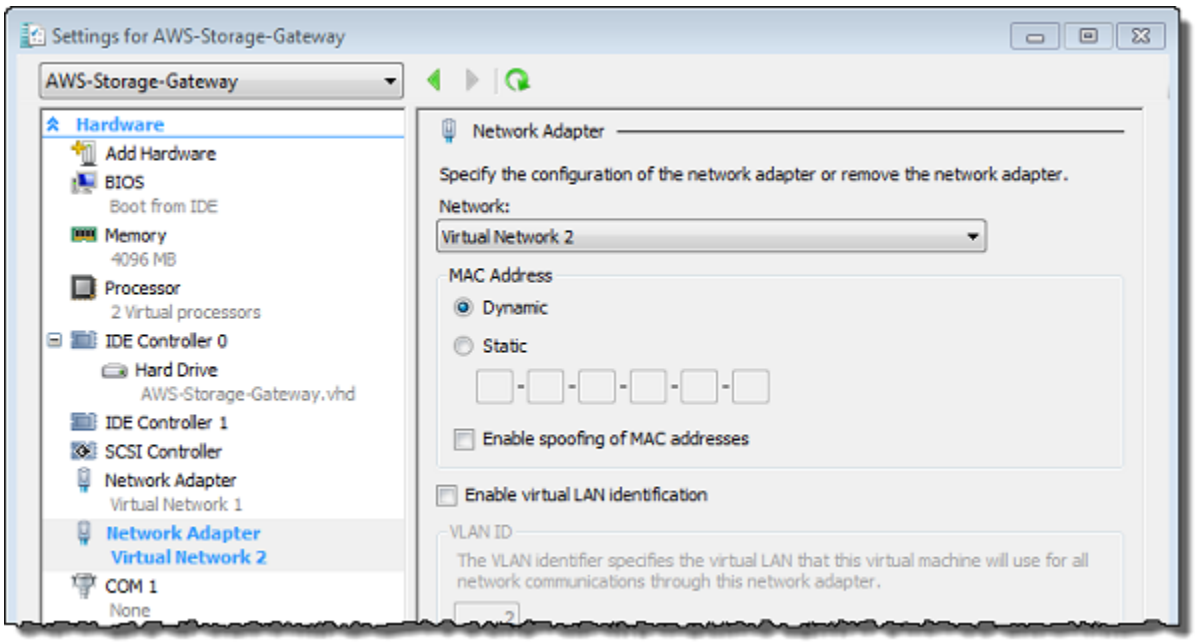


5. 仮想マシンの [Settings] (設定) ダイアログボックスで、[Hardware] (ハードウェア) に [Add Hardware] (ハードウェアを追加) を選択します。
6. [Add Hardware] ペインで [Network Adapter] を選択し、[Add] を選択してデバイスを追加します。



7. ネットワークアダプタを設定し、[Apply] を選択して設定を適用します。

   以下の例では、新しいアダプタとして [Virtual Network 2] が選択されています。



8. [Settings] ダイアログボックスの [Hardware] で 2 つ目のアダプタが追加されたことを確認し、[OK] を選択します。
9. Storage Gateway コンソールでゲートウェイをオンにします。手順については、ボリュームゲートウェイを起動するには を参照してください。
10. [ナビゲーション] ペインで、[ゲートウェイ] を選択し、アダプタを追加したゲートウェイを選択します。2 番目の IP アドレスが [詳細] タブに表示されることを確認します。

> **Note**
>
> Storage Gateway コンソールでファイル共有の情報ページに表示されるマウントコマンドの例には、そのファイル共有に関連付けられたゲートウェイに最後に追加されたネットワークアダプタの IP アドレスが常に含まれます。

、Hyper-VVMware、およびKVMホストに共通するローカルコンソールタスクの詳細については、「」を参照してください。 VM ローカルコンソールでのタスクの実行

ゲートウェイの削除と関連リソースの削除

ゲートウェイを引き続き使用する予定がない場合は、ゲートウェイとそれに関連付けられているリソースを削除することを検討してください。リソースを除去することで、引き続き使用する予定がないリソースに対する課金を回避し、月額利用料金を削減できます。

ゲートウェイを削除すると、そのゲートウェイは AWS Storage Gateway マネジメントコンソールに表示されなくなり、イニシエータへの iSCSI 接続は閉じられます。ゲートウェイを削除する手順は、すべてのゲートウェイタイプで同じです。ただし、関連付けられているリソースを除去するには、削除するゲートウェイのタイプとそれがデプロイされているホストに応じた手順に従います。

ゲートウェイは、Storage Gateway コンソールを使用して、またはプログラムによって削除できます。以下では、Storage Gateway コンソールを使用してゲートウェイを削除する方法について説明します。ゲートウェイをプログラムで削除する場合は、AWS Storage Gateway API「リファレンス」を参照してください。

トピック

Storage Gateway コンソールを使用したゲートウェイの削除

ゲートウェイを削除する手順は、すべてのゲートウェイタイプで同じです。ただし、削除するゲートウェイのタイプとゲートウェイがデプロイされているホストによっては、ゲートウェイに関連付けられているリソースを除去するために追加のタスクを実行する必要がある場合があります。これらのリソースを除去することで、使用する予定のないリソースに対する課金を回避できます。

> **Note**
>
> Amazon EC2インスタンスにデプロイされたゲートウェイの場合、インスタンスは削除するまで存在し続けます。
> 仮想マシン (VM) にデプロイされているゲートウェイの場合、ゲートウェイを削除すると、ゲートウェイ VM は仮想化環境で存在します。VM を削除するには、VMware vSphere クライアント、Microsoft Hyper-V Manager、または Linux カーネルベースの仮想マシン (KVM) クライアントを使用してホストに接続し、VM を削除します。削除したゲートウェイの VM を再利用して新しいゲートウェイをアクティベートすることはできません。

ゲートウェイを削除するには

1. ホーム で Storage Gateway https://console.aws.amazon.com/storagegateway/コンソールを開きます。

2. [ゲートウェイ] を選択し、削除対象のゲートウェイを 1 つ以上選択します。
3. [Actions (アクション)] の [Delete gateway (ゲートウェイを削除)] を選択します。確認のダイアログボックスが表示されます。

> **Warning**
>
> このステップを行う前に、ゲートウェイのボリュームに現在書き込んでいるアプリケーションがないことを確認してください。使用中のゲートウェイを削除すると、データが失われる場合があります。ゲートウェイを削除すると、復元できなくなります。

4. 指定したゲートウェイを削除することを確認し、確認ボックスに「delete」と入力して [削除] を選択します。
5. (オプション) 削除されたゲートウェイに関するフィードバックを提供する場合は、フィードバックダイアログボックスに入力してから [送信] をクリックします。それ以外の場合は、[スキップ] を選択します。

> **Important**
>
> ゲートウェイを削除した後はソフトウェア料金はかかりませんが、仮想テープ、Amazon Elastic Block Store (Amazon EBS) スナップショット、Amazon EC2インスタンスなどのリソースは保持されます。これらのリソースに対する課金は継続されます。Amazon EC2サブスクリプションをキャンセルすることで、Amazon EC2インスタンスと Amazon EBSスナップショットを削除できます。Amazon EC2サブスクリプションを維持する場合は、Amazon EC2コンソールを使用して Amazon EBSスナップショットを削除できます。

オンプレミスでデプロイされているゲートウェイからのリソースの除去

このセクションでは、オンプレミスでデプロイされているゲートウェイからリソースを除去する手順について説明します。

VM にデプロイされているボリュームゲートウェイからのリソースの除去

削除するゲートウェイが仮想マシン (VM) にデプロイされている場合は、以下のアクションを実行してリソースをクリーンアップすることをお勧めします。

- ゲートウェイを削除します。手順については、Storage Gateway コンソールを使用したゲートウェイの削除 を参照してください。

- 不要な Amazon EBSスナップショットをすべて削除します。手順については、「Amazon ユーザーガイド」の「Amazon EBS スナップショットの削除」を参照してください。 EC2

Amazon EC2 インスタンスにデプロイされたゲートウェイからのリソースの削除

Amazon EC2インスタンスにデプロイしたゲートウェイを削除する場合は、ゲートウェイで使用された AWS リソース、特に Amazon EC2インスタンス、Amazon EBSボリューム、テープゲートウェイをデプロイした場合はテープをクリーンアップすることをお勧めします。クリーンアップによって、意図しない使用に対する課金を回避できるためです。

Amazon にデプロイされたキャッシュ型ボリュームからのリソースの削除 EC2

キャッシュ型ボリュームを持つゲートウェイを にデプロイした場合はEC2、以下のアクションを実行してゲートウェイを削除し、そのリソースをクリーンアップすることをお勧めします。

1. 「Storage Gateway コンソールを使用したゲートウェイの削除」で示されているように、Storage Gateway コンソールでゲートウェイを削除します。
2. Amazon EC2コンソールで、EC2インスタンスを再度使用する予定がある場合は、インスタンスを停止します。使用しない場合は、そのインスタンスを終了します。ボリュームを削除する予定である場合は、インスタンスを削除する前に、インスタンスにアタッチされているブロックデバイスとその ID を書き留めます。これらは、削除するボリュームを識別するために必要です。
3. Amazon EC2コンソールで、インスタンスにアタッチされているすべての Amazon EBSボリュームを再度使用する予定がない場合は、それらを削除します。詳細については、「Amazon ユーザーガイド」の「インスタンスとボリュームのクリーンアップ」を参照してください。 EC2

Volume Gateway のパフォーマンスと最適化

このセクションでは、Storage Gateway のパフォーマンスについて説明します。

トピック

ゲートウェイのパフォーマンスの最適化

ゲートウェイサーバーの推奨構成

ゲートウェイのパフォーマンスを最大限に引き出せるように、Storage Gateway では、ゲートウェイのホストサーバーに対して以下のゲートウェイ構成を推奨しています。

- 少なくとも 24 個の専用物理CPUコア
- ボリュームゲートウェイ の場合、ハードウェアは次の量の 専用である必要がありますRAM。
  - 最大キャッシュサイズが 16 GiBのゲートウェイRAM用に 16 GiB 以上予約されている TiB
  - キャッシュサイズが 16 TiB ~ 32 TiB のゲートウェイ用に 32 GiB TiB 以上予約されている RAM TiB
  - キャッシュサイズが 32 TiB ~ 64 TiB のゲートウェイ用に 48 GiB TiB 以上予約されている RAM TiB
- ディスク 1。ゲートウェイキャッシュとして次のように使用します。
  - SSD NVMeコントローラーを使用する。
- ディスク 2。ゲートウェイアップロードバッファとして次のように使用します。
  - SSD NVMeコントローラーを使用する。
- ディスク 3。ゲートウェイアップロードバッファとして次のように使用します。
  - SSD NVMeコントローラーを使用する。
- VM ネットワーク 1 に設定されたネットワークアダプタ 1:
  - VM ネットワーク 1 を使用し、取り込みに使用する VMXnet3 (10 Gbps) を追加します。
- VM ネットワーク 2 に設定されたネットワークアダプタ 2:
  - VM ネットワーク 2 を使用して、 への接続に使用する VMXnet3 (10 Gbps) を追加します AWS。

ゲートウェイへのリソースの追加

次のボトルネックにより、ボリュームゲートウェイのパフォーマンスが理論上の最大持続スループット (AWS クラウドへの帯域幅) を下回る可能性があります。

- CPU コア数
- キャッシュ/アップロードバッファのディスクスループット
- 合計RAM金額
- へのネットワーク帯域幅 AWS
- イニシエータからゲートウェイまでのネットワーク帯域幅

このセクションでは、ゲートウェイのパフォーマンスを最適化するための対策について説明します。以下のガイダンスは、ゲートウェイまたはアプリケーションサーバーへのリソースの追加を前提としています。

以下の 1 つ以上の方法でゲートウェイにリソースを追加することで、ゲートウェイのパフォーマンスを最適化できます。

より高性能なディスクの使用

キャッシュとアップロードバッファのディスクスループットによって、ゲートウェイのアップロードとダウンロードのパフォーマンスが制限される可能性があります。ゲートウェイのパフォーマンスが予想を大幅に下回っている場合は、キャッシュとアップロードバッファのディスクスループットを次の方法で改善することを検討してください。

- 10 RAID RAIDなどのストライプを使用して、理想的にはハードウェアRAIDコントローラーでディスクスループットを向上させます。

  > **Note**
  >
  > RAID (独立ディスクの冗長配列) 、特に 10 RAID などのディスクストライプRAID設定は、データの本文をブロックに分割し、データブロックを複数のストレージデバイスに分散するプロセスです。使用するRAIDレベルは、達成できる正確な速度と耐障害性に影響します。IO ワークロードを複数のディスクにストライピングすることで、RAIDデバイスの全体的なスループットは、単一のメンバーディスクのスループットよりもはるかに高くなります。

- 高性能ディスクを直接接続して使用する。

ゲートウェイのパフォーマンスを最適化するには、ソリッドステートドライブ (SSDs) や NVMeコントローラーなどの高性能ディスクを追加できます。Microsoft Hyper-V の代わりに、ストレージエリアネットワーク (SAN) から直接 VM に仮想ディスクをアタッチすることもできますNTFS。ディスクのパフォーマンスが向上すると、通常、スループットが向上し、1 秒あたりの入出力オペレーションが増えます (IOPS) 。

スループットを測定するには、SamplesAmazon CloudWatch 統計で ReadBytesおよび WriteBytesメトリクスを使用します。例えば、5 分間のサンプル期間における Samples ReadBytesメトリクスの統計を 300 秒で割ると、 が得られますIOPS。原則として、ゲートウェイのこれらのメトリクスを確認するときは、低スループットと低IOPSトレンドを探して、ディスク関連のボトルネックを示します。

> **Note**
>
> CloudWatch メトリクスは、すべてのゲートウェイで使用できるわけではありません。ゲートウェイメトリクスについては、「Storage Gateway のモニタリング」を参照してください。

アップロードバッファディスクをさらに追加する

書き込みスループットを高めるには、少なくとも 2 つのアップロードバッファディスクを追加します。データがゲートウェイに書き込まれると、アップロードバッファディスクにローカルに書き込まれて保存されます。その後、保存されたローカルデータはディスクから非同期的に読み取られ、処理と AWSへのアップロードが行われます。アップロードバッファディスクをさらに追加すると、個別のディスクに対して実行される同時 I/O 操作の量が減る可能性があります。これにより、ゲートウェイへの書き込みスループットが増える可能性があります。

別の物理ディスクを使用したゲートウェイ仮想ディスクのバックアップ

ゲートウェイのディスクをプロビジョニングする場合は、同じ物理ストレージディスクを基盤として使用しているアップロードバッファおよびキャッシュストレージ用にローカルディスクをプロビジョニングしないことを強くお勧めします。例えば、 の場合VMwareESXi、基盤となる物理ストレージリソースはデータストアとして表されます。ゲートウェイ VM をデプロイする場合は、VM ファイルを保存するデータストアを選択します。仮想ディスクをプロビジョニングする場合は (アップロードバッファとして使用する場合など)、仮想ディスクを VM と同じデータストアか、別のデータストアに保存できます。

複数のデータストアがある場合は、作成するローカルストレージのタイプごとに 1 つのデータストアを選択することを強くお勧めします。基になる物理ディスク 1 つのみによってサポートさ

れるデータストアでは、パフォーマンスが低下することがあります。たとえば、そのようなディスクを使用して、ゲートウェイ設定のキャッシュストレージとアップロードバッファの両方がサポートされる場合です。同様に、1 や RAID6 RAID などのパフォーマンスの低いRAID設定にバックアップされたデータストアでは、パフォーマンスが低下する可能性があります。

ゲートウェイホストにCPUリソースを追加する

ゲートウェイホストサーバーの最小要件は、4 つの仮想プロセッサです。ゲートウェイのパフォーマンスを最適化するには、ゲートウェイ VM に割り当てられた各仮想プロセッサが専用CPUコアによってバックアップされていることを確認します。さらに、ホストサーバーの CPUs を過剰にサブスクライブしていないことを確認します。

ゲートウェイホストサーバーCPUsに を追加すると、ゲートウェイの処理能力が向上します。これにより、ゲートウェイは、アプリケーションからローカルストレージへのデータの保存と Amazon S3 へのこのデータのアップロードの両方を並行して処理できます。また、ホストが他のと共有されているときに、ゲートウェイが十分なCPUリソースを確実に取得できるようにCPUsも役立ちますVMs。十分なCPUリソースを提供することは、スループットを向上させる一般的な効果があります。

ゲートウェイと AWS クラウドの間の帯域幅を広げる

帯域幅を との間で増やす AWS と、ゲートウェイへのデータ入力と AWS クラウドへのデータ入力の最大レートが増加します。低速のディスクや、ゲートウェイとイニシエータ間の接続帯域幅不足といった他の要因ではなく、ネットワーク速度がゲートウェイ構成における制限要因となっている場合は、これでゲートウェイのパフォーマンスを向上させることができます。

> **Note**
>
> キャッシュ/アップロードバッファのディスクスループット、CPUコア数、合計RAM量、イニシエータとゲートウェイ間の帯域幅など、ここにリストされているその他の制限要因により、ゲートウェイのパフォーマンスがネットワーク帯域幅よりも低くなる可能性があります。また、ゲートウェイの通常運用に際しては、データ保護のために多くの対策が実施されるため、ネットワーク帯域幅よりもパフォーマンスの実測値が低くなる場合があります。

ボリュームの設定を変更する

ボリュームゲートウェイを使用している場合に、ゲートウェイにストレージボリュームを追加するとゲートウェイへのスループットが低下する場合は、別のゲートウェイにボリュームを追加す

ることを検討してください。特に、ボリュームが高スループットのアプリケーションに使用されている場合は、高スループットのアプリケーション用に別のゲートウェイを作成することを検討してください。ただし、一般的なルールとして、すべての高スループットのアプリケーションに一方のゲートウェイを使用し、すべての低スループットのアプリケーションにもう一方のゲートウェイを使用するといった方法は避けてください。ボリュームのスループットを測定するには、`ReadBytes` および `WriteBytes` メトリクスを使用します。

これらのメトリクスの詳細については、「アプリケーションとゲートウェイの間のパフォーマンスの測定」を参照してください。

iSCSI 設定の最適化

iSCSI イニシエータの iSCSI 設定を最適化して、I/O パフォーマンスを向上させることができます。`MaxReceiveDataSegmentLength` と `FirstBurstLength` には 256 KiB、`MaxBurstLength` には 1 MiB を選択することをお勧めします。iSCSI 設定の設定の詳細については、「」を参照してくださいiSCSI 設定のカスタマイズ。

> **Note**
>
> これらの推奨設定により、全体的なパフォーマンスが向上します。ただし、パフォーマンスを最適化するために必要な特定の iSCSI 設定は、使用するバックアップソフトウェアによって異なります。詳細については、バックアップソフトウェアのドキュメントを参照してください。

アプリケーション環境へのリソースの追加

アプリケーションサーバーとゲートウェイの間の帯域幅を増やす

iSCSI イニシエータとゲートウェイ間の接続により、アップロードとダウンロードのパフォーマンスが制限される場合があります。ゲートウェイのパフォーマンスが予想よりも大幅に悪く、CPUコア数とディスクスループットが既に向上している場合は、次の点を考慮してください。

- ネットワークケーブルをアップグレードして、イニシエータとゲートウェイ間の帯域幅を広げる。

ゲートウェイのパフォーマンスを最適化するには、アプリケーションとゲートウェイ間のネットワーク帯域幅が、アプリケーションのニーズを満たすようにしてください。ゲートウェイの

`ReadBytes` メトリクスと `WriteBytes` メトリクスを使用して、データの合計スループットを測定できます。

アプリケーションでは、必要なスループットと測定されたスループットを比較します。測定されたスループットが必要なスループットを下回る場合、アプリケーションとゲートウェイの間の帯域幅を増やすと、ネットワークがボトルネックであれば、パフォーマンスを向上させることができます。同様に、VM とローカルディスクの間の帯域幅を増やすことができます (直接接続されていない場合)。

アプリケーション環境にCPUリソースを追加する

アプリケーションで追加のCPUリソースを使用できる場合、さらに追加CPUsすると、アプリケーションが I/O 負荷をスケーリングするのに役立ちます。

Storage Gateway でのVMware vSphere 高可用性の使用

Storage Gateway は、高可用性 (VMware HA) と統合された一連のアプリケーションレベルのヘルスチェックVMwareを通じて、 VMware vSphere で高可用性を提供します。このアプローチは、ハードウェア、ハイパーバイザー、またはネットワーク障害からストレージのワークロードを保護するのに役立ちます。また、接続タイムアウトや、ファイル共有またはボリュームを使用できないなどのソフトウェアエラーからの保護にも役立ちます。

vSphere HA は、仮想マシンとそれらが存在するホストをクラスターにプールすることで冗長性を実現します。クラスター内のホストがモニタリングされ、障害が発生した場合、障害が発生したホスト上の仮想マシンは代替ホストで再起動されます。通常、この復旧はデータ損失なしで迅速に行われます。 vSphere HA の詳細については、 VMwareドキュメントの vSphere 「HA の仕組み」を参照してください。

> **Note**
>
> 障害が発生した仮想マシンを再起動し、新しいホストで iSCSI 接続を再確立するために必要な時間は、ホストオペレーティングシステムとリソースの負荷、ディスク速度、ネットワーク接続、SAN/ストレージインフラストラクチャなど、多くの要因によって異なります。フェイルオーバーのダウンタイムを最小限に抑えるには、「ゲートウェイパフォーマンスの最適化ゲートウェイ」で概説されている推奨事項を実装します。

Storage Gateway で VMware HA を使用するには、次の手順を実行します。 Storage Gateway

トピック

HA クラスターを設定する vSphere VMware

まず、VMwareクラスターをまだ作成していない場合は、クラスターを作成します。VMware クラスターの作成方法については、 ドキュメントの vSphere 「HA クラスターの作成」を参照してください。 VMware

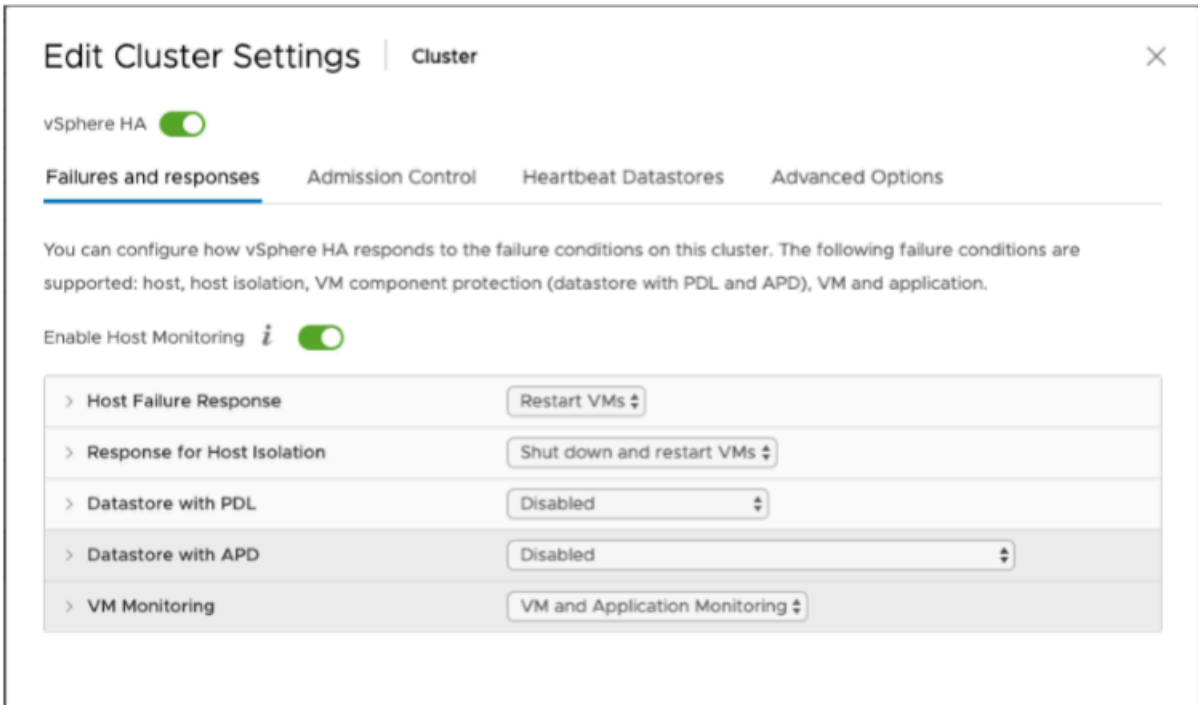
次に、Storage Gateway で動作するようにVMwareクラスターを設定します。

VMware クラスターを設定するには

1. の「クラスター設定の編集」ページでvSphere、VM モニタリングが VM VMware およびアプリケーションモニタリング用に設定されていることを確認します。これを行うには、以下の順序でオプションを設定します。

   - ホスト障害レスポンス： 再起動 VMs
   - ホスト分離のレスポンス： シャットダウンと再起動 VMs
   - を持つデータストアPDL: 無効
   - を持つデータストアAPD: 無効
   - [VM Monitoring]: [VM and Application Monitoring]

   例については、以下のスクリーンショットを参照してください。



2. 次の値を調整して、クラスターの感度を微調整します。

   - [Failure interval] – この期間の後、VM ハートビートが受信されない場合、VM は再起動されます。
   - [Minimum uptime] – クラスターは、VM が VM ツールのハートビートのモニタリングを開始した後でこの時間待機します。
   - [Maximum per-VM resets] – クラスターは、最大リセット時間枠内で最大この回数 VM を再起動します。
   - [Maximum resets time window] – VM ごとの最大リセット回数をカウントする時間枠。

   設定する値がわからない場合は、次の設定例を使用します。

   - [Failure interval]: **30** 秒
   - [Minimum uptime]: **120** 秒
   - [Maximum per-VM resets]: **3**
   - [Maximum resets time window]: **1** 時間

クラスターで他の VMsを実行している場合は、VM にこれらの値を特に設定することをお勧めします。これは、.ova から VM をデプロイするまで実行できません。これらの値の設定の詳細について

は、「(オプション) クラスターVMsに他の のオーバーライドオプションを追加する」を参照してください。

Storage Gateway コンソールから .ova イメージをダウンロードする

ゲートウェイタイプの .ova イメージをダウンロードするには

- Storage Gateway コンソールの [ゲートウェイのセットアップ] ページで、ゲートウェイタイプとホストプラットフォームを選択し、コンソールに表示されるリンクを使用して .ova をダウンロードします。詳細については、「ボリュームゲートウェイをセットアップする」を参照してください。

ゲートウェイのデプロイ

設定したクラスターで、.ova イメージをクラスターのホストの 1 つにデプロイします。

ゲートウェイの .ova イメージをデプロイするには

1. .ova イメージをクラスター内のホストの 1 つにデプロイします。
2. ルートディスクとキャッシュ用に選択したデータストアが、クラスター内のすべてのホストで使用可能であることを確認します。Storage Gateway の .ova ファイルを VMwareまたはオンプレミス環境にデプロイする場合、ディスクは準仮想化SCSIディスクとして記述されます。準仮想化は、ゲートウェイ VM がホストオペレーティングシステムと共同して、VM に追加される仮想ディスクをコンソールが識別できるようにするモードです。

   準仮想化コントローラーを使用するように VM を構成するには

   1. VMware vSphere クライアントで、ゲートウェイ VM のコンテキスト (右クリック) メニューを開き、設定の編集 を選択します。
   2. 仮想マシンのプロパティダイアログボックスで、ハードウェアタブを選択し、SCSIコントローラー 0 を選択し、タイプ の変更 を選択します。
   3. SCSI「コントローラータイプの変更」ダイアログボックスでVMware、「準仮想化コントローラータイプ」を選択し、SCSI「OK」を選択します。

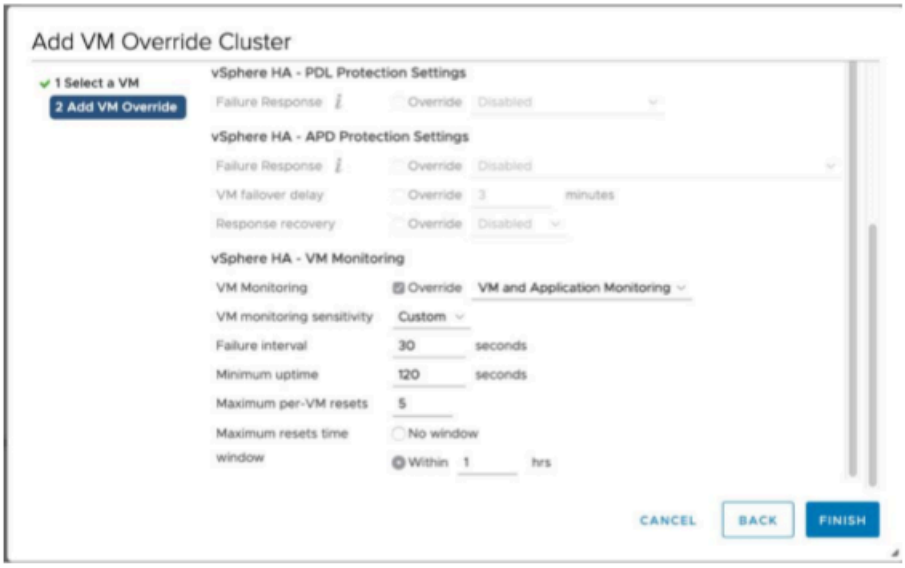
(オプション) クラスターVMsに他の のオーバーライドオプションを追加する

クラスターで他の VMsを実行している場合は、VM ごとにクラスター値を設定することをお勧めします。

クラスターVMsで他の のオーバーライドオプションを追加するには

1. の 概要ページでVMwarevSphere、クラスターを選択してクラスターページを開き、 の設定を選択します。
2. [Configuration] タブを選択し、[VM Overrides] を選択します。
3. 新しい VM オーバーライドオプションを追加して、各値を変更します。

   オーバーライドオプションについては、次のスクリーンショットを参照してください。



ゲートウェイのアクティブ化

ゲートウェイの .ova がデプロイされたら、ゲートウェイをアクティブ化します。ゲートウェイの種類ごとの違いについて説明します。

ゲートウェイをアクティブ化するには

- 以下のトピックで概説されている手順に従ってください。

  a. ボリュームゲートウェイを に接続する AWS

b. 設定を確認してボリュームゲートウェイをアクティブ化する
c. ボリュームゲートウェイを設定する

VMware 高可用性設定をテストする

ゲートウェイをアクティブ化したら、設定をテストします。

VMware HA 設定をテストするには

1. ホーム で Storage Gateway https://console.aws.amazon.com/storagegateway/コンソールを開きます。
2. ナビゲーションペインで、ゲートウェイ を選択し、HA をテストするゲートウェイを選択します。 VMware
3. アクション で、VMwareHA の検証 を選択します。
4. 表示されるVMware高可用性設定の検証ボックスで、OK を選択します。

   > **Note**
   >
   > VMware HA 設定をテストすると、ゲートウェイ VM が再起動され、ゲートウェイへの接続が中断されます。テストの完了には数分かかることがあります。

   テストが成功すると、コンソールのゲートウェイの詳細タブに [Verified (検証済み)] というステータスが表示されます。
5. [終了] を選択します。

VMware HA イベントに関する情報は、Amazon CloudWatch ロググループにあります。詳細については、」を参照してください CloudWatch 。

セキュリティイン AWS Storage Gateway

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、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メリットを得られます。

セキュリティは、 AWS とユーザーの間で共有される責任です。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、Amazon Web Services クラウドで AWS 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担います。 AWS また、 は、安全に使用できるサービスも提供します。コンプライアンスAWS プログラム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者は定期的にセキュリティの有効性をテストおよび検証。 AWS Storage Gateway に適用され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AWS による対象範囲内のサービスコンプライアンスプログラム」を参照してください。
- クラウドのセキュリティ — お客様の責任は、使用する AWS サービスによって決まります。また、お客様は、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、Storage Gateway を使用する際の責任共有モデルの適用方法を理解するのに役立ちます。次のトピックでは、セキュリティおよびコンプライアンスの目的を満たすように Storage Gateway を設定する方法について説明します。また、Storage Gateway リソースのモニタリングや保護に役立つ他の AWS のサービスの使用方法についても説明します。

トピック

AWS Storage Gatewayでのデータ保護

責任 AWS 共有モデル、 AWS Storage Gateway 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 はすべての 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があります AWS クラウド。お客様は、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。また、使用する AWS のサービス のセキュリティ設定と管理タスクもユーザーの責任となります。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FAQ」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」のAWS 「責任共有モデル」とGDPRブログ記事を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント 、 AWS IAM Identity Center または AWS Identity and Access Management () を使用して個々のユーザーを設定することをお勧めしますIAM。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権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。1TLS.2 が必要で、1.3 TLS をお勧めします。
- を使用して APIとユーザーアクティビティの口グ記録を設定します AWS CloudTrail。
- AWS 暗号化ソリューションと、 内のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密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 AWS を介して にアクセスするときに FIPS 140-3 検証済みの暗号化モジュールが必要な場合はAPI、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) 140-3」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報は、タグ、または名前フィールドなどの自由形式のテキストフィールドに配置しないことを強くお勧めします。これは、コンソール、、またはを使用して Storage Gateway または他の AWS のサービス を操作する場合API AWS CLIも同様です AWS SDKs。名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断口グに使用される場合があります。URL を外部サーバーに提供する場合は、そのサーバーへのリクエストを検証URLするために認証情報を に含めないことを強くお勧めします。

を使用したデータ暗号化 AWS KMS

Storage Gateway は、SSL/TLS (セキュアソケットレイヤー/トランスポートレイヤーセキュリティ) を使用して、ゲートウェイアプライアンスと AWS ストレージ間で転送されるデータを暗号化し

ます。デフォルトでは、Storage Gateway は Amazon S3-Managed暗号化キー (SSE-S3) を使用して、Amazon S3 に保存するすべてのデータをサーバー側で暗号化します。Storage Gateway を使用してAPI、 AWS Key Management Service （ SSE-KMS) キーによるサーバー側の暗号化を使用してクラウドに保存されているデータを暗号化するようにゲートウェイを設定できます。

> **Important**
>
> サーバー側の暗号化に AWS KMS キーを使用する場合は、対称キーを選択する必要があります。Storage Gateway では、非対称キーはサポートされていません。詳細については、AWS Key Management Service デベロッパーガイドの対称キーと非対称キーの使用を参照してください。

ファイル共有の暗号化

ファイル共有の場合、 SSE- を使用して AWS KMSマネージドキーでオブジェクトを暗号化するようにゲートウェイを設定できますKMS。Storage Gateway を使用してファイル共有に書き込まれたデータを暗号化APIする方法については、「 AWS Storage Gateway APIリファレンス」の「CreateNFSFile共有」を参照してください。

ボリュームの暗号化

キャッシュ型ボリュームと保存型ボリュームの場合、Storage Gateway を使用して AWS KMSマネージドキーを使用してクラウドに保存されているボリュームデータを暗号化するようにゲートウェイを設定できますAPI。 Storage Gateway マネージドキーの 1 つをKMSキーとして指定できます。ボリュームの暗号化に使用するキーは、ボリュームの作成後に変更することはできません。Storage Gateway を使用してキャッシュ型ボリュームまたは保存型ボリュームに書き込まれたデータを暗号化APIする方法については、「 AWS Storage Gateway APIリファレンスCreateStorediSCSIVolume」のCreateCachediSCSIVolume「」または「」を参照してください。

テープの暗号化

仮想テープの場合、Storage Gateway を使用して、クラウドに保存されているテープデータを AWS KMSマネージドキーで暗号化するようにゲートウェイを設定できますAPI。 Storage Gateway マネージドキーの 1 つをKMSキーとして指定できます。テープデータの暗号化に使用するキーは、テープの作成後に変更することはできません。Storage Gateway を使用して仮想テープに書き込まれたデータを暗号化APIする方法については、「 AWS Storage Gateway APIリファレンスCreateTapes」の「」を参照してください。

AWS KMS を使用してデータを暗号化する場合は、次の点に注意してください。

- データはクラウドでの保管時に暗号化されます。つまり、Amazon S3 内でデータが暗号化されます。
- IAM ユーザーは、 オペレーションを呼び出す AWS KMS APIために必要なアクセス許可を持っている必要があります。詳細については、「 AWS Key Management Service デベロッパーガイド」の「 でのIAMポリシーの使用 AWS KMS」を参照してください。
- AWS AWS KMS キーを削除または非アクティブ化するか、グラントトークンを取り消すと、ボリュームまたはテープ上のデータにアクセスできなくなります。詳細については、「 AWS Key Management Service デベロッパーガイド」のKMS「キーの削除」を参照してください。
- KMS暗号化されたボリュームからスナップショットを作成すると、スナップショットは暗号化されます。スナップショットはボリュームのKMSキーを継承します。
- KMS暗号化されたスナップショットから新しいボリュームを作成すると、そのボリュームは暗号化されます。新しいボリュームには別のKMSキーを指定できます。

> **Note**
>
> Storage Gateway は、 で暗号化されたボリュームまたは でKMS暗号化されたKMSスナップショットの復旧ポイントからの暗号化されていないボリュームの作成をサポートしていません。

の詳細については AWS KMS、「 とは」を参照してください AWS Key Management Service。

ボリューム用の CHAP 認証の設定

Storage Gateway では、iSCSI イニシエータが iSCSI ターゲットとしてボリュームに接続されます。Storage Gateway では、チャレンジハンドシェイク認証プロトコル (CHAP) を使用して iSCSI とイニシエータの接続が認証されます。CHAP は、ストレージボリュームターゲットへのアクセスが試みられる際に認証を要求することによって、プレイバック攻撃に対する保護を提供します。ボリュームターゲットごとに、1 つまたは複数の CHAP 認証情報を定義できます。さまざまなイニシエーター用のこれらの認証情報は、[Configure CHAP credentials] ダイアログボックスで表示、編集できます。

CHAP 認証情報を設定するには

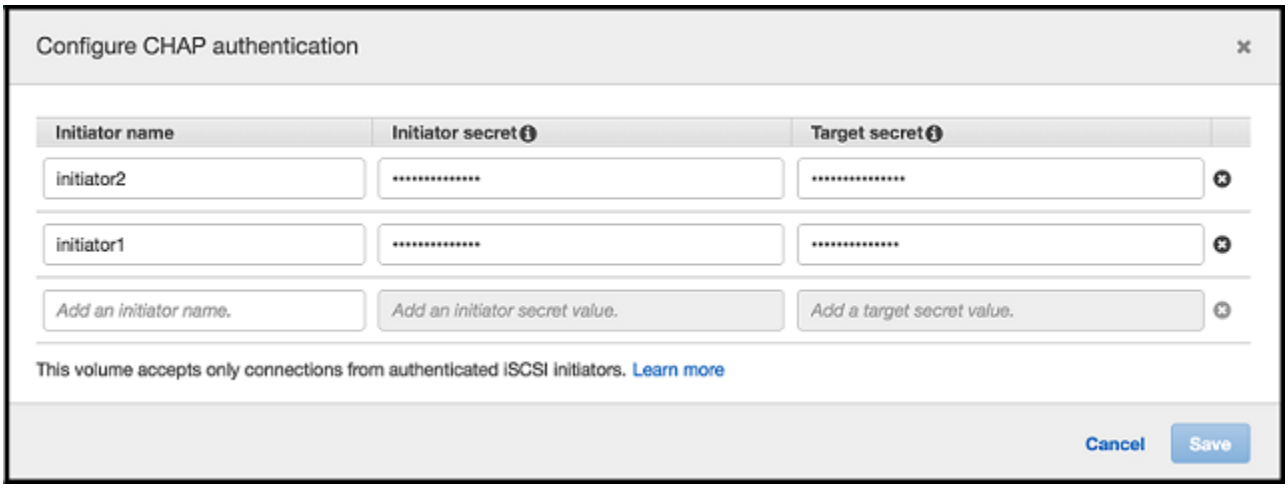
1. Storage Gateway コンソールで [Volumes] (ボリューム) を選択し、CHAP 認証情報を設定するボリュームを選択します。
2. [アクション] メニューで、[CHAP 認証の設定] を選択します。

3. [イニシエータ名] にイニシエータの名前を入力します。この名前は 1 文字以上、255 文字以内にしてください。
4. [イニシエータのシークレット] に、iSCSI イニシエータを認証するために使用する秘密のフレーズを入力します。イニシエータの秘密のフレーズは、12～16 文字である必要があります。
5. [Target secret] で、相互 CHAP のターゲットを認証するために使用する秘密のフレーズを入力します。ターゲットの秘密のフレーズは、12～16 文字である必要があります。
6. [Save] を選択してエントリを保存します。

CHAP 認証情報を表示または更新するには、そのオペレーションを実行するために必要な IAM ロールのアクセス許可を割り当てられている必要があります。

CHAP 認証情報の表示および編集

各ユーザーの CHAP 認証情報を追加、削除、または更新できます。CHAP 認証情報を表示または編集するために必要な IAM ロールのアクセス許可を割り当てられている必要があります。また、イニシエーターゲットが、機能しているゲートウェイにアタッチされていることも必要です。



CHAP 認証情報を追加するには

1. Storage Gateway コンソールで [Volumes] (ボリューム) を選択し、CHAP 認証情報を追加するボリュームを選択します。
2. [アクション] メニューで、[CHAP 認証の設定] を選択します。
3. [Configure CHAPS] ページで、各ボックスに [イニシエータ名]、[イニシエータのシークレット]、および [ターゲットのシークレット] を指定し、[保存] を選択します。

CHAP 認証情報を削除するには

1. Storage Gateway コンソールで [Volumes] (ボリューム) を選択し、CHAP 認証情報を削除するボリュームを選択します。
2. [アクション] メニューで、[CHAP 認証の設定] を選択します。
3. 削除する認証情報の横にある [X] をクリックし、[保存] を選択します。

CHAP 認証情報を更新するには

1. Storage Gateway コンソールで [Volumes] (ボリューム) を選択し、CHAP を更新するボリュームを選択します。
2. [アクション] メニューで、[CHAP 認証の設定] を選択します。
3. [Configure CHAP credentials] ページで、更新する認証情報のエントリを変更します。
4. [保存] を選択します。

Identity and Access Management for AWS Storage Gateway

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制御 AWS のサービス するのに役立つ です。IAM 管理者は、誰を認証 (サインイン) し、誰に リソースの使用 AWS SGWを承認する (アクセス許可を付与する) かを制御します。IAM は AWS のサービス 追加料金なしで使用できる です。

トピック

対象者

AWS Identity and Access Management （ IAM) の使用方法は、 で行う作業によって異なります AWS SGW。

サービスユーザー – サービスを使用して AWS SGWジョブを実行する場合、管理者から必要な認証情報とアクセス許可が与えられます。さらに多くの AWS SGW機能を使用して作業を行う場合は、追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解しておくと、管理者に適切な許可をリクエストするうえで役立ちます。の機能にアクセスできない場合は、 AWS SGW「」を参照してくださいAWS Storage Gateway のアイデンティティとアクセスのトラブルシューティング。

サービス管理者 – 社内のリソースを担当 AWS SGWしている場合は、通常、 へのフルアクセスがあります AWS SGW。サービスユーザーがどの AWS SGW機能やリソースにアクセスするかを決めるのは管理者の仕事です。次に、サービスユーザーのアクセス許可を変更するリクエストをIAM管理者に送信する必要があります。このページの情報を確認して、 の基本概念を理解してくださいIAM。会社で を と使用する方法の詳細については、IAM AWS SGW「」を参照してくださいAWS Storage Gateway と の連携方法 IAM。

IAM 管理者 - IAM管理者は、 へのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります AWS SGW。で使用できるアイデンティティベースのポリシーの例 AWS SGWを表示するにはIAM、「」を参照してくださいAWS Storage Gateway のアイデンティティベースのポリシーの例。

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。として、IAMユーザーとして AWS アカウントのルートユーザー、または IAMロールを引き受けることによって認証 （ にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM Identity Center （ IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook の認証情報は、フェデレーティッド ID の例です。フェデレーティッド ID としてサインインすると、管理者は以前に IAMロールを使用して ID フェデレーションをセットアップしていました。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、 AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「 ユーザーガイド」の「 へのサインイン AWS アカウント方法AWS サインイン 」を参照してください。

AWS プログラムで にアクセスする場合、 はソフトウェア開発キット (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、 認証情報を使用してリクエストに暗号で署名します。 AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。推奨される方法を使用してリクエストを自分で署名する方法の詳細については、「 IAMユーザーガイド」のAWS API「リクエストの署名」を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、 AWS では、アカウントのセキュリティを高めるために多要素認証 (MFA) を使用することをお勧めします。詳細については、「 AWS IAM Identity Center ユーザーガイド」の「多要素認証」および「 ユーザーガイド」の「 での多要素認証 (MFA) AWS IAM の使用」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての およびリソースへの AWS のサービス 完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「 IAMユーザーガイド」の「ルートユーザーの認証情報を必要とするタスク」を参照してください。

フェデレーティッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、一時的な認証情報を使用して にアクセスするための ID プロバイダーとのフェデレーションの使用を要求 AWS のサービス します。

フェデレーティッド ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、AWS Directory Service、アイデンティティセンターディレクトリのユーザー、または ID ソースを通じて提供された認証情報 AWS のサービス を使用して にアクセスするユーザーです。フェデレーティッド ID が にアクセスすると AWS アカウント、ロールを引き受け、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、 AWS IAM Identity Centerを使用することをお勧めします。Identity Center でユーザーとグループを作成することも、独自の IAM ID ソース内のユーザーとグループのセットに接続して同期して、すべての AWS アカウント とアプリケーションで使用することもできます。IAM Identity Center の詳細については、「 ユーザーガイド」のIAM「Identity Center とはAWS IAM Identity Center 」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を持つIAMユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAMユーザーとの長期的な認証情報を必要とする特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「 ユーザーガイド」の「長期的な認証情報を必要とするユースケースでアクセスキーを定期的にローテーションするIAM」を参照してください。

IAM グループは、IAMユーザーのコレクションを指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、 という名前のグループIAMAdminsを作成し、そのグループにIAMリソースを管理するアクセス許可を付与できます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、「 ユーザーガイド」のIAM「 (ロールではなく) ユーザーを作成する場合IAM」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。これは IAM ユーザーと似ていますが、特定のユーザーに関連付けられていません。IAM ロール を切り替える AWS Management Console ことで、 で ロールを一時的に引き受けることができます。ロールを引き受けるには、 または AWS API オペレーションを AWS CLI 呼び出すか、カスタム を使用します URL。ロールの使用方法の詳細については、「 ユーザーガイド」のIAM「ロールの使用IAM」を参照してください。

IAM 一時的な認証情報を持つ ロールは、以下の状況で役立ちます。

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロールの詳細については、「 ユーザーガイド」の「サードパーティー ID プロバイダーのロールの作成IAM」を参照してください。IAM Identity Center を使用する場合は、アクセス許可セットを設定します。ID が認証後にアクセスできる内容を制御するために、IAMIdentity Center はアクセス

許可セットを のロールに関連付けますIAM。アクセス許可セットの詳細については、「AWS IAM Identity Center ユーザーガイド」の「アクセス許可セット」を参照してください。

- 一時的なIAMユーザーアクセス許可 – IAM ユーザーまたはロールは、 IAMロールを引き受けて、特定のタスクに対して異なるアクセス許可を一時的に引き受けることができます。
- クロスアカウントアクセス – IAMロールを使用して、別のアカウントのユーザー (信頼されたプリンシパル) がアカウントのリソースにアクセスすることを許可できます。クロスアカウントアクセスを許可する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、(ロールをプロキシとして使用する代わりに) ポリシーをリソースに直接アタッチできます。クロスアカウントアクセスのロールとリソースベースのポリシーの違いについては、「 ユーザーガイド」の「 でのクロスアカウントリソースアクセスIAMIAM」を参照してください。
- クロスサービスアクセス — 一部の は、他の の機能 AWS のサービス を使用します AWS のサービス。例えば、サービスで呼び出しを行うと、そのサービスが Amazon でアプリケーションを実行EC2したり、Amazon S3 にオブジェクトを保存したりするのが一般的です。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するための権限が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール – サービスロールは、ユーザーに代わってアクションを実行するためにサービスが引き受ける IAMロールです。IAM 管理者は、 内からサービスロールを作成、変更、削除できますIAM。詳細については、「 ユーザーガイド」の「 にアクセス許可を委任するロールの作成 AWS のサービスIAM」を参照してください。
  - サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。
- Amazon で実行されているアプリケーション EC2 – IAMロールを使用して、EC2インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管

理できます。これは、EC2インスタンス内にアクセスキーを保存するよりも望ましいです。 AWS ロールをEC2インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルには ロールが含まれており、EC2インスタンスで実行されているプログラムが一時的な認証情報を取得できるようにします。詳細については、「 ユーザーガイド」の「 IAMロールを使用して Amazon EC2インスタンスで実行されているアプリケーションにアクセス許可を付与するIAM」を参照してください。

IAM ロールとIAMユーザーのどちらを使用するかについては、「 ユーザーガイド」の「 (ユーザーではなく) IAMロールを作成する場合IAM」を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、 AWS ID またはリソースにアタッチします。ポリシーは、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義する のオブジェクトです。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) AWS がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーはJSONドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「 ユーザーガイド」のJSON「ポリシーの概要IAM」を参照してください。

管理者はポリシーを使用して AWS JSON、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。必要なリソースに対してアクションを実行するアクセス許可をユーザーに付与するために、IAM管理者はIAMポリシーを作成できます。その後、管理者はIAMポリシーをロールに追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行に使用するメソッドに関係なく、アクションのアクセス許可を定義します。例えば、`iam:GetRole`アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 AWS Management Console、、 AWS CLIまたは AWS からロール情報を取得できますAPI。

アイデンティティベースのポリシー

ID ベースのポリシーは、IAMユーザー、ユーザーのグループ、ロールなどの ID にアタッチできるJSONアクセス許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行でき

るアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「 ユーザーガイド」のIAM「ポリシーの作成IAM」を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。管理ポリシーとインラインポリシーのどちらかを選択する方法については、「 IAM ユーザーガイド」の「管理ポリシーとインラインポリシーの選択」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースにアタッチするJSONポリシードキュメントです。リソースベースのポリシーの例としては、IAMロールの信頼ポリシー や Amazon S3 バケットポリシー などがあります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーIAMでは、 の AWS 管理ポリシーを使用できません。

アクセスコントロールリスト (ACLs)

アクセスコントロールリスト (ACLs) は、リソースへのアクセス許可を持つプリンシパル (アカウントメンバー、ユーザー、またはロール) を制御します。ACLs はリソースベースのポリシーに似ていますが、JSONポリシードキュメント形式を使用しません。

Amazon S3、 AWS WAF、および Amazon VPCは、 をサポートするサービスの例ですACLs。の詳細についてはACLs、Amazon Simple Storage Service デベロッパーガイドの「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS は、一般的ではない追加のポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 – アクセス許可の境界は、アイデンティティベースのポリシーがIAMエンティティ (IAMユーザーまたはロール) に付与できるアクセス許可の上限を設定する高度な機能です。エ

ンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。Principal フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、「 IAMユーザーガイド」の「 IAMエンティティのアクセス許可の境界」を参照してください。

- サービスコントロールポリシー (SCPs) – SCPsは、 の組織または組織単位 (OU) に対する最大アクセス許可を指定するJSONポリシーです AWS Organizations。 AWS Organizations は、 AWS アカウント ビジネスが所有する複数の をグループ化して一元管理するためのサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCPs) をアカウントの一部またはすべてに適用できます。は、各 を含むメンバーアカウントのエンティティのアクセス許可SCP を制限します AWS アカウントのルートユーザー。Organizations と の詳細についてはSCPs、「 AWS Organizations ユーザーガイド」の「サービスコントロールポリシー」を参照してください。
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「 ユーザーガイド」の「セッションポリシーIAM」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。複数のポリシータイプが関係する場合にリクエストを許可するかどうか AWS を決定する方法については、「 ユーザーガイド」の「ポリシー評価ロジックIAM」を参照してください。

AWS Storage Gateway と の連携方法 IAM

IAM を使用して へのアクセスを管理する前に AWS SGW、 で使用できるIAM機能を確認してください AWS SGW。

IAM AWS Storage Gatewayで使用できる機能

IAM 機能	AWS SGW サポート
アイデンティティベースのポリシー	あり
リソースベースのポリシー	なし
ポリシーアクション	あり
ポリシーリソース	はい
ポリシー条件キー (サービス固有)	あり
ACLs	なし
ABAC (ポリシー内のタグ)	部分的
一時的な認証情報	あり
転送アクセスセッション (FAS)	あり
サービスロール	あり
サービスリンクロール	あり

およびその他の AWS のサービスがほとんどの IAM 機能と連携する方法 AWS SGWの概要を把握するには、 IAM ユーザーガイドのAWS 「 と連携する のサービスIAM」を参照してください。

のアイデンティティベースのポリシー AWS SGW

アイデンティティベースのポリシーのサポート: あり

ID ベースのポリシーは、IAMユーザー、ユーザーのグループ、ロールなどの ID にアタッチできるJSONアクセス許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「 ユーザーガイド」のIAM「ポリシーの作成IAM」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否されたアクションとリソース、およびアクションが許可または拒否される条件を指定できます。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できませ

ん。JSON ポリシーで使用できるすべての要素については、「 ユーザーガイド」の「 IAMJSONポリシー要素リファレンスIAM」を参照してください。

のアイデンティティベースのポリシーの例 AWS SGW

アイデンティティベースのポリシーの例 AWS SGWを表示するには、「」を参照してくださいAWS Storage Gateway のアイデンティティベースのポリシーの例。

内のリソースベースのポリシー AWS SGW

リソースベースのポリシーのサポート: なし

リソースベースのポリシーは、リソースにアタッチするJSONポリシードキュメントです。リソースベースのポリシーの例としては、IAMロールの信頼ポリシー や Amazon S3 バケットポリシー などがあります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

クロスアカウントアクセスを有効にするには、リソースベースのポリシーで、アカウント全体または別のアカウントのIAMエンティティをプリンシパルとして指定できます。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる にある場合 AWS アカウント、信頼されたアカウントのIAM管理者は、プリンシパルエンティティ (ユーザーまたはロール) にリソースへのアクセス許可も付与する必要があります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーをさらに付与する必要はありません。詳細については、「 ユーザーガイド」の「 でのクロスアカウントリソースアクセスIAMIAM」を参照してください。

のポリシーアクション AWS SGW

ポリシーアクションのサポート: あり

管理者はポリシーを使用して AWS JSON、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

JSON ポリシーの Action要素は、ポリシーでアクセスを許可または拒否するために使用できるアクションを記述します。ポリシーアクションの名前は通常、関連する AWS APIオペレーションと同じです。一致するAPIオペレーションがないアクセス許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは、依存アクションと呼ばれます。

このアクションは、関連付けられたオペレーションを実行するための権限を付与するポリシーで使用されます。

アクションのリスト AWS SGWを確認するには、「サービス認証リファレンス」の AWS Storage Gateway で定義されるアクション」を参照してください。

の AWS SGWポリシーアクションは、アクションの前に次のプレフィックスを使用します。

```
sgw
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

```
"Action": [
      "sgw:action1",
      "sgw:action2"
         ]
```

アイデンティティベースのポリシーの例 AWS SGWを表示するには、「」を参照してくださいAWS Storage Gateway のアイデンティティベースのポリシーの例。

のポリシーリソース AWS SGW

ポリシーリソースのサポート: あり

管理者はポリシーを使用して AWS JSON、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

Policy ResourceJSON要素は、アクションが適用されるオブジェクトを指定します。ステートメントには、Resource または NotResource 要素を含める必要があります。ベストプラクティスとし

て、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

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

リソースタイプとその のリスト AWS SGWを確認するにはARNs、「サービス認証リファレンス」の AWS Storage Gateway で定義されるリソース」を参照してください。各リソースARNの を指定できるアクションについては、「AWS Storage Gateway で定義されるアクション」を参照してください。

アイデンティティベースのポリシーの例 AWS SGWを表示するには、「」を参照してくださいAWS Storage Gateway のアイデンティティベースのポリシーの例。

のポリシー条件キー AWS SGW

サービス固有のポリシー条件キーのサポート: あり

管理者はポリシーを使用して AWS JSON、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルが、どのリソースに対してどのような条件下でアクションを実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成することで、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の Condition 要素を指定する場合、または 1 つの Condition 要素に複数のキーを指定する場合、 AWS では AND 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 は論理ORオペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば、リソースにIAMユーザー名でタグ付けされている場合にのみ、リソースへのアクセス許可をIAMユーザーに付与できます。詳細については、「 ユーザーガイド」のIAM「ポリシー要素: 変数とタグIAM」を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートします。すべての AWS グローバル条件キーを確認するには、「 ユーザーガイド」のAWS 「 グローバル条件コンテキストキーIAM」を参照してください。

条件キーのリスト AWS SGWを確認するには、「サービス認証リファレンス」のAWS Storage Gateway の条件キー」を参照してください。条件キーを使用できるアクションとリソースについては、「AWS Storage Gateway で定義されるアクション」を参照してください。

アイデンティティベースのポリシーの例 AWS SGWを表示するには、「」を参照してくださいAWS Storage Gateway のアイデンティティベースのポリシーの例。

ACLs の AWS SGW

をサポートACLs： いいえ

アクセスコントロールリスト (ACLs) は、リソースへのアクセス許可を持つプリンシパル (アカウントメンバー、ユーザー、またはロール) を制御します。ACLs はリソースベースのポリシーに似ていますが、JSONポリシードキュメント形式を使用しません。

ABAC と AWS SGW

サポート ABAC (ポリシー内のタグ): 部分的

属性ベースのアクセスコントロール (ABAC) は、属性に基づいてアクセス許可を定義する認可戦略です。では AWS、これらの属性はタグ と呼ばれます。タグは、IAMエンティティ (ユーザーまたはロール) および多くの AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、の最初のステップですABAC。次に、プリンシパルのタグがアクセスしようとしているリソースのタグと一致する場合に、オペレーションを許可するABACポリシーを設計します。

ABAC は、急速に成長している環境や、ポリシー管理が煩雑になる状況に役立ちます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

の詳細についてはABAC、「 IAMユーザーガイド」の「 とはABAC」を参照してください。のセットアップ手順を含むチュートリアルを表示するにはABAC、「 ユーザーガイド」の「属性ベースのアクセスコントロール (ABAC) を使用するIAM」を参照してください。

での一時的な認証情報の使用 AWS SGW

一時的な認証情報のサポート: あり

一部の AWS のサービス は、一時的な認証情報を使用してサインインすると機能しません。一時的な認証情報 AWS のサービス を使用する などの詳細については、「 ユーザーガイド」のAWS のサービス 「 と連携IAMする IAM 」を参照してください。

ユーザー名とパスワード以外の AWS Management Console 方法で にサインインする場合、一時的な認証情報を使用します。例えば、会社のシングルサインオン (SSO) リンク AWS を使用して にアクセスすると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えの詳細については、「 IAMユーザーガイド」の「ロールへの切り替え (コンソール) 」を参照してください。

一時的な認証情報は、 AWS CLI または を使用して手動で作成できます AWS API。その後、これらの一時的な認証情報を使用して . AWS recommends にアクセスできます AWS。これは、長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成することを推奨しています。詳細については、「」の「一時的なセキュリティ認証情報IAM」を参照してください。

の転送アクセスセッション AWS SGW

転送アクセスセッションをサポート (FAS): はい

IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するための権限が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

AWS SGW のサービスロール

サービスロールのサポート: あり

サービスロールは、ユーザーに代わってアクションを実行するためにサービスが引き受ける IAM ロールです。IAM 管理者は、 内からサービスロールを作成、変更、削除できますIAM。詳細につい

ては、「 ユーザーガイド」の「 にアクセス許可を委任するロールの作成 AWS のサービスIAM」を参照してください。

> **Warning**
>
> サービスロールのアクセス許可を変更すると、機能が破損 AWS SGWする可能性があります。が指示する場合 AWS SGW以外は、サービスロールを編集しないでください。

のサービスにリンクされたロール AWS SGW

サービスリンクロールのサポート: あり

サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

サービスにリンクされたロールの作成または管理の詳細については、「 AWS と連携する のサービスIAM」を参照してください。表の中から、[Service-linked role] (サービスにリンクされたロール) 列に Yes と記載されたサービスを見つけます。サービスリンクロールに関するドキュメントをサービスで表示するには、はい リンクを選択します。

AWS Storage Gateway のアイデンティティベースのポリシーの例

デフォルトでは、ユーザーとロールにはリソースを作成または変更 AWS SGWするアクセス許可はありません。また、、 AWS Command Line Interface （ AWS CLI ） AWS Management Console、または を使用してタスクを実行することはできません AWS API。必要なリソースに対してアクションを実行するアクセス許可をユーザーに付与するために、IAM管理者はIAMポリシーを作成できます。その後、管理者はIAMポリシーをロールに追加し、ユーザーはロールを引き受けることができます。

これらのポリシードキュメント例を使用してIAMアイデンティティベースのJSONポリシーを作成する方法については、「 ユーザーガイド」のIAM「ポリシーの作成IAM」を参照してください。

ARNs 各リソースタイプの の形式など AWS SGW、 で定義されるアクションとリソースタイプの詳細については、「サービス認証リファレンス」のAWS Storage Gateway のアクション、リソース、および条件キー」を参照してください。

トピック

- ポリシーのベストプラクティス
- コンソール AWS SGWの使用
- 自分の権限の表示をユーザーに許可する

ポリシーのベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かがリソースを作成、アクセス、または削除 AWS SGWできるどうかを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可を付与するには、多くの一般的なユースケースにアクセス許可を付与する AWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義して、アクセス許可をさらに減らすことをお勧めします。詳細については、「 ユーザーガイド」の「 AWS 管理ポリシー」または「 ジョブ機能の 管理ポリシーIAM」を参照してください。 AWS
- 最小特権のアクセス許可を適用する – IAMポリシーでアクセス許可を設定する場合は、タスクの実行に必要なアクセス許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用してアクセス許可を適用する方法の詳細については、「 ユーザーガイド」の「 のポリシーとアクセス許可IAMIAM」を参照してください。
- IAM ポリシーの条件を使用してアクセスをさらに制限する – ポリシーに条件を追加して、アクションとリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを を使用して送信する必要があることを指定できますSSL。条件を使用して、 などの特定の を介してサービスアクションが使用される場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、「 ユーザーガイド」のIAMJSON「ポリシー要素: 条件IAM」を参照してください。
- IAM Access Analyzer を使用してIAMポリシーを検証し、安全で機能的なアクセス許可を確保する – IAM Access Analyzer は、ポリシーがポリシー言語 (JSON) とIAMベストプラクティスに準拠するように、新規および既存のIAMポリシーを検証します。IAM Access Analyzer には、安全で機能的なポリシーの作成に役立つ 100 を超えるポリシーチェックと実用的な推奨事項が用意されています。詳細については、「 ユーザーガイド」のIAM「Access Analyzer ポリシーの検証IAM」を参照してください。
- 多要素認証を要求する (MFA) – でIAMユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化MFAするために をオンにします。API オペレー

ションが呼び出されるMFAタイミングを要求するには、ポリシーにMFA条件を追加します。詳細については、「 IAMユーザーガイド」のMFA「 で保護されたAPIアクセスの設定」を参照してください。

のベストプラクティスの詳細についてはIAM、「 ユーザーガイド」の「 のセキュリティのベストプラクティスIAMIAM」を参照してください。

コンソール AWS SGWの使用

AWS Storage Gateway コンソールにアクセスするには、最小限のアクセス許可が必要です。これらのアクセス許可により、 のリソースの詳細を AWS SGW一覧表示および表示できます AWS アカウント。最小限必要な許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

AWS CLI または のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません AWS API。代わりに、実行しようとしているAPIオペレーションに一致するアクションのみへのアクセスを許可します。

ユーザーとロールが引き続きコンソール AWS SGWを使用できるようにするには、エンティティに AWS SGW*ConsoleAccess*または *ReadOnly* AWS 管理ポリシーもアタッチします。詳細については、「 ユーザーガイド」の「ユーザーへのアクセス許可の追加IAM」を参照してください。

自分の権限の表示をユーザーに許可する

この例では、IAMユーザーがユーザー ID にアタッチされているインラインポリシーと管理ポリシーを表示できるようにするポリシーを作成する方法を示します。このポリシーには、コンソールで、または AWS CLI または を使用してプログラムでこのアクションを実行するアクセス許可が含まれています AWS API。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
```

```
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Storage Gateway のアイデンティティとアクセスのトラブルシューティング

次の情報は、 および の使用 AWS SGW時に発生する可能性がある一般的な問題の診断と修正に役立ちますIAM。

トピック

- でアクションを実行する権限がない AWS SGW
- iam を実行する権限がありません。PassRole
- 自分の 以外のユーザーに自分のリソース AWS アカウント へのアクセス AWS SGWを許可したい

でアクションを実行する権限がない AWS SGW

「I am not authorized to perform an action in Amazon Bedrock」というエラーが表示された場合、そのアクションを実行できるようにポリシーを更新する必要があります。

次の例のエラーは、mateojacksonIAMユーザーが コンソールを使用して架空の*my-example-widget*リソースの詳細を表示しようとしているが、架空のsgw:*GetWidget*アクセス許可がない場合に発生します。

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

この場合、sgw:*GetWidget* アクションを使用して *my-example-widget*リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

iam を実行する権限がありません。PassRole

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して にロールを渡すことができるようにする必要があります AWS SGW。

一部の AWS のサービス では、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、そのサービスに既存のロールを渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

次の例のエラーは、 というIAMユーザーがコンソールを使用して marymajor でアクションを実行しようする場合に発生します AWS SGW。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

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

この場合、Mary のポリシーを更新してメアリーに iam:PassRole アクションの実行を許可する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

自分の 以外のユーザーに自分のリソース AWS アカウント へのアクセス AWS SGW を許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまた

はアクセスコントロールリスト (ACLs) をサポートするサービスの場合、それらのポリシーを使用して、ユーザーにリソースへのアクセスを許可できます。

詳細については、以下を参照してください。

- がこれらの機能をサポートしているかどうか AWS SGWを確認するには、「」を参照してくださいAWS Storage Gateway と の連携方法 IAM。
- 所有している のリソースへのアクセスを提供する方法については、 AWS アカウント 「 ユーザーガイド」の「所有 AWS アカウント している別の のIAMユーザーへのアクセスを提供するIAM」を参照してください。
- リソースへのアクセスをサードパーティー に提供する方法については AWS アカウント、「 ユーザーガイド」の「サードパーティー AWS アカウント が所有する へのアクセスを提供するIAM」を参照してください。
- ID フェデレーションを通じてアクセスを提供する方法については、 IAMユーザーガイドの「外部認証されたユーザーへのアクセスの提供 (ID フェデレーション)」を参照してください。
- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いについては、「 ユーザーガイド」の「 でのクロスアカウントリソースアクセスIAMIAM」を参照してください。

でのログ記録とモニタリング AWS Storage Gateway

Storage Gateway は AWS CloudTrail、Storage Gateway のユーザー、ロール、または サービスによって実行されたアクションを記録する AWS サービスStorage Gateway。 は、Storage Gateway のすべてのAPI呼び出しをイベントとして CloudTrail キャプチャします。キャプチャされた呼び出しには、Storage Gateway コンソールからの呼び出しと、Storage Gateway APIオペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、Storage Gateway の CloudTrail イベントなど、Amazon S3 バケットへのイベントの継続的な配信をアクティブ化できます。証跡を設定しない場合でも、 CloudTrail コンソールのイベント履歴 で最新のイベントを表示できます。で収集された情報を使用して CloudTrail、Storage Gateway 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。

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

での Storage Gateway 情報 CloudTrail

CloudTrail アカウントを作成すると、 が Amazon Web Services アカウントでアクティブ化されます。Storage Gateway でアクティビティが発生すると、そのアクティビティは CloudTrail イベン

ト履歴 の他の AWS サービスイベントとともにイベントに記録されます。AWS アカウントでの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、「イベント履歴を使用した CloudTrail イベントの表示」を参照してください。

Storage Gateway のイベントなど、Amazon Web Services のアカウントのイベントを継続的に記録するには、証跡を作成します。証跡により、 はログファイル CloudTrail を Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成すると、証跡はすべての AWS リージョンに適用されます。証跡は、 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 Amazon S3 バケットにログファイルを配信します。さらに、 CloudTrail ログで収集されたイベントデータをより詳細に分析し、それに基づいて行動するように、他の AWS サービスを設定できます。詳細については、次を参照してください:

- 証跡の作成のための概要
- CloudTrail サポートされているサービスと統合
- の Amazon SNS Notifications の設定 CloudTrail
- 複数のリージョンからの CloudTrail ログファイルの受信と複数のアカウントからの CloudTrail ログファイルの受信

Storage Gateway のアクションはすべて記録され、[Actions] (アクション) トピックで説明されます。例えば、`ActivateGateway`、、および `ShutdownGateway`アクションを呼び出すと`ListGateways`、 CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます:

- リクエストがルートまたは AWS Identity and Access Management （ IAM) ユーザー認証情報のどちらを使用して行われたか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが別の AWS サービスによって行われたかどうか。

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

Storage Gateway のログファイルエントリを理解する

証跡は、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

スからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータ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。

次の例は、 アクションを示す CloudTrail ログエントリを示しています。

```
{ "Records": [{
                "eventVersion": "1.02",
                "userIdentity": {
                "type": "IAMUser",
                "principalId": "AIDAII5AUEPBH2M7JTNVC",
                "arn": "arn:aws:iam::111122223333:user/StorageGateway-team/JohnDoe",
                "accountId": "111122223333",
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                 "userName": "JohnDoe"
               },
                  "eventTime": "2014-12-04T16:19:00Z",
                  "eventSource": "storagegateway.amazonaws.com",
                  "eventName": "ActivateGateway",
                  "awsRegion": "us-east-2",
                  "sourceIPAddress": "192.0.2.0",
                  "userAgent": "aws-cli/1.6.2 Python/2.7.6 Linux/2.6.18-164.el5",
                   "requestParameters": {
                                        "gatewayTimezone": "GMT-5:00",
                                        "gatewayName": "cloudtrailgatewayvtl",
                                        "gatewayRegion": "us-east-2",
                                        "activationKey": "EHFBX-1NDD0-P0IVU-PI259-
DHK88",
                                        "gatewayType": "VTL"
                                             },
                                             "responseElements": {
                                                                    "gatewayARN":
 "arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayvtl"
                                             },
                                             "requestID":
 "54BTFGNQI71987UJD2IHTCT8NF1Q8GLLE1QEU3KPGG6F0KSTAUU0",
                                             "eventID": "635f2ea2-7e42-45f0-
bed1-8b17d7b74265",
                                             "eventType": "AwsApiCall",
                                             "apiVersion": "20130630",
                                             "recipientAccountId": "444455556666"
             }]
}
```

次の例は、 アクションを示す CloudTrail ListGatewaysログエントリをIを示しています。

```
{
 "Records": [{
               "eventVersion": "1.02",
               "userIdentity": {
                                "type": "IAMUser",
                                "principalId": "AIDAII5AUEPBH2M7JTNVC",
                                "arn": "arn:aws:iam::111122223333:user/StorageGateway-
team/JohnDoe",
                                "accountId:" 111122223333", " accessKeyId ":"
 AKIAIOSFODNN7EXAMPLE",
                                " userName ":" JohnDoe "
                                },

                                " eventTime ":" 2014 - 12 - 03T19: 41: 53Z ",
                                " eventSource ":" storagegateway.amazonaws.com ",
                                " eventName ":" ListGateways ",
                                " awsRegion ":" us-east-2 ",
                                " sourceIPAddress ":" 192.0.2.0 ",
                                " userAgent ":" aws - cli / 1.6.2 Python / 2.7.6
 Linux / 2.6.18 - 164.el5 ",
                                " requestParameters ":null,
                                " responseElements ":null,
                                "requestID ":"
 6U2N42CU37KAO8BG6V1I23FRSJ1Q8GLLE1QEU3KPGG6F0KSTAUU0 ",
                                " eventID ":" f76e5919 - 9362 - 48ff - a7c4 -
 d203a189ec8d ",
                                " eventType ":" AwsApiCall ",
                                " apiVersion ":" 20130630 ",
                                " recipientAccountId ":" 444455556666"
             }]
}
```

AWS Storage Gateway のコンプライアンス検証

サードパーティーの監査者は、複数の コンプライアンスプログラムの一環として AWS Storage Gateway のセキュリティと AWS コンプライアンスを評価します。これには SOC、、PCI、ISO、Fed RAMP、、HIPAA、C5MTSC、K-、ENSHighISMS、OSPAR、および HITRUST が含まれますCSF。

特定のコンプライアンスプログラムの対象となる AWS サービスのリストについては、「コンプライアンスプログラムAWS による対象範囲内のサービスコンプライアンスプログラム」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。

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 AWS Artifact。詳細については、「 でのレポートのダウンロード AWS Artifact」の」を参照してください。

Storage Gateway を使用する際のお客様のコンプライアンス責任は、データの機密性、企業のコンプライアンス目的、適用法規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が提供されています。

- セキュリティと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に重点を置いたベースライン環境を にデプロイする手順について説明します AWS。
- HIPAA セキュリティとコンプライアンスのアーキテクチャに関するホワイトペーパー — このホワイトペーパーでは、企業が AWS を使用して HIPAA準拠のアプリケーションを作成する方法について説明します。
- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- 「 デベロッパーガイド」のルールによるリソースの評価 — この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub – この AWS サービスは、 内のセキュリティ状態を包括的に把握 AWS し、セキュリティ業界標準とベストプラクティスへの準拠を確認するのに役立ちます。

In AWS Storage Gateway の耐障害性

AWS 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に構築されています。 AWS リージョンは、低レイテンシー、高スループット、および高度に冗長なネットワークで接続された、物理的に分離および分離された複数のアベイラビリティーゾーンを提供します。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が高く、フォールトトレラントで、スケーラブルです。

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 「 グローバルインフラストラクチャ」を参照してください。

Storage Gateway には、 AWS グローバルインフラストラクチャに加えて、データの耐障害性とバックアップのニーズをサポートするのに役立ついくつかの機能があります。

- VMware vSphere 高可用性 (VMware HA) を使用して、ハードウェア、ハイパーバイザー、またはネットワーク障害からストレージワークロードを保護します。詳細については、「Storage Gateway でのVMware vSphere 高可用性の使用」を参照してください。
- AWS Backup を使用してボリュームをバックアップします。詳細については、「ボリュームのバックアップ」を参照してください。
- 復旧ポイントからボリュームのクローンを作成します。詳細については、「ボリュームをクローンする」を参照してください。

AWS Storage Gateway 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である AWS Storage Gateway「Amazon Web Services: セキュリティプロセスの概要」に記載されている AWS グローバルネットワークセキュリティの手順で保護されています。

が AWS 公開したAPI呼び出しを使用して、ネットワーク経由で Storage Gateway にアクセスします。クライアントは Transport Layer Security (TLS) 1.2 をサポートしている必要があります。クライアントは、エフェメラル Diffie-Hellman (PFS) や楕円曲線エフェメラル Diffie-Hellman () などの完全前方秘匿性 (DHE) を備えた暗号スイートもサポートする必要がありますECDHE。これらのモードは、Java 7 以降など、ほとんどの最新システムでサポートされています。

さらに、 リクエストは、 IAMプリンシパルに関連付けられたアクセスキー ID と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。

> **Note**
>
> AWS Storage Gateway アプライアンスはマネージド仮想マシンとして扱い、インストールへのアクセスや変更を一切試みないでください。通常のゲートウェイ更新メカニズム以外の方法を使用してスキャンソフトウェアをインストールしたり、ソフトウェアパッケージを更新しようとすると、ゲートウェイが誤動作し、ゲートウェイをサポートまたは修正する機能に影響を与える可能性があります。
> AWS CVEsは、定期的にレビュー、分析、修正を行います。これらの問題の修正は、通常のソフトウェアリリースサイクルの一部として Storage Gateway に組み込みます。これらの修正は、通常、スケジュールされたメンテナンスウィンドウ中の通常のゲートウェイ更新プロ

セスの一部として適用されます。ゲートウェイの更新の詳細については、「コンソール」を参照してください。

AWS セキュリティのベストプラクティス

AWS には、独自のセキュリティポリシーを開発および実装する際に考慮すべきいくつかのセキュリティ機能が用意されています。これらのベストプラクティスは一般的なガイドラインであり、完全なセキュリティソリューションを提供するものではありません。これらのプラクティスは顧客の環境に必ずしも適切または十分でない可能性があるので、処方箋ではなく、あくまで有用な検討事項とお考えください。詳細については、「AWS Security Best Practices」を参照してください。

ゲートウェイのトラブルシューティング

次に、ゲートウェイ、ファイル共有、ボリューム、仮想テープ、およびスナップショットに関連する問題のトラブルシューティングについて説明します。オンプレミスゲートウェイのトラブルシューティング情報は、 VMwareESXiクライアントと Microsoft Hyper-V クライアントの両方にデプロイされたゲートウェイを対象としています。ファイル共有のトラブルシューティング情報は、ファイルゲートウェイタイプに適用されます。ボリュームのトラブルシューティング情報は、ボリュームゲートウェイタイプに適用されます。テープのトラブルシューティング情報はテープゲートウェイタイプに適用されます。ゲートウェイの問題のトラブルシューティング情報は、 CloudWatch メトリクスの使用に適用されます。高可用性問題のトラブルシューティング情報は、高可用性 (HA) VMware vSphere プラットフォームで実行されているゲートウェイを対象としています。

トピック

トラブルシューティング: Storage Gateway コンソールでゲートウェイがオフライン

次のトラブルシューティング情報を使用して、ゲートウェイがオフラインであることがコンソールに表示される AWS Storage Gateway 場合の対処方法を決定します。

ゲートウェイは、次の 1 つ以上の理由でオフラインとして表示される場合があります。

- ゲートウェイが Storage Gateway サービスエンドポイントに到達できません。
- ゲートウェイが予期せずシャットダウンしました。
- ゲートウェイに関連付けられたキャッシュディスクが切断または変更されたか、失敗しました。

ゲートウェイをオンラインに戻すには、ゲートウェイがオフラインになった原因となった問題を特定して解決します。

関連付けられたファイアウォールまたはプロキシを確認する

プロキシを使用するようにゲートウェイを設定した場合、またはゲートウェイをファイアウォールの背後に配置した場合は、プロキシまたはファイアウォールのアクセスルールを確認します。プロキシまたはファイアウォールは、Storage Gateway に必要なネットワークポートとサービスエンドポイントとの間のトラフィックを許可する必要があります。詳細については、https://docs.aws.amazon.com/storagegateway/latest/vgw/Requirements.html#networks」を参照してください。

ゲートウェイのトラフィックの継続的な検査SSLまたはディープパケット検査を確認する

ゲートウェイと 間のネットワークトラフィックに対して SSLまたは のディープパケットインスペクションが現在実行されている場合 AWS、ゲートウェイは必要なサービスエンドポイントと通信できない可能性があります。ゲートウェイをオンラインに戻すには、検査を無効にする必要があります。

ハイパーバイザーホストで停電やハードウェア障害がないか確認します。

ゲートウェイのハイパーバイザーホストで停電やハードウェア障害が発生すると、ゲートウェイが予期せずシャットダウンし、アクセスできなくなる可能性があります。電源とネットワーク接続を復元すると、ゲートウェイに再び到達できるようになります。

ゲートウェイがオンラインに戻ったら、必ずデータを復旧する手順を実行してください。詳細については、」「データ復旧に関するベストプラクティス」を参照してください。

関連付けられたキャッシュディスクに関する問題を確認する

ゲートウェイに関連付けられたキャッシュディスクの少なくとも 1 つが削除、変更、サイズ変更された場合、または破損した場合、ゲートウェイはオフラインになる可能性があります。

作業キャッシュディスクがハイパーバイザーホストから削除された場合：

1. ゲートウェイをシャットダウンします。
2. ディスクを再追加します。

> **Note**
>
> ディスクを同じディスクノードに追加してください。

3. ゲートウェイを再起動します。

キャッシュディスクが破損している場合、置き換えられた場合、またはサイズが変更された場合：

1. ゲートウェイをシャットダウンします。
2. キャッシュディスクをリセットします。
3. キャッシュストレージ用にディスクを再設定します。
4. ゲートウェイを再起動します。

トラブルシューティング: ゲートウェイのアクティベーション中の内部エラー

Storage Gateway のアクティベーションリクエストは、2 つのネットワークパスを通過します。クライアントから送信された受信アクティベーションリクエストは、ポート 80 を介してゲートウェイの仮想マシン (VM) または Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに接続します。ゲートウェイがアクティベーションリクエストを正常に受信すると、ゲートウェイは Storage Gateway エンドポイントと通信してアクティベーションキーを受け取ります。ゲートウェイが Storage Gateway エンドポイントに到達できない場合、ゲートウェイは内部エラーメッセージでクライアントに応答します。

次のトラブルシューティング情報を使用して、 をアクティブ化しようとしたときに内部エラーメッセージが表示された場合の対処方法を決定します AWS Storage Gateway。

> **Note**
>
> - 必ず最新の仮想マシンイメージファイルまたは Amazon マシンイメージ (AMI) バージョンを使用して新しいゲートウェイをデプロイしてください。古い を使用するゲートウェイをアクティブ化しようとすると、内部エラーが表示されますAMI。

- をダウンロードする前に、デプロイするゲートウェイタイプが正しいことを確認してくださいAMI。ゲートウェイタイプAMIsごとに .ova ファイルと は異なり、互換性はありません。

パブリックエンドポイントを使用してゲートウェイをアクティブ化する際のエラーを解決する

パブリックエンドポイントを使用してゲートウェイをアクティブ化する際のアクティベーションエラーを解決するには、次のチェックと設定を実行します。

必要なポートを確認する

オンプレミスにデプロイされたゲートウェイの場合は、ローカルファイアウォールでポートが開いていることを確認します。Amazon EC2インスタンスにデプロイされたゲートウェイの場合、インスタンスのセキュリティグループでポートが開いていることを確認します。ポートが開いていることを確認するには、サーバーからパブリックエンドポイントで telnet コマンドを実行します。このサーバーは、ゲートウェイと同じサブネットに存在する必要があります。例えば、次の telnet コマンドは、ポート 443 への接続をテストします。

```
telnet d4kdq0yaxexbo.cloudfront.net 443
telnet storagegateway.region.amazonaws.com 443
telnet dp-1.storagegateway.region.amazonaws.com 443
telnet proxy-app.storagegateway.region.amazonaws.com 443
telnet client-cp.storagegateway.region.amazonaws.com 443
telnet anon-cp.storagegateway.region.amazonaws.com 443
```

ゲートウェイ自体がエンドポイントに到達できることを確認するには、ゲートウェイのローカル VM コンソール (オンプレミスにデプロイされたゲートウェイ用) にアクセスします。または、ゲートウェイのインスタンス (Amazon にデプロイされたゲートウェイの場合EC2) SSHに移動することもできます。次に、ネットワーク接続テストを実行します。テストが を返すことを確認します[PASSED]。詳細については、テスト」「インターネットへのゲートウェイ接続のテスト」を参照してください。

> **Note**
>
> ゲートウェイコンソールのデフォルトのログインユーザー名は でadmin、デフォルトのパスワードは ですpassword。

ファイアウォールのセキュリティがゲートウェイからパブリックエンドポイントに送信されるパケットを変更しないことを確認する

SSL 検査、ディープパケット検査、またはその他の形式のファイアウォールセキュリティは、ゲートウェイから送信されるパケットを妨げる可能性があります。アクティベーションエンドポイントが期待する内容からSSL証明書が変更されると、SSLハンドシェイクは失敗します。進行中のSSL検査がないことを確認するには、ポート 443 のメインアクティベーションエンドポイント (anon-cp.storagegateway.region.amazonaws.com) で OpenSSL コマンドを実行します。このコマンドは、ゲートウェイと同じサブネットにあるマシンから実行する必要があります。

```
$ openssl s_client -connect  anon-cp.storagegateway.region.amazonaws.com:443 -
servername anon-cp.storagegateway.region.amazonaws.com
```

> **Note**
>
> 置換 *region* を で使用します AWS リージョン。

進行中のSSL検査がない場合、コマンドは次のようなレスポンスを返します。

```
$ openssl s_client -connect anon-cp.storagegateway.us-east-2.amazonaws.com:443 -
servername anon-cp.storagegateway.us-east-2.amazonaws.com
CONNECTED(00000003)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-2.amazonaws.com
verify return:1
---
Certificate chain
 0 s:/CN=anon-cp.storagegateway.us-east-2.amazonaws.com
   i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
 1 s:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
   i:/C=US/O=Amazon/CN=Amazon Root CA 1
 2 s:/C=US/O=Amazon/CN=Amazon Root CA 1
   i:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
 3 s:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
   i:/C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification Authority
```

```
---
```

SSL 検査が進行中の場合、レスポンスには次のような変更された証明書チェーンが表示されます。

```
$ openssl s_client -connect  anon-cp.storagegateway.ap-southeast-1.amazonaws.com:443 -
servername anon-cp.storagegateway.ap-southeast-1.amazonaws.com
CONNECTED(00000003)
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.ap-southeast-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

アクティベーションエンドポイントは、SSL証明書を認識する場合にのみSSLハンドシェイクを受け入れます。つまり、エンドポイントへのゲートウェイのアウトバウンドトラフィックは、ネットワーク内のファイアウォールによって実行される検査から除外する必要があります。これらの検査には、SSL検査またはディープパケット検査があります。

ゲートウェイの時刻同期を確認する

時間偏りが多すぎると、SSLハンドシェイクエラーが発生する可能性があります。オンプレミスゲートウェイの場合、ゲートウェイのローカル VM コンソールを使用して、ゲートウェイの時刻同期を確認できます。時間スキューは 60 秒以下にする必要があります。詳細については、の同期」を参照してください。

System Time Management オプションは、Amazon EC2インスタンスでホストされているゲートウェイでは使用できません。Amazon EC2ゲートウェイが適切に時刻を同期できるようにするには、Amazon EC2インスタンスがポート UDP および 123 TCP 経由で次のNTPサーバープールリストに接続できることを確認します。

- 0.amazon.pool.ntp.org
- 1.amazon.pool.ntp.org
- 2.amazon.pool.ntp.org

- 3.amazon.pool.ntp.org

Amazon VPCエンドポイントを使用してゲートウェイをアクティブ化する際のエラーを解決する

Amazon Virtual Private Cloud (Amazon VPC) エンドポイントを使用してゲートウェイをアクティブ化する際のアクティベーションエラーを解決するには、次のチェックと設定を実行します。

必要なポートを確認する

ローカルファイアウォール (オンプレミスにデプロイされたゲートウェイの場合) またはセキュリティグループ (Amazon にデプロイされたゲートウェイの場合EC2) 内の必要なポートが開いていることを確認します。ゲートウェイを Storage Gateway VPCエンドポイントに接続するために必要なポートは、ゲートウェイをパブリックエンドポイントに接続するときに必要なポートとは異なります。Storage Gateway VPCエンドポイントに接続するには、次のポートが必要です。

- TCP 443
- TCP 1026
- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

詳細については、の作成 VPCエンドポイントの作成 Storage Gateway」を参照してください。

さらに、Storage Gateway VPCエンドポイントにアタッチされているセキュリティグループを確認します。エンドポイントにアタッチされたデフォルトのセキュリティグループでは、必要なポートが許可されない場合があります。ゲートウェイの IP アドレス範囲から必要なポートへのトラフィックを許可する新しいセキュリティグループを作成します。次に、そのセキュリティグループをVPCエンドポイントにアタッチします。

> **Note**
>
> Amazon VPCコンソールを使用して、VPCエンドポイントにアタッチされているセキュリティグループを確認します。コンソールから Storage Gateway VPCエンドポイントを表示し、セキュリティグループタブを選択します。

必要なポートが開いていることを確認するには、Storage Gateway VPCエンドポイントで telnet コマンドを実行します。これらのコマンドは、ゲートウェイと同じサブネットにあるサーバーから実行する必要があります。アベイラビリティーゾーンを指定しないDNS名前でテストを実行できます。例えば、次の telnet コマンドは、vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com というDNS名前を使用して必要なポート接続をテストします。

```
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 443
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1026
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1027
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1028
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1031
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 2222
```

ファイアウォールのセキュリティによってゲートウェイから Storage Gateway Amazon VPCエンドポイントに送信されるパケットが変更されないことを確認します。

SSL 検査、ディープパケット検査、またはその他の形式のファイアウォールセキュリティは、ゲートウェイから送信されるパケットを妨げる可能性があります。アクティベーションエンドポイントが期待する内容からSSL証明書が変更されると、SSLハンドシェイクは失敗します。進行中のSSL検査がないことを確認するには、Storage Gateway VPCエンドポイントで OpenSSL コマンドを実行します。このコマンドは、ゲートウェイと同じサブネットにあるマシンから実行する必要があります。必要なポートごとに コマンドを実行します。

```
$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:443 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1026 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1028 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

```
$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1031 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:2222 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

進行中のSSL検査がない場合、コマンドは次のようなレスポンスを返します。

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-1.amazonaws.com
verify return:1
---
Certificate chain
 0 s:CN = anon-cp.storagegateway.us-east-1.amazonaws.com
   i:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
 1 s:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
   i:C = US, O = Amazon, CN = Amazon Root CA 1
 2 s:C = US, O = Amazon, CN = Amazon Root CA 1
   i:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
 3 s:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
   i:C = US, O = "Starfield Technologies, Inc.", OU = Starfield Class 2 Certification
 Authority
---
```

SSL 検査が進行中の場合、レスポンスには次のような変更された証明書チェーンが表示されます。

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
```

```
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.us-
east-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.us-east-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

アクティベーションエンドポイントは、SSL証明書を認識する場合にのみSSLハンドシェイクを受け入れます。つまり、必要なポートを介したVPCエンドポイントへのゲートウェイのアウトバウンドトラフィックは、ネットワークファイアウォールによって実行される検査から除外されます。これらの検査には、SSL検査やディープパケット検査などがあります。

ゲートウェイの時刻同期を確認する

時間偏りが多すぎると、SSLハンドシェイクエラーが発生する可能性があります。オンプレミスゲートウェイの場合、ゲートウェイのローカル VM コンソールを使用して、ゲートウェイの時刻同期を確認できます。時間スキューは 60 秒以下にする必要があります。詳細については、の同期」を参照してください。

System Time Management オプションは、Amazon EC2インスタンスでホストされているゲートウェイでは使用できません。Amazon EC2ゲートウェイが適切に時刻を同期できるようにするには、Amazon EC2インスタンスがポート UDP および 123 TCP 経由で次のNTPサーバープールリストに接続できることを確認します。

- 0.amazon.pool.ntp.org
- 1.amazon.pool.ntp.org
- 2.amazon.pool.ntp.org
- 3.amazon.pool.ntp.org

HTTP プロキシをチェックし、関連するセキュリティグループ設定を確認する

アクティベーションの前に、オンプレミスゲートウェイ VM 上の Amazon 上のHTTPプロキシが、ポート 3128 上の Squid プロキシとしてEC2設定されているかどうかを確認します。この場合、以下を確認します。

- Amazon のHTTPプロキシにアタッチされたセキュリティグループには、インバウンドルールEC2が必要です。このインバウンドルールでは、ゲートウェイ VM の IP アドレスからのポート 3128 での Squid プロキシトラフィックを許可する必要があります。
- Amazon EC2VPCエンドポイントにアタッチされたセキュリティグループには、インバウンドルールが必要です。これらのインバウンドルールでは、Amazon のHTTPプロキシの IP アドレスからのポート 1026-1028、1031、2222、および 443 でのトラフィックを許可する必要がありますEC2。

パブリックエンドポイントを使用してゲートウェイをアクティブ化し、同じ に Storage Gateway VPCエンドポイントがある場合のエラーの解決 VPC

同じ に Amazon Virtual Private Cloud (Amazon VPC) エンポイントがある場合に、パブリックエンドポイントを使用してゲートウェイをアクティブ化する際のエラーを解決するにはVPC、次のチェックと設定を実行します。

Storage Gateway VPCエンドポイントでプライベートDNS名を有効にする設定が有効になっていないことを確認します。

プライベートDNS名を有効にするが有効になっている場合、そのゲートウェイからパブリックエンドポイントVPCにゲートウェイをアクティブ化することはできません。

プライベートDNS名オプションを無効にするには：

1. Amazon VPCコンソール を開きます。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. Storage Gateway VPCエンドポイントを選択します。
4. [アクション] を選択します。
5. プライベートDNS名の管理 を選択します。
6. プライベートDNS名を有効にする では、このエンドポイント の有効化 をクリアします。
7. プライベートDNS名の変更を選択して設定を保存します。

オンプレミスゲートウェイの問題のトラブルシューティング

オンプレミスゲートウェイで作業する際に発生する可能性がある一般的な問題と、ゲートウェイのトラブルシューティングに役立つように AWS Support をアクティブ化する方法に関する情報は、次のとおりです。

次の表は、オンプレミスのゲートウェイを使用しているときに遭遇する可能性がある典型的な問題を一覧にしたものです。

問題	実行するアクション
ゲートウェイの IP アドレスが見つかりません。	ハイパーバイザークライアントを使用してホストに接続し、ゲートウェイの IP アドレスを見つけます。 • の場合VMwareESXi、VM の IP アドレスは、概要タブの vSphere クライアントにあります。 • Microsoft Hyper-V の場合、VM の IP アドレスはローカルコンソールにログインすると見つかります。 それでもゲートウェイ IP アドレスが見つからない場合 • VM の電源が入っていることを確認してください。VM がオンになっていないと、IP アドレスはゲートウェイに割り当てられません。 • VM の起動が終了するまでお待ちください。VM をオンにしてからゲートウェイが起動シーケンスを完了するのに、数分かかる場合があります。
ネットワークまたはファイアウォールに問題があります。	• ゲートウェイに対して適切なポートを許可します。 • SSL 証明書の検証/検査をアクティブ化しないでください。Storage Gateway は相互TLS認証を使用します。これは、サードパーティーアプリケーションがいずれかの証明書を傍受/署名しようとすると失敗します。 • ファイアウォールまたはルーターを使用してネットワークトラフィックをフィルタリングまたは制限する場合は、これらのサービスエンドポイントに対し AWSへのアウトバウンド通信を許可するように、対象のファイアウォールおよびルーターを設定する

問題	実行するアクション
	必要があります。ネットワークおよびファイアウォールの要件の詳細については、ネットワークとファイアウォールの要件を参照してください。
Storage Gateway マネジメントコンソールで [Proceed to Activation] (アクティベーションに進む) ボタンをクリックすると、ゲートウェイのアクティベーションは失敗します。	• クライアントから VM に Ping を送信し、ゲートウェイ VM にアクセスできることを確認します。 • VM がインターネットに接続していることを確認します。それ以外の場合は、SOCKSプロキシを設定する必要があります。その設定方法の詳細については、「オンプレミスのゲートウェイでのプロキシ経由のルーティング」を参照してください。 • ホストに正しい時刻があること、ホストが Network Time Protocol (NTP) サーバーに自動的に時刻を同期するように設定されていること、ゲートウェイ VM に正しい時刻があることを確認します。ハイパーバイザーホストと の時刻の同期についてはVMs、「」を参照してくださいゲートウェイ VM の時刻の同期。 • 以上の手順を実行したら、Storage Gateway コンソールと [Setup and Activate Gateway] (ゲートウェイのセットアップとアクティベーション) ウィザードを使用して、ゲートウェイのデプロイを再試行できます。 • SSL 証明書の検証/検査をアクティブ化しないでください。Storage Gateway は相互TLS認証を使用します。これは、サードパーティーアプリケーションがいずれかの証明書を傍受/署名しようとすると失敗します。 • VM に 7.5 GB 以上の があることを確認しますRAM。7.5 GB 未満の がある場合、ゲートウェイの割り当ては失敗しますRAM。詳細については、「Volume Gateway の設定要件」を参照してください。

問題	実行するアクション
アップロードバッファ領域として割り当てられているディスクを削除する必要があります。たとえば、ゲートウェイのアップロードバッファ領域の量を減らしたり、エラーが発生したアップロードバッファとして使用されているディスクを置き換えたりする必要が生じる場合があります。	アップロードバッファ領域として割り当てられているディスクを削除する手順については、「ゲートウェイからのディスクの削除」を参照してください。
ゲートウェイと AWSの間の帯域幅を改善する必要があります。	アプリケーションとゲートウェイ VM を接続するネットワークアダプタ (NIC) AWS で へのインターネット接続を設定 AWS することで、ゲートウェイから への帯域幅を向上させることができます。このアプローチは、 への高帯域幅接続があり、特にスナップショット AWS の復元中に帯域幅の競合を回避したい場合に便利です。高スループットのワークロードが要求される場合、AWS Direct Connect を使用して、オンプレミスのゲートウェイと AWSの間の専用ネットワーク接続を確立できます。ゲートウェイから への接続の帯域幅を測定するには AWS、ゲートウェイの `CloudBytesDownloaded` および `CloudBytesUploaded` メトリクスを使用します。この詳細については、「ゲートウェイと AWSの間のパフォーマンスの測定」を参照してください。インターネット接続を改善すれば、アップロードバッファがいっぱいになることがありません。

問題	実行するアクション

ゲートウェイへのスループットまたはゲートウェイからのスループットがゼロに落ちます。	• Storage Gateway コンソールの Gateway タブで、ゲートウェイ VM の IP アドレスがハイパーバイザークライアントソフトウェア (VMware vSphere クライアントまたは Microsoft Hyper-V Manager) を使用して表示されるものと同じであることを確認します。 Storage Gateway 同じでない場合、「ゲートウェイ VM のシャットダウン」に示すように Storage Gateway コンソールからゲートウェイを再起動します。再起動後、Storage Gateway コンソールの [Gateway] (ゲートウェイ) タブにある [IP Addresses] (IP アドレス) リスト内のアドレスは、ゲートウェイの IP アドレスと一致するはずです。ゲートウェイの IP アドレスはハイパーバイザークライアントから判断します。
	  • VMware の場合ESXi、VM の IP アドレスは、概要タブの vSphere クライアントにあります。
	  • Microsoft Hyper-V の場合、VM の IP アドレスはローカルコンソールにログインすると見つかります。
	• 「」の説明 AWS に従って、ゲートウェイの への接続を確認しますゲートウェイのインターネット接続のテスト。
	• ゲートウェイのネットワークアダプタ設定を確認し、ゲートウェイに対して有効にする予定のすべてのインターフェイスが有効になっていることを確認します。ゲートウェイのネットワークアダプタ設定を表示するには、「ゲートウェイのネットワークの設定」の指示に従い、ゲートウェイのネットワーク設定を表示するためのオプションを選択します。
	
	Amazon CloudWatch コンソールからゲートウェイとの間のスループットを表示できます。ゲートウェイと との間のスループットの測定の詳細については AWS、「」を参照してくださいゲートウェイと AWSの間のパフォーマンスの測定。

Microsoft Hyper-V への Storage Gateway のインポート (デプロイ) に問題がある。	「Microsoft Hyper-V セットアップのトラブルシューティング」を参照してください。ここでは、Microsoft Hyper-V でゲートウェイをデプロイするための一般的な問題を説明しています。

問題	実行するアクション
「ゲートウェイのボリュームに書き込まれたデータが AWS内に安全に保存されていません」というメッセージを受信する。	このメッセージを受信するのは、ゲートウェイ VM が別のゲートウェイ VM のクローンまたはスナップショットから作成された場合です。そうでない場合は、 AWS Supportにお問い合わせください。

AWS Support オンプレミスでホストされているゲートウェイのトラブルシューティングに役立つ の許可

Storage Gateway には、ゲートウェイの問題のトラブルシューティングに役立つゲートウェイへのアクセス AWS Support の有効化など、いくつかのメンテナンスタスクを実行するために使用できるローカルコンソールが用意されています。デフォルトでは、ゲートウェイ AWS Support へのアクセスは無効になっています。このアクセスは、ホストのローカルコンソールを通して有効にします。ゲートウェイ AWS Support へのアクセスを許可するには、まずホストのローカルコンソールにログインし、Storage Gateway のコンソールに移動してから、サポートサーバーに接続します。

ゲートウェイ AWS Supportへのアクセスを許可するには

1. ホストのローカルコンソールにログインします。
   - VMware ESXi – 詳細については、「」を参照してください[を使用したゲートウェイローカルコンソールへのアクセス VMware ESXi]。
   - Microsoft Hyper-V – 詳細については、「[Microsoft Hyper-V でゲートウェイのローカルコンソールにアクセスする]」を参照してください。
2. プロンプトで、対応する番号を入力して [ゲートウェイコンソール] を選択します。
3. 「**h**」と入力して、利用可能なコマンドのリストを開きます。
4. 次のいずれかを行います。
   - ゲートウェイがパブリックエンドポイントを使用している場合は、AVAILABLECOMMANDSウィンドウで「」と入力**`open-support-channel`**して、Storage Gateway のカスタマーサポートに接続します。TCP ポート 22 を許可して、 へのサポートチャネルを開くことができます AWS。カスタマーサポートに接続する際、Storage Gateway はサポート番号を割り当てます。サポート番号を書き留めます。

- ゲートウェイがVPCエンドポイントを使用している場合は、AVAILABLECOMMANDSウィンドウで「」と入力します**`open-support-channel`**。ゲートウェイがアクティブ化されていない場合は、VPCエンドポイントまたは IP アドレスを指定して、Storage Gateway のカスタマーサポートに接続します。TCP ポート 22 を許可して、 へのサポートチャネルを開くことができます AWS。カスタマーサポートに接続する際、Storage Gateway はサポート番号を割り当てます。サポート番号を書き留めます。

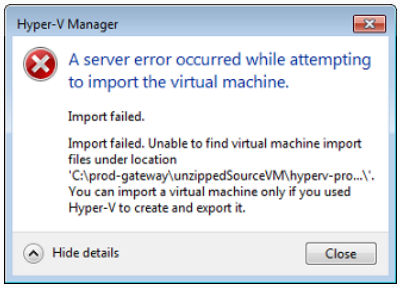
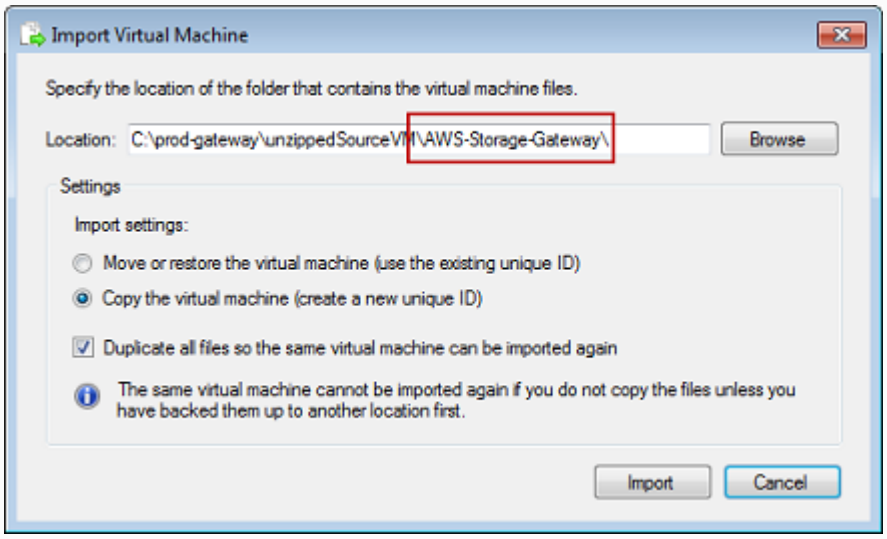
> **Note**
>
> チャンネル番号が Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ポート番号ではありません。代わりに、ゲートウェイは Storage Gateway サーバーへの Secure Shell (SSH) (TCP 22) 接続を行い、接続のサポートチャネルを提供します。

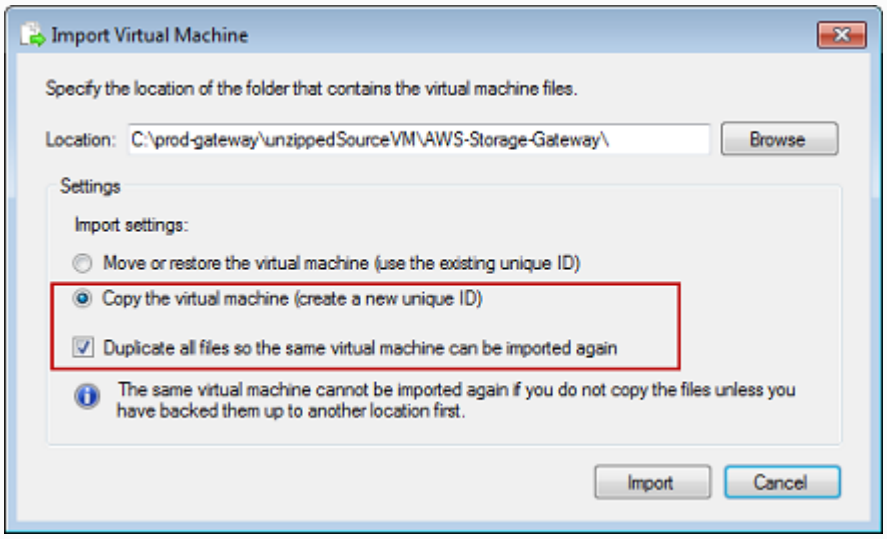
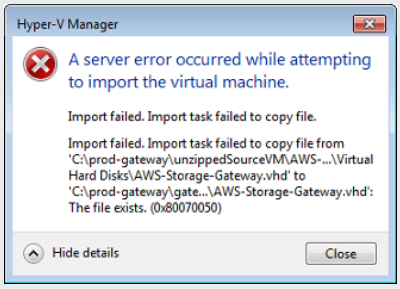
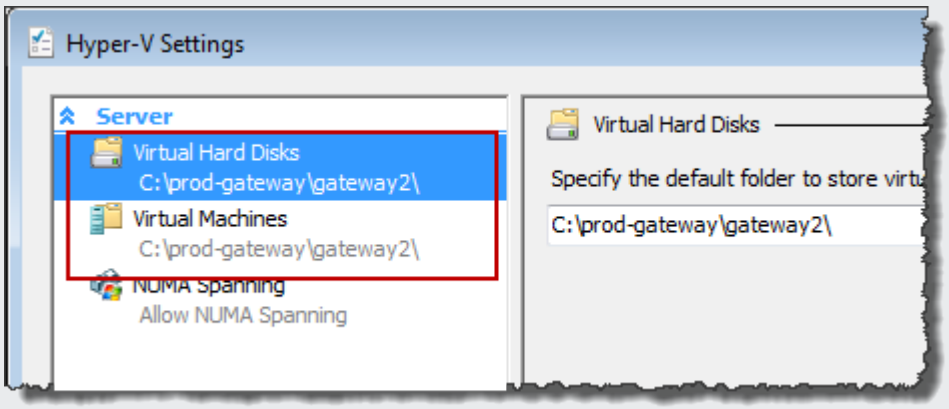
5. サポートチャネルが確立されたら、 にサポートサービス番号を提供して AWS Support 、 がトラブルシューティングのサポートを提供 AWS Support できるようにします。
6. サポートセッションが完了したら、「**`q`**」と入力してセッションを終了します。サポートセッションが完了したことを Amazon Web Services サポートが通知するまでは、セッションを終了しないようにします。
7. 「**`exit`**」と入力して、ゲートウェイコンソールからログアウトします。
8. プロンプトに従ってローカルコンソールを終了します。

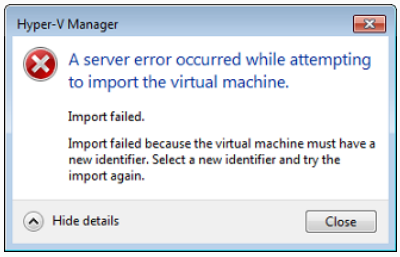
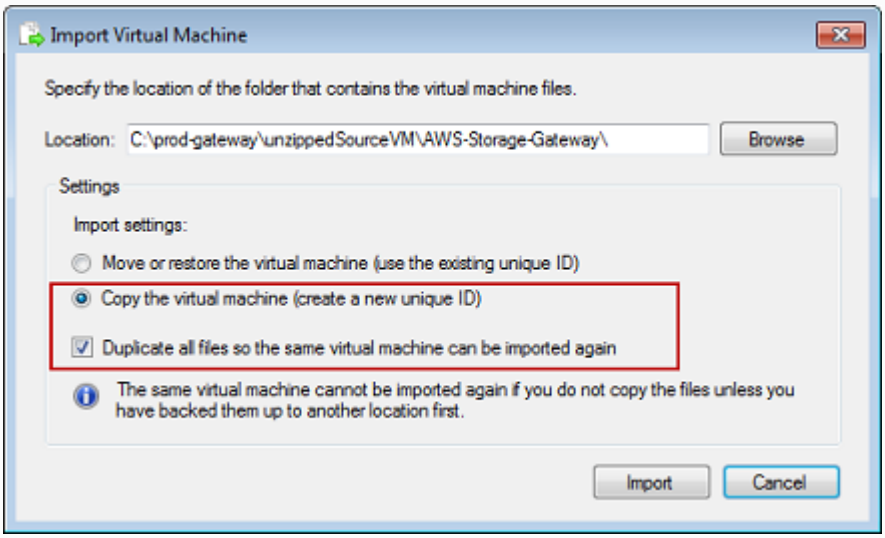
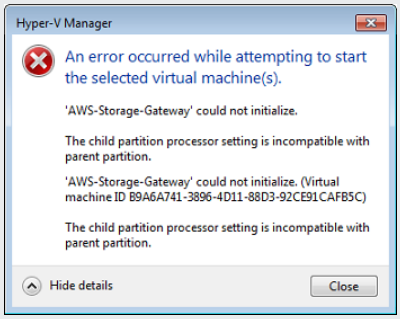
Microsoft Hyper-V セットアップのトラブルシューティング

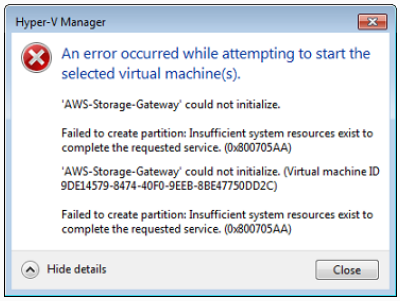
次の表は、Microsoft Hyper-V プラットフォームに Storage Gateway をデプロイする際に発生する可能性がある一般的な問題の一覧です。

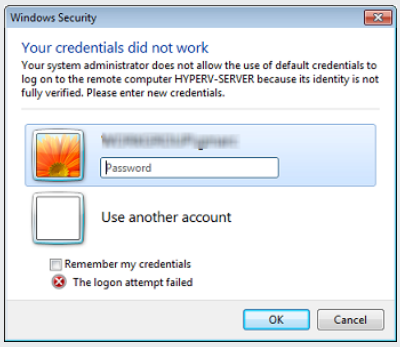
問題	実行するアクション
ゲートウェイをインポートしようとすると、「インポートに失敗しました。場所 ... では、仮想マシンのインポートファイルが見つかりません。」という工	このエラーは、次の原因で発生することがあります。 • 解凍されていないゲートウェイソースファイルのルートをポイントしている場合。[Import Virtual Machine] ダイアログボックスで指定した場所の最後のパートは、次の例が示すように、`AWS-Storage-Gateway` となっている必要があります。

問題	実行するアクション
ラーメッセージが表示されます。  	 • ゲートウェイを既にデプロイしていて、[Import Virtual Machine] (仮想マシンのインポート) ダイアログボックスで、[Copy the virtual machine] (仮想マシンのコピー) オプションを選択していなかったか、[Duplicate all files] (すべてのファイルを複製する) オプションをオンにしていなかった場合、解凍したゲートウェイファイルがある場所に仮想マシンが作成されていて、この場所から再度インポートすることはできません。この問題を解決するには、未解凍のゲートウェイソースファイルの最新コピーを入手して、新しい場所にコピーします。インポートのソースとして新しい場所を使用します。次の例は、未解凍ソースファイルが置かれている 1 つの場所から複数のゲートウェイを作成する場合にオンにすべきオプションを示しています。

問題	実行するアクション
	
ゲートウェイをインポートしようとすると、「インポートに失敗しました。ファイルをコピーできませんでした。」というエラーメッセージが表示されます。 	既にゲートウェイをデプロイしていて、仮想ハードディスクファイルと仮想マシン構成ファイルを保存するデフォルトのフォルダを再利用しようとすると、このエラーが発生します。この問題を解決するには、[Hyper-V Settings] ダイアログボックスで新しい場所を指定します。 

問題	実行するアクション
ゲートウェイをインポートしようとすると、「インポートできませんでした。仮想マシンに新しい識別子が必要です。新しい識別子を選択して、インポートを再試行してください。」というエラーメッセージが表示されます。 	ゲートウェイをインポートするときは、[Import Virtual Machine] (仮想マシンのインポート) ダイアログボックスで、[Copy the virtual machine] (仮想マシンのコピー) オプションを選択し、[Duplicate all files] (すべてのファイルを複製する) オプションをオンにしていることを確認して、VM の新しい一意の ID を作成します。次の例は、使用する必要がある [Import Virtual Machine] ダイアログボックスのオプションを示しています。 
ゲートウェイ VM を起動しようとすると、「子パーティションのプロセッサの設定が親パーティションと互換性がありません。」というエラーメッセージが表示されます。 	このエラーは通常、ゲートウェイで必要とされる CPU と、ホストで使用可能な CPU の不一致が原因で発生します。VM の CPU 数が、基本ハイパーバイザーでサポートされていることを確認します。 Storage Gateway の要件の詳細については、「Volume Gateway の設定要件」を参照してください。

問題	実行するアクション
ゲートウェイ VM を起動しようとすると、「パーティションを作成できませんでした。要求されたサービスを完了するには、リソースが不十分です。」というエラーメッセージが表示されます。 	このエラーは通常、ゲートウェイで必要とされる RAM と、ホストで使用可能な RAM の不一致が原因で発生します。 Storage Gateway の要件の詳細については、「Volume Gateway の設定要件」を参照してください。
スナップショットとゲートウェイソフトウェアのアップデートが、予想とわずかに異なる時刻に発生します。	ゲートウェイの VM のクロックが実際の時刻からずれている可能性があります (クロックドリフトと呼ばれています)。ローカルゲートウェイコンソールの時刻同期オプションを使って、VM の時刻を確認して修正します。詳細については、「ゲートウェイ VM の時刻の同期」を参照してください。
解凍済みの Microsoft Hyper-V Storage Gateway ファイルを、ホストファイルシステムに保存する必要があります。	一般的な Microsoft Windows サーバーと同じようにホストにアクセスします。たとえば、ハイパーバイザーホストの名前が `hyperv-server` の場合、UNC パス `\\hyperv-server\c$` という UNC パスを使用できます。このパスは `hyperv-server` という名前が解決可能であるか、あるいはローカルホストファイルで定義されていることを前提としています。

問題	実行するアクション
ハイパーバイザーへの接続時に、認証情報の入力を求められます。 	Sconfig.cmd ツールを使って、ハイパーバイザーホストのローカル管理者として、自分のユーザー認証情報を追加します。
Broadcom ネットワークアダプタを使用する Hyper-V ホストで仮想マシンキュー (VMQ) を有効にすると、ネットワークパフォーマンスが低下することがあります。	回避策については、Microsoft のドキュメント「VMQが有効になっている場合、Windows Server 2012 Hyper-V ホスト上の仮想マシンのネットワークパフォーマンスが低下する」を参照してください。

Amazon EC2ゲートウェイの問題のトラブルシューティング

以下のセクションでは、Amazon にデプロイされたゲートウェイで発生する可能性がある一般的な問題について説明しますEC2。オンプレミスゲートウェイと Amazon にデプロイされたゲートウェイの違いの詳細についてはEC2、「」を参照してくださいAmazon EC2インスタンスをデプロイしてボリュームゲートウェイをホストする。

トピック

- 少し時間が経ってもゲートウェイのアクティベーションが実行されない
- インスタンスリストにEC2ゲートウェイインスタンスが見つからない
- Amazon EBSボリュームを作成しましたが、EC2ゲートウェイインスタンスにアタッチできません
- EC2 ゲートウェイのボリュームターゲットにイニシエータをアタッチできない
- ストレージボリュームを追加するときに利用可能なディスクがないというメッセージが表示される

- アップロードバッファ領域を削減するために、アップロードバッファ領域として割り当てられたディスクを削除したい
- EC2 ゲートウェイとの間のスループットがゼロに低下する
- EC2 ゲートウェイ AWS Support のトラブルシューティングを支援したい
- Amazon EC2シリアルコンソールを使用してゲートウェイインスタンスに接続する場合

少し時間が経ってもゲートウェイのアクティベーションが実行されない

Amazon EC2コンソールで以下を確認します。

- インスタンスに関連付けられているセキュリティグループでポート 80 が有効になっています。セキュリティグループルールの追加の詳細については、「Amazon ユーザーガイド」の「セキュリティグループルールの追加」を参照してください。 EC2
- ゲートウェイインスタンスに実行中の印が付いています。Amazon EC2コンソールでは、インスタンスの状態値は である必要がありますRUNNING。
- 「」で説明されているように、Amazon EC2インスタンスタイプが最小要件を満たしていることを確認しますストレージの要件。

問題を修正したら、ゲートウェイを再度アクティブ化してみてください。これを行うには、Storage Gateway コンソールを開き、Amazon に新しいゲートウェイをデプロイEC2を選択し、インスタンスの IP アドレスを再入力します。

インスタンスリストにEC2ゲートウェイインスタンスが見つからない

インスタンスにリソースタグを指定せずに多くのインスタンスを実行中の場合は、起動したインスタンスの判断が困難になることがあります。この場合、ゲートウェイインスタンスを見つけるために、次のアクションを実行できます。

- インスタンスの説明タブで Amazon マシンイメージ (AMI) の名前を確認します。Storage Gateway に基づくインスタンスは、テキスト で始まるAMI必要がありますaws-storage-gateway-ami。
- Storage Gateway に基づいて複数のインスタンスがある場合はAMI、インスタンスの起動時間をチェックして正しいインスタンスを見つけます。

Amazon EBSボリュームを作成しましたが、EC2ゲートウェイインスタンスにアタッチできません

対象の Amazon EBSボリュームがゲートウェイインスタンスと同じアベイラビリティーゾーンにあることを確認します。アベイラビリティーゾーンに不一致がある場合は、インスタンスと同じアベイラビリティーゾーンに新しい Amazon EBSボリュームを作成します。

EC2 ゲートウェイのボリュームターゲットにイニシエータをアタッチできない

インスタンスを起動したセキュリティグループに、iSCSI アクセスに使用しているポートを許可するルールが含まれていることを確認します。通常、ポートは 3260 に設定されています。ボリュームへの接続の詳細については、「ボリュームの Windows クライアントへの接続」を参照してください。

ストレージボリュームを追加するときに利用可能なディスクがないというメッセージが表示される

新しくアクティベートしたゲートウェイには、ボリュームストレージが定義されていません。ボリュームストレージを定義するには、アップロードバッファおよびキャッシュストレージとして使用するために、先にゲートウェイにローカルディスクを割り当てる必要があります。Amazon にデプロイされたゲートウェイの場合EC2、ローカルディスクはインスタンスにアタッチされた Amazon EBSボリュームです。このエラーメッセージは、インスタンスに Amazon EBSボリュームが定義されていないために発生する可能性があります。

ゲートウェイを実行しているインスタンスに定義されているブロックデバイスを確認します。ブロックデバイス (に付属するデフォルトデバイスAMI) が 2 つしかない場合は、ストレージを追加する必要があります。その設定方法の詳細については、「Amazon EC2インスタンスをデプロイしてボリュームゲートウェイをホストする」を参照してください。2 つ以上の Amazon EBSボリュームをアタッチしたら、ゲートウェイでボリュームストレージを作成してみてください。

アップロードバッファ領域を削減するために、アップロードバッファ領域として割り当てられたディスクを削除したい

「割り当てるアップロードバッファのサイズの決定」の手順を実行します。

EC2 ゲートウェイとの間のスループットがゼロに低下する

ゲートウェイインスタンスが実行中であることを確認します。たとえば、再起動に起因してインスタンスが起動中の場合、インスタンスが再開するのを待ちます。

また、ゲートウェイ IP が変更されていないことを確認します。インスタンスを停止し、再開した場合、インスタンスの IP アドレスが変わっている可能性があります。その場合、新しいゲートウェイをアクティブ化する必要があります。

Amazon CloudWatch コンソールからゲートウェイとの間のスループットを表示できます。ゲートウェイと との間のスループットの測定の詳細については AWS、「」を参照してくださいゲートウェイと AWSの間のパフォーマンスの測定。

EC2 ゲートウェイ AWS Support のトラブルシューティングを支援したい

Storage Gateway には、ゲートウェイの問題のトラブルシューティングに役立つゲートウェイへのアクセス AWS Support の有効化など、いくつかのメンテナンスタスクの実行に使用できるローカルコンソールが用意されています。デフォルトでは、ゲートウェイ AWS Support へのアクセスは無効になっています。このアクセスは、Amazon EC2ローカルコンソールから提供します。Secure Shell () を使用して Amazon EC2ローカルコンソールにログインしますSSH。経由で正常にログインするにはSSH、インスタンスのセキュリティグループにTCPポート 22 を開くルールが必要です。

> **Note**
>
> 既存のセキュリティグループに新しいルールを追加すると、新しいルールが、そのセキュリティグループを使用するすべてのインスタンスに適用されます。セキュリティグループとセキュリティグループルールを追加する方法の詳細については、「Amazon ユーザーガイド」の「Amazon EC2 セキュリティグループ」を参照してください。 EC2

がゲートウェイ AWS Support に接続できるようにするには、まず Amazon EC2インスタンスのローカルコンソールにログインし、Storage Gateway のコンソールに移動して、アクセスを提供します。

Amazon EC2インスタンスにデプロイされたゲートウェイ AWS Support へのアクセスを有効にするには

1. Amazon EC2インスタンスのローカルコンソールにログインします。手順については、「Amazon EC2 ユーザーガイド」の「インスタンスへの接続」を参照してください。

   次のコマンドを使用して、EC2インスタンスのローカルコンソールにログインできます。

```
ssh -i PRIVATE-KEY admin@INSTANCE-PUBLIC-DNS-NAME
```

> **Note**
>
> - *PRIVATE-KEY* は、Amazon EC2インスタンスの起動に使用したEC2キーペアのプライベート証明書を含む.pemファイルです。詳細については、「Amazon ユーザーガイド」の「キーペアのパブリックキーの取得」を参照してください。 EC2
> - *INSTANCE-PUBLIC-DNS-NAME* は、ゲートウェイが実行されている Amazon EC2インスタンスのパブリックドメインネームシステム (DNS) 名です。このパブリックDNS名を取得するには、EC2コンソールで Amazon EC2インスタンスを選択し、説明タブをクリックします。

2. プロンプトで「**6 - Command Prompt**」と入力して、 AWS Support Channel コンソールを開きます。
3. **h** を入力してAVAILABLECOMMANDSウィンドウを開きます。
4. 次のいずれかを行います。

   - ゲートウェイがパブリックエンドポイントを使用している場合は、AVAILABLECOMMANDSウィンドウで「」と入力**open-support-channel**して、Storage Gateway のカスタマーサポートに接続します。TCP ポート 22 を許可して、 へのサポートチャネルを開くことができます AWS。カスタマーサポートに接続する際、Storage Gateway はサポート番号を割り当てます。サポート番号を書き留めます。
   - ゲートウェイがVPCエンドポイントを使用している場合は、AVAILABLECOMMANDSウィンドウで「」と入力します**open-support-channel**。ゲートウェイがアクティブ化されていない場合は、VPCエンドポイントまたは IP アドレスを指定して、Storage Gateway のカスタマーサポートに接続します。TCP ポート 22 を許可して、 へのサポートチャネルを開くことができます AWS。カスタマーサポートに接続する際、Storage Gateway はサポート番号を割り当てます。サポート番号を書き留めます。

> **Note**
>
> チャンネル番号が Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ポート番号ではありません。代わりに、ゲートウェイは Storage Gateway サーバーへの Secure Shell (SSH) (TCP 22) 接続を行い、接続のサポートチャネルを提供します。

5. サポートチャネルが確立されたら、 にサポートサービス番号を提供して AWS Support 、 がトラブルシューティングのサポートを提供 AWS Support できるようにします。
6. サポートセッションが完了したら、「**q**」と入力してセッションを終了します。サポートセッションが完了したことが AWS Support 通知されるまで、セッションを閉じないでください。
7. 「**exit**」と入力して、Storage Gateway コンソールを終了します。
8. コンソールメニューに従って Storage Gateway インスタンスからログアウトします。

Amazon EC2シリアルコンソールを使用してゲートウェイインスタンスに接続する場合

Amazon EC2シリアルコンソールを使用して、起動、ネットワーク設定、その他の問題のトラブルシューティングを行うことができます。手順とトラブルシューティングのヒントについては、「Amazon Elastic Compute Cloud ユーザーガイド」の「Amazon EC2シリアルコンソール」を参照してください。

ハードウェアアプライアンスの問題のトラブルシューティング

以下のトピックでは、Storage Gateway Hardware Appliance を使用する際に発生する可能性がある問題と、そのトラブルシューティング対策を示します。

サービスの IP アドレスを特定できない

サービスに接続するときは、ホストの IP アドレスではなく、サービスの IP アドレスを使用していることを確認します。サービスのコンソールでサービスの IP アドレスを設定し、ハードウェアコンソールでホストの IP アドレスを設定します。ハードウェアコンソールは、ハードウェアアプライアンスを起動すると表示されます。ハードウェアコンソールからサービスコンソールにアクセスするには、[Open Service Console (サービスコンソールを開く)] を選択します。

ファクトリーリセットを実行するにはどうすればよいですか

アプライアンスでファクトリーリセットを実行する必要がある場合は、以下のサポートセクションの説明に従って、サポートについて Storage Gateway Hardware Appliance チームにお問い合わせください。

リモート再起動を実行するにはどうすればよいですか

アプライアンスのリモート再起動を実行する必要がある場合は、Dell iDRAC 管理インターフェイスを使用して再起動できます。詳細については、Dell Technologies ウェブサイトの「iDRAC9 Virtual Power cycle: Remotely power cycle Dell EMC PowerEdge Servers」を参照してください。 InfoHub

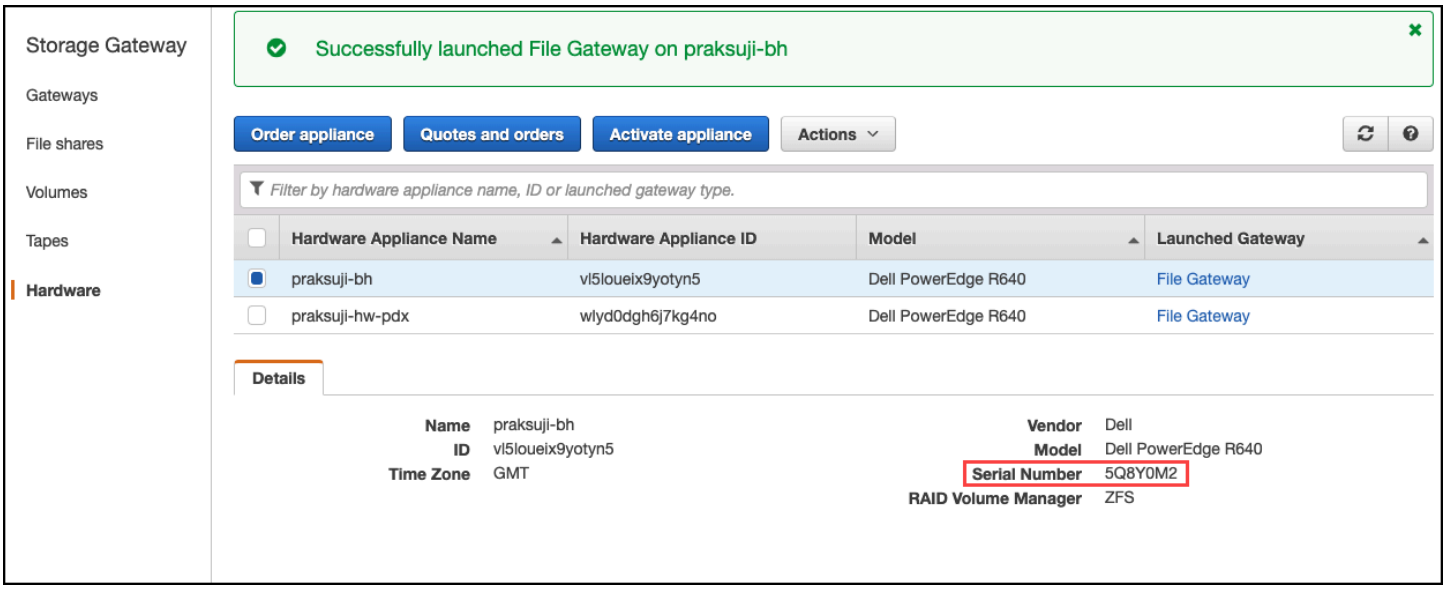
Dell iDRAC サポートはどこで入手できますか？

Dell PowerEdge R640 サーバーには、Dell iDRAC 管理インターフェイスが付属しています。次の構成を推奨します。

- iDRAC 管理インターフェイスを使用する場合は、デフォルトのパスワードを変更する必要があります。iDRAC 認証情報の詳細については、「Dell PowerEdge - i のデフォルトのサインイン認証情報は何ですかDRAC？」を参照してください。
- セキュリティ違反 up-to-date を防ぐため、ファームウェアが であることを確認してください。
- iDRAC ネットワークインターフェイスを通常の (em) ポートに移動すると、パフォーマンスの問題が発生したり、アプライアンスが正常に機能しなくなる可能性があります。

ハードウェアアプライアンスのシリアル番号が見つからない

ハードウェアアプライアンスのシリアル番号を確認するには、Storage Gateway コンソールの [ハードウェアアプライアンスの概要] ページに移動します (下図を参照)。
Storage Gateway コンソールの [ハードウェア] タブ。アプライアンスが選択され、詳細が表示されています。



Storage Gateway コンソールの [ハードウェア] タブ。アプライアンスが選択され、詳細が表示されています。

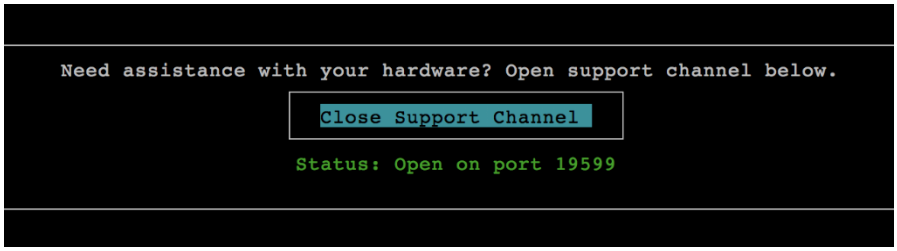
ハードウェアアプライアンスのサポートの依頼先

Storage Gateway Hardware Appliance のサポートへのお問い合わせについては、「AWS Support」を参照してください。

AWS Support チームは、ゲートウェイの問題をリモートでトラブルシューティングするために、サポートチャネルをアクティブ化するよう求める場合があります。このポートは、ゲートウェイの通常のオペレーションでは開いておく必要はありませんが、トラブルシューティングでは必要です。以下の手順に示すように、ハードウェアコンソールからサポートチャネルをアクティブ化することができます。

のサポートチャネルを開くには AWS

1. ハードウェアコンソールを開きます。
2. 次に示すように、[Open Support Channel (サポートチャネルを開く)] を選択します。
   ハードウェアアプライアンスコンソール。サポートチャネルのステータスが表示されています。

   ハードウェアアプライアンスコンソール。サポートチャネルのステータスが表示されています。

   ネットワーク接続やファイアウォールに問題がなければ、割り当てられたポート番号が 30 秒以内に表示されます。
3. ポート番号を書き留めて、 に渡します AWS Support。

ボリュームの問題のトラブルシューティング

このセクションでは、ボリュームを使用しているときに発生する可能性のある最も一般的な問題と、これらを修正する際に推奨されるアクションについて説明します。

トピック

- ボリュームが設定されていないとコンソールに表示される

- ボリュームは復旧不可能であるとコンソールに表示される
- ゲートウェイキャッシュ型が到達不可能なためデータを復旧する場合
- ボリュームのステータスが PASS THROUGH であるとコンソールに表示される
- ボリュームの整合性を確認し、エラーがある場合は修正する
- ボリュームの iSCSI ターゲットが Windows のディスク管理コンソールに表示されない
- ボリュームの iSCSI ターゲット名を変更したい
- スケジュールしたボリュームのスナップショットが実行されなかった
- 障害が発生したディスクの取り外しまたは交換が必要な場合
- アプリケーションからボリュームへのスループットがゼロに低下した
- ゲートウェイのキャッシュディスクでエラーが発生する
- ボリュームのスナップショットのステータスが予想以上に長い時間にわたって PENDING のままである
- 高可用性のヘルス通知

ボリュームが設定されていないとコンソールに表示される

Storage Gateway コンソールで、ボリュームのステータスが「UPLOAD BUFFER NOT CONFIGURED (アップロードバッファが構成されていません)」と表示されている場合は、アップロードバッファ容量をゲートウェイに追加します。ゲートウェイのアップロードバッファが設定されていない場合、ゲートウェイを使用してアプリケーションデータを格納することはできません。詳細については、「ゲートウェイ用のアップロードアップロードバッファまたはキャッシュストレージを追加して設定するには」を参照してください。

ボリュームは復旧不可能であるとコンソールに表示される

保管型ボリュームの場合、Storage Gateway コンソールにボリュームのステータスが「IRRECOVERABLE (回復不可能)」と表示されていたら、このボリュームはもう使用できません。Storage Gateway コンソールで、ボリュームの削除を試みることができます。ボリュームにデータがある場合は、新しいボリュームを作成するときに、最初にボリュームを作成するために使用された VM のローカルディスクに基づいて、データを復旧できます。新しいボリュームを作成するとき、[Preserve existing data] を選択します。ボリュームを作成する前に、必ずボリュームの保留スナップショットを削除してください。詳細については、「スナップショットの削除」を参照してください。Storage Gateway コンソールでボリュームを削除できない場合は、ボリュームに割り当てられ

ているディスクが VM から不適切に削除されたために、アプライアンスから削除できない可能性があります。

キャッシュ型ボリュームでは、Storage Gateway コンソールが示すボリュームのステータスが IRRECOVERABLE であれば、このボリュームはもう使用できません。ボリュームにデータがある場合、ボリュームのスナップショットを作成し、スナップショットからデータを回復したり、最後の復旧ポイントからボリュームをクローンしたりすることができます。データを復旧した後、こののボリュームは削除できます。詳細については、「ゲートウェイキャッシュ型が到達不可能なためデータを復旧する場合」を参照してください。

保存型ボリュームでは、回復不可能なボリュームの作成に使用されたディスクから新しいボリュームを作成できます。詳細については、「ボリュームの作成」を参照してください。ボリュームステータスについては、「ボリュームステータスと移行について」を参照してください。

ゲートウェイキャッシュ型が到達不可能なためデータを復旧する場合

ゲートウェイが到達不可能になった時は (シャットダウン時など)、ボリューム復旧ポイントからスナップショットを作成し、そのスナップショットを使用するか、または既存ボリュームの最後の復旧ポイントから新しいボリュームをクローンすることができます。ボリューム復旧ポイントからのクローンは、スナップショットを作成するよりも素早く経済的です。ボリュームのクローン作成に関する詳細については、「ボリュームをクローンする」を参照してください。

Storage Gateway には、キャッシュ型ボリュームゲートウェイアーキテクチャで各ボリュームの復旧ポイントが用意されています。ボリューム復旧ポイントとは、ボリュームのすべてのデータに整合性があり、そこからスナップショットを作成したり、ボリュームをクローンしたりできる時点です。

ボリュームのステータスが PASS THROUGH であるとコンソールに表示される

ボリュームのステータスが「PASSTHROUGH (パススルー)」であると Storage Gateway コンソールに表示されることがあります。ボリュームのステータスがパススルーとなる場合、複数の理由が考えられます。アクションが必要な理由と、そうでない理由があります。

たとえば、ゲートウェイのアップロードバッファ領域が完全に消費されているためボリュームのステータスが PASS THROUGH になっている場合には、アクションが必要です。アップロードバッファが過去に超過したかどうかを確認するには、Amazon CloudWatch コンソールで `UploadBufferPercentUsed`メトリクスを表示できます。詳細については、「」を参照してくださいアップロードバッファのモニタリング。アップロードバッファ領域を使い切ったためゲートウェイのステータスが PASS THROUGH になっている場合、ゲートウェイに追加のアップロードバッ

ファ領域を割り当てる必要があります。バッファ領域を追加すると、ボリュームのステータスが自動的に PASS THROUGH から BOOTSTRAPPING (ブートストラップ) に変わり、さらに AVAILABLE (使用可能) に変わります。ボリュームのステータスが BOOTSTRAPPING のとき、ゲートウェイはボリュームのディスクからデータを読み取り、このデータを Amazon S3 にアップロードして、必要に応じてキャッチアップします。ゲートウェイがキャッチアップを完了し、ボリュームデータを Amazon S3 に保存すると、ボリュームのステータスが AVAILABLE になり、スナップショットを再開できるようになります。ボリュームのステータスが PASS THROUGH または BOOTSTRAPPING になっても、ボリュームディスクとの間のデータの読み書きは続行できます。アップロードバッファ容量の追加に関する詳細については、割り当てるアップロードバッファのサイズの決定 を参照してください。

アップロードバッファを超過する前に、操作を行うには、ゲートウェイのアップロードバッファにしきい値アラームを設定できます。詳細については、「ゲートウェイのアップロードバッファの上限アラームを設定するには」を参照してください。

一方、たとえば、別のボリュームがブートストラップ中であるためブートストラップを待っているボリュームのステータスが PASS THROUGH である場合には、アクションは不要です。ゲートウェイはボリュームを 1 つずつ起動します。

まれに、PASS THROUGH ステータスにより、アップロードバッファに割り当てられているディスクに障害が発生したことが示されることがあります。その場合、ディスクを取り除く必要があります。詳細については、「ボリュームゲートウェイ」を参照してください。ボリュームステータスについては、「ボリュームステータスと移行について」を参照してください。

ボリュームの整合性を確認し、エラーがある場合は修正する

ゲートウェイが Microsoft Windows イニシエータを使用してそのボリュームに接続している場合は、Windows CHKDSK ユーティリティを使用して、ボリュームの整合性を確認し、ボリュームにエラーがある場合はエラーを修正できます。Windows では、ボリュームの破損が検出されたときに自動的に CHKDSK ツールを実行できます。または、ユーザー自身がこのツールを実行することもできます。

ボリュームの iSCSI ターゲットが Windows のディスク管理コンソールに表示されない

ボリュームの iSCSI ターゲットが Windows のディスク管理コンソールに表示されない場合は、ゲートウェイのアップロードバッファが設定されていることを確認します。詳細については、「ゲートウェイ用のアップロードアップロードバッファまたはキャッシュストレージを追加して設定するには」を参照してください。

ボリュームの iSCSI ターゲット名を変更したい

ボリュームの iSCSI ターゲット名を変更するには、そのボリュームを削除し、新しいターゲット名で再度追加する必要があります。この操作を行うと、ボリューム上のデータを保持できます。

スケジュールしたボリュームのスナップショットが実行されなかった

スケジュールしたボリュームのスナップショットが実行されなかった場合は、ボリュームのステータスがパススルーであるかどうか、またはスケジュールしたスナップショットの実行時刻の直前にゲートウェイのアップロードバッファが完全に消費されていたかどうかを確認します。Amazon CloudWatch コンソールでゲートウェイの `UploadBufferPercentUsed`メトリクスを確認し、このメトリクスのアラームを作成できます。詳細については、アップロードバッファのモニタリングおよびゲートウェイのアップロードバッファの上限アラームを設定するにはを参照してください。

障害が発生したディスクの取り外しまたは交換が必要な場合

障害が発生したボリュームディスクや、不要なボリュームを交換する必要がある場合は、まず Storage Gateway コンソールを使用してボリュームを削除する必要があります。詳細については、「ボリュームを削除するには」を参照してください。次に、ハイパーバイザークライアントを使用して、バックアップストレージを削除します。

- VMware ESXi の場合、ボリュームの削除 の説明に基づき、バックアップストレージを削除します。
- Microsoft Hyper-V の場合、バックアップストレージを削除します。

アプリケーションからボリュームへのスループットがゼロに低下した

アプリケーションからボリュームへのスループットがゼロに低下した場合は、以下を試してください。

- VMware vSphere クライアントを使用している場合は、ボリュームの [Host IP] アドレスが、vSphere クライアントの [Summary] タブに表示されるアドレスの 1 つと一致していることを確認します。ストレージボリュームの [Host IP] (ホスト IP) アドレスは、Storage Gateway コンソールのボリュームの [Details] (詳細) タブで確認できます。ゲートウェイに新しい静的 IP アドレスを割り当てたときなどは、IP アドレスに不一致が発生することがあります。不一致がある場合、「ゲートウェイ VM のシャットダウン」に示されているように、Storage Gateway コンソールからゲートウェイを再起動します。再起動後、[ISCSI Target Info] (ISCSI ターゲット情報) タブ

のストレージボリュームの [Host IP] (ホスト IP) アドレスは、ゲートウェイの [Summary] (概要) タブの vSphere クライアントに表示される IP アドレスと一致するはずです。

- ボリュームの [ホスト IP] ボックスに IP アドレスがなく、ゲートウェイがオンラインである場合。たとえば、2 つ以上のネットワークアダプタを備えたゲートウェイのネットワークアダプタの IP アドレスに関連付けられたボリュームを作成するときにこの状態が発生することがあります。ボリュームに関連付けられているネットワークアダプタを取り外すか無効にすると、IP アドレスが [ホスト IP] に表示されなくなる場合があります。この問題に対処するには、ボリュームを削除し、その既存のデータを保持したまま再度作成します。
- アプリケーションで使用する iSCSI イニシエータが現在、ストレージボリュームの iSCSI ターゲットにマッピングされていることを確認します。ストレージボリュームへの接続の詳細については、ボリュームの Windows クライアントへの接続 を参照してください。

ボリュームのスループットを表示し、Amazon CloudWatch コンソールからアラームを作成できます。アプリケーションからボリュームへのスループットの測定に関する詳細については、「アプリケーションとゲートウェイの間のパフォーマンスの測定」を参照してください。

ゲートウェイのキャッシュディスクでエラーが発生する

ゲートウェイの 1 つ以上のキャッシュディスクに障害が発生した場合、仮想テープとボリュームに対する読み取りおよび書き込みオペレーションがゲートウェイによって禁止されます。通常の機能を再開するには、次の手順に従ってゲートウェイを再設定します。

- キャッシュディスクにアクセスできない、または使用できない場合は、ゲートウェイ構成からディスクを削除します。
- キャッシュディスクがまだアクセス可能で使用可能な場合は、ゲートウェイに再接続します。

> **Note**
>
> キャッシュディスクを削除した場合、ゲートウェイが通常の機能を再開したとき、クリーンデータがあるテープまたはボリューム (キャッシュディスクと Amazon S3 とのデータが同期している場合) は引き続き使用できます。例えば、ゲートウェイに 3 つのキャッシュディスクがあり、2 つを削除した場合、クリーンであるテープまたはボリュームは AVAILABLE ステータスになります。他のテープおよびボリュームは、IRRECOVERABLE ステータスになります。
>
> ゲートウェイのキャッシュディスクとして工フェメラルディスクを使用したり、キャッシュディスクを工フェメラルドライブにマウントしたりすると、ゲートウェイのシャットダウン

時にキャッシュディスクが失われます。キャッシュディスクと Amazon S3 が同期していないときにゲートウェイをシャットダウンすると、データが失われる可能性があります。そのため、エフェメラルドライブやディスクを使用することは推奨されていません。

ボリュームのスナップショットのステータスが予想以上に長い時間にわたって PENDING のままである

ボリュームのスナップショットが予想以上に長い時間にわたって保留中状態のままである場合は、ゲートウェイ VM が予期せずクラッシュしたか、ボリュームのステータスがパススルーまたは回復不能に変わった可能性があります。これらのいずれかの場合、スナップショットのステータスは PENDING のままになり、スナップショットは正常に完了しません。この場合は、スナップショットを削除することをお勧めします。詳細については、「スナップショットの削除」を参照してください。

ボリュームのステータスが使用可能に戻ったら、ボリュームの新しいスナップショットを作成します。ボリュームステータスについては、「ボリュームステータスと移行について」を参照してください。

高可用性のヘルス通知

VMware vSphere High Availability (HA) プラットフォームでゲートウェイを実行すると、ヘルス通知が表示される場合があります。ヘルス通知の詳細については、「高可用性に関する問題のトラブルシューティング」を参照してください。

高可用性に関する問題のトラブルシューティング

可用性の問題が発生した場合の対処方法については、以下を参照してください。

トピック

- ヘルス通知
- メトリクス

ヘルス通知

VMware vSphere HA でゲートウェイを実行すると、すべてのゲートウェイが設定された Amazon CloudWatch ロググループに次のヘルス通知を生成します。これらの通知は、`AvailabilityMonitor` と呼ばれるログストリームに入ります。

トピック

通知: Reboot

ゲートウェイ VM の再起動時に、再起動通知が表示される場合があります。VM ハイパーバイザーの管理コンソールまたは Storage Gateway コンソールを使用して、ゲートウェイ VM を再起動できます。また、ゲートウェイのメンテナンスサイクル中にゲートウェイソフトウェアを使用して再起動することもできます。

実行するアクション

再起動の時間がゲートウェイで設定されたメンテナンス開始時間から 10 分以内である場合、これは通常の発生であり、問題の兆候ではありません。メンテナンス期間外に著しく再起動が発生した場合は、ゲートウェイを手動で再起動したかどうかを確認します。

通知: HardReboot

ゲートウェイ VM が予期せず再起動された場合、`HardReboot` 通知が表示されることがあります。このような再起動の原因としては、電源の喪失、ハードウェア障害、またはその他のイベントが考えられます。VMware ゲートウェイの場合、vSphere High Availability のアプリケーションの監視によるリセットにより、このイベントがトリガーされることがあります。

実行するアクション

ゲートウェイがこのような環境で実行されている場合は、`HealthCheckFailure` 通知の有無を確認し、VM の VMware イベントログを調べます。

通知: HealthCheckFailure

VMware vSphere HA のゲートウェイでは、ヘルスチェックが不合格になり、VM の再起動が要求されたときに `HealthCheckFailure` 通知が表示される場合があります。このイベントは、`AvailabilityMonitorTest` 通知によって示される可用性をモニタリングするためのテスト中にも発生します。この場合、`HealthCheckFailure` 通知の発生が想定されます。

> **Note**
>
> この通知は VMware ゲートウェイ専用です。

実行するアクション

`AvailabilityMonitorTest` 通知が表示されることなくこのイベントが繰り返し発生する場合は、VM インフラストラクチャに問題 (ストレージ、メモリなど) がないか確認してください。追加のサポートが必要な場合は、 にお問い合わせください AWS Support。

通知: AvailabilityMonitorTest

VMware vSphere HA のゲートウェイでは、VMware で可用性とアプリケーションのモニタリングシステムのテストを実行すると、`AvailabilityMonitorTest` 通知が表示されます。

メトリクス

`AvailabilityNotifications` メトリクスはすべてのゲートウェイで使用できます。このメトリクスは、ゲートウェイによって生成された可用性関連のヘルス通知の数です。Sum 統計情報を使用して、ゲートウェイで可用性関連のイベントが発生しているかどうかを調べます。イベントの詳細については、設定した CloudWatch ロググループにお問い合わせください。

データを復旧するためのベストプラクティス

まれに、ゲートウェイで回復不可能な障害が発生する場合があります。そのような障害は、仮想マシン (VM)、ゲートウェイ自体、ローカルストレージなどの場所で発生する可能性があります。障害が発生した場合、データの回復に関する以下の該当するセクションの手順に従うことをお勧めします。

> **Important**
>
> Storage Gateway では、ハイパーバイザーによって作成されたスナップショットから、または Amazon EC2 Amazon マシンイメージ (AMI) からのゲートウェイ VM の復元はサポートさ

れていません。ゲートウェイ VM が正しく機能しない場合、新しいゲートウェイをアクティブ化し、以下の手順を使用してデータをそのゲートウェイに復旧します。

トピック

予期しない仮想マシンのシャットダウンからの復旧

VM が予期せずにシャットダウンした場合 (停電時など)、ゲートウェイは到達不可能になります。電源とネットワーク接続が復旧されると、ゲートウェイは到達可能になり、通常の動作を開始します。データを回復するためにその時点で実行可能ないくつかのステップを以下に示します。

- 停止によりネットワーク接続の問題が発生した場合、問題をトラブルシューティングできます。ネットワーク接続をテストする方法については、「ゲートウェイのインターネット接続のテスト」を参照してください。
- キャッシュ型ボリュームの設定の場合、ゲートウェイが到達可能になると、ボリュームが BOOTSTRAPPING ステータスになります。この機能により、ローカルに保存されたデータが引き続き と同期されます AWS。このステータスの詳細については、「ボリュームステータスと移行について」を参照してください。
- ゲートウェイが正しく機能せず、予期しないシャットダウンの結果としてボリュームまたはテープに問題が発生した場合、データを回復できます。データの復旧方法については、シナリオに当てはまる以下のクションを参照してください。

正しく機能していないゲートウェイまたは VM からのデータの復旧

ゲートウェイまたは仮想マシンが正しく機能していない場合は、Amazon S3 内のボリュームにアップロード AWS されて保存されたデータを復元できます。キャッシュボリュームゲートウェイの場合、復旧スナップショットからデータを復旧します。保管型ボリュームゲートウェイの場合、ボ

リュームの最新の Amazon EBS スナップショットからデータを復元できます。テープゲートウェイの場合、復旧ポイントから新しいテープゲートウェイに 1 つ以上のテープを復旧します。

キャッシュ型ボリュームゲートウェイが到達不可能になった場合、以下のステップを使用して復旧スナップショットからデータを復旧できます。

1. で AWS Management Console、正しく機能していないゲートウェイを選択し、復旧するボリュームを選択し、そこから復旧スナップショットを作成します。
2. 新しいボリュームゲートウェイをデプロイしてアクティブ化します。または、正常に機能する既存のボリュームゲートウェイがある場合、そのゲートウェイを使用してボリュームデータを復旧できます。
3. 作成したスナップショットを見つけ、機能しているゲートウェイの新しいボリュームにスナップショットを復旧します。
4. オンプレミスのアプリケーションサーバーで、新しいボリュームを iSCSI デバイスとしてマウントします。

復旧スナップショットからキャッシュ型ボリュームデータを復旧する方法の詳細については、「ゲートウェイキャッシュ型が到達不可能なためデータを復旧する場合」を参照してください。

回復不可能なボリュームからのデータの復旧

ボリュームのステータスが IRRECOVERABLE の場合、このボリュームを使用することはできません。

保管型ボリュームでは、以下のステップを使用して、回復不可能なボリュームから新しいボリュームにデータを取得できます。

1. 回復不可能なボリュームの作成に使用されたディスクから新しいボリュームを作成します。
2. 新しいボリュームを作成するとき、既存のデータを保持します。
3. 回復不可能なボリュームの保留中のスナップショットジョブをすべて削除します。
4. ゲートウェイから回復不可能なボリュームを削除します。

キャッシュ型ボリュームについては、新しいボリュームのクローンには最後の復旧ポイントを使用することをお勧めします。

回復不可能なボリュームから新しいボリュームにデータを取得する方法の詳細については、「ボリュームは復旧不可能であるとコンソールに表示される」を参照してください。

正しく機能していないキャッシュディスクからのデータの復旧

キャッシュディスクで障害が発生した場合、以下のステップを使用し、状況に応じてデータを復旧することをお勧めします。

- キャッシュディスクがホストから削除されたために障害が発生した場合は、ゲートウェイをシャットダウンし、ディスクを再追加してゲートウェイを再起動します。
- キャッシュディスクが破損したかアクセスできない場合、ゲートウェイをシャットダウンしてキャッシュディスクをリセットし、キャッシュストレージ用にディスクを再設定してゲートウェイを再起動します。

破損したファイルシステムからのデータの復旧

ファイルシステムが破損した場合、**fsck** コマンドを使用してファイルシステムにエラーがないかチェックし、修復できます。ファイルシステムを修復できる場合、以下で説明するようにファイルシステムのそのボリュームからデータを復旧できます。

1. 仮想マシンをシャットダウンし、Storage Gateway マネジメントコンソールを使用して復旧スナップショットを作成します。このスナップショットは、 に保存されている最新のデータを表します AWS。

   > **Note**
   >
   > ファイルシステムを修復できない場合、またはスナップショットの作成プロセスが正常に完了しない場合は、フォールバックとしてこのスナップショットを使用します。

   復旧スナップショットの作成方法については、「ゲートウェイキャッシュ型が到達不可能なためデータを復旧する場合」を参照してください。
2. **fsck** コマンドを使用してファイルシステムにエラーがないかチェックし、修復を試みます。
3. ゲートウェイ VM を再起動します。
4. ハイパーバイザーホストが起動を開始したら、シフトキーを押したままにして grub ブートメニューを表示します。
5. メニューで、編集する [**e**] を押します。
6. カーネル行 (2 行目) を選択し、**e** を押して編集します。

7. カーネルコマンドラインに **init=/bin/bash** オプションを追加します。スペースを使用して、ここで追加したオプションと前のオプションを区切ります。
8. console= 行を両方とも削除し、= 記号に続く値をすべて (カンマで区切られた値も含めて) 削除します。
9. **Return** を押して変更を保存します。
10. **b** を押して、変更したカーネルオプションでコンピューターを起動します。コンピューターが起動して bash# プロンプトが表示されます。
11. 「**/sbin/fsck -f *dev/sda1***」と入力してプロンプトからこのコマンドを手動で実行し、ファイルシステムをチェックして修理します。/dev/sda1 パスに対してコマンドが機能しない場合は、**lsblk** を使用して / のルートファイルシステムデバイスを特定し、代わりにそのパスを使用できます。
12. ファイルシステムチェックと修復が完了したら、インスタンスを再起動します。grub の設定が元の値に戻り、ゲートウェアが通常どおり起動します。
13. 元のゲートウェイから作成されているスナップショットが完成するまで待ち、スナップショットデータを検証します。

元のボリュームをそのまま使い続けることも、復旧スナップショットまたは完成したスナップショットに基づく新しいボリュームを使用して新しいゲートウェイを作成することもできます。または、このボリュームから完成したスナップショットから新しいボリュームを作成することもできます。

アクセス不能なデータセンターからのデータの復旧

ゲートウェイまたはデータセンターが何らかの理由でアクセス不能である場合は、異なるデータセンターにある別のゲートウェイにデータを復元するか、Amazon EC2 インスタンスにホストされているゲートウェイに復元することができます。別のデータセンターへのアクセス権がない場合は、Amazon EC2 インスタンスにゲートウェイを作成することをお勧めします。手順は、データ復旧元のゲートウェイの種類によって異なります。

アクセス無効なデータセンターのボリュームゲートウェイからデータを復旧するには

1. Amazon EC2 ホストで新しいボリュームゲートウェイを作成してアクティブ化します。詳細については、「Amazon EC2インスタンスをデプロイしてボリュームゲートウェイをホストする」を参照してください。

> **Note**
>
> ゲートウェイ保管型ボリュームは Amazon EC2 インスタンスにホストすることはできません。

2. 新しいボリュームを作成し、ターゲットゲートウェイとして EC2 ゲートウェイを選択します。詳細については、「ボリュームの作成」を参照してください。

   復旧するボリュームの最新の復旧ポイントからの Amazon EBS スナップショットまたはクローンに基づいて新しいボリュームを作成します。

   ボリュームがスナップショットに基づいている場合、そのスナップショット ID を指定します。

   復旧ポイントからボリュームのクローンを作成する場合は、ソースボリュームを選択します。

Storage Gateway に関するその他のリソース

このセクションでは、ゲートウェイのセットアップや管理に役立つ AWS とサードパーティーのソフトウェア、ツール、リソース、および Storage Gateway のクォータについて説明します。

トピック

ゲートウェイ VM ホストのデプロイと設定

トピック

Storage Gateway VMwareの の設定

Storage Gateway VMware用に を設定するときは、VM 時間をホスト時間と同期させ、ストレージをプロビジョニングするときに準仮想化ディスクコントローラーを使用するように VM を設定し、ゲートウェイ VM をサポートするインフラストラクチャレイヤーの障害から保護します。

トピック

VM の時刻とホストの時刻の同期

ゲートウェイを正常にアクティブ化するには、VM の時刻をホストの時刻と同期し、ホストの時刻を正しく設定する必要があります。このセクションでは、最初に VM の時刻をホストの時刻に同期します。次に、ホスト時間を確認し、必要に応じてホスト時間を設定し、その時間を Network Time Protocol (NTP) サーバーに自動的に同期するようにホストを設定します。

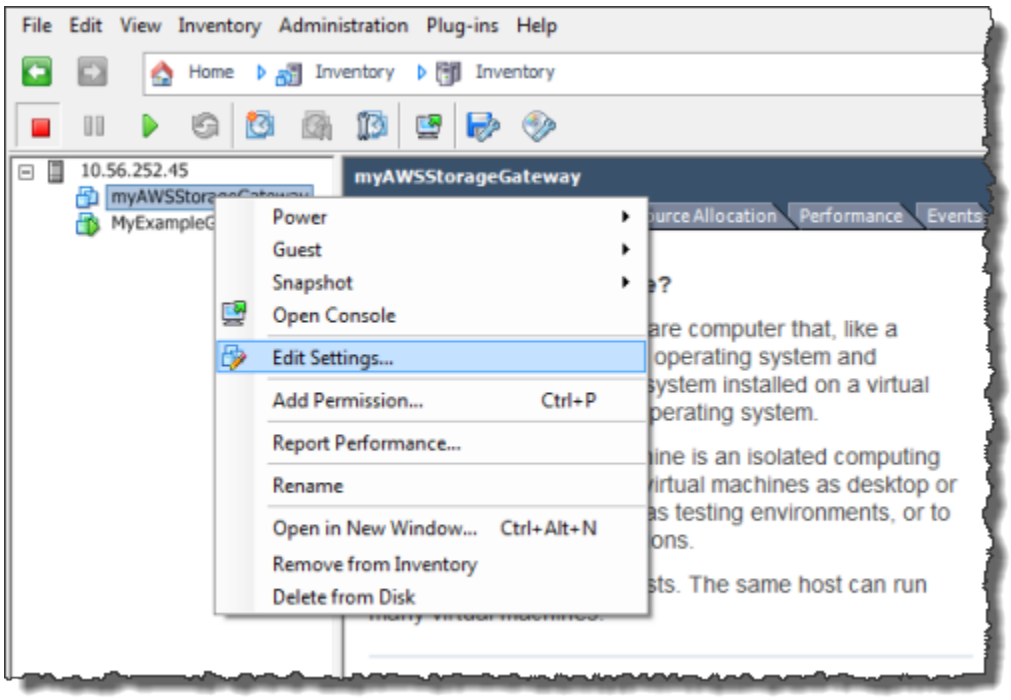
> **Important**
>
> ゲートウェイを正常にアクティブ化するには、VM の時刻とホストの時刻を同期する必要があります。

VM の時刻とホストの時刻を同期するには

1. VM の時刻を構成します。

   a. vSphere クライアントで、ゲートウェイ VM のコンテキスト (右クリック) メニューを開き、設定の編集 を選択します。

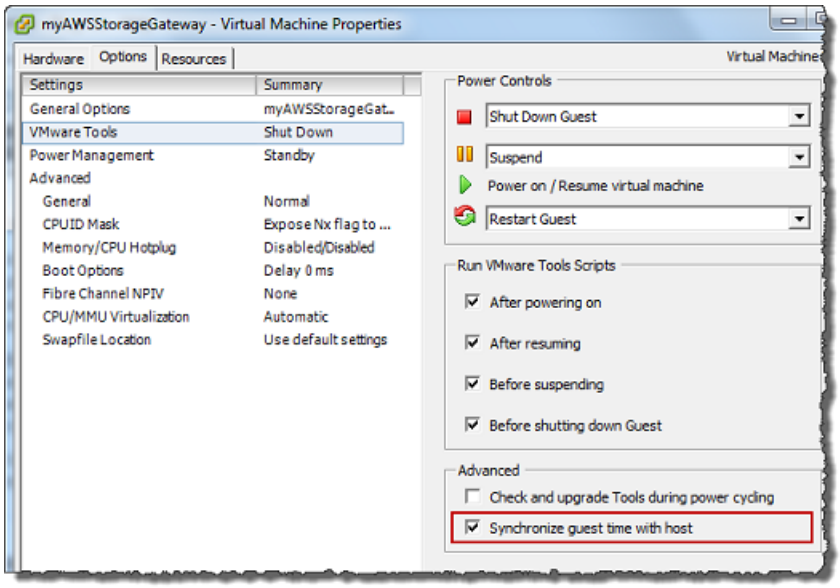
      [Virtual Machine Properties] ダイアログボックスが開きます。



b. オプションタブを選択し、オプションリストでVMwareツールを選択します。

c. [Synchronize guest time with host] オプションをチェックして、[OK] を選択します。

VM の時刻がホストと同期されます。



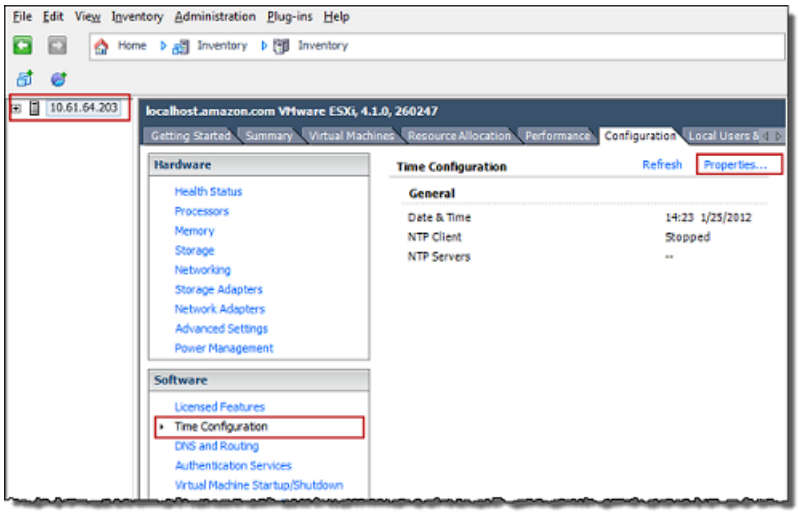
2. ホストの時刻を構成します。

ホストの時計が正しい時刻に設定されてかを確認するのは重要です。ホストクロックを設定していない場合は、次の手順を実行してホストクロックを設定して NTPサーバーと同期します。

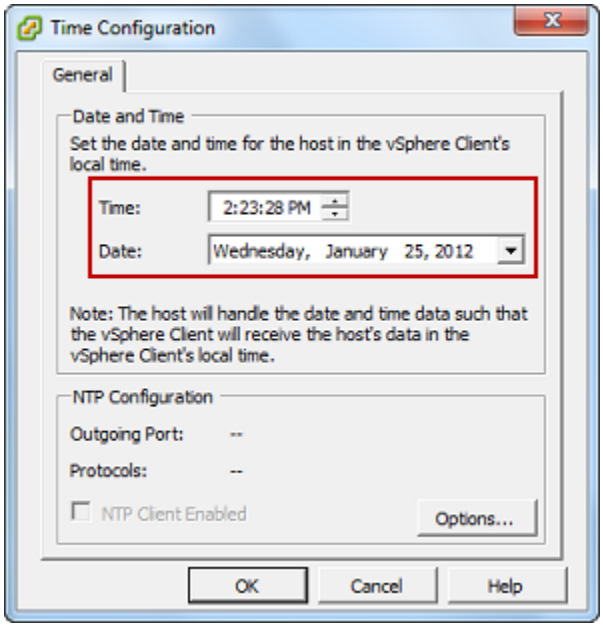
a. VMware vSphere クライアントで、左側のペインで vSphere ホストノードを選択し、設定タブを選択します。

b. [Software] (ソフトウェア) パネルで [Time Configuration] (時刻設定) を選択してから、[Properties] (プロパティ) リンクを選択します。

[Time Configuration] ダイアログボックスが表示されます。

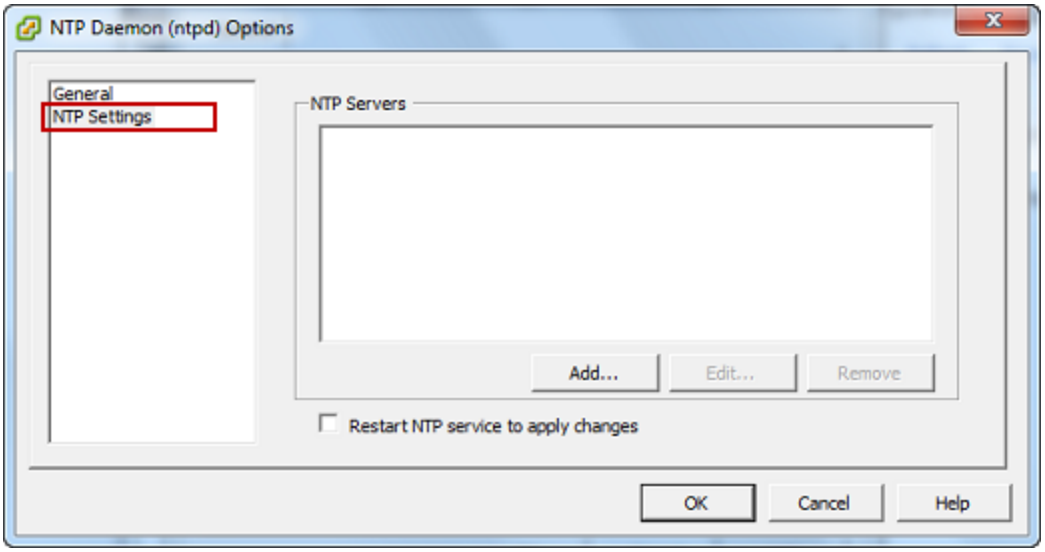


c. [Date and Time] パネルで、日付と時刻を設定します。



d. 時刻を NTPサーバーに自動的に同期するようにホストを設定します。

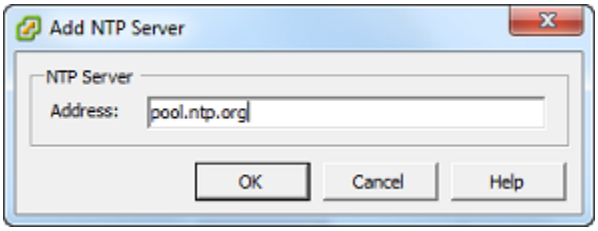
i. 「時間設定」ダイアログボックスで「オプション」を選択し、NTP「デーモン (ntpd) オプション」ダイアログボックスで、左側のペインでNTP「設定」を選択します。



ii. 追加 を選択して新しいNTPサーバーを追加します。

iii. NTP 「サーバーの追加」ダイアログボックスで、NTPサーバーの IP アドレスまたは完全修飾ドメイン名を入力し、「OK」を選択します。

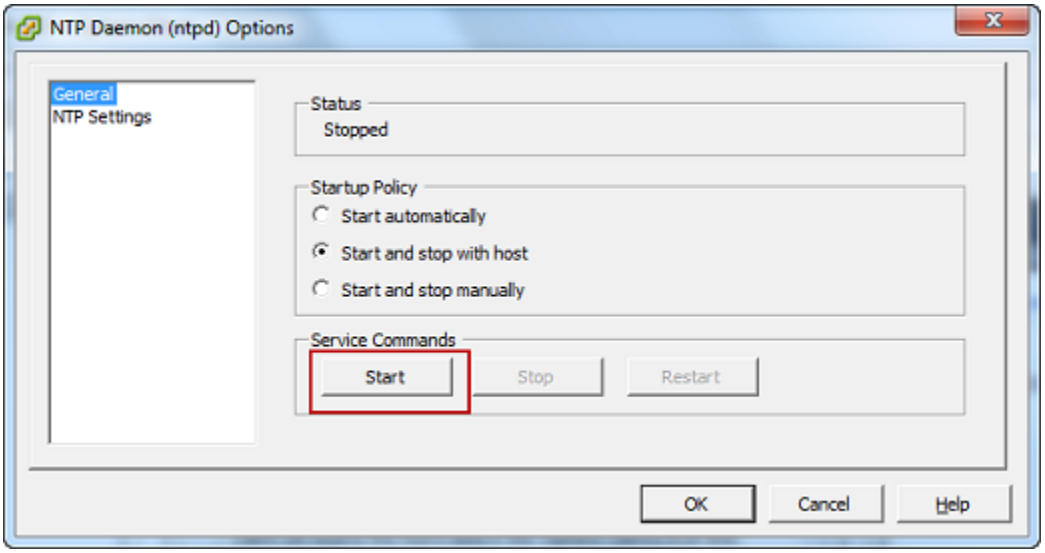
次の例のように、`pool.ntp.org` を使用することができます。



iv. NTP デーモン (ntpd) オプションダイアログボックスで、左側のペインで全般を選択します。

v. [Service Commands] ペインで、[Start] を選択してサービスを開始します。

このNTPサーバーリファレンスを変更するか、後で別のサーバーを追加する場合は、新しいサーバーを使用するにはサービスを再起動する必要があることに注意してください。



e. OK を選択してNTP、デーモン (ntpd) オプションダイアログボックスを閉じます。

f. [OK] を選択して [Time Configuration] ダイアログボックスを閉じます。

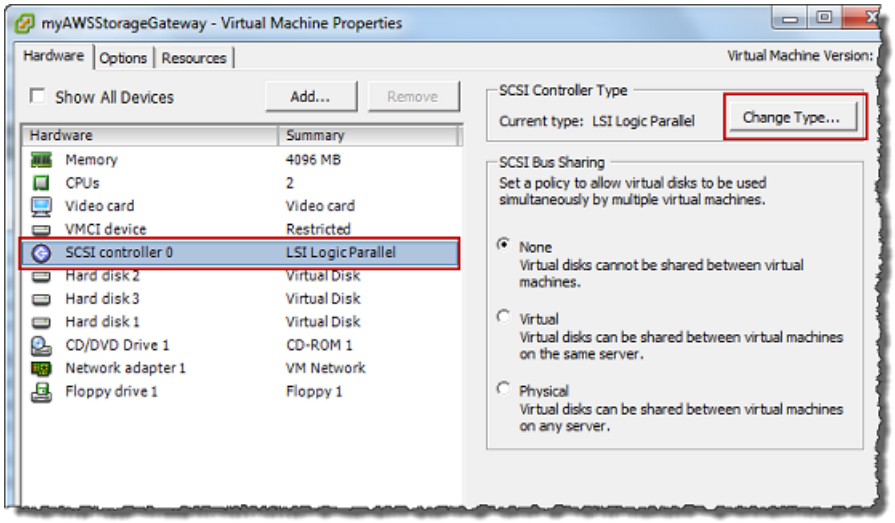
並列仮想化ディスクコントローラーを使用するように AWS Storage Gateway VM を設定する

このタスクでは、VM が準仮想化を使用するように iSCSI コントローラーを設定します。準仮想化は、ゲートウェイ VM がホストオペレーティングシステムと共同して、VM に追加される仮想ディスクをコンソールが識別できるようにするモードです。

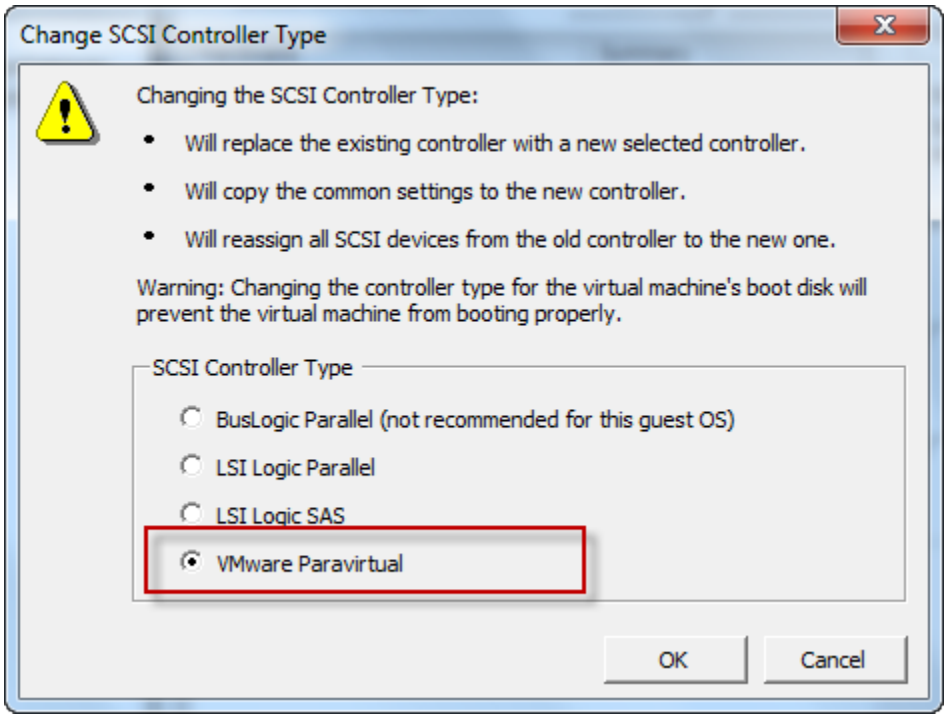
> **Note**
>
> ゲートウェイコンソールでこれらのディスクを設定するときに、ディスクの識別の問題を防ぐために、このステップを完了する必要があります。

準仮想化コントローラーを使用するように VM を構成するには

1. VMware vSphere クライアントで、ゲートウェイ VM のコンテキスト (右クリック) メニューを開き、設定の編集 を選択します。
2. 仮想マシンのプロパティダイアログボックスで、ハードウェアタブを選択し、SCSIコントローラー 0 を選択し、タイプ の変更を選択します。



3. SCSI「コントローラータイプの変更」ダイアログボックスでVMware、「準仮想化コントローラータイプ」を選択し、「OK」を選択します。 SCSI



高可用性での Storage Gateway VMware の使用

VMware 高可用性 (HA) は、ゲートウェイ VM をサポートするインフラストラクチャレイヤーの障害から保護 vSphere できる のコンポーネントです。VMware HA は、クラスターとして設定された複数のホストを使用してこれを行い、ゲートウェイ VM を実行しているホストが失敗した場合、クラスター内の別のホストでゲートウェイ VM を自動的に再起動できるようにします。VMware HA の詳

細については、 VMwareウェブサイトのVMware vSphere 「高可用性クラスターのベストプラクティス」を参照してください。

VMware HA で Storage Gateway を使用するには、次の操作を行うことをお勧めします。

- Storage Gateway VM を含むVMwareESX.ovaダウンロード可能なパッケージをクラスター内の 1 つのホストにのみデプロイします。
- .ova パッケージをデプロイする場合は、1 つのホストだけにローカルではないデータストアを選択してください。代わりに、クラスターのすべてのホストにアクセスできるデータストアを使用します。1 つのホストだけにローカルなデータストアを選択し、そのホストに障害が発生した場合、データソースはクラスター内の他のホストからアクセスできない可能性があります。また、他のホストへのフェイルオーバーが成功しない可能性があります。
- フェイルオーバー中にイニシエータがストレージボリュームターゲットから切断されないようにするには、オペレーティングシステムの推奨 iSCSI 設定に従ってください。フェイルオーバーが発生した場合、ゲートウェイ VM がフェイルオーバークラスター内の新しいホストで開始するまで、数秒から数分かかることがあります。Windows クライアントと Linux クライアントの両方で推奨される iSCSI タイムアウトは、フェイルオーバーが発生するのにかかる一般的な時間よりも長くなります。Windows クライアントのタイムアウト設定のカスタマイズに関する詳細については、「Windows iSCSI 設定のカスタマイズ」を参照してください。Linux クライアントのタイムアウト設定のカスタマイズに関する詳細については、「Linux iSCSI 設定のカスタマイズ」を参照してください。
- クラスタリングを利用して .ova パッケージをクラスターにデプロイした場合、プロンプトが表示されたら、ホストを選択します。その他の方法として、クラスター内のホストに直接デプロイすることもできます。

ゲートウェイ VM の時刻の同期

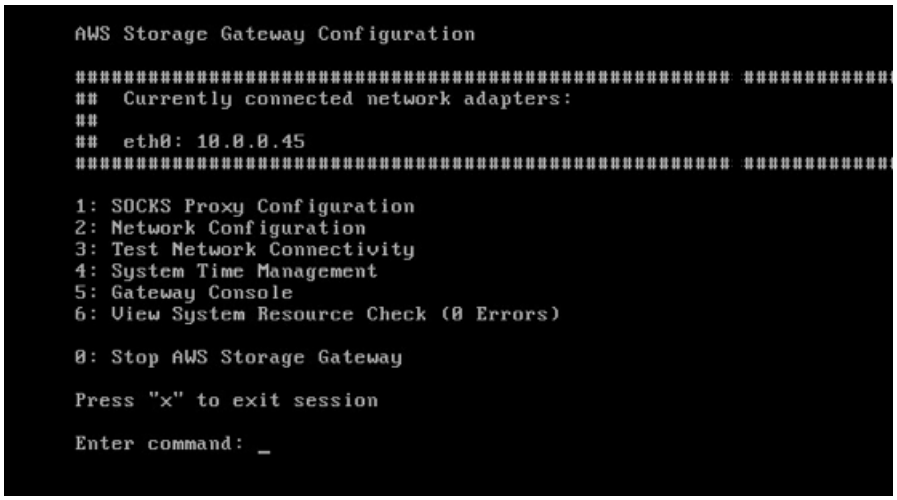
にデプロイされたゲートウェイではVMwareESXi、ハイパーバイザーのホスト時間を設定し、VM 時間をホストに同期するだけで、時間のずれを回避できます。詳細については、「VM の時刻とホストの時刻の同期」を参照してください。Microsoft Hyper-V にデプロイされたゲートウェイの場合は、次の手順を使用して定期的に VM の時刻を確認する必要があります。

ハイパーバイザーゲートウェイ VM の時刻を表示して Network Time Protocol (NTP) サーバーに同期するには

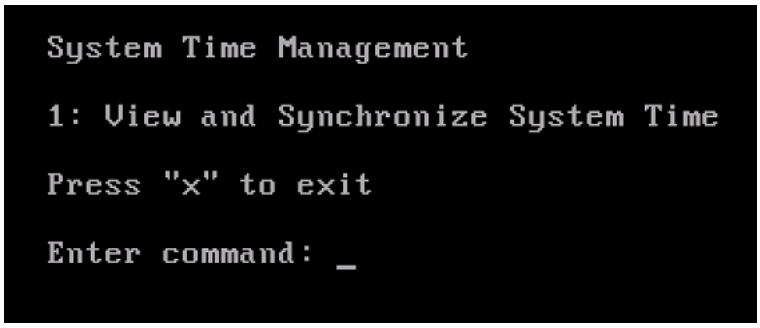
1. ゲートウェイのローカルコンソールにログインします。

- VMware ESXi ローカルコンソールへのログインの詳細については、「」を参照してくださいを使用したゲートウェイローカルコンソールへのアクセス VMware ESXi。
- Microsoft Hyper-V ローカルコンソールへのログインの詳細については、「Microsoft Hyper-V でゲートウェイのローカルコンソールにアクセスする」を参照してください。
- Linux カーネルベースの Virtuam マシン (KVM) のローカルコンソールへのログインの詳細については、「」を参照してくださいLinux を使用したゲートウェイローカルコンソールへのアクセス KVM。

2. [Storage Gateway Configuration] (Storage Gateway 設定) メインメニューで、[System Time Management] (システム時刻管理) に **4** を入力します。



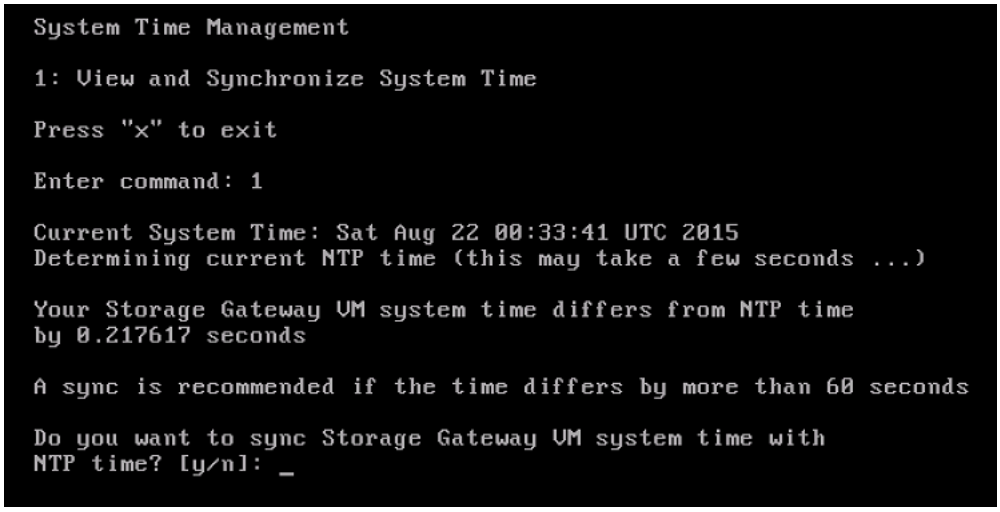
3. [System Time Management] (システム時刻管理) メニューで、[View and Synchronize System Time] (システム時刻の表示と同期) に **1** を入力します。



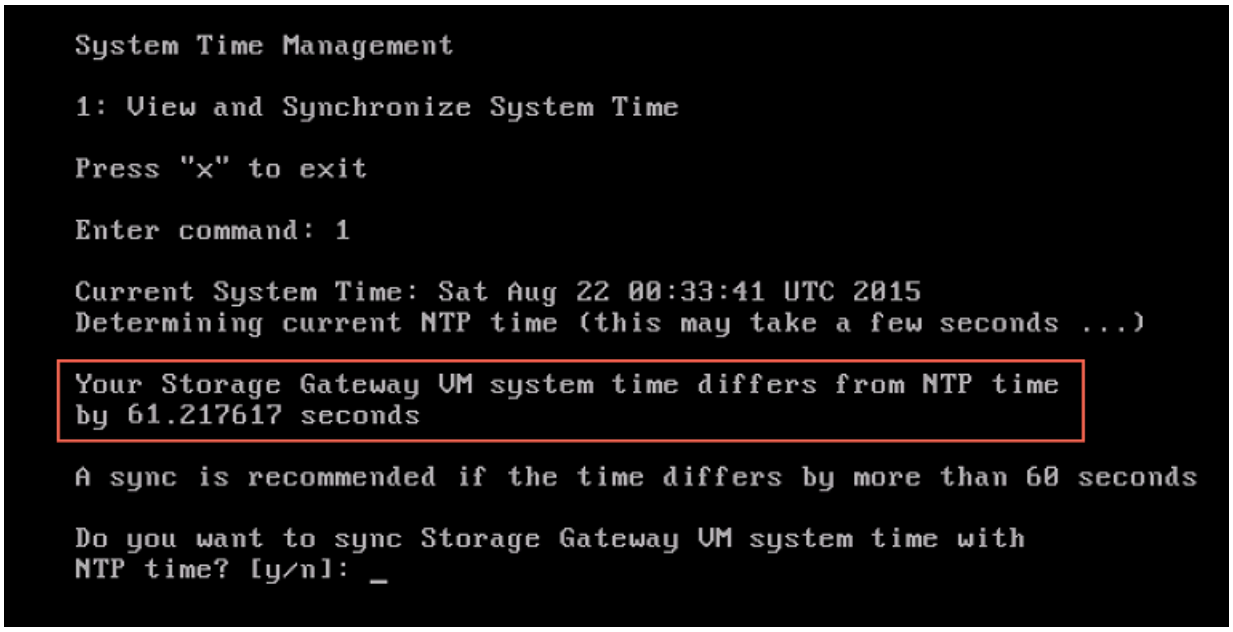
4. VM の時刻を同期する必要があることが結果で示されている場合はNTP、 と入力します**y**。それ以外の場合は、「**n**」と入力します。

   同期するために「**y**」と入力した後で、同期にしばらく時間がかかることがあります。

次のスクリーンショットでは、時刻の同期が必要ない VM を示します。



次のスクリーンショットでは、時刻の同期が必要な VM を示します。



Amazon EC2インスタンスをデプロイしてボリュームゲートウェイをホストする

Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにボリュームゲートウェイをデプロイしてアクティブ化できます。 AWS Storage Gateway Amazon マシンイメージ (AMI) はコミュニティとして利用できますAMI。

> **Note**
>
> Storage Gateway コミュニティAMIsは によって公開され、完全にサポートされています AWS。パブリッシャーが検証済みプロバイダー AWSである であることがわかります。ボリュームゲートウェイは、次の命名規則AMIsを使用します。AMI 名前に追加されたバージョン番号は、バージョンリリースごとに変わります。
>
> `aws-storage-gateway-CLASSIC-2.9.0`

Amazon EC2インスタンスをデプロイしてボリュームゲートウェイをホストするには

1. Storage Gateway コンソールを使用して、新しいゲートウェイのセットアップを開始します。手順については、「ボリュームゲートウェイをセットアップする」を参照してください。プラットフォームオプションセクションに到達したら、ホストプラットフォーム として Amazon EC2 を選択し、次のステップを使用してボリュームゲートウェイ をホストする Amazon EC2インスタンスを起動します。

   > **Note**
   >
   > Amazon EC2ホストプラットフォームは、キャッシュ型ボリュームのみをサポートします。ストアドボリュームゲートウェイをEC2インスタンスにデプロイすることはできません。

2. インスタンスを起動 を選択して、Amazon EC2コンソールでテンプレートを開きます AWS Storage Gateway AMI。ここでは、追加の設定を行うことができます。

   Quicklaunch を使用して、デフォルト設定で Amazon EC2インスタンスを起動します。Amazon EC2 Quicklaunch のデフォルトセプシフィケーションの詳細については、「Amazon の Amazon のクイック起動設定仕様EC2。

3. 名前 に、Amazon EC2インスタンスの名前を入力します。インスタンスがデプロイされたら、この名前を検索して、Amazon EC2コンソールのリストページでインスタンスを検索できます。

4. [インスタンスタイプ] セクションの [インスタンスタイプ] で、インスタンスのハードウェア構成を選択します。ハードウェア構成は、ゲートウェイをサポートするための所定の最小要件を満たしている必要があります。m5.xlarge インスタンスタイプから使い始めてみることを推奨します。このインスタンスタイプは、ゲートウェイが正しく機能するための最小要件を満たしています。詳細については、「Amazon EC2インスタンスタイプの要件」を参照してください。

必要に応じて、起動後のインスタンスのサイズ変更を行うことができます。詳細については、「Amazon ユーザーガイド」の「インスタンスのサイズ変更」を参照してください。 EC2

> **Note**
>
> 特定のインスタンスタイプ、特に i3 はNVMeSSDディスクEC2を使用します。このことが原因で、ボリュームゲートウェイの起動時または停止時に問題が起きる場合があります。例えば、キャッシュからデータが失われる可能性があります。`CachePercentDirty` Amazon CloudWatch メトリクスをモニタリングし、そのパラメータが の場合にのみシステムを起動または停止します`0`。ゲートウェイのメトリクスのモニタリングの詳細については、 CloudWatch ドキュメントのStorage Gateway のメトリクスとディメンション」を参照してください。

5. [キーペア (ログイン)] セクションの [キーペア名 - 必須] で、インスタンスに安全に接続するために使用するキーペアを選択します。必要に応じて新しいキーペアを作成できます。詳細については、「Amazon Elastic Compute Cloud Linux インスタンス用ユーザーガイド」の「キーペアを作成する」を参照してください。
6. [ネットワーク設定] セクションで、事前設定された設定内容を確認し、[編集] を選択して以下のフィールドを変更します。

   a. VPC - 必須の で、Amazon EC2インスタンスを起動する VPC を選択します。詳細については、「Amazon Virtual Private Cloud ユーザーガイド」の「Amazon のVPC仕組み」を参照してください。 Amazon Virtual Private Cloud

   b. (オプション) サブネット で、Amazon EC2インスタンスを起動するサブネットを選択します。

   c. [Auto-assign Public IP] (パブリック IP の自動割当て) で、[Enable] (有効化) を選択します。
7. [ファイアウォール (セキュリティグループ)] サブセクションで、事前設定された設定内容を確認します。必要に応じて、Amazon EC2インスタンス用に作成する新しいセキュリティグループのデフォルトの名前と説明を変更するか、既存のセキュリティグループからファイアウォールルールを適用するかを選択できます。
8. [インバウンドセキュリティグループのルール] サブセクションで、クライアントがインスタンスへの接続に使用するポートを開くファイアウォールルールを追加します。ボリュームゲートウェイに必要なポートの詳細については、「ポート要件」を参照してください。ファイアウォールルールの追加の詳細については、「Amazon Elastic Compute Cloud Linux インスタンス用ユーザーガイド」の「セキュリティグループのルール」を参照してください。

> **Note**
>
> ボリュームゲートウェイでは、インバウンドトラフィックとゲートウェイのアクティベーション中の 1 回限りのHTTPアクセスに対してTCPポート 80 を開く必要があります。このポートは、アクティブ化の後で閉じることができます。
> さらに、アクセスSCSIするにはTCPポート 3260 を開く必要があります。

9. [高度なネットワーク設定] サブセクションで、事前設定された設定内容を確認し、適宜変更します。
10. [ストレージを設定] ページで [新しいボリュームの追加] を選択して、ゲートウェイインスタンスにストレージを追加します。

> **Important**
>
> 事前設定されたルートEBSボリューム に加えて、キャッシュストレージ用に 165 GiB 以上の容量を持つ Amazon EBSボリュームを少なくとも 1 つ追加し、アップロードバッファ用に 150 GiB 以上の容量を持つ Amazon ボリュームを少なくとも 1 つ追加する必要があります。 パフォーマンスを向上させるには、それぞれ 150 GiB 以上のキャッシュストレージに複数のEBSボリュームを割り当てることをお勧めします。

11. [高度な詳細] セクションで、事前設定された設定内容を確認し、適宜変更します。
12. インスタンスを起動 を選択して、設定された設定で新しい Amazon EC2ゲートウェイインスタンスを起動します。
13. 新しいインスタンスが正常に起動したことを確認するには、Amazon コンソールのインスタンスページに移動し、名前で新しいインスタンスを検索します。 EC2[インスタンスの状態] に [実行中] と緑のチェックマークが表示されていること、また、ステータスチェックが完了し、緑色のチェックマークが表示されていることを確認します。
14. 詳細ページからインスタンスを選択します。インスタンスの概要セクションからパブリックIPv4アドレスをコピーし、Storage Gateway コンソールのゲートウェイのセットアップページに戻り、ボリュームゲートウェイ のセットアップを再開します。

Storage Gateway コンソールを使用するか、 AWS Systems Manager ゲートウェイボリュームStorage Gatewayの起動に使用する AMI ID を決定できます。

AMI ID を確認するには、次のいずれかを実行します。

- Storage Gateway コンソールを使用して、新しいゲートウェイのセットアップを開始します。手順については、「ボリュームゲートウェイをセットアップする」を参照してください。プラットフォームオプションセクションに到達したら、ホストプラットフォーム として Amazon EC2 を選択し、インスタンスを起動 を選択して Amazon EC2コンソールでテンプレートを開きます AWS Storage Gateway AMI。

  EC2 コミュニティAMIページにリダイレクトされ、 で AWS リージョンの AMI ID を確認できます URL。

- Systems Manager パラメータストアにクエリを実行します。 AWS CLI または Storage Gateway を使用してAPI、`/aws/service/storagegateway/ami/CACHED/latest`キャッシュ型ボリュームゲートウェイまたはストアドボリュームゲートウェイの名前空間の Systems Manager パブリックパラメータ`/aws/service/storagegateway/ami/STORED/latest`をクエリできます。例えば、次のCLIコマンドを使用すると、指定した AMIで現在の の ID が返され AWS リージョン ます。

```
aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/
STORED/latest
```

  CLI コマンドは、次のような出力を返します。

```
{
    "Parameter": {
        "Type": "String",
        "LastModifiedDate": 1561054105.083,
        "Version": 4,
        "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/
STORED/latest",
        "Name": "/aws/service/storagegateway/ami/STORED/latest",
        "Value": "ami-123c45dd67d891000"
    }
}
```

Amazon EC2 をデフォルト設定でデプロイする

このトピックでは、Amazon EC2 ホストをデフォルト設定でデプロイする手順を説明します。

Amazon Elastic Compute Cloud (Amazon EC2) インスタンスでボリュームゲートウェイをデプロイしてアクティブ化できます。 AWS Storage Gateway Amazon マシンイメージ (AMI) は、コミュニティ AMI として利用できます。

> **Note**
>
> Storage Gateway コミュニティ AMI は公開されており、 AWSがフルサポートを提供しています。パブリッシャーが検証済みプロバイダー AWSである であることがわかります。

1. Amazon EC2 インスタンスをセットアップするには、ワークフローの [プラットフォームオプション] セクションで [ホストプラットフォーム] として [Amazon EC2] を選択します。Amazon EC2 インスタンスの設定手順については、「Amazon EC2 インスタンスをデプロイしてボリュームゲートウェイをホストする」を参照してください。
2. インスタンスの起動を選択して、Amazon EC2 コンソールで AWS Storage Gateway AMI テンプレートを開き、インスタンスタイプ 、ネットワーク設定、ストレージの設定 などの追加設定をカスタマイズします。
3. オプションで、Storage Gateway コンソールで [デフォルト設定を使用] を選択し、デフォルト設定で Amazon EC2 インスタンスをデプロイできます。

   [デフォルト設定を使用] を選択した場合、Amazon EC2 インスタンスには、以下のデフォルト設定が適用されます。

   - インスタンスタイプ — m5.xlarge
   - ネットワーク設定
     - [VPC] で、EC2 インスタンスを実行する VPC を選択します。
     - [サブネット] で、EC2 インスタンスを起動するサブネットを指定します。

     > **Note**
     >
     > VPC サブネットは、VPC 管理コンソールでパブリック IPv4 アドレスの自動割り当て設定が有効になっている場合にのみ、ドロップダウンに表示されます。

   - 自動割り当てパブリック IP — 有効

   EC2 セキュリティグループが作成され、EC2 インスタンスに関連付けられます。このセキュリティグループには、次のインバウンドポートルールが適用されます。

> **Note**
>
> ゲートウェイをアクティブ化する間は、ポート 80 を開く必要があります。このポートはアクティブ化の直後に閉じます。それ以降、EC2 インスタンスには、選択した VPC の他のポートでのみアクセスできます。
> ゲートウェイの iSCSI ターゲットには、ゲートウェイと同じ VPC 内のホストからのみアクセスできます。iSCSI ターゲットに VPC 外部のホストからアクセスする必要がある場合は、適切なセキュリティグループルールを更新する必要があります。
> セキュリティグループはいつでも編集できます。Amazon EC2 インスタンスの詳細ページに移動し、[セキュリティ] を選択します。[セキュリティグループの詳細] に移動し、セキュリティグループ ID を選択してください。

ポート	プロトコル	ファイルシステムプロトコル				
80	TCP	アクティブ化のための HTTP アクセス				
3260	TCP	iSCSI				

- ストレージを設定

デフォルト設定	AMI ルートボリューム	ボリューム 2 キャッシュ	ボリューム 3 キャッシュ			
デバイス名		'/dev/sdb'	'/dev/sdc'			

デフォルト設定	AMI ルートボリューム	ボリューム 2 キャッシュ	ボリューム 3 キャッシュ			
サイズ	80 GiB	165 GiB	150 GiB			
ボリュームタイプ	gp3	gp3	gp3			
IOPS	3000	3000	3000			
終了時に削除	はい	はい	はい			
暗号化された	いいえ	いいえ	いいえ			
スループット	125	125	125			

Amazon EC2インスタンスメタデータオプションの変更

インスタンスメタデータサービス (IMDS) は、Amazon インスタンスメタデータへの安全なアクセスを提供するEC2インスタンス上のコンポーネントです。インスタンスは、IMDSバージョン 1 (IMDSv1) を使用する受信メタデータリクエストを受け入れるか、すべてのメタデータリクエストでIMDSバージョン 2 () を使用するように設定できますIMDSv2。IMDSv2 はセッション指向のリクエストを使用し、 へのアクセスを試みるために使用できるいくつかのタイプの脆弱性を軽減しますIMDS。の詳細についてはIMDSv2、「Amazon Elastic Compute Cloud ユーザーガイド」の「インスタンスメタデータサービスバージョン 2 の仕組み」を参照してください。

Storage Gateway をホストするすべての Amazon EC2インスタンスIMDSv2に を要求することをお勧めします。IMDSv2 は、新しく起動されたすべてのゲートウェイインスタンスでデフォルトで必要です。IMDSv1 メタデータリクエストを受け入れるようにまだ設定されている既存のインスタンスがある場合は、「Amazon Elastic Compute Cloud ユーザーガイドIMDSv2」の「 の使用が必要」を参照して、 の使用を要求するようにインスタンスメタデータオプションを変更する手順を確認してくださいIMDSv2。この変更を適用しても、インスタンスを再起動する必要はありません。

ボリュームゲートウェイ

トピック

ゲートウェイからのディスクの削除

基になるディスクをゲートウェイから削除することはお勧めしませんが、障害が発生したディスクがあるときなどは、ディスクをゲートウェイから削除することが必要になる場合があります。

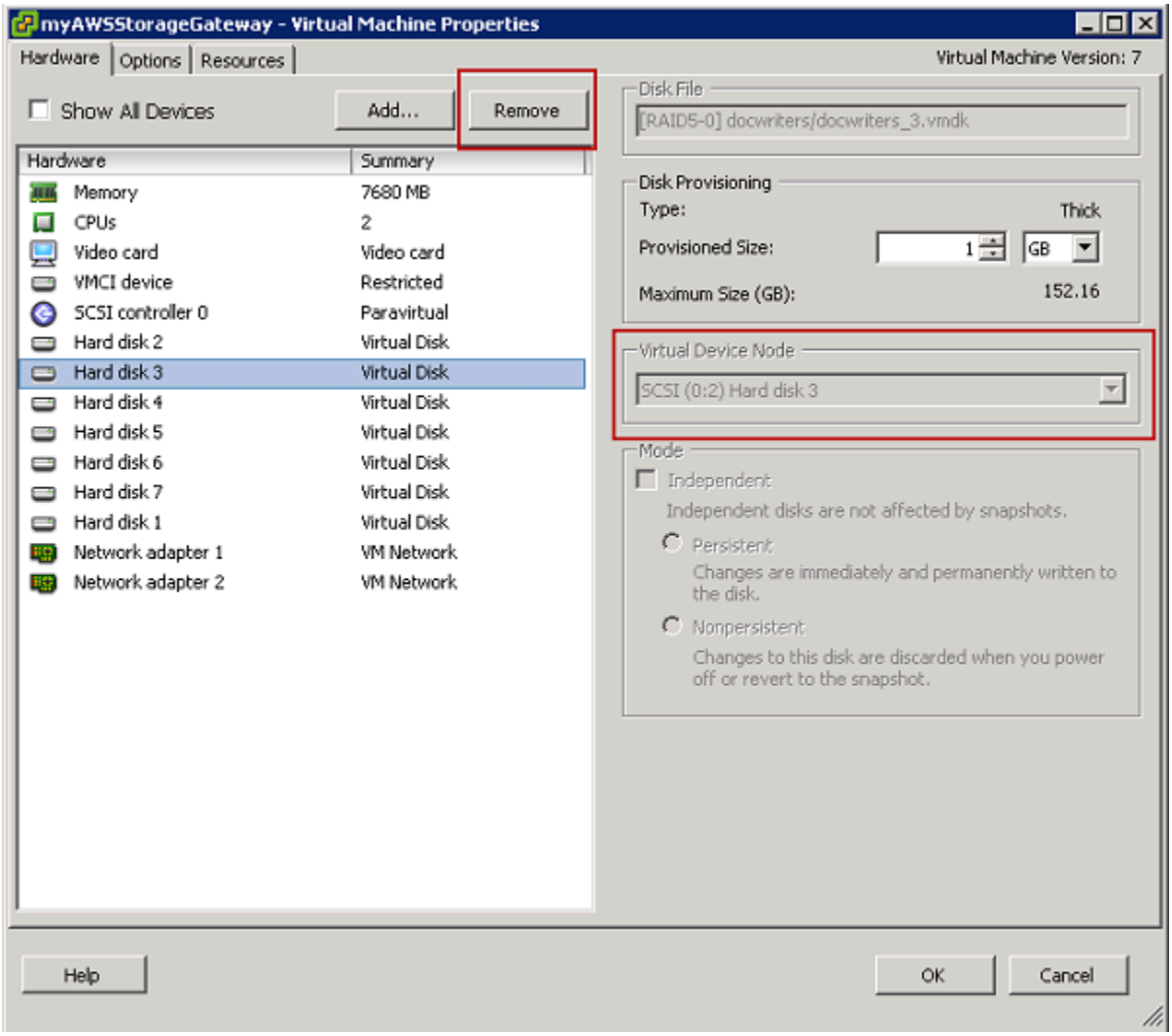
でホストされているゲートウェイからのディスクの削除 VMware ESXi

VMware ハイパーバイザーでホストされているゲートウェイからディスクを削除するには、次の手順を使用します。

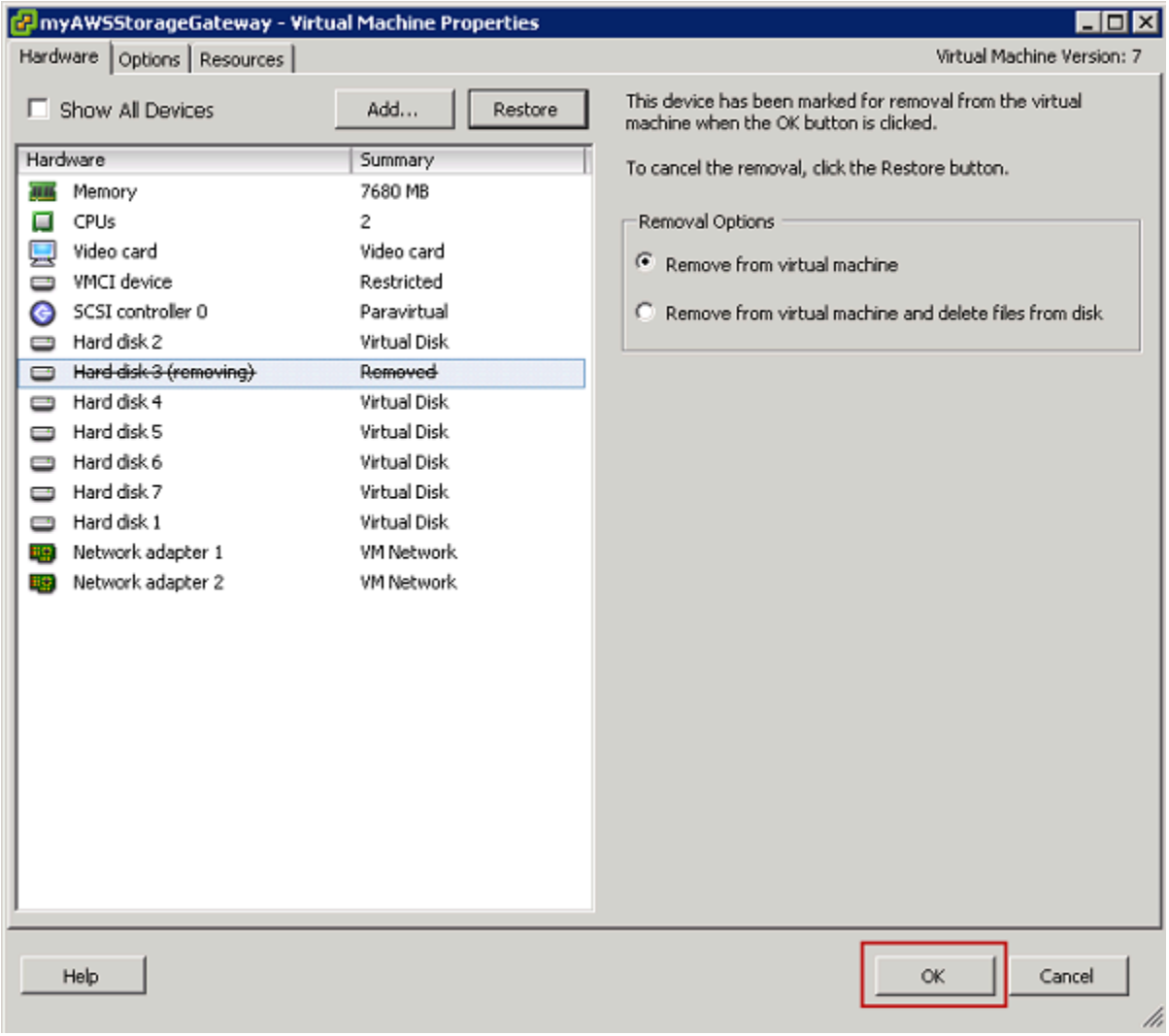
アップロードバッファに割り当てられたディスクを削除するには (VMware ESXi)

1. vSphere クライアントでコンテキスト (右クリック) メニューを開き、ゲートウェイ VM の名前を選択し、設定の編集 を選択します。
2. [Virtual Machine Properties] ダイアログボックスの [Hardware] タブで、アップロードバッファ領域として割り当てられているディスクを選択し、[Remove] を選択します。

   [Virtual Machine Properties] (仮想マシンのプロパティ) ダイアログボックスの [Virtual Device Node] (仮想デバイスノード) の値が、前に書き留めた値と同じであることを確認します。そうすることで、正しいディスクを削除することができます。



3. [Removal Options] パネルでオプションを選択し、[OK] を選択して、ディスクを削除するプロセスを完了します。



Microsoft Hyper-V でホストされているゲートウェイからのディスクの削除

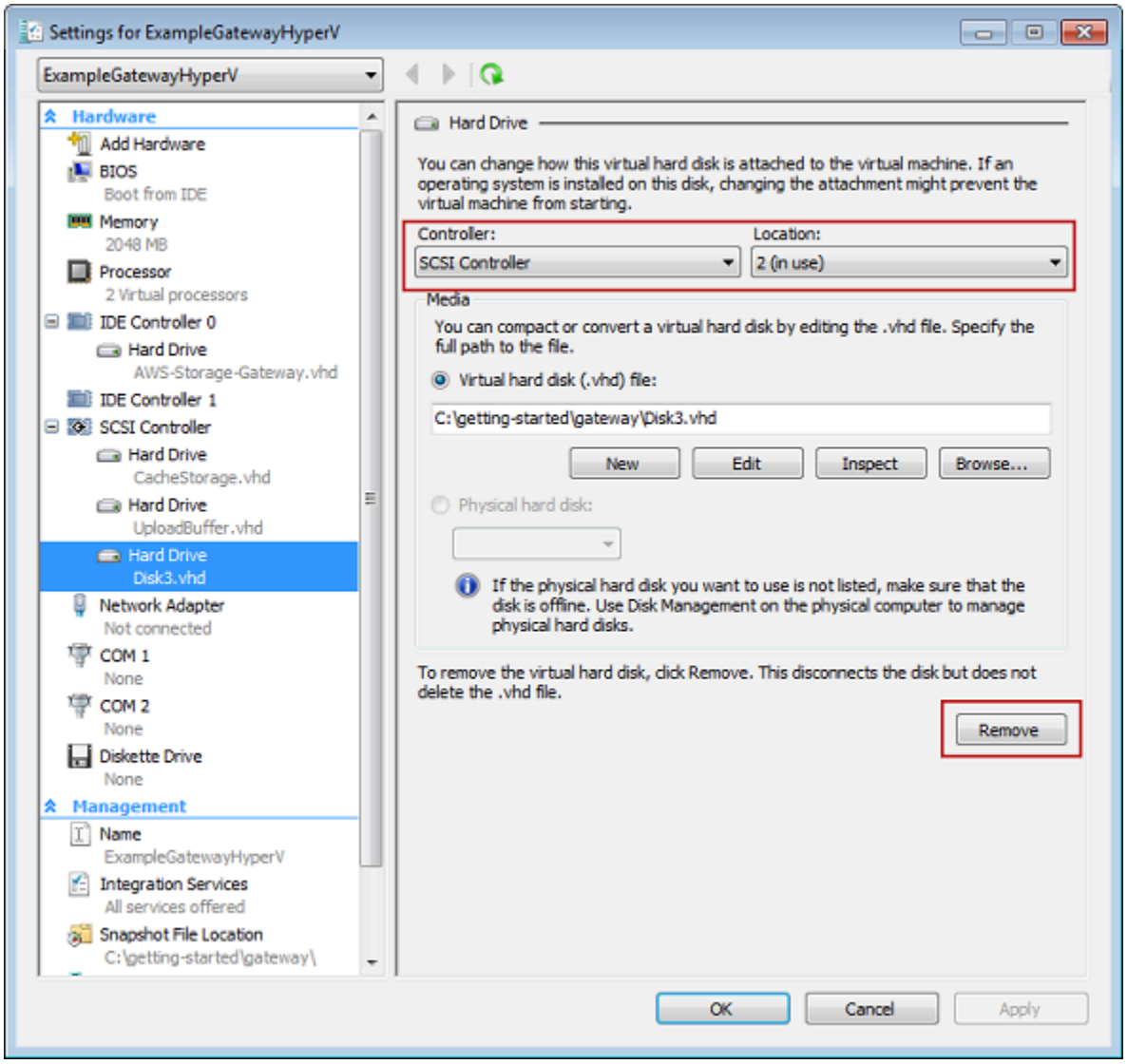
Microsoft Hyper-V ハイパーバイザーでホストされているゲートウェイからディスクを削除するには、次の手順に従います。

アップロードバッファ (Microsoft Hyper-V) として割り当てられた基盤となるディスクを削除するには

1. Microsoft Hyper-V Manager でコンテキスト (右クリック) メニューを開き、ゲートウェイ VM の名前を選択して、[Settings] を選択します。
2. [Settings] ダイアログボックスの [Hardware] リストで、削除するディスクを選択し、[Remove] を選択します。

ゲートウェイに追加するディスクは、ハードウェアリストの SCSI Controller エントリの下に表示されます。[Controller] 値と [Location] 値が、前に書き留めた値と同じであることを確認します。そうすることで、正しいディスクを削除することができます。

Microsoft Hyper-V Manager に表示される最初のSCSIコントローラーはコントローラー 0 です。



3. [OK] を選択して変更を適用します。

Linux でホストされているゲートウェイからのディスクの削除 KVM

Linux カーネルベースの仮想マシン (KVM) ハイパーバイザーでホストされているゲートウェイからディスクをデタッチするには、次のようなvirshコマンドを使用できます。

```
$ virsh detach-disk domain_name /device/path
```

KVM ディスクの管理の詳細については、Linux ディストリビューションのドキュメントを参照してください。

Amazon EC2ゲートウェイの Amazon EBSボリュームの追加と削除

ゲートウェイを最初に Amazon EC2インスタンスとして実行するように設定したとき、アップロードバッファとキャッシュストレージとして使用する Amazon EBSボリュームを割り当てました。時間の経過とともに、アプリケーションのニーズの変化に応じて、この使用のために追加の Amazon EBSボリュームを割り当てることができます。以前に割り当てられた Amazon EBSボリュームを削除することで、割り当てたストレージを減らすこともできます。Amazon の詳細についてはEBS、「Amazon ユーザーガイド」の「Amazon Elastic Block Store (Amazon EBS)」を参照してください。 EC2

ゲートウェイにストレージを追加する前に、ゲートウェイのアプリケーションニーズに基づいて、アップロードバッファとキャッシュストレージのサイズを設定する方法を確認してください。これを行うには、「割り当てるアップロードバッファのサイズの決定」と「割り当てるキャッシュストレージのサイズの決定」を参照してください。

アップロードバッファおよびキャッシュストレージとして割り当てることができる最大ストレージにはクォータがあります。インスタンスには必要な数の Amazon EBSボリュームをアタッチできますが、これらのボリュームをアップロードバッファとして設定し、これらのストレージクォータまでのキャッシュストレージスペースとしてのみ設定できます。詳細については、「AWS Storage Gateway クォータ」を参照してください。

Amazon EBSボリュームを追加してゲートウェイに設定するには

1. Amazon EBSボリュームを作成します。手順については、「Amazon ユーザーガイド」の「Amazon EBSボリュームの作成または復元」を参照してください。 EC2
2. Amazon EBSボリュームを Amazon EC2インスタンスにアタッチします。手順については、「Amazon ユーザーガイド」の「インスタンスへの Amazon EBSボリュームのアタッチ」を参照してください。 EC2
3. 追加した Amazon EBSボリュームをアップロードバッファまたはキャッシュストレージとして設定します。手順については、Storage Gateway のローカルディスクの管理 を参照してください。

アップロードバッファに割り当てた量のストレージが不要になることがあります。

Amazon EBSボリュームを削除するには

> **Warning**
>
> これらのステップは、アップロードバッファ領域として割り当てられた Amazon EBS ボリュームにのみ適用され、キャッシュに割り当てられたボリュームには適用されません。

1. 「ゲートウェイ VM のシャットダウン」セクションで説明されているアプローチに従ってゲートウェイをシャットダウンします。
2. Amazon EBSボリュームを Amazon EC2インスタンスからデタッチします。手順については、「Amazon ユーザーガイド」の「インスタンスから Amazon EBSボリュームをデタッチする」を参照してください。 EC2
3. Amazon EBSボリュームを削除します。手順については、「Amazon ユーザーガイド」の「Amazon EBSボリュームの削除」を参照してください。 EC2
4. 「ゲートウェイ VM のシャットダウン」セクションで説明されているアプローチに従ってゲートウェイを起動します。

ゲートウェイのアクティベーションキーを取得する

ゲートウェイのアクティベーションキーを受け取るには、ゲートウェイ仮想マシン (VM) にウェブリクエストを行います。VM はアクティベーションキーを含むリダイレクトを返します。アクティベーションキーは、ゲートウェイの設定を指定するための `ActivateGateway` API アクションのパラメータの 1 つとして渡されます。詳細については、Storage Gateway API リファレンスActivateGatewayの「」を参照してください。

> **Note**
>
> ゲートウェイのアクティベーションキーは、未使用の場合 30 分で有効期限が切れます。

ゲートウェイ VM に対して行うリクエストには、アクティベーションが発生する AWS リージョンが含まれます。応答のリダイレクトで返される URL には、`activationkey` と呼ばれるクエリ文字列パラメータが含まれています。このクエリ文字列パラメータが、アクティベーションキーです。クエリ文字列の形式は次のようになります。`http://`*`gateway_ip_address`*`/?activationRegion=`*`activation_region`*このクエリの出力で、アクティベーションリージョンとキーの両方が返されます。

URL には、vpcEndpoint、VPC エンドポイントタイプを使用して接続するゲートウェイの VPC エンドポイント ID も含まれています。

> **Note**
>
> Storage Gateway ハードウェアアプライアンス、VM イメージテンプレート、Amazon EC2 Amazon マシンイメージ (AMI) には、このページで説明するウェブリクエストを受信して応答するために必要な HTTP サービスが事前設定されています。ゲートウェイに追加のサービスをインストールすることは必須ではなく、推奨もされていません。

トピック

Linux (curl)

次の例では、Linux (curl) を使用してアクティベーションキーを取得する方法を示しています。

> **Note**
>
> 強調表示された変数を、ゲートウェイの実際の値に置き換えてください。指定できる値は次のとおりです。
>
> - *gateway_ip_address* - ゲートウェイの IPv4 アドレス。例: 172.31.29.201
> - *gateway_type* - 、、STORED、VTLFILE_S3、または などCACHED、アクティブ化するゲートウェイのタイプFILE_FSX_SMB。
> - *region_code* - ゲートウェイをアクティブ化するリージョン。「AWS 全般のリファレンス」の「リージョンエンドポイント」を参照してください。このパラメータが指定されていない場合、または指定された値がスペルミスであるか、有効なリージョンと一致しない場合、コマンドはデフォルトでus-east-1リージョンになります。
> - *vpc_endpoint* - ゲートウェイのVPC エンドポイント名。例: vpce-050f90485f28f2fd0-iep0e8vq.storagegateway.us-west-2.vpce.amazonaws.com

パブリックエンドポイントのアクティベーションキーを取得するには:

```
curl "http://gateway_ip_address/?activationRegion=region_code&no_redirect"
```

VPC エンドポイントのアクティベーションキーを取得するには:

```
curl "http://gateway_ip_address/?
activationRegion=region_code&vpcEndpoint=vpc_endpoint&no_redirect"
```

Linux (bash/zsh)

次の例では、Linux (bash/zsh) を使用して HTTP レスポンスを取得し、HTTP ヘッダーを解析してアクティベーションキーを取得する方法を示します。

```
function get-activation-key() {
  local ip_address=$1
  local activation_region=$2
  if [[ -z "$ip_address" || -z "$activation_region" || -z "$gateway_type" ]]; then
    echo "Usage: get-activation-key ip_address activation_region gateway_type"
    return 1
  fi

  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region&gatewayType=$gateway_type"); then
    activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')
    echo "$activation_key_param" | cut -f2 -d=
  else
    return 1
  fi
}
```

Microsoft Windows PowerShell

次の例は、Microsoft Windows を使用して PowerShell HTTP レスポンスを取得し、HTTP ヘッダーを解析して、アクティベーションキーを取得する方法を示しています。

```
function Get-ActivationKey {
  [CmdletBinding()]
  Param(
```

```
    [parameter(Mandatory=$true)][string]$IpAddress,
    [parameter(Mandatory=$true)][string]$ActivationRegion,
    [parameter(Mandatory=$true)][string]$GatewayType
  )
  PROCESS {
    $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion&gatewayType=$GatewayType" -MaximumRedirection 0 -
ErrorAction SilentlyContinue
    if ($request) {
      $activationKeyParam = $request.Headers.Location | Select-String -Pattern
 "activationKey=([A-Z0-9-]+)"
      $activationKeyParam.Matches.Value.Split("=")[1]
    }
  }
}
```

ローカルコンソールを使用する

次の例では、ローカルコンソールを使用してアクティベーションキーを生成し、表示する方法を示しています。

ローカルコンソールからゲートウェイのアクティベーションキーを取得するには

1. ローカルコンソールにログインします。Windows コンピュータから Amazon EC2 インスタンスに接続する場合は、admin としてログインします。
2. ログイン後に [AWS Appliance Activation - Configuration] メインメニューが表示されたら、`0` を選択して [Get activation key] を選択します。
3. [Storage Gateway for gateway family] オプションを選択します。
4. プロンプトが表示されたら、ゲートウェイをアクティブ化する AWS リージョンを入力します。
5. ネットワークタイプとして 1 [Public] または 2 [VPC endpoint] を入力します。
6. エンドポイントタイプとして 1 [Standard] または 2 [Federal Information Processing Standard (FIPS)] を入力します。

iSCSI イニシエーターの接続

ゲートウェイを管理するときは、Internet Small Computer System Interface (iVTL) ターゲットとして公開されているボリュームまたは仮想テープライブラリ (SCSI) デバイスを使用します。ボリュームゲートウェイの場合、iSCSI ターゲットはボリュームです。テープゲートウェイの場合、ターゲット

はVTLデバイスです。この作業の一環として、これらのターゲットへの接続、iSCSI 設定のカスタマイズ、Red Hat Linux クライアントからの接続、チャレンジハンドシェイク認証プロトコル () の設定などのタスクを実行しますCHAP。

トピック

- ボリュームの Windows クライアントへの接続
- ボリュームまたはVTLデバイスを Linux クライアントに接続する
- iSCSI 設定のカスタマイズ
- iSCSI ターゲットのCHAP認証の設定

iSCSI 標準は、IP ベースのストレージデバイスとクライアント間の接続を開始および管理するためのインターネットプロトコル (IP) ベースのストレージネットワーク標準です。次のリストでは、iSCSI 接続と関係するコンポーネントの説明に使用される用語の一部を定義します。

iSCSI イニシエーター

iSCSI ネットワークのクライアントコンポーネント。イニシエータは iSCSI ターゲットにリクエストを送信します。イニシエータはソフトウェアまたはハードウェアで実装できます。Storage Gateway は、ソフトウェアイニシエータのみをサポートします。

ターゲットSCSI

イニシエータからのリクエストを受信して応答する iSCSI ネットワークのサーバーコンポーネント。各ボリュームは iSCSI ターゲットとして公開されます。各 iSCSI ターゲットに iSCSI イニシエータを 1 つだけ接続します。

Microsoft iSCSI イニシエータ

クライアントコンピュータ (ゲートウェイにデータを書き込むアプリケーションを実行しているコンピュータ) を外部の i SCSIベースの配列 (ゲートウェイ) に接続できる Microsoft Windows コンピュータ上のソフトウェアプログラム。接続は、ホストコンピュータのイーサネットネットワークアダプタカードを使用して行われます。Microsoft iSCSI イニシエータは、Windows 8.1、Windows 10、Windows Server 2012 R2、Windows Server 2016、および Windows Server 2019 の Storage Gateway で検証されています。イニシエータはこれらのオペレーティングシステムに組み込まれています。

Red Hat iSCSI イニシエータ

`iscsi-initiator-utils` Resource Package Manager (RPM) パッケージは、Red Hat Linux 用のソフトウェアに実装された iSCSI イニシエータを提供します。パッケージには、iSCSI プロトコル用のサーバーデーモンが含まれています。

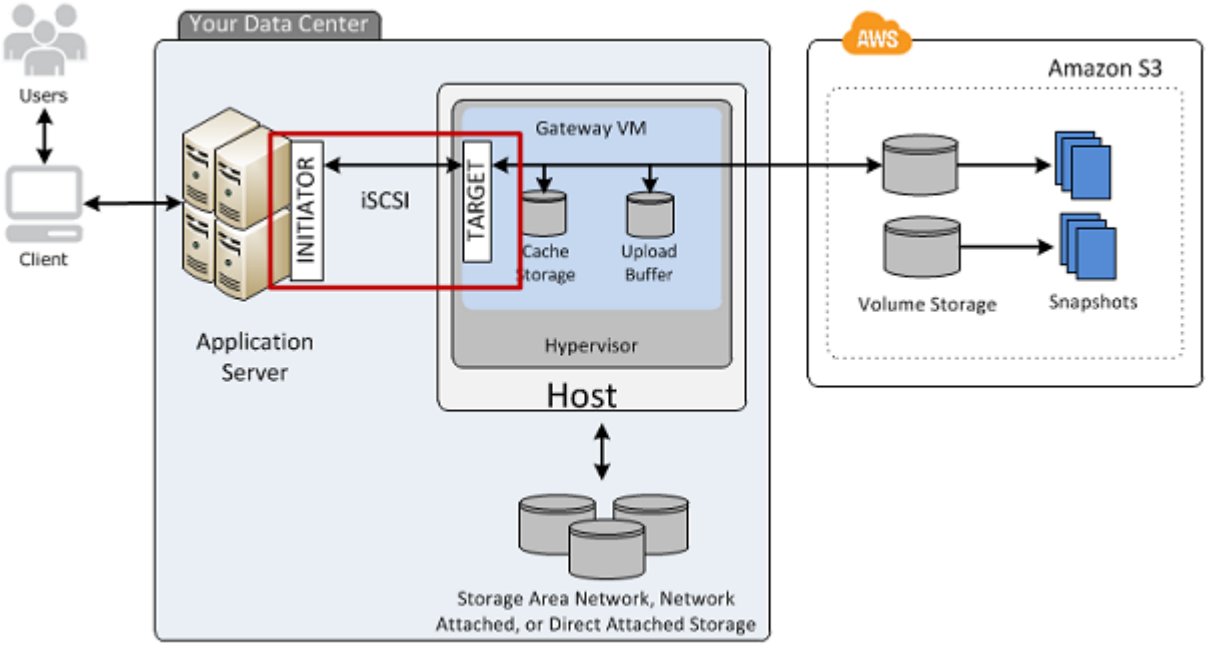
各タイプのゲートウェイは iSCSI デバイスに接続でき、以下で説明するようにそれらの接続をカスタマイズできます。

ボリュームの Windows クライアントへの接続

ボリュームゲートウェイは、ゲートウェイ用に作成したボリュームを iSCSI ターゲットとして公開します。詳細については、「クライアントへのボリュームの接続」を参照してください。

> **Note**
>
> ボリュームターゲットに接続するには、ゲートウェイにアップロードバッファが設定されている必要があります。アップロードバッファがゲートウェイに対して設定されていない場合、ボリュームのステータスは UPLOAD BUFFER NOT と表示されますCONFIGURED。保管型ボリュームセットアップでゲートウェイのアップロードバッファを設定するには、「ゲートウェイ用のアップロードアップロードバッファまたはキャッシュストレージを追加して設定するには」を参照してください。キャッシュ型ボリュームセットアップでゲートウェイのアップロードバッファを設定するには、「ゲートウェイ用のアップロードアップロードバッファまたはキャッシュストレージを追加して設定するには」を参照してください。

次の図は、Storage Gateway アーキテクチャの全体像における iSCSI ターゲットを示しています。詳細については、「ボリュームゲートウェイの仕組み (アーキテクチャ)」を参照してください。



ボリュームには、Windows クライアントまたは Red Hat Linux クライアントから接続できます。オプションで、どちらのクライアントタイプCHAPにも を設定できます。

ゲートウェイは、指定した名前の iSCSI ターゲットとしてボリュームを公開します。先頭には が付きますiqn.1997-05.com.amazon:。例えば、ターゲット名として を指定した場合myvolume、ボリュームへの接続に使用する iSCSI ターゲットは ですiqn.1997-05.com.amazon:myvolume。i経由でボリュームをマウントするようにアプリケーションを設定する方法の詳細についてはSCSI、「」を参照してくださいボリュームの Windows クライアントへの接続。

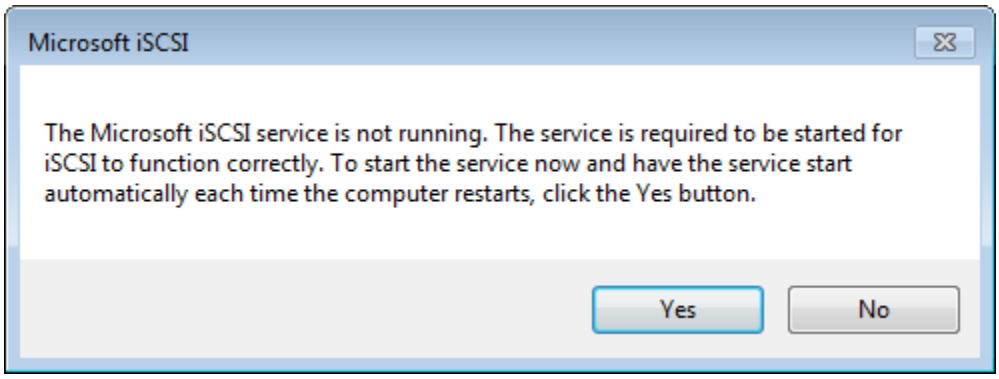
目的	参照先
Windows からボリュームに接続します。	Microsoft Windows クライアントへの接続
Red Hat Linux からボリュームに接続します。	Red Hat Enterprise Linux クライアントへの接続
Windows および Red Hat Linux のCHAP認証を設定します。	iSCSI ターゲットのCHAP認証の設定

Windows クライアントをストレージボリュームに接続するには

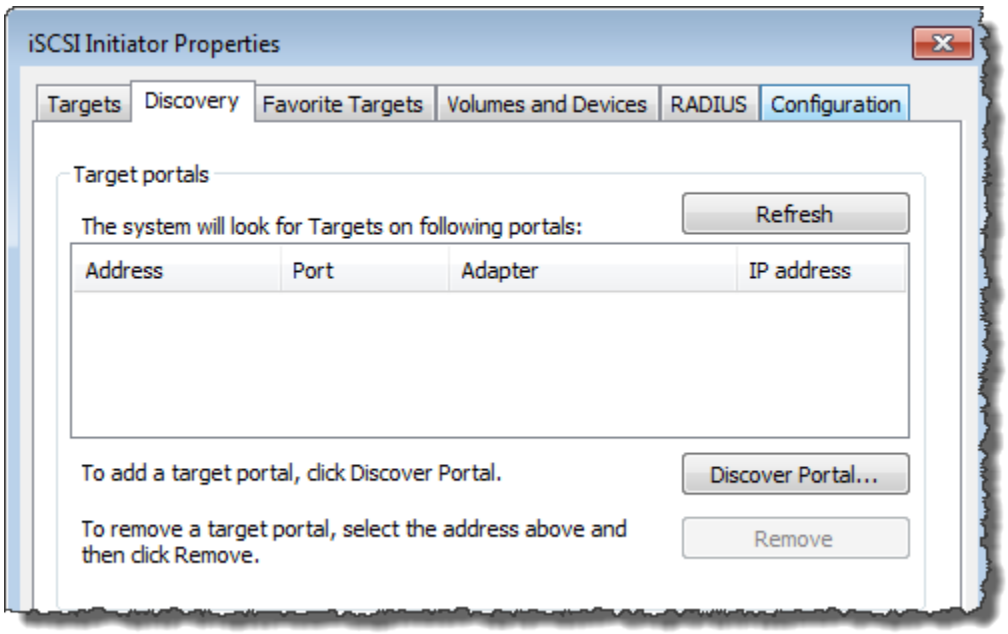
1. Windows クライアントコンピュータのスタートメニュー**iscsicpl.exe**で、「プログラムとファイルの検索」ボックスに「」と入力し、iSCSI イニシエータプログラムを見つけて実行します。

   > **Note**
   >
   > iSCSI イニシエータを実行するには、クライアントコンピュータに対する管理者権限が必要です。

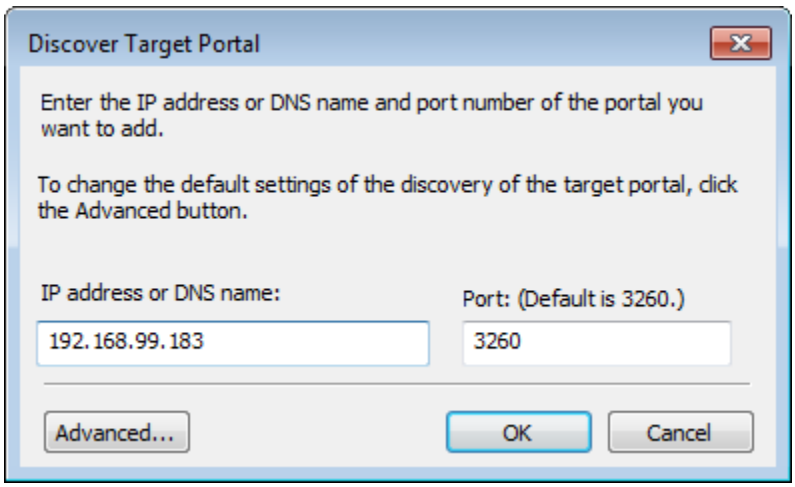
2. プロンプトが表示されたら、はいを選択して Microsoft iSCSI イニシエータサービスを開始します。



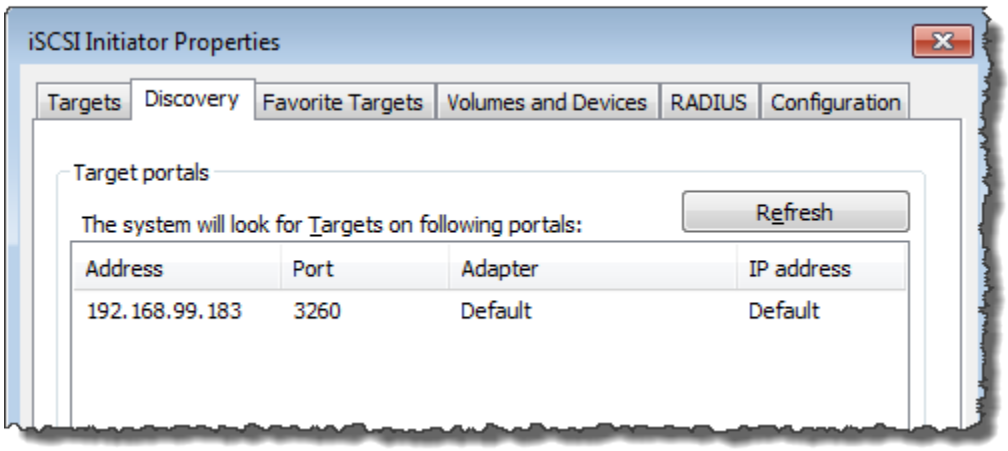
3. iSCSI Initiator Properties ダイアログボックスで、Discover タブを選択し、Discover Portal を選択します。



4. 「ターゲットポータルの検出」ダイアログボックスで、IP アドレスまたは名前 に iSCSI ターゲットの IP アドレスを入力し、OK を選択します。 DNS ゲートウェイの IP アドレスを取得するには、Storage Gateway コンソールの [Gateway] (ゲートウェイ) タブを確認します。Amazon EC2インスタンスにゲートウェイをデプロイした場合、パブリック IP またはDNSアドレスは Amazon EC2コンソールの説明タブにあります。



これで IP アドレスは、[Discovery] タブの [Target portals] のリストに表示されます。

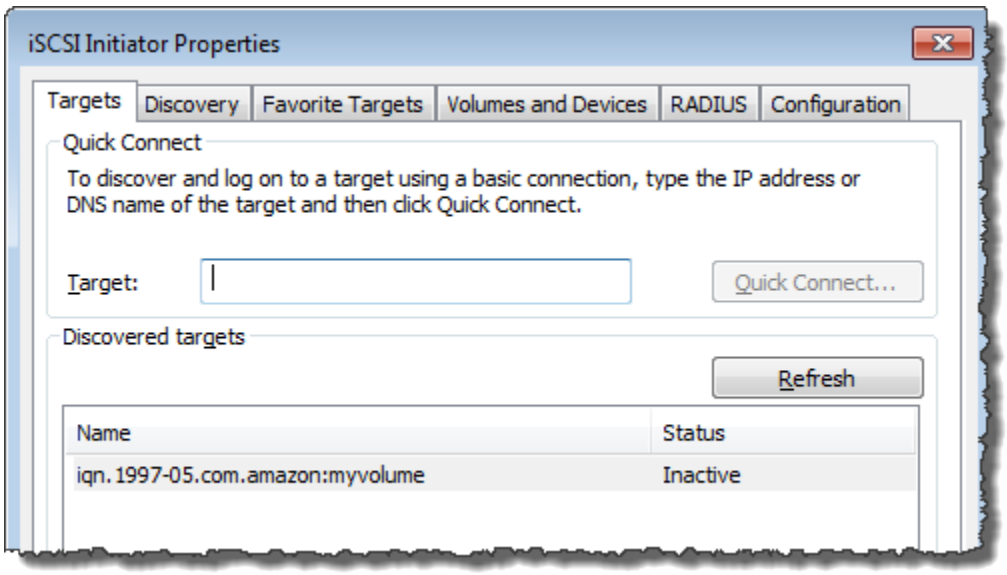


> **⚠ Warning**
>
> Amazon EC2インスタンスにデプロイされているゲートウェイの場合、パブリックインターネット接続を介したゲートウェイへのアクセスはサポートされていません。Amazon EC2インスタンスの Elastic IP アドレスをターゲットアドレスとして使用することはできません。

5. ゲートウェイのストレージボリュームターゲットに新しいターゲットポータルを接続します。

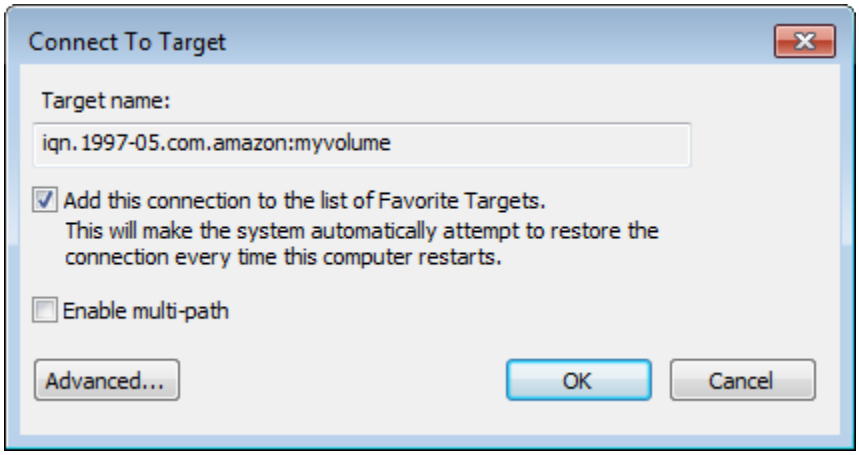
   a. [Targets] タブを選択します。

      新しいターゲットポータルが非アクティブのステータスで表示されます。表示されるターゲット名は、ステップ 1 でストレージボリュームに指定した名前と同じになるはずです。

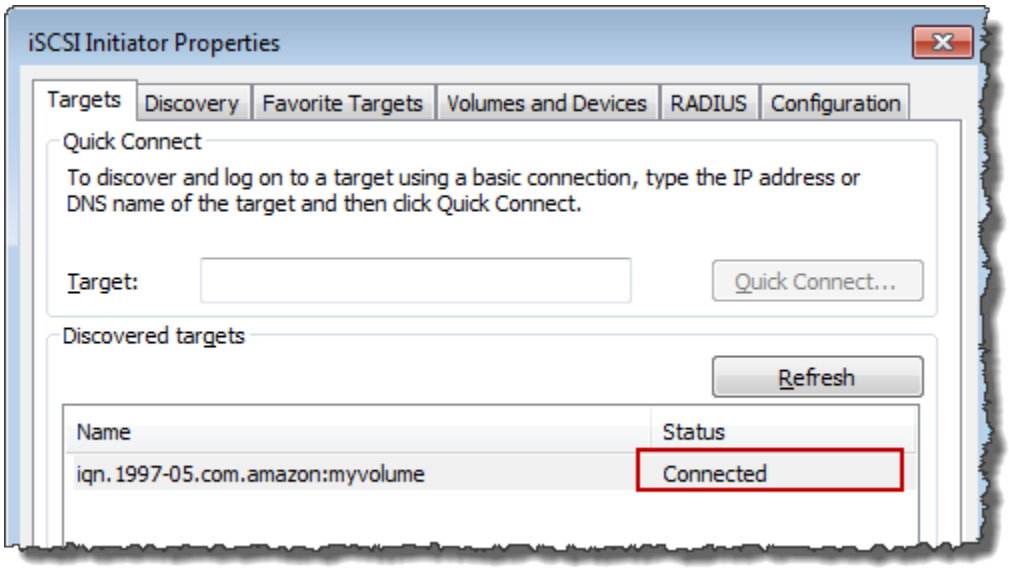


b. ターゲットを選択し、[Connect] を選択します。

ターゲット名がまだ入力されていない場合は、ステップ 1 に示すように、ターゲットの名前を入力します。[Connect to Target] (ターゲットに接続) ダイアログボックスで、[Add this connection to the list of Favorite Targets] (この接続をターゲットの「お気に入り」リストに追加) を選択してから、[OK] をクリックします。



c. [Target] (ターゲット) タブで、ターゲットの [Status] (ステータス) が、ターゲットが接続されていることを示す値 [Connected] (接続済) であることを確認し、[OK] をクリックします。



これで、このストレージボリュームにデータを保存できるように Windows 用に初期化して、フォーマットを実行する準備が整いました。そのためには、Windows Disk Management ツールを使用します。

> **Note**
>
> この演習では必須ではありませんが、「」で説明されているように、実際のアプリケーションの iSCSI 設定をカスタマイズすることを強くお勧めしますWindows iSCSI 設定のカスタマイズ。

ボリュームまたはVTLデバイスを Linux クライアントに接続する

Red Hat Enterprise Linux (RHEL) を使用する場合、 `iscsi-initiator-utils`RPMパッケージを使用してゲートウェイ iSCSI ターゲット (ボリュームまたはVTLデバイス) に接続します。

Linux クライアントを iSCSI ターゲットに接続するには

1. `iscsi-initiator-utils` RPM パッケージがクライアントにまだインストールされていない場合は、インストールします。

   パッケージをインストールするには、以下のコマンドを使用できます。

   ```
   sudo yum install iscsi-initiator-utils
   ```

2. iSCSI デーモンが実行されていることを確認します。

   a. 次のいずれかのコマンドを使用して、iSCSI デーモンが実行されていることを確認します。

      5 RHEL または 6 の場合は、次のコマンドを使用します。

      ```
      sudo /etc/init.d/iscsi status
      ```

      7 RHEL の場合は、次のコマンドを使用します。

      ```
      sudo service iscsid status
      ```

   b. ステータスコマンドが running ステータスを返さない場合は、次のいずれかのコマンドを使用してデーモンを起動します。

5 RHEL または 6 の場合は、次のコマンドを使用します。

```
sudo /etc/init.d/iscsi start
```

7 RHEL の場合は、次のコマンドを使用します。RHEL 7 の場合、通常、iscsidサービスを明示的に開始する必要はありません。

```
sudo service iscsid start
```

3. ゲートウェイに定義されているボリュームまたはVTLデバイスターゲットを検出するには、次の検出コマンドを使用します。

```
sudo /sbin/iscsiadm --mode discovery --type sendtargets --portal [GATEWAY_IP]:3260
```

ゲートウェイの IP アドレスを に置き換えます。*[GATEWAY_IP]* 前述のコマンドの 変数。ゲートウェイ IP は、Storage Gateway コンソールのボリュームの iSCSI ターゲット情報プロパティにあります。

discovery コマンドの出力は、次の出力例のようになります。

ボリュームゲートウェイの場合: *[GATEWAY_IP]*:3260, 1
iqn.1997-05.com.amazon:myvolume

テープゲートウェイの場合: iqn.1997-05.com.amazon:*[GATEWAY_IP]*-tapedrive-01

iSCSI 修飾名 (IQN) は、IQN値が組織に固有であるため、前に示した名前とは異なります。ターゲットの名前は、ボリュームを作成したときに指定した名前です。Storage Gateway コンソールでボリュームを選択すると、iSCSI ターゲット情報プロパティペインにもこのターゲット名が表示されます。

4. ターゲットに接続するには、以下のコマンドを使用します。

正しい を指定する必要があることに注意してください。*[GATEWAY_IP]* connect コマンドIQN の と 。

> **Warning**
>
> Amazon EC2インスタンスにデプロイされているゲートウェイの場合、パブリックインターネット接続を介したゲートウェイへのアクセスはサポートされていませ

ん。Amazon EC2インスタンスの Elastic IP アドレスをターゲットアドレスとして使用することはできません。

```
sudo /sbin/iscsiadm --mode node --targetname
 iqn.1997-05.com.amazon:[ISCSI_TARGET_NAME] --portal [GATEWAY_IP]:3260,1 --login
```

5. ボリュームがクライアントマシン (イニシエータ) にアタッチされていることを確認するには、次のコマンドを使用します。

```
ls -l /dev/disk/by-path
```

コマンドの出力は、次の出力例のようになります。

```
lrwxrwxrwx. 1 root root 9 Apr 16 19:31 ip-[GATEWAY_IP]:3260-iscsi-
iqn.1997-05.com.amazon:myvolume-lun-0 -> ../../sda
```

イニシエータをセットアップした後、「」で説明されているように iSCSI 設定をカスタマイズすることを強くお勧めしますLinux iSCSI 設定のカスタマイズ。

iSCSI 設定のカスタマイズ

イニシエータを設定したら、イニシエータがターゲットから切断されないように iSCSI 設定をカスタマイズすることを強くお勧めします。

次の手順に示すように iSCSI タイムアウト値を増やすことで、長時間かかる書き込みオペレーションや、ネットワークの中断などの一時的な問題にアプリケーションが対応しやすくなります。

> **Note**
>
> レジストリを変更する前に、レジストリのバックアップコピーを作成する必要があります。レジストリを使用する際のバックアップコピーの作成およびその他のベストプラクティスについては、Microsoft TechNet Library の「レジストリのベストプラクティス」を参照してください。

トピック

- Windows iSCSI 設定のカスタマイズ

- Linux iSCSI 設定のカスタマイズ
- ボリュームゲートウェイの Linux ディスクタイムアウト設定のカスタマイズ

Windows iSCSI 設定のカスタマイズ

Windows クライアントを使用する場合は、Microsoft iSCSI イニシエータを使用してゲートウェイボリュームに接続します。ボリュームに接続する方法については、「クライアントへのボリュームの接続」を参照してください。

1. テープゲートウェイデバイスを Windows クライアントに接続します。
2. バックアップアプリケーションを使用している場合は、デバイスを使用するようにアプリケーションを設定します。

Windows iSCSI の設定をカスタマイズするには

1. リクエストをキューに保持する最大時間を長くします。

   a. レジストリエディタ (`Regedit.exe`) を起動します。

   b. 次に示すように、iSCSI コントローラー設定を含むデバイスクラスのグローバルに一意の識別子 (GUID) キーに移動します。

   > **Warning**
   >
   > 00ControlSet1 や 00ControlSet2 などの別のコントロールセットではなく、CurrentControlSetサブキーで作業していることを確認してください。

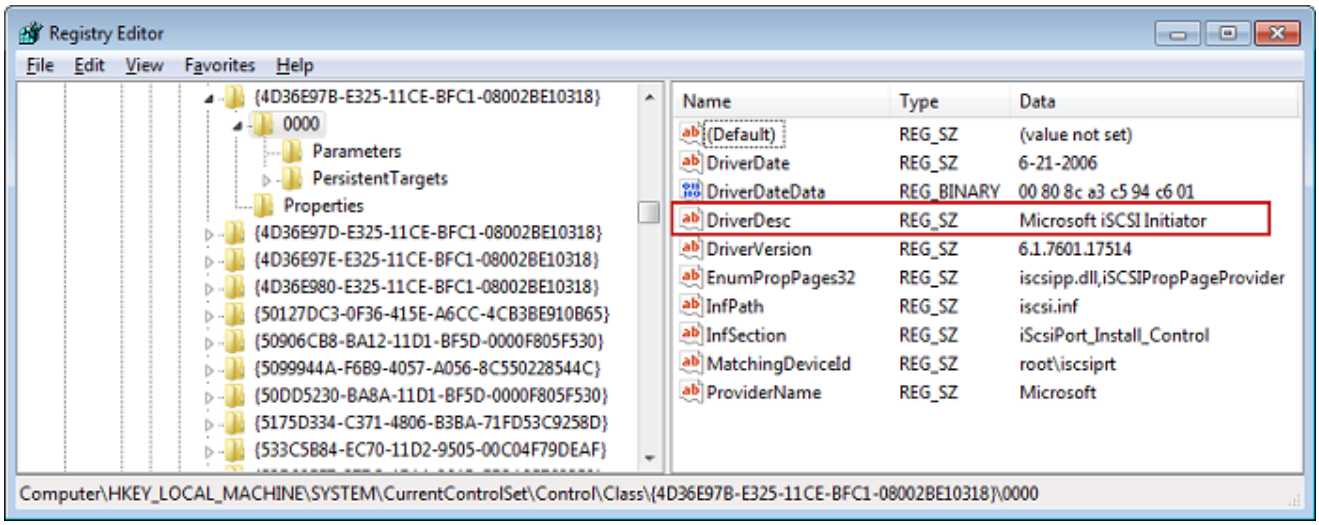
   ```
   HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}
   ```

   c. 次に示すように、Microsoft iSCSI イニシエータの サブキーを検索します。*[<Instance Number]*.

   キーは、`0000` などの 4 桁の数字で表されます。

```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-
BFC1-08002BE10318}\[<Instance Number]
```

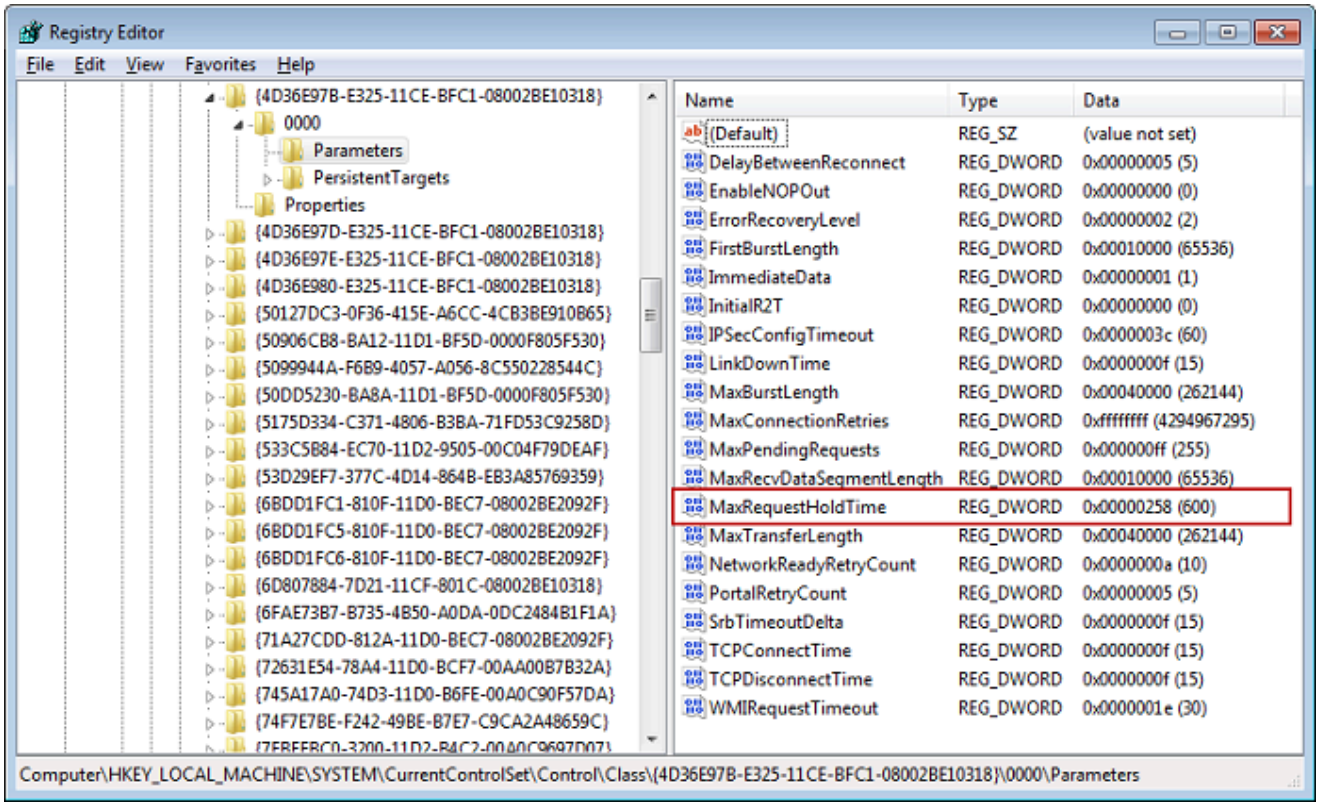
コンピュータにインストールされている内容によっては、Microsoft iSCSI イニシエータがサブキー ではない場合があります0000。次の例で示すように、DriverDesc という文字列の値が Microsoft iSCSI Initiator であることを調べることによって、正しいサブキーを選択したことを確認できます。



d. iSCSI 設定を表示するには、Parameters サブキーを選択します。

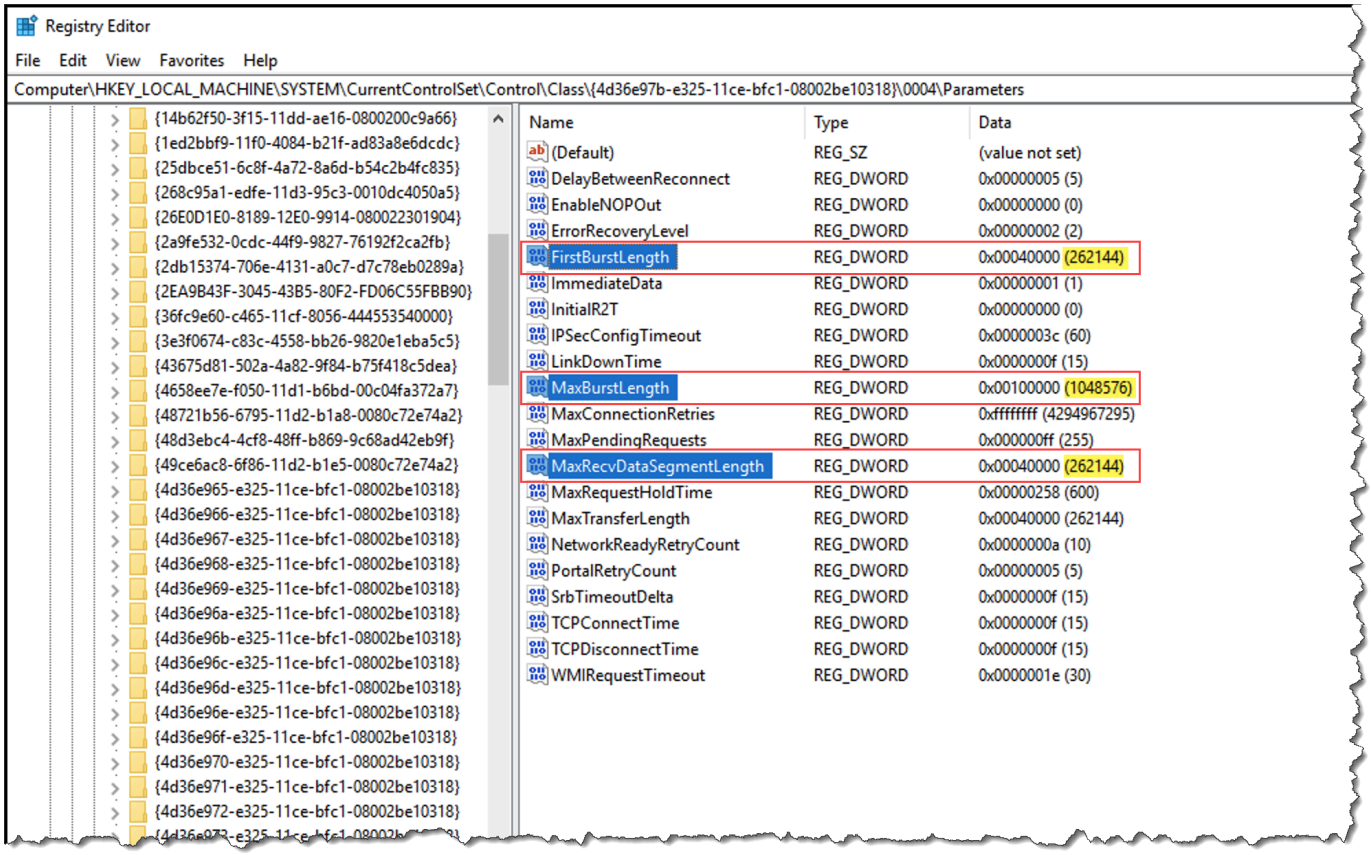
e. (32 ビット) 値のコンテキスト MaxRequestHoldTime DWORD (右クリック) メニューを開き、 の変更 を選択し、値を に変更します**600**。

MaxRequestHoldTime は、Microsoft iSCSI イニシエータがDevice Removalイベントの上部レイヤーに通知する前に、未処理のコマンドを保持して再試行する秒数を指定します。この値は、次の例に示すように、600 秒の保持時間を表します。



2. 次のパラメータを変更することで、iSCSI パケットで送信できるデータの最大量を増やすことができます。

   - FirstBurstLength は、未承諾の書き込みリクエストで送信できるデータの最大量を制御します。この値を **262144**、または Windows OS のデフォルト値のいずれか大きい方に設定します。
   - MaxBurstLength は に似ていますがFirstBurstLength、非推奨の書き込みシーケンスで送信できるデータの最大量を設定します。この値を **1048576**、または Windows OS のデフォルト値のいずれか大きい方に設定します。
   - MaxRecvDataSegmentLength は、単一のプロトコルデータユニット () に関連付けられているデータセグメントの最大サイズを制御しますPDU。この値を **262144**、または Windows OS のデフォルト値のいずれか大きい方に設定します。



> **Note**
>
> さまざまなバックアップソフトウェアを最適化して、さまざまな iSCSI 設定を最適に使用できます。これらのパラメータのどの値により最高のパフォーマンスが得られるかを確認するには、バックアップソフトウェアのドキュメントを参照してください。

3. 次に示すように、ディスクタイムアウトの値を大きくします。

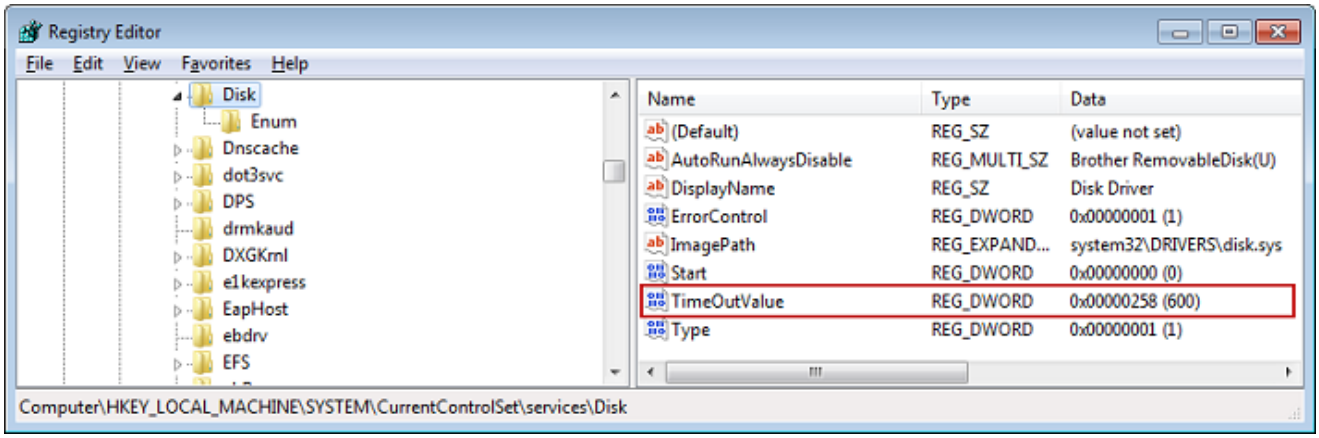
   a. レジストリエディタ (`Regedit.exe`) をまだ起動していない場合は、起動します。

   b. 次に示すようにCurrentControlSet、 のサービスサブキーのディスクサブキーに移動します。

   ```
   HKEY_Local_Machine\SYSTEM\CurrentControlSet\Services\Disk
   ```

   c. (32 ビット) 値のコンテキスト TimeOutValue DWORD (右クリック) メニューを開き、 の変更 を選択し、値を に変更します**600**。

TimeOutValue は、イニシエータが接続を削除して再確立してセッション復旧を試みるまでに、ターゲットからの応答を待機する秒SCSI数を指定します。この値は、次の例に示すように、600 秒のタイムアウト期間を表します。



4. 新しい設定値を有効にするために、システムを再起動します。

   再起動する前に、ボリュームへのすべての書き込みオペレーションの結果がフラッシュされていることを確認する必要があります。そのためには、再起動の前に、マッピングされたすべてのストレージボリュームのディスクをオフラインにします。

Linux iSCSI 設定のカスタマイズ

ゲートウェイのイニシエータを設定したら、イニシエータがターゲットから切断されないように iSCSI 設定をカスタマイズすることを強くお勧めします。次に示すように iSCSI タイムアウト値を増やすことで、長時間かかる書き込みオペレーションや、ネットワークの中断などの一時的な問題への対応がアプリケーションにより適切になります。

> **Note**
>
> コマンドは、Linux のタイプごとにわずかに異なる場合があります。次の例は、Red Hat Linux に基づいています。

Linux iSCSI の設定をカスタマイズするには

1. リクエストをキューに保持する最大時間を長くします。

   a. `/etc/iscsi/iscsid.conf` ファイルを開き、次の行を探します。

```
node.session.timeo.replacement_timeout = [replacement_timeout_value]
node.conn[0].timeo.noop_out_interval = [noop_out_interval_value]
node.conn[0].timeo.noop_out_timeout = [noop_out_timeout_value]
```

b. 設定: *[replacement_timeout_value]* 値を に設定します**600**。

設定: *[noop_out_interval_value]* 値を に設定します**60**。

設定: *[noop_out_timeout_value]* 値を に設定します**600**。

これら 3 つの値の単位はすべて秒です。

> **Note**
>
> ゲートウェイを検出する前に、iscsid.conf を設定する必要があります。既にゲートウェイを検出している場合や、ターゲットにログインしている場合、またはその両方が該当する場合は、次のコマンドを使用して検出データベースからエントリを削除できます。その後、再検出または再ログインを行って、新しい設定を取得できます。
>
> ```
> iscsiadm -m discoverydb -t sendtargets -p [GATEWAY_IP]:3260 -o delete
> ```

2. 各レスポンスで送信できるデータ量の最大値を増やします。

a. /etc/iscsi/iscsid.conf ファイルを開き、次の行を探します。

```
node.session.iscsi.FirstBurstLength = [replacement_first_burst_length_value]
node.session.iscsi.MaxBurstLength = [replacement_max_burst_length_value]
node.conn[0].iscsi.MaxRecvDataSegmentLength
 = [replacement_segment_length_value]
```

b. パフォーマンスを向上させるには、以下の値をお勧めします。バックアップソフトウェアは異なる値を使用するように最適化されている場合もあるため、最良の結果を得るにはバックアップソフトウェアのドキュメントを参照してください。

設定: *[replacement_first_burst_length_value]* または Linux OS **262144** のデフォルトのうち、いずれか大きい方の値。

設定: *[replacement_max_burst_length_value]* または Linux OS **1048576** のデフォルトのうち、いずれか大きい方の値。

設定: *[replacement_segment_length_value]* または Linux OS **262144** のデフォルトのうち、いずれか大きい方の値。

> **Note**
>
> さまざまなバックアップソフトウェアを最適化して、さまざまな iSCSI 設定を最適に使用できます。これらのパラメータのどの値により最高のパフォーマンスが得られるかを確認するには、バックアップソフトウェアのドキュメントを参照してください。

3. システムを再起動して、新しい設定値を有効にします。

   再起動する前に、テープへのすべての書き込みオペレーションの結果がフラッシュされていることを確認します。これを行うには、再起動の前に、テープをアンマウントします。

ボリュームゲートウェイの Linux ディスクタイムアウト設定のカスタマイズ

ボリュームゲートウェイを使用している場合は、前のセクションで説明した iSCSI 設定に加えて、次の Linux ディスクタイムアウト設定をカスタマイズできます。

Linux ディスクタイムアウト設定をカスタマイズするには

1. ルールファイルのディスクタイムアウトの値を大きくします。

   a. 5 RHELつのイニシエータを使用している場合は、 `/etc/udev/rules.d/50-udev.rules` ファイルを開き、次の行を見つけます。

   ```
   ACTION=="add", SUBSYSTEM=="scsi" , SYSFS{type}=="0|7|14", \
   RUN+="/bin/sh -c 'echo [timeout] > /sys$$DEVPATH/timeout'"
   ```

   このルールファイルは RHEL 6 つまたは 7 つのイニシエータに存在しないため、次のルールを使用して作成する必要があります。

   ```
   ACTION=="add", SUBSYSTEMS=="scsi" , ATTRS{model}=="Storage Gateway",
   RUN+="/bin/sh -c 'echo [timeout] > /sys$$DEVPATH/timeout'"
   ```

RHEL 6 のタイムアウト値を変更するには、次のコマンドを使用して、前述のコード行を追加します。

```
sudo vim /etc/udev/rules.d/50-udev.rules
```

RHEL 7 のタイムアウト値を変更するには、次のコマンドを使用して、前述のコード行を追加します。

```
sudo su -c "echo 600 > /sys/block/[device name]/device/timeout"
```

b. 設定: *[timeout]* 値を に設定します**600**。

この値は、タイムアウト値が 600 秒であることを表します。

2. システムを再起動して、新しい設定値を有効にします。

再起動する前に、ボリュームへのすべての書き込みオペレーションの結果がフラッシュされていることを確認します。そのためには、再起動の前に、ストレージボリュームをアンマウントします。

3. 次のコマンドを使用して設定をテストできます。

```
udevadm test [PATH_TO_ISCSI_DEVICE]
```

このコマンドは、iSCSI デバイスに適用される udev ルールを表示します。

iSCSI ターゲットのCHAP認証の設定

Storage Gateway は、チャレンジハンドシェイク認証プロトコル () を使用して、ゲートウェイと iSCSI イニシエータ間の認証をサポートしますCHAP。CHAP は、i SCSIイニシエータのアイデンティティがボリュームとVTLデバイスターゲットへのアクセスを認証されていることを定期的に検証することで、再生攻撃に対する保護を提供します。

> **Note**
>
> CHAP 設定はオプションですが、強くお勧めします。

を設定するにはCHAP、Storage Gateway コンソールと、ターゲットへの接続に使用するイSCSIニシエータソフトウェアの両方で設定する必要があります。Storage Gateway は相互 を使用します。これはCHAP、イニシエータがターゲットを認証し、ターゲットがイニシエータを認証するときです。

ターゲットCHAPの相互 を設定するには

1. CHAP 「」の説明に従って、Storage Gateway コンソールで を設定しますStorage Gateway コンソールでボリュームターゲットCHAPに を設定するには。
2. クライアントイニシエータソフトウェアで、CHAP設定を完了します。
   - Windows クライアントCHAPで相互 を設定するには、「」を参照してくださいWindows クライアントCHAPで相互 を設定するには。
   - Red Hat Linux クライアントCHAPで相互 を設定するには、「」を参照してくださいRed Hat Linux クライアントCHAPで相互 を設定するには。

Storage Gateway コンソールでボリュームターゲットCHAPに を設定するには

この手順では、ボリュームの読み書きに使用される 2 つのシークレットキーを指定します。同じキーを、クライアントのイニシエータを設定する手順でも使用します。

1. Storage Gateway コンソールのナビゲーションペインで、[Volumes] (ボリューム) を選択します。
2. アクション で、CHAP認証の設定 を選択します。
3. CHAP 「認証の設定」ダイアログボックスで、リクエストされた情報を入力します。
   a. イニシエーター名 には、iSCSI イニシエーターの名前を入力します。この名前は Amazon iSCSI 修飾名 (IQN) で、先頭にターゲット名が`iqn.1997-05.com.amazon:`続きます。次に例を示します。

      ```
      iqn.1997-05.com.amazon:your-volume-name
      ```

      イニシエータ名は、iSCSI イニシエータソフトウェアを使用して確認できます。例えば、Windows クライアントの場合、名前は iSCSI イニシエータの設定タブの値です。詳細については、「Windows クライアントCHAPで相互 を設定するには」を参照してください。

> **Note**
>
> イニシエータ名を変更するには、まず を非アクティブ化しCHAP、iSCSI イニシエータソフトウェアでイニシエータ名を変更してから、新しい名前CHAPでアクティブ化する必要があります。

b. [Secret used to Authenticate Initiator] (イニシエータ認証に使用するシークレットキー) に、要求されるシークレットキーを入力します。

このシークレットキーは、12 文字以上、16 文字以下である必要があります。この値は、イニシエータ (Windows クライアント) がターゲットCHAPに参加するために知っておく必要があるシークレットキーです。

c. ターゲットの認証に使用されるシークレット (相互 CHAP) には、リクエストされたシークレットを入力します。

このシークレットキーは、12 文字以上、16 文字以下である必要があります。この値は、ターゲットがイニシエータCHAPに参加するために知っておく必要があるシークレットキーです。

> **Note**
>
> ターゲットを認証するために使用されるシークレットキーは、イニシエータを認証するためのシークレットキーとは異なるものである必要があります。

d. [Save] を選択します。

4. 詳細タブを選択し、iSCSI CHAP認証が true に設定されていることを確認します。

Windows クライアントCHAPで相互 を設定するには

この手順では、コンソールCHAPでボリュームCHAPの設定に使用したのと同じキーを使用して、Microsoft iSCSI イニシエータで を設定します。

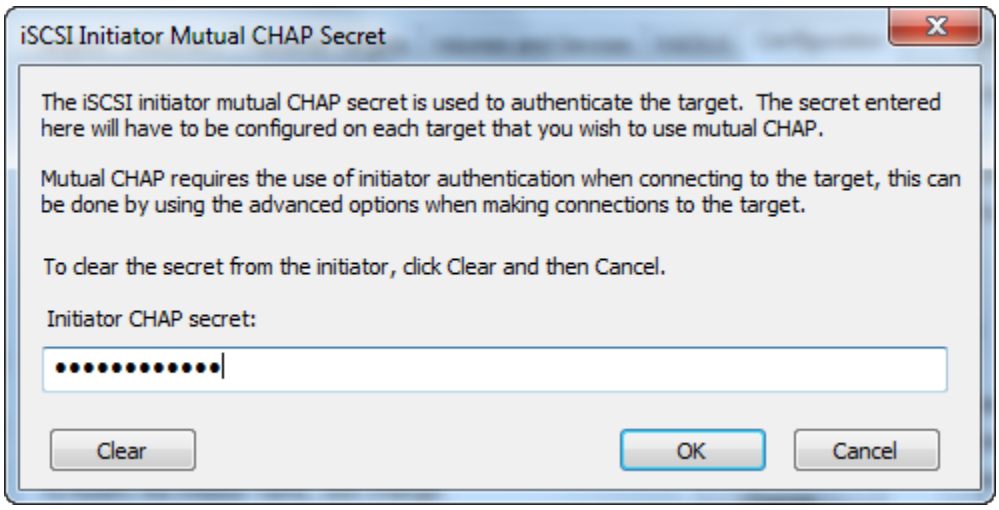
1. iSCSI イニシエータがまだ開始されていない場合は、Windows クライアントコンピュータのスタートメニューで、実行 を選択し、 と入力し**iscsicpl.exe**、OK を選択してプログラムを実行します。
2. イニシエータ (Windows クライアント) の相互CHAP設定を行います。

   a. [設定] タブを選択します。

   > **Note**
   >
   > [Initiator Name] の値は、イニシエータおよび会社に固有の値です。前述の名前は、Storage Gateway コンソールのCHAP「認証の設定」ダイアログボックスで使用した値です。
   > 例の画像で表示されている名前は、デモンストレーション用です。

   b. を選択しますCHAP。

   c. iSCSI Initiator Mutual Chap Secret ダイアログボックスに、相互CHAPシークレット値を入力します。

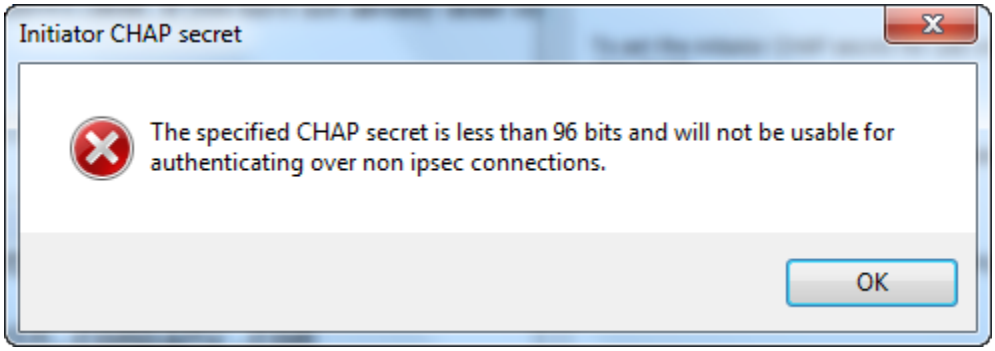


このダイアログボックスには、イニシエータ (Windows クライアント) がターゲット (ストレージボリューム) を認証するために使用するシークレットキーを入力します。このシークレットキーを使用すると、ターゲットはイニシエータに対する読み書きを実行できます。こ

のシークレットは、Configure CHAP Authentication ダイアログボックスの「ターゲットの認証に使用されるシークレット (相互CHAP) 」ボックスに入力されたシークレットと同じです。詳細については、「iSCSI ターゲットのCHAP認証の設定」を参照してください。

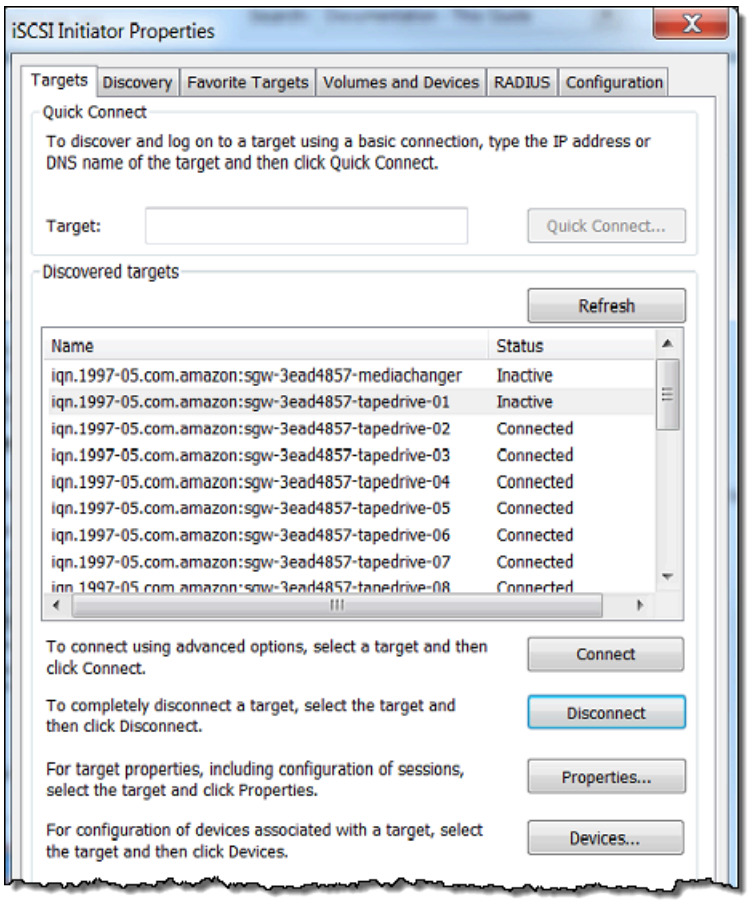
d. 入力したキーが 12 文字未満または 16 文字を超える場合は、イニシエーターCHAPシークレットエラーダイアログボックスが表示されます。

[OK] をクリックし、もう一度キーを入力します。



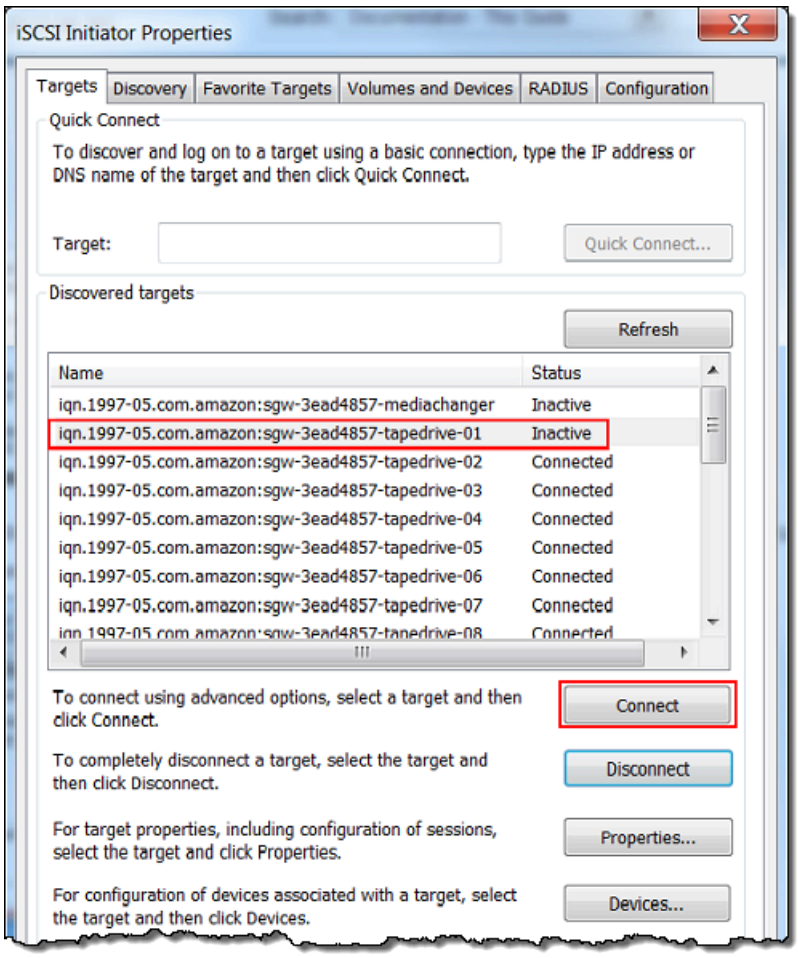
3. 相互設定を完了するために、イニシエータのシークレットを使用してターゲットCHAPを設定します。

a. [Targets] タブを選択します。

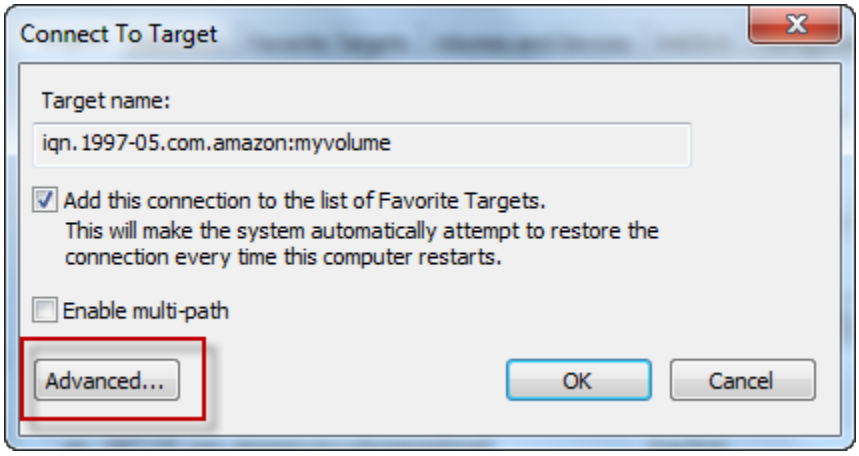


b. 設定するターゲットCHAPが現在接続されている場合は、ターゲットを選択し、切断 を選択して、ターゲットを切断します。

c. に設定するターゲットを選択しCHAP、Connect を選択します。



d. [Connect to Target] ダイアログボックスで [Advanced] を選択します。



e. 詳細設定ダイアログボックスで、 を設定しますCHAP。

i. でCHAPログをアクティブ化を選択します。

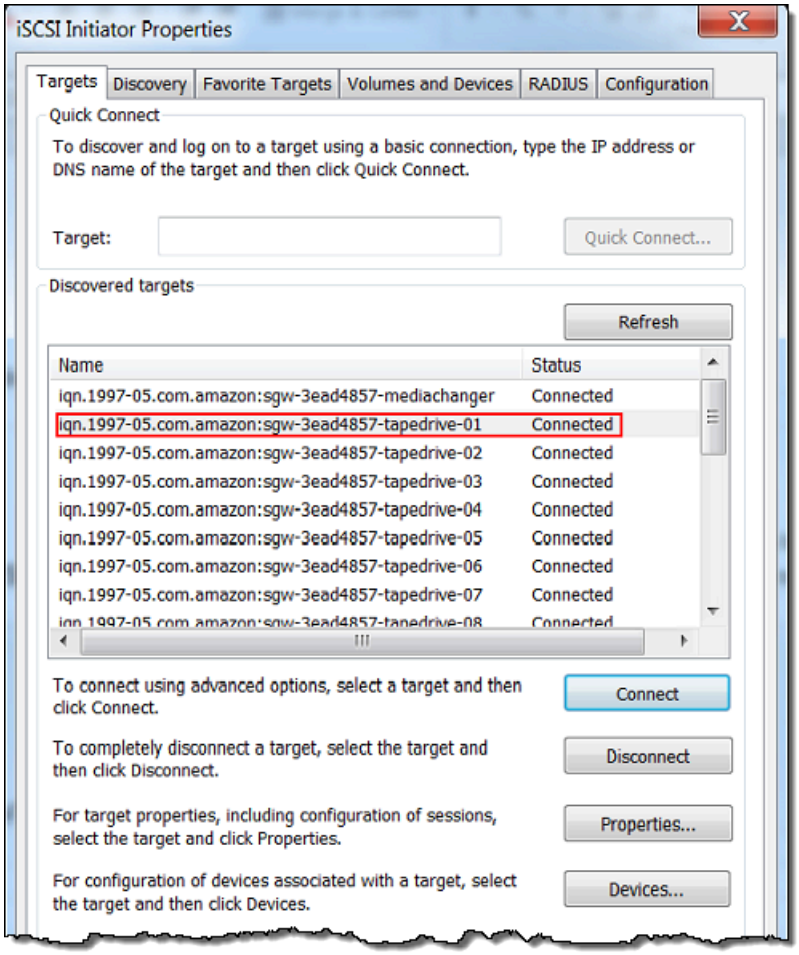
ii. イニシエータを認証するために必要なシークレットキーを入力します。このシークレットは、Configure Authentication ダイアログボックスの「Initiator の認証に使用されるシークレットCHAP」ボックスに入力されたシークレットと同じです。詳細については、「iSCSI ターゲットのCHAP認証の設定」を参照してください。

iii. [Perform mutual authentication] を選択します。

iv. [OK] を選択して変更を適用します。

f. [Connect to Target] ダイアログボックスで [OK] を選択します。

4. 正しいシークレットキーを指定した場合、ターゲットのステータスが [Connected] と表示されます。



Red Hat Linux クライアントCHAPで相互 を設定するには

この手順では、Linux iSCSI イニシエータCHAPで、Storage Gateway コンソールでボリュームCHAPの設定に使用したのと同じキーを使用して を設定します。

1. iSCSI デーモンが実行されていること、およびターゲットにすでに接続していることを確認します。これら 2 つのタスクを完了していない場合は、「Red Hat Enterprise Linux クライアントへの接続」を参照してください。
2. を設定しようとしているターゲットの既存の設定を切断して削除しますCHAP。

   a. ターゲット名を検索し、定義済みの設定であることを確認するには、次のコマンドを使用して、保存されている設定の一覧を表示します。

   ```
   sudo /sbin/iscsiadm --mode node
   ```

   b. ターゲットから切断します。

   次のコマンド**myvolume**は、Amazon iSCSI 修飾名 () で定義されている という名前のターゲットから切断しますIQN。状況IQNに応じて、ターゲット名 と を変更します。

   ```
   sudo /sbin/iscsiadm --mode node --logout GATEWAY_IP:3260,1
    iqn.1997-05.com.amazon:myvolume
   ```

   c. ターゲットの設定を削除します。

   次のコマンドは、**myvolume** ターゲットに対する設定を削除します。

   ```
   sudo /sbin/iscsiadm --mode node --op delete --targetname
    iqn.1997-05.com.amazon:myvolume
   ```

3. iSCSI 設定ファイルを編集して をアクティブ化しますCHAP。

   a. イニシエータ (つまり、使用しているクライアント) の名前を取得します。

   次のコマンドは、/etc/iscsi/initiatorname.iscsi ファイルからイニシエータの名前を取得します。

   ```
   sudo cat /etc/iscsi/initiatorname.iscsi
   ```

   このコマンドの出力は次のようになります。

   ```
   InitiatorName=iqn.1994-05.com.redhat:8e89b27b5b8
   ```

   b. /etc/iscsi/iscsid.conf ファイルを開きます。

   c. ファイル内の次の行のコメントを解除し、 の正しい値を指定します。*username*, *password*, *username_in* および *password_in*.

```
node.session.auth.authmethod = CHAP
node.session.auth.username = username
node.session.auth.password = password
node.session.auth.username_in = username_in
node.session.auth.password_in = password_in
```

指定する値の説明については、次の表を参照してください。

構成設定	値
username	この手順の前のステップで検出したイニシエータ名です。この値は、iqn で始まります。例えば、 **iqn.1994-05.com.redhat:8e89b27b5b8** は有効な *username* 値。
password	イニシエータ (使用しているクライアント) がボリュームと通信するときにイニシエータを認証するために使用されるシークレットキー。
username_in	ターゲットボリュームIQNの 。この値は、iqn で始まり、ターゲット名で終わります。例えば、 **iqn.1997-05.com.amazon:myvolume** は有効な *username_in* 値。
password_in	ターゲット (ボリューム) がイニシエータと通信するときにターゲットを認証するために使用されるシークレットキー。

d. 設定ファイルの変更を保存して、ファイルを閉じます。

4. ターゲットを検出して、ログインします。そのためには、「Red Hat Enterprise Linux クライアントへの接続」の手順に従ってください。

Storage Gateway AWS Direct Connect での の使用

AWS Direct Connect は、内部ネットワークを Amazon Web Services クラウドにリンクします。Storage Gateway AWS Direct Connect で を使用すると、高スループットのワークロードニーズに合わせた接続を作成し、オンプレミスゲートウェイと 間の専用ネットワーク接続を提供できます AWS。

Storage Gateway ではパブリックエンドポイントを使用します。 AWS Direct Connect 接続を配置すると、パブリック仮想インターフェイスを作成して、トラフィックを Storage Gateway エンドポイントにルーティングできます。パブリック仮想インターフェイスは、お客様のネットワークパスの中でインターネットサービスプロバイダーをバイパスします。Storage Gateway サービスのパブリックエンドポイントは、その場所と同じ AWS リージョン AWS Direct Connect にあることも、別の AWS リージョンにあることもできます。

次の図は、 が Storage Gateway と AWS Direct Connect どのように連携するかの例を示しています。
AWS ダイレクト接続を使用してクラウドに接続された Storage Gateway を示す ネットワークアーキテクチャ。

次の手順では、機能するゲートウェイを作成済みであることを前提としています。

Storage Gateway AWS Direct Connect で を使用するには

1. オンプレミスデータセンターと Storage Gateway エンドポイント間の AWS Direct Connect 接続を作成して確立します。接続の作成方法の詳細については、AWS Direct Connect ユーザーガイドの「使用の開始 AWS Direct Connect」を参照してください。
2. オンプレミスの Storage Gateway アプライアンスを AWS Direct Connect ルーターに接続します。
3. パブリック仮想インターフェイスを作成し、それに応じてオンプレミスのルーターを設定します。Direct Connect を使用しても、VPCエンドポイントは で作成する必要がありますHAProxy。詳細については、AWS Direct Connect ユーザーガイドの「仮想インターフェイスを作成する」を参照してください。

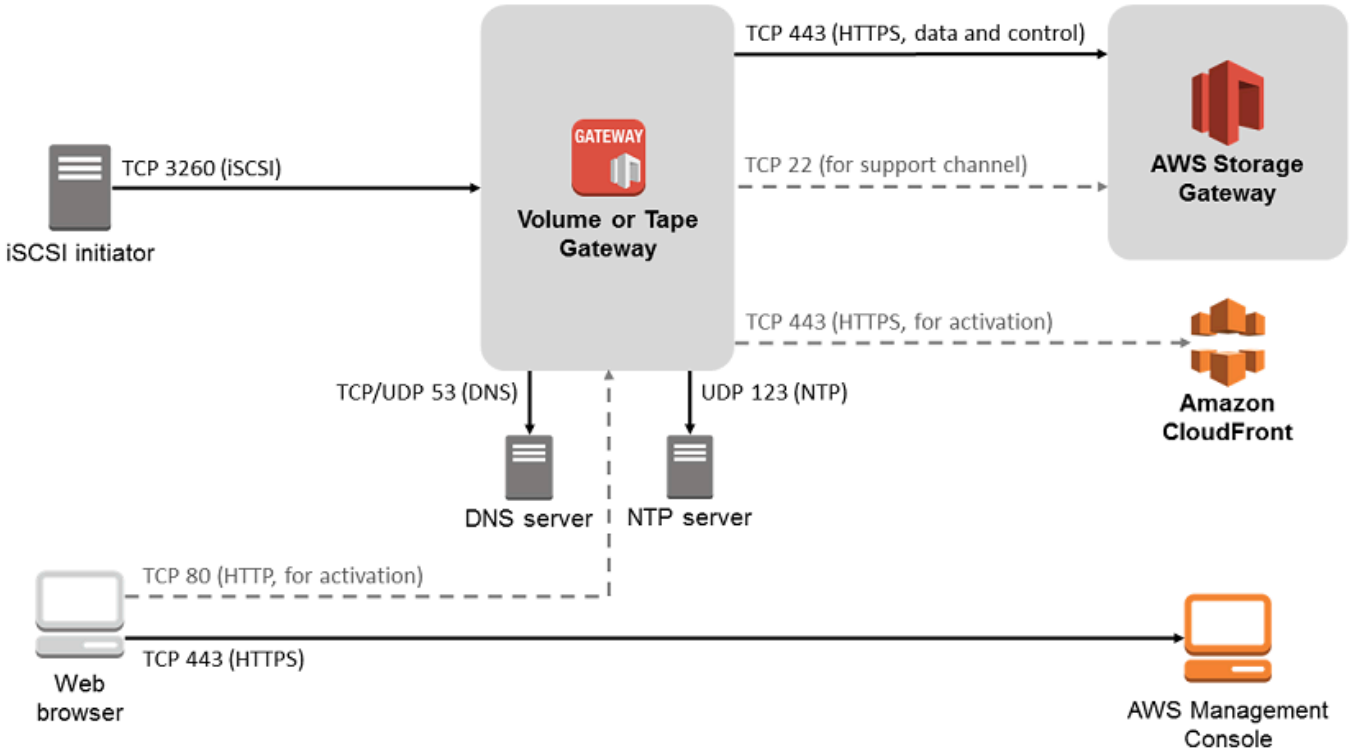
の詳細については AWS Direct Connect、「 ユーザーガイド」の「 とは AWS Direct ConnectAWS Direct Connect 」を参照してください。

ボリュームゲートウェイのネットワークポート要件

Storage Gateway には、オペレーションのために以下のポートが必要です。一部のポートは、すべてのゲートウェイタイプに共通で、それらに必要です。他のポートは、特定のゲートウェイタイプで必要です。このセクションでは、ボリュームゲートウェイに必要なポートの図とリストを掲載しています。

ボリュームゲートウェイ

次の図は、ボリュームゲートウェイのオペレーションのために開く必要があるすべてのポートを示しています。



以下のポートは、すべてのゲートウェイタイプに共通で、それらに必要です。

From	目的	[プロトコル]	[ポート]	用途	
Storage Gateway VM	AWS	Transmission Control Protocol (TCP)	443 (HTTPS)	Storage Gateway アウトバウンド VM から AWS サービスエンドポイントへの通信用。サービスエンドポイントの詳細については、「ファイアウォール	

From	目的	[プロトコル]	[ポート]	用途	
				とルーターを介したAWS Storage Gateway アクセスの許可」を参照してください。	

From	目的	[プロトコル]	[ポート]	用途	
ウェブブラウザ	Storage Gateway VM	TCP	80 (HTTP)	Storage Gateway のアクティベーションキーは、ローカルシステムにより取得されます。ポート 80 は Storage Gateway アプライアンスのアクティベーション時にのみ使用されます。 Storage Gateway VM には、ポート 80 へのパブリックアクセスは不要です。ポート 80 へのアクセスに必要なレベルはネットワークの設定によって決まります。Storage Gateway マネジメントコンソールからゲートウェイをアクティブ	

From	目的	[プロトコル]	[ポート]	用途	
				化する場合、コンソールに接続するホストには、ゲートウェイのポート 80 に対するアクセス権限が必要です。	
Storage Gateway VM	ドメインネームサービス (DNS) サーバー	ユーザーデータグラムプロトコル (UDP)/UDP	53 (DNS)	Storage Gateway VM とDNSサーバー間の通信用。	
Storage Gateway VM	AWS	TCP	22 (サポートチャネル)	AWS Support ゲートウェイの問題のトラブルシューティングに役立つゲートウェイへのアクセスを に許可します。このポートは、ゲートウェイの通常のオペレーションでは開いておく必要はありませんが、トラブルシューティングでは必要です。	

From	目的	[プロトコル]	[ポート]	用途	
Storage Gateway VM	Network Time Protocol (NTP) サーバー	UDP	123 (NTP)	VM 時間をホスト時間に同期するためにローカルシステムで使用されます。Storage Gateway VM は、次のNTPサーバーを使用するように設定されています。 • 0.amazon.pool.ntp.org • 1.amazon.pool.ntp.org • 2.amazon.pool.ntp.org • 3.amazon.pool.ntp.org	
Storage Gateway ハードウェアアプライアンス	Hypertext Transfer Protocol (HTTP) プロキシ	TCP	8080 (HTTP)	アクティベーションのために一時的に必要です。	

共通ポートに加えて、ボリュームゲートウェイには次のポートも必要です。

From	目的	[プロトコル]	[ポート]	用途	
iSCSI イニシエーター	Storage Gateway VM	TCP	3260 (iSCSI)	ゲートウェイによって公開される iSCSI ターゲットに接続するためのローカルシステム。	

ゲートウェイへの接続

ホストを選択してゲートウェイ VM をデプロイしたら、ゲートウェイを接続してアクティブ化します。これを行うには、ゲートウェイ VM の IP アドレスが必要です。ゲートウェイのローカルコンソールから IP アドレスを取得します。ローカルコンソールにログインし、コンソールページの先頭から IP アドレスを取得します。

オンプレミスでデプロイされているゲートウェイでは、ハイパーバイザーでも IP アドレスを取得できます。Amazon EC2ゲートウェイの場合、Amazon EC2マネジメントコンソールから Amazon EC2 インスタンスの IP アドレスを取得することもできます。ゲートウェイの IP アドレスを見つける方法については、次の 1 つを参照してください。

- VMware ホスト: を使用したゲートウェイローカルコンソールへのアクセス VMware ESXi
- HyperV ホスト: Microsoft Hyper-V でゲートウェイのローカルコンソールにアクセスする
- Linux カーネルベースの仮想マシン (KVM) ホスト: Linux を使用したゲートウェイローカルコンソールへのアクセス KVM
- EC2 ホスト: Amazon EC2ホストからの IP アドレスの取得

IP アドレスが見つかったら、それを書き留めます。Storage Gateway コンソールに戻り、コンソールで IP アドレスを入力します。

Amazon EC2ホストからの IP アドレスの取得

ゲートウェイがデプロイされている Amazon EC2インスタンスの IP アドレスを取得するには、EC2 インスタンスのローカルコンソールにログインします。コンソールページの先頭から IP アドレスを

取得します。手順については、Amazon EC2 Gateway ローカルコンソールへのログイン を参照してください。

Amazon EC2マネジメントコンソールから IP アドレスを取得することもできます。アクティベーションにはパブリック IP の使用が推奨されます。パブリック IPアドレスを取得するには、手順 1 を使用します。代わりに Elastic IP アドレスの使用を選択した場合、手順 2 を参照してください。

手順 1: パブリック IP アドレスを使用してゲートウェイに接続するには

1. で Amazon EC2コンソールを開きますhttps://console.aws.amazon.com/ec2/。
2. ナビゲーションペインで、インスタンス を選択し、ゲートウェイがデプロイされているEC2インスタンスを選択します。
3. 下部の [説明] タブを選択し、パブリック IP を書き留めます。この IP アドレスを使用してゲートウェイに接続します。Storage Gateway コンソールに戻り、IP アドレスを入力します。

アクティベーションに Elastic IP アドレスを使用する場合、次の手順を使用します。

手順 2: elastic IP アドレスを使用してゲートウェイに接続するには

1. で Amazon EC2コンソールを開きますhttps://console.aws.amazon.com/ec2/。
2. ナビゲーションペインで、インスタンス を選択し、ゲートウェイがデプロイされているEC2インスタンスを選択します。
3. 下部の [説明] タブを選択してから、[Elastic IP] 値を書き留めます。この elastic IP アドレスを使用して、ゲートウェイに接続します。Storage Gateway コンソールに戻り、elastic IP アドレスを入力します。
4. ゲートウェイがアクティブ化されたら、アクティブ化したゲートウェイを選択し、下部パネルのVTLデバイスタブを選択します。
5. すべてのVTLデバイスの名前を取得します。
6. 各ターゲットでは、以下のコマンドを実行してターゲットを設定します。

   ```
   iscsiadm -m node -o new -T [$TARGET_NAME] -p [$Elastic_IP]:3260
   ```

7. 各ターゲットで、以下のコマンドを実行してログインします。

   ```
   iscsiadm -m node -p [$ELASTIC_IP]:3260 --login
   ```

   これで、ゲートウェイはEC2インスタンスの Elastic IP アドレスを使用して接続されます。

Storage Gateway のリソースとリソースについて IDs

Storage Gateway では、プライマリリソースはゲートウェイですが、ボリューム 、仮想テープ 、ターゲット iSCSI、vtl デバイス などのリソースタイプがあります。これらは、サブリソースと呼ばれ、ゲートウェイに関連付けられている場合にのみ存在します。

これらのリソースとサブリソースには、次の表に示すように、一意の Amazon リソースネーム (ARNs) が関連付けられています。

リソースタイプ	ARN 形式
ゲートウェイ ARN	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`*
ボリューム ARN	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`* `/volume/`*`volume-id`*
ターゲット ARN (iSCSI ターゲット)	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`* `/target/`*`iSCSItarget`*

Storage Gateway は、EC2インスタンス、EBSボリューム、スナップショットの使用もサポートしています。これらのリソースは、Storage Gateway で使用される Amazon EC2リソースです。

リソースの使用 IDs

リソースを作成すると、Storage Gateway によってリソースに一意のリソース ID が割り当てられます。このリソース ID はリソース の一部ですARN。リソース ID は、リソース ID にハイフンと 8 文字の英数字の一意の組み合わせが続く形式です。たとえば、ゲートウェイ ID は `sgw-12A3456B` という形式であり、この `sgw` がゲートウェイのリソース ID です。ボリューム ID は `vol-3344CCDD` という形式であり、この `vol` がボリュームのリソース ID です。

仮想テープの場合は、最大 4 文字のプレフィックスをバーコード ID の先頭につけてテープを整理できます。

Storage Gateway リソースIDsは大文字です。ただし、これらのリソースを Amazon IDsで使用するとAPI、Amazon EC2 はリソースを小文字IDsでEC2想定します。で使用するには、リソース ID EC2 を小文字に変更する必要がありますAPI。たとえば、ボリュームの ID が Storage Gateway では `vol-1122AABB` であるとします。この ID を EC2 で使用する場合はAPI、 に変更する必要がありますvol-1122aabb。そうしないと、 が期待どおりに動作しないEC2API可能性があります。

Storage Gateway リソースのタグ付け

Storage Gateway では、タグを使用してリソースを管理できます。タグを付けることにより、メタデータをリソースに追加し、リソースを簡単に管理できるように分類できます。タグはそれぞれ、ユーザー定義の 1 つのキーと 1 つの値で構成されています。タグはゲートウェイ、ボリューム、および仮想テープに追加できます。追加したタグに基づいて、これらのリソースを検索したりフィルタリングしたりできます。

例えば、組織内の各部門が使用する Storage Gateway リソースを識別するためにタグを使用できます。経理部が使用するゲートウェイとボリュームには、`key=department`、`value=accounting` のようにタグを付けます。このタグでフィルタリングを実行して、経理部が使用するすべてのゲートウェイとボリュームを特定し、この情報を使用してコストを確認できます。詳細については、「コスト配分タグの使用」と「Tag Editor の使用」を参照してください。

タグが付いている仮想テープをアーカイブしても、そのテープのタグはアーカイブで維持されます。同様に、そのテープをアーカイブから別のゲートウェイで取得しても、そのタグは新しいゲートウェイで維持されます。

タグには意味論的意味はなく、タグは文字列として解釈されます。

タグには以下の制限があります。

- タグのキーと値は大文字と小文字が区別されます。
- 1 つのリソースに付けることができるタグの最大数は 50 です。
- タグキーを `aws:` で始めることはできません。このプレフィックスは AWS 専用として予約されています。
- キープロパティの有効な文字は、UTF-8 文字、数字、スペース、特殊文字 + - = . _ : / および @ です。

タグの操作

Storage Gateway コンソール、Storage Gateway 、APIまたは Storage Gateway Storage Gateway コマンドラインインターフェイス (CLI) を使用してタグを操作できます。以下の手順は、コンソールでタグを追加する方法、編集する方法、および削除する方法を示しています。

タグを追加するには

1. ホーム で Storage Gateway https://console.aws.amazon.com/storagegateway/コンソールを開きます。
2. ナビゲーションペインで、タグを付けるリソースを選択します。

   たとえば、ゲートウェイにタグを付ける場合は、[Gateways] を選択してから、ゲートウェイのリストからタグを付けるゲートウェイを選択します。
3. [Tags] を選択してから、[Add/edit tags] を選択します。
4. [Add/edit tags] ダイアログボックスで、[Create tag] を選択します。
5. [Key] でキーを、[Value] で値を入力します。たとえば、キーに [**Department**] を、値に [**Accounting**] を入力できます。

   > **Note**
   >
   > [Value] ボックスは空白のままにすることができます。

6. [Create Tag] を選択してタグを追加します。1 つのリソースに複数のタグを追加できます。
7. タグの追加が終了したら、[Save] を選択します。

タグを編集するには

1. ホーム で Storage Gateway https://console.aws.amazon.com/storagegateway/コンソールを開きます。
2. タグを編集するリソースを選択します。
3. [Tags] を選択して、[Add/edit tags] ダイアログボックスを開きます。
4. 編集するタグの横にある鉛筆アイコンを選択し、タグを編集します。
5. タグの編集が終了したら、[Save] を選択します。

タグを削除するには

1. ホーム で Storage Gateway https://console.aws.amazon.com/storagegateway/コンソールを開きます。
2. タグを削除するリソースを選択します。
3. [Tags] を選択してから、[Add/edit tags] を選択して [Add/edit tags] ダイアログボックスを開きます。
4. 削除するタグの横にある [X] アイコンを選択してから、[Save] を選択します。

AWS Storage Gatewayのオープンソースコンポーネントの使用

このセクションでは、Storage Gateway の機能を提供するために活用しているサードパーティ製のツールとライセンスについて説明します。

AWS Storage Gateway ソフトウェアに含まれている、特定のオープンソースソフトウェアコンポーネントのソースコードは、以下の場所からダウンロードできます。

- にデプロイされたゲートウェイの場合はESXi、sources.tar VMware をダウンロードします。https://s3.amazonaws.com/aws-storage-gateway-terms/sources.tar
- Microsoft Hyper-V にデプロイされたゲートウェイの場合は、sources_hyperv.tar をダウンロードします。
- Linux カーネルベースの仮想マシン (KVM) にデプロイされたゲートウェイの場合は、sources_.tar をダウンロードしますKVM。

この製品には、OpenSSL Toolkit (http://www.openssl.org/) で使用するために Open Project SSLによって開発されたソフトウェアが含まれています。依存するすべてのサードパーティー製ツールの関連ライセンスについては、サードパーティーのライセンスを参照してください。

AWS Storage Gateway クォータ

このトピックでは、Storage Gateway のボリュームとテープのクォータ、設定、およびパフォーマンスの制限について説明します。

トピック

- ボリュームのクォータ

ボリュームのクォータ

次の表は、ボリュームのクォータの一覧です。

説明	キャッシュボリューム	保管型ボリューム
ボリュームの最大サイズ **Note** サイズが 16 TiB を超えるキャッシュ型ボリュームからスナップショットを作成する場合は、Storage Gateway ボリュームに復元できますが、Amazon Elastic Block Store (Amazon EBS) ボリュームには復元できません。	32 TiB	16 TiB
ゲートウェイあたりの最大ボリューム数	32	32
ゲートウェイのすべてのボリュームの合計サイズ	1,024 TiB	512 TiB

ゲートウェイのローカルディスクの推奨サイズ

次の表は、デプロイされるゲートウェイのローカルディスクストレージの推奨サイズを示しています。

ゲートウェイタイプ	キャッシュ (最小)	キャッシュ (最大)	アップロードバッファ (最小)	アップロードバッファ (最大)	その他の必要なローカルディスク
キャッシュ型ボリュームゲートウェイ	150 GiB	64 TiB	150 GiB	2 TiB	—
保管型ボリュームゲートウェイ	—	—	150 GiB	2 TiB	1 つまたは複数の保管されたボリューム

> **Note**
>
> キャッシュおよびアップロードバッファ用として、1 つ以上のローカルドライブを、最大容量まで構成することができます。
> 既存のゲートウェイにキャッシュまたはアップロードバッファを追加する場合は、ホスト (ハイパーバイザーまたは Amazon EC2インスタンス) に新しいディスクを作成することが重要です。ディスクがキャッシュやアップロードバッファとして割り当て済みである場合は、既存のディスクサイズを変更しないでください。

API Storage Gateway のリファレンス

コンソールの使用に加えて、 AWS Storage Gateway APIを使用して、ゲートウェイをプログラムで設定および管理できます。このセクションでは、 AWS Storage Gateway オペレーション、認証のリクエスト署名、エラー処理について説明します。Storage Gateway で利用できるリージョンとエンドポイントの詳細については、「AWS 全般のリファレンス」の「AWS Storage Gateway エンドポイントとクォータ」を参照してください。

> **Note**
>
> を使用してアプリケーションを開発するときに、 を使用 AWS SDKsすることもできます AWS Storage Gateway。 AWS SDKs for Java、.NET、および は基盤となる をPHPラップし AWS Storage Gateway API、プログラミングタスクを簡素化します。SDK ライブラリのダウンロードについては、「サンプルコードライブラリ」を参照してください。

トピック

Storage Gateway の必須リクエストヘッダー

このセクションでは、Storage Gateway へのすべてのPOSTリクエストで送信する必要がある必須ヘッダーについて説明します。呼び出したいオペレーション、リクエストの日付、リクエストの送信者としてのユーザーの承認を示す情報など、リクエストに関するキー情報を識別するHTTPヘッダーを含めます。ヘッダーは大文字と小文字を区別されず、ヘッダーの順序は重要ではありません。

次の例は、 ActivateGatewayオペレーションで使用されるヘッダーを示しています。

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
Content-Type: application/x-amz-json-1.1
```

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120425/us-east-2/
storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target,
 Signature=9cd5a3584d1d67d57e61f120f35102d6b3649066abdd4bf4bbcf05bd9f2f8fe2
x-amz-date: 20120912T120000Z
x-amz-target: StorageGateway_20120630.ActivateGateway
```

以下は、Storage Gateway へのPOSTリクエストに含める必要があるヘッダーです。以下に示す「x-amz」で始まるヘッダーは、 AWS固有のヘッダーです。リストされている他のすべてのヘッダーは、HTTPトランザクションで使用される一般的なヘッダーです。

[Header] (ヘッダー)	説明
`Authorization`	Authorization ヘッダーには、リクエストがリクエスタに対して有効なアクションかどうかを Storage Gateway が判別するための、リクエストに関するいくつかの情報が含まれています。このヘッダーの形式は次のとおりです (改行は読みやすくするために追加されています)。 `Authorization: AWS4-HMAC_SHA456 Credentials= YourAccessKey /yyymmdd/region/storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target, Signature= CalculatedSignature` 前述の構文では、、年YourAccessKey、月、日 (yyyymmdd)、リージョン 、および を指定しますCalculatedSignature。認証ヘッダーの形式は、 AWS V4 署名プロセスの要件によって決まります。署名の詳細については、トピック リクエストへの署名 を参照してください。
`Content-Type`	Storage Gateway に対するすべてのリクエストでは、コンテンツタイプとして `application/x-amz-json-1.1` を使用します。 `Content-Type: application/x-amz-json-1.1`
`Host`	ホストヘッダーは、リクエストを送信する Storage Gateway エンドポイントを指定するために使用します。例えば `storagegateway.us-east-2.amazonaws.com` は、米国東部 (オハイオ) リージョンのエ

[Header] (ヘッダー)	説明
	ンドポイントを表します。Storage Gateway で利用できるエンドポイントの詳細については、「AWS 全般のリファレンス」の「AWS Storage Gateway エンドポイントとクォータ」を参照してください。 `Host: storagegateway. region.amazonaws.com`
`x-amz-date`	ヘッダーまたは AWS `x-amz-date` HTTPDateヘッダーのいずれかにタイムスタンプを指定する必要があります。(一部のHTTPクライアントライブラリでは、 Dateヘッダーを設定できません。) `x-amz-date` ヘッダーがある場合には、そのリクエストの認証時に Storage Gateway により `Date` ヘッダーが無視されます。`x-amz-date` 形式は「TYYYYMMDD」Z 形式の ISO8601 Basic HHMMSSである必要があります。ヘッダーDateと `x-amz-date` ヘッダーの両方を使用する場合、日付ヘッダーの形式は ISO8601 である必要はありません。 `x-amz-date: YYYYMMDD'T'HHMMSS'Z'`
`x-amz-target`	このヘッダーは、 のバージョンAPIと、リクエストするオペレーションを指定します。ターゲットヘッダー値は、APIバージョンをAPI名前と連結することで形成され、次の形式になります。 `x-amz-target: StorageGateway_ APIversion .operationName` operationName 値 (「」などActivateGateway) は、APIリストから確認できますAPI Storage Gateway のリファレンス。

リクエストへの署名

Storage Gateway では、リクエストに署名することで、送信するすべてのリクエストを認証する必要があります。リクエストに署名するには、暗号化ハッシュ関数を使用してデジタル署名を計算します。暗号化ハッシュは、入力データから一意のハッシュ値生成して返す関数です。ハッシュ関数に渡される入力データとしては、リクエストのテキスト、およびシークレットアクセスキーが該当しま

す。ハッシュ関数から返されるハッシュ値をリクエストに署名として含めます。署名は、リクエストの Authorization ヘッダーの一部です。

Storage Gateway は、受け取ったリクエストに対して、その署名に使用されたものと同じハッシュ関数と入力を使用して署名を再計算します。再計算された署名とリクエスト内の署名が一致した場合、Storage Gateway はそのリクエストを処理します。それ以外の場合、リクエストは拒否されます。

Storage Gateway は、AWS 署名バージョン 4 を使用した認証をサポートしています。署名の計算プロセスは 3 つのタスクに分けることができます。

- タスク 1: 正規リクエストを作成する

  HTTP リクエストを正規形式に再配置します。Storage Gateway は、送信された署名と比較するための再計算に正規化形式を使用するので、署名には正規化形式の使用が必須です。
- タスク 2: 署名対象の文字列を作成する

  暗号化ハッシュ関数への入力値の 1 つとして使用する文字列を作成します。署名文字列と呼ばれる文字列は、ハッシュアルゴリズムの名前、要求日付、認証情報スコープの文字列、および前のタスクで正規化されたリクエストを結合したものです。認証情報スコープの文字列自体は、日付、リージョン、およびサービス情報を結合したものです。
- タスク 3: 署名を作成する

  2 つの入力文字列 (署名文字列と派生キー) を受け付ける暗号化ハッシュ関数を使用して、リクエストの署名を作成します。派生キーは、シークレットアクセスキーから開始し、認証情報スコープ文字列を使用して一連のハッシュベースのメッセージ認証コード () を作成することによって計算されますHMACs。

署名の計算例

次の例では、 の署名の作成の詳細について説明しますListGateways。実際の署名計算方法を確認するときに、この例を参考にしてください。その他の参考計算例については、アマゾン ウェブ サービス用語集の「Signature Version 4 Test Suite」を参照してください。

例では、次のように想定しています。

- リクエストのタイムスタンプは「Mon, 10 Sep 2012 00:00:00」ですGMT。
- エンドポイントは、米国東部 (オハイオ) リージョンです。

一般的なリクエスト構文 (JSON本文を含む) は次のとおりです。

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
x-amz-Date: 20120910T000000Z
Authorization: SignatureToBeCalculated
Content-type: application/x-amz-json-1.1
x-amz-target: StorageGateway_20120630.ListGateways
{}
```

タスク 1: 正規リクエストを作成する に対して計算されたリクエストの正規形式は次のとおりです。

```
POST
/

content-type:application/x-amz-json-1.1
host:storagegateway.us-east-2.amazonaws.com
x-amz-date:20120910T000000Z
x-amz-target:StorageGateway_20120630.ListGateways

content-type;host;x-amz-date;x-amz-target
44136fa355b3678a1146ad16f7e8649e94fb4fc21fe77e8310c060f61caaff8a
```

正規リクエストの最後の行はリクエストボディのハッシュです。また、正規リクエストの 3 行目が空であることに注意してください。これは、この API (または Storage Gateway) のクエリパラメータがないためですAPIs。

タスク 2: 署名対象の文字列を作成する のための 署名用の文字列は次のとおりです。

```
AWS4-HMAC-SHA256
20120910T000000Z
20120910/us-east-2/storagegateway/aws4_request
92c0effa6f9224ac752ca179a04cecbede3038b0959666a8160ab452c9e51b3e
```

署名する文字列の最初の行はアルゴリズム、2 行目はタイムスタンプ、3 行目は認証情報スコープ、最後の行はタスク 1 で作成した正規リクエストのハッシュです。

タスク 3: 署名を作成する の場合、派生キーは、次のように表すことができます。

```
derived key = HMAC(HMAC(HMAC(HMAC("AWS4" + YourSecretAccessKey,"20120910"),"us-
east-2"),"storagegateway"),"aws4_request")
```

シークレットアクセスキー wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY を使用する場合、計算された署名は次のようになります。

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

最後のステップは、Authorization ヘッダーの構築です。デモンストレーションアクセスキー の場合AKIAIOSFODNN7EXAMPLE、ヘッダー (読みやすいように改行を追加) は次のとおりです。

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120910/us-east-2/
storagegateway/aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

エラーレスポンス

トピック

このセクションでは、 AWS Storage Gateway エラーに関するリファレンス情報を提供します。これらのエラーは、エラー例外とオペレーションエラーコードを表しています。例えば、リクエスト署名に問題がある場合、エラー例外は任意のAPIレスポンスによってInvalidSignatureException返されます。ただし、オペレーションエラーコードActivationKeyInvalidは ActivateGateway に対してのみ返されますAPI。

エラーの種類に応じて、Storage Gateway は例外だけを返すことも、例外とオペレーションエラーコードの両方を返すこともあります。エラーレスポンスの例を エラーレスポンス に示します。

例外

次の表に例外を示します AWS Storage Gateway API。 AWS Storage Gateway オペレーションがエラーレスポンスを返すと、レスポンス本文にはこれらの例外のいずれかが含まれま

す。InternalServerError と InvalidGatewayRequestException は、特定のオペレーションエラーコードを表示するオペレーションエラーコード オペレーションエラーコード メッセージの 1 つを返します。

Exception	メッセージ	HTTP ステータスコード
IncompleteSignatureException	指定された署名は不完全です。	400 Bad Request
InternalFailure	リクエストの処理は、不明なエラー、例外、または失敗により実行できませんでした。	500 Internal Server Error
InternalServerError	オペレーションエラーコード のオペレーションエラーコードメッセージの 1 つ。	500 Internal Server Error
InvalidAction	要求されたアクション、またはオペレーションは無効です。	400 Bad Request
InvalidClientTokenId	提供された X.509 証明書または AWS アクセスキー ID がレコードに存在しません。	403 Forbidden
InvalidGatewayRequestException	オペレーションエラーコード のオペレーションエラーコードメッセージの 1 つ。	400 Bad Request
InvalidSignatureException	計算したリクエスト署名が、指定された署名と一致しません。 AWS アクセスキーと署名方法を確認します。	400 Bad Request
MissingAction	リクエストに、アクションまたはオペレーションのパラメータが含まれていません。	400 Bad Request
MissingAuthenticationToken	リクエストには、有効な (登録された) AWS アクセスキー ID または X.509	403 Forbidden

Exception	メッセージ	HTTP ステータスコード
	証明書が含まれている必要があります。	
RequestExpired	リクエストの有効時間、またはリクエスト時間が過ぎています (どちらも 15 分間のパディング)。もしくは、リクエスト時間の発生が 15 分以上先です。	400 Bad Request
SerializationException	シリアル化の実行中にエラーが発生しました。JSON ペイロードの形式が適切であることを確認します。	400 Bad Request
ServiceUnavailable	サーバーの一時的な障害により、リクエストは失敗しました。	503 Service Unavailable
SubscriptionRequiredException	AWS アクセスキー ID にはサービスのサブスクリプションが必要です。	400 Bad Request
ThrottlingException	速度を超過しました。	400 Bad Request
TooManyRequests	Too many requests。	429 リクエストが多すぎます
UnknownOperationException	不明のオペレーションが指定されました。有効なオペレーションの一覧を Storage Gateway のオペレーションに示します。	400 Bad Request
UnrecognizedClientException	リクエストに含まれているセキュリティトークンが無効です。	400 Bad Request
ValidationException	入力パラメータの値が正しくないか、範囲外です。	400 Bad Request

オペレーションエラーコード

次の表は、 AWS Storage Gateway オペレーションエラーコードと、コードを返APIsすことができる とのマッピングを示しています。すべてのオペレーションエラーコードは、例外 で説明しているとおりに、2 つの一般的な例外 (`InternalServerError` もしくは `InvalidGatewayRequestException`) のいずれかと同時に返されます。

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
`ActivationKeyExpired`	指定されたアクティベーションキーの有効期限が切れました。	ActivateGateway
`ActivationKeyInvalid`	指定されたアクティベーションキーは無効です。	ActivateGateway
`ActivationKeyNotFound`	指定されたアクティベーションキーは見つかりませんでした。	ActivateGateway
`BandwidthThrottleScheduleNotFound`	指定された帯域幅スロットルは見つかりませんでした。	DeleteBandwidthRateLimit
`CannotExportSnapshot`	指定されたスナップショットはエクスポートできません。	CreateCachediSCSIVolume CreateStorediSCSIVolume
`InitiatorNotFound`	指定されたイニシエータは見つかりませんでした。	DeleteChapCredentials
`DiskAlreadyAllocated`	指定されたディスクは、既に割り当てられています。	AddCache AddUploadBuffer AddWorkingStorage

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
		CreateStorediSCSIVolume
DiskDoesNotExist	指定されたディスクは存在しません。	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
DiskSizeNotGigAligned	指定されたディスクは、ギガバイトに対応していません。	CreateStorediSCSIVolume
DiskSizeGreaterThanVolumeMaxSize	指定されたディスクサイズは、最大ボリュームサイズを超えています。	CreateStorediSCSIVolume
DiskSizeLessThanVolumeSize	指定されたディスクサイズは、ボリュームサイズ未満です。	CreateStorediSCSIVolume
DuplicateCertificateInfo	指定された証明書情報が重複しています。	ActivateGateway

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
GatewayInternalError	ゲートウェイ内部エラーが発生しました。	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
GatewayNotConnected	指定されたゲートウェイは、接続されていません。	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
GatewayNotFound	指定されたゲートウェイは、見つかりませんでした。	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
		ListLocalDisks ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
GatewayProxyNetworkConnectionBusy	指定されたゲートウェイプロキシネットワーク接続はビジーです。	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
InternalError	内部エラーが発生しました。	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
InvalidParameters	指定されたリクエストに不正なパラメータが含まれています。	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
LocalStorageLimitExceeded	ローカルストレージの上限を超えました。	AddCache AddUploadBuffer AddWorkingStorage
LunInvalid	指定された LUNが正しくありません。	CreateStorediSCSIVolume

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
MaximumVolumeCountExceeded	最大ボリューム数を超えました。	CreateCachediSCSIVolume CreateStorediSCSIVolume DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes
NetworkConfigurationChanged	ゲートウェイのネットワーク構成が変更されました。	CreateCachediSCSIVolume CreateStorediSCSIVolume

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
NotSupported	指定されたオペレーションは、サポートされていません。	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
OutdatedGateway	指定されたゲートウェイは、最新のものではありません。	ActivateGateway
SnapshotInProgressException	指定されたスナップショットは処理中です。	DeleteVolume
SnapshotIdInvalid	指定されたスナップショットは無効です。	CreateCachediSCSIVolume CreateStorediSCSIVolume

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
StagingAreaFull	ステージングエリアが満杯です。	CreateCachediSCSIVolume CreateStorediSCSIVolume
TargetAlreadyExists	指定されたターゲットは、既に存在しています。	CreateCachediSCSIVolume CreateStorediSCSIVolume
TargetInvalid	指定されたターゲットは無効です。	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials UpdateChapCredentials
TargetNotFound	指定されたターゲットは、見つかりませんでした。	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials DeleteVolume UpdateChapCredentials

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
UnsupportedOperationForGatewayType	指定されたオペレーションは、ゲートウェイタイプに対して有効ではありません。	AddCache AddWorkingStorage CreateCachediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteSnapshotSchedule DescribeCache DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes DescribeUploadBuffer DescribeWorkingStorage ListVolumeRecoveryPoints
VolumeAlreadyExists	指定されたボリュームは、既に存在しています。	CreateCachediSCSIVolume CreateStorediSCSIVolume
VolumeIdInvalid	指定されたボリュームは無効です。	DeleteVolume
VolumeInUse	指定されたボリュームは、既に使われています。	DeleteVolume

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
VolumeNotFound	指定されたボリュームは、見つかりませんでした。	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint DeleteVolume DescribeCachediSCSIVolumes DescribeSnapshotSchedule DescribeStorediSCSIVolumes UpdateSnapshotSchedule
VolumeNotReady	指定されたボリュームは、準備できていません。	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint

エラーレスポンス

エラーが発生した場合、レスポンスヘッダー情報には、以下の項目が含まれています。

- Content-Type: application/x-amz-json-1.1
- 適切な 4xxまたは5xxHTTPステータスコード

エラーレスポンスの本文には、発生したエラーに関する情報が含まれています。次のサンプルエラーは、すべてのエラーレスポンスに共通する、レスポンスエレメントの出力構文を示します。

```
{
    "__type": "String",
    "message": "String",
    "error":
        { "errorCode": "String",
          "errorDetails": "String"
        }
```

```
}
```

次の表は、前の構文で示したJSONエラーレスポンスフィールドについて説明しています。

__type

例外 からの例外の 1 つ。

型: 文字列

error

API固有のエラーの詳細が含まれます。一般的なエラー (つまり、 に固有ではないAPI) では、このエラー情報は表示されません。

タイプ: コレクション

errorCode

オペレーションエラーコードの 1 つ。

型: 文字列

errorDetails

このフィールドは、 の最新バージョンでは使用されませんAPI。

型: 文字列

メッセージ

オペレーションエラーコードメッセージの 1 つ 。

型: 文字列

エラーレスポンスの例

を使用して DescribeStorediSCSIVolumes、存在しないゲートウェイARNリクエスト入力を指定するAPIと、次のJSON本文が返されます。

```
{
  "__type": "InvalidGatewayRequestException",
  "message": "The specified volume was not found.",
  "error": {
```

```
    "errorCode": "VolumeNotFound"
  }
}
```

Storage Gateway がリクエストで送信された署名と一致しない署名を計算した場合、次のJSON本文が返されます。

```
{
  "__type": "InvalidSignatureException",
  "message": "The request signature we calculated does not match the signature you
 provided."
}
```

Storage Gateway のオペレーション

Storage Gateway オペレーションのリストについては、「 AWS Storage Gateway APIリファレンス」の「アクション」を参照してください。

「ボリュームゲートウェイユーザーガイド」のドキュメント履歴

- API バージョン : 2013-06-30
- ドキュメントの最新更新日: 2020 年 11 月 24 日

次の表に、2018 年 4 月以降の AWS Storage Gateway ユーザーガイドの各リリースにおける重要な変更点を示します。このドキュメントの更新に関する通知については、 RSSフィードをサブスクライブできます。

変更	説明	日付
メンテナンスの更新をオンまたはオフにするオプションを追加	Storage Gateway は、オペレーティングシステムとソフトウェアのアップグレード、安定性、パフォーマンス、セキュリティに対処するための修正、新機能へのアクセスなど、定期的なメンテナンス更新を受け取ります。デプロイ内の個々のゲートウェイでこれらの更新を有効または無効にする設定ができるようになりました。詳細については、「コンソール」「コンソールを使用したゲートウェイの更新の管理 AWS Storage Gateway」を参照してください。	2024 年 6 月 6 日
Snowball Edge でのテープゲートウェイのサポートの廃止	Snowball Edge デバイスでテープゲートウェイをホストすることはできなくなりました。	2024 年 3 月 14 日

サードパーティ製アプリケーションを使用してゲートウェイの設定をテストする手順を更新	サードパーティ製アプリケーションを使用してゲートウェイの設定をテストする手順で、バックアップジョブの進行中にゲートウェイが再起動した場合に想定される動作についての説明が追記されました。詳細については、「」を参照してください。	2023 年 10 月 24 日
推奨 CloudWatch アラームの更新	この CloudWatch HealthNotifications アラームは に適用され、すべてのゲートウェイタイプとホストプラットフォームに推奨されます。HealthNotifications および AvailabilityNotifications の推奨構成設定も更新されました。詳細については、CloudWatch 」「アラームを理解する」を参照してください。	2023 年 10 月 2 日

テープゲートウェイとボリュームゲートウェイのユーザーガイドを分離	以前は「Storage Gateway ユーザーガイド」にテープゲートウェイとボリュームゲートウェイの両方のタイプの情報を記載していましたが、「テープゲートウェイユーザーガイド」と「ボリュームゲートウェイユーザーガイド」に分割し、それぞれに該当タイプのゲートウェイに関する情報のみを記載するようにしました。詳細については、「テープゲートウェイユーザーガイド」と「ボリュームゲートウェイユーザーガイド」を参照してください。	2022 年 3 月 23 日
ゲートウェイの作成手順を更新	Storage Gateway コンソールを使用してゲートウェイを作成する手順が、すべてのゲートウェイタイプについて更新されました。詳細については、「ゲートウェイを作成する」を参照してください。	2022 年 1 月 18 日

テープのインターフェイスが新しくなりました	AWS Storage Gateway コンソールのテープの概要ページが、新しい検索およびフィルタリング機能で更新されました。新機能について説明するため、このガイドに記載されている関連するすべての手順が更新されました。詳細については、「Managing Your Tape Gateway」を参照してください。	2021 年 9 月 23 日
テープゲートウェイ用 Quest NetVault Backup 13 のサポート	テープゲートウェイは、Microsoft Windows Server 2012 R2 または Microsoft Windows Server 2016 で実行されている Quest NetVault Backup 13 をサポートするようになりました。詳細については、「Quest NetVault Backup を使用したセットアップのテスト」を参照してください。	2021 年 8 月 22 日
テープゲートウェイおよびボリュームゲートウェイのガイドから S3 ファイルゲートウェイのトピックが削除されました	テープゲートウェイおよびボリュームゲートウェイのユーザーガイドでは、ゲートウェイの種類を個別に設定するお客様にとってわかりやすくなるよう、不要なトピックがいくつか削除されました。	2021 年 7 月 21 日

Windows および Linux for Tape Gateway での IBM Spectrum Protect 8.1.10 のサポート	テープゲートウェイは、Microsoft Windows Server および Linux で実行されている IBM Spectrum Protect バージョン 8.1.10 をサポートするようになりました。詳細については、IBM「Spectrum Protect を使用したセットアップのテスト」を参照してください。	2020 年 11 月 24 日
フェデRAMPレーションコンプライアンス	Storage Gateway が FedRAMP に準拠するようになりました。詳細については、「Compliance validation for Storage Gateway」を参照してください。	2020 年 11 月 24 日
スケジュールベースの帯域幅のスロットリング	Storage Gateway のテープゲートウェイとボリュームゲートウェイで、スケジュールベースの帯域幅のスロットリングがサポートされるようになりました。詳細については、「Storage Gateway コンソールを使用した帯域幅スロットリングのスケジューリング」を参照してください。	2020 年 11 月 9 日

キャッシュ型ボリュームおよびテープゲートウェイのローカルキャッシュストレージが 4 倍増加	Storage Gateway のキャッシュ型ボリュームおよびテープゲートウェイで、最大 64 TB のローカルキャッシュがサポートされるようになりました。より大きな作業データセットへの低レイテンシーアクセスが実現するため、オンプレミスアプリケーションのパフォーマンスが向上します。詳細については、「ゲートウェイのローカルディスクの推奨サイズ」を参照してください。	2020 年 11 月 9 日
ゲートウェイの移行	Storage Gateway で、キャッシュ型のボリュームゲートウェイを新しい仮想マシンに移行できるようになりました。詳細については、「Moving Cached Volumes to a New Cached Volume Gateway Virtual Machine」を参照してください。	2020 年 9 月 10 日

テープ保持ロックと write-once-read-many（WORM) テープ保護のサポート	Storage Gateway は、仮想テープのテープ保持ロックをサポートし、多数の () を読み取ると書き込みますWORM。テープ保持ロックを使用すると、アーカイブされた仮想テープの保持モードと期間を指定できます。これにより、一定期間 (最大 100 年間)、削除されるのを防ぐことができます。これには、テープの削除や保存設定の変更が可能なユーザーに関するアクセス許可のコントロールが含まれます。詳細については、「Using Tape Retention Lock」を参照してください。WORMがアクティブ化された仮想テープは、仮想テープライブラリ内のアクティブなテープのデータを上書きまたは消去できないようにします。詳細については、「Write Once, Read Many (WORM) Tape Protection」を参照してください。	2020 年 8 月 19 日
コンソールを使用したハードウェアアプライアンスの注文	AWS Storage Gateway コンソールからハードウェアアプライアンスを注文できるようになりました。詳細については、「Storage Gateway ハードウェアアプライアンスの使用」を参照してください。	2020 年 8 月 12 日

新しい AWS リージョンでの連邦情報処理標準 (FIPS) エンドポイントのサポート	米国東部 (オハイオ)、米国東部 (バージニア北部)、米国西部 (北カリフォルニア)、米国西部 (オレゴン)、カナダ (中部) の各リージョンのFIPSエンドポイントでゲートウェイをアクティブ化できるようになりました。詳細については、「AWS 全般のリファレンス」の「AWS Storage Gateway エンドポイントとクォータ」を参照してください。	2020 年 7 月 31 日
ゲートウェイの移行	Storage Gateway で、テープおよび保管型のボリュームゲートウェイを新しい仮想マシンに移行できるようになりました。詳細については、「新しいゲートウェイへのデータの移動」を参照してください。	2020 年 7 月 31 日
Storage Gateway コンソールで Amazon CloudWatch アラームを表示する	Storage Gateway コンソールで CloudWatch アラームを表示できるようになりました。詳細については、」「アラームを理解する CloudWatch 」を参照してください。	2020 年 5 月 29 日

連邦情報処理標準 (FIPS) エンドポイントのサポート	リージョン内のFIPSエンドポイントを使用してゲートウェイを AWS GovCloud (US) アクティブ化できるようになりました。ボリュームゲートウェイのFIPSエンドポイントを選択するには、「サービスエンドポイントの選択」を参照してください。テープゲートウェイのFIPSエンドポイントを選択するには、「テープゲートウェイを に接続する AWS」を参照してください。	2020 年 5 月 22 日
新しい AWS リージョン	Storage Gateway がアフリカ (ケープタウン) および欧州 (ミラノ) リージョンで利用できるようになりました。詳細については、「AWS 全般のリファレンス」の「AWS Storage Gateway エンドポイントとクォータ」を参照してください。	2020 年 5 月 7 日

S3 Intelligent-Tiering ストレージクラスのサポート	Storage Gateway で S3 Intelligent-Tiering ストレージクラスがサポートされるようになりました。S3 Intelligent-Tiering ストレージクラスは、パフォーマンスの低下や、オペレーション上のオーバーヘッドを発生させることなく、最もコスト効率の高いストレージアクセス階層に自動的にデータを移動することで、ストレージコストを最小限に抑えます。詳細については、Amazon Simple Storage Service ユーザーガイドで「アクセスパターンが変化する、またはアクセスパターンが不明なデータを、自動的に最適化するためのストレージクラス」を参照してください。	2020 年 4 月 30 日
テープゲートウェイの書き込みおよび読み取りパフォーマンスが 2 倍に向上	Storage Gateway のテープゲートウェイの仮想テープ間で、書き込みおよび読み取りパフォーマンスが 2 倍向上しました。バックアップや復元に要する時間が短縮されます。詳細については、Storage Gateway ユーザーガイドの「Performance Guidance for Tape Gateways」を参照してください。	2020 年 4 月 23 日

自動テープ作成のサポート	Storage Gateway で、新しい仮想テープを自動的に作成できるようになりました。テープゲートウェイは、設定された最小数のテープを利用可能な状態に維持するために、自動的に新しい仮想テープを作成し、これらの新しいテープをバックアップアプリケーションでインポートできるようにします。このため、バックアップジョブを中断なく実行できるようになります。詳細については、Storage Gateway ユーザーガイドの「Creating Tapes Automatically」を参照してください。	2020 年 4 月 23 日
新しい AWS リージョン	Storage Gateway が AWS GovCloud（米国東部）リージョンで利用可能になりました。詳細については、「AWS 全般のリファレンス」の「AWS Storage Gateway エンドポイントとクォータ」を参照してください。	2020 年 3 月 12 日

Linux カーネルベースの仮想マシン (KVM) ハイパーバイザーのサポート	Storage Gateway で、KVM 仮想化プラットフォームにオンプレミスゲートウェイをデプロイできるようになりました。にデプロイされたゲートウェイKVMは、既存のオンプレミスゲートウェイと同じ機能を備えています。詳細については、Storage Gateway ユーザーガイドの「Supported Hypervisors and Host Requirements」を参照してください。	2020 年 2 月 4 日
VMware vSphere 高可用性のサポート	Storage Gateway では、ハードウェアVMware、ハイパーバイザー、またはネットワーク障害からストレージワークロードを保護するために、 での高可用性がサポートされるようになりました。詳細については、Storage Gateway ユーザーガイドの「Storage Gateway での VMware vSphere 高可用性の使用Storage Gateway」を参照してください。このリリースでは、パフォーマンス向上も行われています。詳細については、Storage Gateway ユーザーガイドの「Performance」を参照してください。	2019 年 11 月 20 日

テープゲートウェイの新しい AWS リージョン	テープゲートウェイが南米 (サンパウロ) リージョンで利用可能になりました。詳細については、「AWS 全般のリファレンス」の「AWS Storage Gateway エンドポイントとクォータ」を参照してください。	2019 年 9 月 24 日
Linux での IBM Spectrum Protect バージョン 7.1.9 のサポート、およびテープゲートウェイの最大テープサイズが 5 TiB に増加	テープゲートウェイは、Microsoft Windows での実行に加えて、Linux で実行される IBM Spectrum Protect (Tivoli Storage Manager) バージョン 7.1.9 をサポートするようになりました。詳細については、Storage Gateway ユーザーガイドのIBM「Spectrum Protect を使用したセットアップのテスト」を参照してください。 Storage Gateway また、テープゲートウェイで仮想テープの最大容量が 2.5 TiB から 5 TiB に増加しました。詳細については、Storage Gateway ユーザーガイドの「Quotas for Tapes」を参照してください。	2019 年 9 月 10 日

Amazon CloudWatch Logs のサポート	Amazon CloudWatch Log Groups でファイルゲートウェイを設定して、ゲートウェイとそのリソースのエラーとヘルスに関する通知を受け取ることができるようになりました。詳細については、「Storage Gateway ユーザーガイド」の「Amazon CloudWatch Log Groups によるゲートウェイのヘルスとエラーに関する通知の取得」を参照してください。 Storage Gateway	2019 年 9 月 4 日
新しい AWS リージョン	Storage Gateway が、アジアパシフィック (香港) リージョンで利用できるようになりました。詳細については、「AWS 全般のリファレンス」の「AWS Storage Gateway エンドポイントとクォータ」を参照してください。	2019 年 8 月 14 日
新しい AWS リージョン	Storage Gateway が、中東 (バーレーン) リージョンで利用できるようになりました。詳細については、「AWS 全般のリファレンス」の「AWS Storage Gateway エンドポイントとクォータ」を参照してください。	2019 年 7 月 29 日

仮想プライベートクラウドでのゲートウェイのアクティブ化のサポート (VPC)	でゲートウェイをアクティブ化できるようになりましたVPC。オンプレミスのソフトウェアアプライアンスとクラウドベースのストレージインフラストラクチャの間にプライベート接続を作成することができます。詳細については、「仮想プライベートクラウドでゲートウェイをアクティブ化する」を参照してください。	2019年6月20日
S3 Glacier Flexible Retrieval から S3 Glacier Deep Archive への仮想テープの移行に対応	コストの効率化と長期間のデータ保管用に、S3 Glacier Flexible Retrieval ストレージクラスにアーカイブされている仮想テープを S3 Glacier Deep Archive ストレージクラスに移動できるようになりました。詳細については、「S3 Glacier Flexible Retrieval から S3 Glacier Deep Archive へのテープの移動」を参照してください。	2019 年 5 月 28 日

SMB Microsoft Windows のファイル共有のサポート ACLs	ファイルゲートウェイでは、Microsoft Windows アクセスコントロールリスト (ACLs) を使用して、サーバーメッセージブロック (SMB) ファイル共有へのアクセスを制御できるようになりました。詳細については、「Microsoft Windows ACLsを使用してSMBファイル共有 へのアクセスを制御する」を参照してください。	2019 年 5 月 8 日
S3 Glacier Deep Archive との統合	テープゲートウェイは S3 Glacier Deep Archive と統合できます。S3 Glacier Deep Archive で仮想テープを長期データ保持用にアーカイブできるようになりました。詳細については、「仮想テープのアーカイブ」を参照してください。	2019 年 3 月 27 日

欧州での Storage Gateway ハードウェアアプライアンスの可用性	Storage Gateway ハードウェアアプライアンスが、欧州で利用できるようになりました。詳細については、「AWS 全般のリファレンス」の「AWS Storage Gateway ハードウェアアプライアンスリージョン」を参照してください。さらに、Storage Gateway ハードウェアアプライアンスで利用可能なストレージを 5 TB から 12 TB に増やし、取り付けられている銅線ネットワークカードを 10 ギガビットの光ファイバーネットワークカードに交換できます。詳細については、「ハードウェアアプライアンスの設定」を参照してください。	2019 年 2 月 25 日
との統合 AWS Backup	Storage Gateway は と統合されます AWS Backup。 AWS Backup を使用して、Cloud-Backed ストレージに Storage Gateway ボリュームを使用するオンプレミスのビジネスアプリケーションをバックアップできるようになりました。詳細については、「ボリュームのバックアップ」を参照してください。	2019 年 1 月 16 日

Bacula Enterprise と IBM Spectrum Protect のサポート	テープゲートウェイが Bacula Enterprise と IBM Spectrum Protect をサポートするようになりました。Storage Gateway は、Veritas 、Veritas Backup Exec NetBackup、Quest NetVault バックアップの新しいバージョンもサポートするようになりました。これらのバックアップアプリケーションを使用してデータを Amazon S3 にバックアップし、オフラインストレージ (S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive) に直接アーカイブできるようになりました。詳細については、「バックアップソフトウェアを使用してゲートウェイのセットアップをテストする」を参照してください。	2018 年 11 月 13 日

Storage Gateway ハードウェアアプライアンスのサポート	Storage Gateway ハードウェアアプライアンスには、サードパーティーのサーバーにプリインストールされた Storage Gateway ソフトウェアが含まれています。 AWS Management Consoleからアプライアンスを管理できます。アプライアンスは、ファイルゲートウェイ、テープゲートウェイ、およびボリュームゲートウェイをホストできます。詳細については、「Using the Storage Gateway Hardware Appliance」を参照してください。	2018 年 9 月 18 日
Microsoft System Center 2016 Data Protection Manager との互換性 (DPM)	テープゲートウェイが Microsoft System Center 2016 Data Protection Manager () と互換性があるようになりましたDPM。Microsoft を使用してデータを Amazon S3 にDPMバックアップし、オフラインストレージ (S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive) に直接アーカイブできるようになりました。詳細については、「Microsoft System Center Data Protection Manager を使用したセットアップのテスト」を参照してください。	2018 年 7 月 18 日

Server Message Block (SMB) プロトコルのサポート	ファイルゲートウェイは、サーバーメッセージブロック (SMB) プロトコルのサポートをファイル共有に追加しました。詳細については、「ファイル共有の作成」を参照してください。	2018 年 6 月 20 日
ファイル共有、キャッシュ型ボリューム、および仮想テープの暗号化のサポート	AWS Key Management Service （ AWS KMS) を使用して、ファイル共有、キャッシュ型ボリューム、または仮想テープに書き込まれたデータを暗号化できるようになりました。現在、 を使用してこれを行うことができます AWS Storage Gateway API。詳細については、「Data encryption using AWS KMS」を参照してください。	2018 年 12 月 6 日

NovaStor DataCenter/Network のサポート	テープゲートウェイが NovaStor DataCenter/Network をサポートするようになりました。NovaStor DataCenter/Network バージョン 6.4 または 7.1 を使用してデータを Amazon S3 にバックアップし、オフラインストレージ (S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive) に直接アーカイブできるようになりました。詳細については、NovaStor DataCenter「/Network を使用したセットアップのテスト」を参照してください。	2018 年 5 月 24 日

以前の更新

以下の表に、2018 年 5 月より前の 『AWS Storage Gateway ユーザーガイド』の各リリースにおける重要な変更点を示します。

変更	説明	変更日
S3 1 ゾーン_IA ストレージクラスのサポート	ファイルゲートウェイで、S3 1 ゾーン_IA をファイル共有のデフォルトのストレージクラスとして選択できるようになりました。このストレージクラスを使用すると、Amazon S3 の単一のアベイラビリティーゾーンにオブジェクトデータを保存できます。詳細については、「Create a file share」を参照してください。	2018 年 4 月 4 日
新しいリージョン	テープゲートウェイがアジアパシフィック (シンガポール) リージョンで利用できるようになりました。詳細については、「AWS リージョン Storage Gateway をサポートする」を参照してください。	2018 年 4 月 3 日

変更	説明	変更日
Amazon S3 バケットの更新キャッシュ通知、リクエスタ支払い、および既定ACLsのサポート。	ファイルゲートウェイで、ゲートウェイによる Amazon S3 バケットのキャッシュの更新が完了したときに、通知を受けることができるようになりました。詳細については、Storage Gateway APIリファレンスのRefreshCache「.html」を参照してください。 ファイルゲートウェイを使用して、バケット所有者ではなくリクエスタまたはリーダーがアクセス料金を支払うことができるようになりました。 ファイルゲートウェイでは、NFSファイル共有にマッピングされる S3 バケットの所有者にフルコントロールを付与できるようになりました。 詳細については、「Create a file share」を参照してください。	2018 年 3 月 1 日
Dell EMC NetWorker V9.x のサポート	テープゲートウェイが Dell EMC NetWorker V9.x をサポートするようになりました。Dell EMC NetWorker V9.x を使用してデータを Amazon S3 にバックアップし、オフラインストレージ (S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive) に直接アーカイブできるようになりました。詳細については、「Dell を使用したセットアップのテストEMC NetWorker」を参照してください。	2018 年 2 月 27 日
新しいリージョン	Storage Gateway が欧州 (パリ) リージョンで利用可能になりました。詳細については、「AWS リージョン Storage Gateway をサポートする」を参照してください。	2017 年 12 月 18 日

変更	説明	変更日
ファイルアップロード通知とMIME タイプの推測のサポート	ファイル共有に書き込まれたすべてのファイルがAmazon S3 にアップロードされたときに、NFSファイルゲートウェイから通知を受け取ることができるようになりました。詳細については、Storage Gateway APIリファレンスNotifyWhenUploadedの「」を参照してください。 ファイルゲートウェイで、ファイル拡張子に基づいてMIMEアップロードされたオブジェクトのタイプを推測できるようになりました。詳細については、「Create a file share」を参照してください。	2017 年 11 月 21 日
VMware ESXi Hypervisor バージョン 6.5 のサポート	AWS Storage Gateway で VMware ESXi Hypervisor バージョン 6.5 がサポートされるようになりました。これは、バージョン 4.1、5.0、5.1、5.5、および 6.0 に加えてサポートされます。詳細については、「サポートされているハイパーバイザーとホストの要件」を参照してください。	2017 年 9 月 13 日
Commvault 11 との互換性	テープゲートウェイが Commvault 11 に対応しました。Commvault を使用してデータを Amazon S3 にバックアップし、オフラインストレージ (S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive) に直接アーカイブできるようになりました。詳細については、「Commvault を使用したセットアップのテスト」を参照してください。	2017 年 9 月 12 日
Microsoft Hyper-V ハイパーバイザーのファイルゲートウェイサポート	Microsoft Hyper-V ハイパーバイザーにファイルゲートウェイをデプロイできるようになりました。詳細については、サポートされているハイパーバイザーとホストの要件 を参照してください。	2017 年 6 月 22 日

変更	説明	変更日
3 ~ 5 時間のテープをアーカイブから取得するサポート	テープゲートウェイでは、3 ~ 5 時間でテープをアーカイブから取得できるようになりました。バックアップアプリケーションまたは仮想テープライブラリ () からテープに書き込まれるデータの量を決定することもできますVTL。詳細については、「テープの使用状況の表示」を参照してください。	2017 年 5 月 23 日
新しいリージョン	Storage Gateway がアジアパシフィック (ムンバイ) リージョンで利用可能になりました。詳細については、「AWS リージョン Storage Gateway をサポートする」を参照してください。	2017 年 5 月 02 日
ファイル共有の設定に更新します ファイル共有のためのキャッシュ更新のサポート	ファイルゲートウェイで、ファイル共有の設定にマウントオプションが追加されました。ファイル共有に squash と読み取り専用オプションを設定できるようになりました。詳細については、「Create a file share」を参照してください。 ファイルゲートウェイで、最後にバケットのコンテンツのリストが取得され、その結果がキャッシュに保存された時点以降に Amazon S3 バケットに追加または削除されたオブジェクトを、検出できるようになりました。詳細については、「 APIリファレンス RefreshCache」の「」を参照してください。	2017 年 3 月 28 日
ボリュームのクローンをサポート	キャッシュ型ボリュームゲートウェイの場合、 は既存のボリュームからボリュームのクローンを作成する機能をサポートする AWS Storage Gateway ようになりました。詳細については、「ボリュームをクローンする」を参照してください。	2017 年 3 月 16 日

変更	説明	変更日
Amazon でのファイルゲートウェイのサポート EC2	AWS Storage Gateway で、Amazon にファイルゲートウェイをデプロイできるようになりましたEC2。コミュニティ として利用可能になった Storage Gateway Amazon マシンイメージ (AMI) EC2を使用して、Amazon でファイルゲートウェイを起動できます AMI。 Storage Gateway ファイルゲートウェイを作成してEC2インスタンスにデプロイする方法については、Amazon S3 ファイルゲートウェイの作成とアクティブ化」または「Amazon FSx ファイルゲートウェイの作成とアクティブ化」を参照してください。ファイルゲートウェイ を起動する方法については AMI、「Amazon EC2ホストでの S3 ファイルゲートウェイのデプロイ」または「Amazon EC2ホストでの FSxファイルゲートウェイのデプロイ」を参照してください。	2017 年 2 月 08 日
Arcserve 17 との互換性	テープゲートウェイが Arcserve 17 に対応しました。Arcserve を使用してデータを Amazon S3 にバックアップし、S3 Glacier Flexible Retrieval に直接アーカイブできるようになりました。詳細については、「Arcserve Backup r17.0 を使用したセットアップのテスト」を参照してください。	2017 年 1 月 17 日
新しいリージョン	Storage Gateway は、欧州 (ロンドン) リージョンで利用可能になりました。詳細については、「AWS リージョン Storage Gateway をサポートする」を参照してください。	2016 年 12 月 13 日
新しいリージョン	Storage Gateway は、カナダ (中部) リージョンで利用可能になりました。詳細については、「AWS リージョン Storage Gateway をサポートする」を参照してください。	2016 年 12 月 08 日

変更	説明	変更日
ファイルゲートウェイのサポート	Storage Gateway で、ボリュームゲートウェイとテープゲートウェイに加えてファイルゲートウェイも利用できるようになりました。File Gateway はサービスと仮想ソフトウェアアプライアンスを組み合わせて、ネットワークファイルシステム () などの業界標準のファイルプロトコルを使用して Amazon S3 にオブジェクトを保存および取得できるようにしますNFS。ゲートウェイは、NFSマウントポイント上のファイルとして Amazon S3 内のオブジェクトへのアクセスを提供します。	2016 年 11 月 29 日
Backup Exec 16	テープゲートウェイが Backup Exec 16 に対応しました。Backup Exec 16 を使用してデータを Amazon S3 にバックアップし、オフラインストレージ (S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive) に直接アーカイブできるようになりました。詳細については、「Veritas Backup Exec を使用したセットアップのテスト」を参照してください。	2016 年 11 月 7 日
Micro Focus (HPE) Data Protector 9.x との互換性	テープゲートウェイが Micro Focus (HPE) Data Protector 9.x と互換性を持つようになりました。HP E Data Protector を使用してデータを Amazon S3 にバックアップし、S3 Glacier Flexible Retrieval に直接アーカイブできるようになりました。詳細については、「Micro Focus (HPE) Data Protector を使用したセットアップのテスト」を参照してください。	2016 年 11 月 2 日
新しいリージョン	Storage Gateway が米国東部 (オハイオ) リージョンで利用可能になりました。詳細については、「AWS リージョン Storage Gateway をサポートする」を参照してください。	2016 年 10 月 17 日

変更	説明	変更日
Storage Gateway コンソールの再設計	ゲートウェイ、ボリューム、仮想テープを簡単に設定、管理、モニタリングできるよう、Storage Gateway マネジメントコンソールが再設計されました。ユーザーインターフェイスで、フィルタリングできるビューが提供され、 CloudWatch や Amazon などの統合 AWS サービスに直接リンクできるようになりましたEBS。詳細については、「にサインアップする AWS Storage Gateway」を参照してください。	2016 年 8 月 30 日
Veeam Backup & Replication V9 アップデート 2 以降のバージョンとの互換性	テープゲートウェイが Veeam Backup & Replication V9 アップデート 2 以降のバージョン (バージョン 9.0.0.1715 以降) に対応しました。Veeam Backup Replication V9 Update 2 以降を使用して、データを Amazon S3 にバックアップし、オフラインストレージ (S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive) に直接アーカイブできるようになりました。詳細については、「Veeam Backup & Replication を使用したセットアップのテスト」を参照してください。	2016 年 8 月 15 日
ボリュームとスナップショットが長くなる IDs	Storage Gateway では、ボリュームとスナップショットIDsの の導入時間が長くなっています。ボリューム、スナップショット、およびその他のサポートされている AWS リソースに対して、長い ID 形式をアクティブ化できます。詳細については、「Storage Gateway のリソースとリソースについて IDs」を参照してください。	2016 年 4 月 25 日

変更	説明	変更日
新しいリージョン ストレージ容量が最大 512 TiB の保存型ボリュームのサポート Storage Gateway ローカルコンソールに対して行われたゲートウェイのその他の更新と機能の強化	テープゲートウェイが、アジアパシフィック (ソウル) リージョンで使用できるようになりました。詳細については、「AWS リージョン Storage Gateway をサポートする」を参照してください。 保存型ボリュームの場合、ストレージ容量が最大 512 TiB のストレージボリュームを最大 32 個 (各ボリュームのサイズは最大 16 TiB) 作成できるようになりました。詳細については、「保管型ボリュームのアーキテクチャ」および「AWS Storage Gateway クォータ」を参照してください。 仮想テープライブラリ内のすべてのテープの合計サイズは 1 PiB に増加します。詳細については、「AWS Storage Gateway クォータ」を参照してください。 Storage Gateway コンソールで VM ローカルコンソールのパスワードを設定できるようになりました。詳細については、Storage Gateway コンソールからのローカルコンソールパスワードの設定 を参照してください。	2016 年 3 月 21 日
for Dell EMC NetWorker 8.x との互換性	テープゲートウェイが Dell EMC NetWorker 8.x と互換性があるようになりました。Dell を使用してデータを Amazon S3 にEMC NetWorker バックアップし、オフラインストレージ (S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive) に直接アーカイブできるようになりました。詳細については、「Dell を使用したセットアップのテストEMC NetWorker」を参照してください。	2016 年 2 月 29 日

変更	説明	変更日
VMware ESXi Hypervisor バージョン 6.0 および Red Hat Enterprise Linux 7 iSCSI イニシエータのサポート	AWS Storage Gateway で VMware ESXi Hypervisor バージョン 6.0 と Red Hat Enterprise Linux 7 iSCSI イニシエータがサポートされるようになりました。詳細については、「サポートされているハイパーバイザーとホストの要件」および「サポートされている iSCSI イニシエータ」を参照してください。	2015 年 10 月 20 日
コンテンツの再編成	このリリースでは、ドキュメントが改善されており、新たに含められた「アクティブ化したゲートウェイの管理」セクションに、すべてのゲートウェイソリューションに共通の管理タスクがまとめられています。次に、デプロイしてアクティベートした後のゲートウェイを管理する方法が記載されています。詳細については、「ゲートウェイを管理する」を参照してください。	

変更	説明	変更日
ストレージ容量が最大 1,024 TiB のキャッシュ型ボリュームのサポート	キャッシュ型ボリュームの場合、ストレージ容量が最大 1,024 TiB のストレージボリュームを最大 32 個作成できるようになりました。詳細については、「キャッシュ型ボリュームのアーキテクチャ」および「AWS Storage Gateway クォータ」を参照してください。	2015 年 9 月 16 日
VMware ESXi ハイパーバイザーでの VMXNET3 (10 GbE) ネットワークアダプタタイプのサポート	ゲートウェイがVMwareESXiハイパーバイザーでホストされている場合は、VMXNET3アダプタータイプを使用するようにゲートウェイを再設定できます。詳細については、「ゲートウェイのネットワークアダプタの設定」を参照してください。	
パフォーマンスの拡張	Storage Gateway の最大アップロード速度が 120 MB/秒に向上し、最大ダウンロード速度が 20 MB/秒に向上しました。	
Storage Gateway のローカルコンソールの拡張と更新	Storage Gateway ローカルコンソールが更新および強化され、メンテナンスタスクを実行するための機能が追加されました。詳細については、「ゲートウェイのネットワークの設定」を参照してください。	
タグ指定のサポート	Storage Gateway でリソースのタグ付けがサポートされるようになりました。ゲートウェイ、ボリューム、および仮想テープにタグを追加して、簡単に管理できるようになりました。詳細については、「Storage Gateway リソースのタグ付け」を参照してください。	2015 年 9 月 2 日
Quest (旧 Dell) NetVault Backup 10.0 との互換性	テープゲートウェイが Quest NetVault Backup 10.0 と互換性があるようになりました。Quest NetVault Backup 10.0 を使用してデータを Amazon S3 にバックアップし、オフラインストレージ (S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive) に直接アーカイブできるようになりました。詳細については、「Quest NetVault Backup を使用したセットアップのテスト」を参照してください。	2015 年 6 月 22 日

変更	説明	変更日
保管型ボリュームゲートウェイのセットアップ用 16 TiB ストレージボリュームのサポート	Storage Gateway で、保管型ボリュームのゲートウェイの設定用に 16 TiB ストレージボリュームがサポートされるようになりました。16 TiB ストレージボリュームを 12 個作成できるようになりました (ストレージは最大 192 TiB)。詳細については、「保管型ボリュームのアーキテクチャ」を参照してください。	2015 年 6 月 3 日
Storage Gateway ローカルコンソールでのシステムリソースチェックのサポート	これで、システムリソース (仮想CPUコア、ルートボリュームサイズ、RAM) がゲートウェイが正しく機能するのに十分かどうかを判断できます。詳細については、ゲートウェイシステムリソースのステータスの表示 または ゲートウェイシステムリソースのステータスの表示 を参照してください。	
Red Hat Enterprise Linux 6 iSCSI イニシエータのサポート	Storage Gateway が Red Hat Enterprise Linux 6 iSCSI イニシエータをサポートするようになりました。詳細については、「Volume Gateway の設定要件」を参照してください。 このリリースでは、次のように Storage Gateway が改良および更新されています。 • Storage Gateway コンソールから、最後にソフトウェア更新が正常にゲートウェイに適用された日時を確認できるようになりました。詳細については、「ゲートウェイの更新の管理」を参照してください。 • Storage Gateway では、ストレージボリュームに接続されたイニシエータを一覧表示するためにAPI使用できる SCSIが提供されるようになりました。詳細については、 APIリファレンスListVolumeInitiatorsの「」を参照してください。	

変更	説明	変更日
Microsoft Hyper-V hypervisor バージョン 2012 および 2012 R2 のサポート	Storage Gateway で、Microsoft Hyper-V hypervisor バージョン 2012 および 2012 R2 がサポートされるようになりました。これは、Microsoft Hyper-V hypervisor バージョン 2008 R2 に加えてサポートされます。詳細については、「サポートされているハイパーバイザーとホストの要件」を参照してください。	2015 年 4 月 30 日
Symantec Backup Exec 15 との互換性	テープゲートウェイが Symantec Backup Exec 15 に対応しました。Symantec Backup Exec 15 を使用してデータを Amazon S3 にバックアップし、オフラインストレージ (S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive) に直接アーカイブできるようになりました。詳細については、「Veritas Backup Exec を使用したセットアップのテスト」を参照してください。	2015 年 4 月 6 日
CHAP ストレージボリュームの 認証サポート	Storage Gateway で、ストレージボリュームのCHAP認証の設定がサポートされるようになりました。詳細については、「ボリュームのCHAP認証を設定する」を参照してください。	2015 年 4 月 2 日
VMware ESXi Hypervisor バージョン 5.1 および 5.5 のサポート	Storage Gateway で VMware ESXi Hypervisor バージョン 5.1 および 5.5 がサポートされるようになりました。これは、VMwareESXiHypervisor バージョン 4.1 および 5.0 のサポートに追加されています。詳細については、「サポートされているハイパーバイザーとホストの要件」を参照してください。	2015 年 30 月 3 日

変更	説明	変更日
Windows CHKDSKユーティリティのサポート	Storage Gateway で Windows CHKDSKユーティリティがサポートされるようになりました。このユーティリティを使用すると、ボリュームの整合性を確認し、ボリューム上のエラーを修正することができます。詳細については、「ボリュームの問題のトラブルシューティング」を参照してください。	2015 年 3 月 04 日
との統合 AWS CloudTrail による API通話のキャプチャ	Storage Gateway は、Amazon Web Services アカウントの Storage Gateway によって、または Storage Gateway に代わって行われた AWS CloudTrail. AWS CloudTrail captures API呼び出しと統合され、指定した Amazon S3 バケットにログファイルが配信されるようになりました。詳細については、「での ログ記録とモニタリング AWS Storage Gateway」を参照してください。 このリリースで、Storage Gateway は次の点で改良および更新されました。 • キャッシュストレージにダーティデータがある仮想テープ (AWSにアップロードされていないコンテンツを含むテープ) は、ゲートウェイのキャッシュ型ドライブの変更時に復旧されるようになりました。詳細については、「回復不可能なゲートウェイからの仮想テープの復旧」を参照してください。	2014 年 12 月 16 日

変更	説明	変更日
追加のバックアップソフトウェアやメディアチェンジャーとの互換性	テープゲートウェイが、次のバックアップソフトウェアに対応しました。 • Symantec Backup Exec 2014 • Microsoft System Center 2012 R2 Data Protection Manager • Veeam Backup & Replication V7 • Veeam Backup & Replication V8 Storage Gateway 仮想テープライブラリ (VTL) でこれらの 4 つのバックアップソフトウェア製品を使用して Amazon S3 にバックアップし、オフラインストレージ (S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive) に直接アーカイブできるようになりました。詳細については、「バックアップソフトウェアを使用してゲートウェイのセットアップをテストする」を参照してください。 Storage Gateway で、新しいバックアップソフトウェアと連携する追加のメディアチェンジャーが提供されるようになりました。 このリリースには、その他の AWS Storage Gateway 改善や更新が含まれています。	2014 年 11 月 3 日
欧州 (フランクフルト) リージョン	Storage Gateway は、欧州 (フランクフルト) リージョンで利用可能になりました。詳細については、「AWS リージョン Storage Gateway をサポートする」を参照してください。	2014 年 10 月 23 日

変更	説明	変更日
コンテンツの再編成	すべてのゲートウェイソリューションに共通の「はじめに」セクションを作成しました。次に、ゲートウェイをダウンロード、デプロイ、およびアクティブ化するための手順を説明します。ゲートウェイをデプロイおよびアクティブ化した後は、保管型ボリューム、キャッシュ型ボリューム、テープゲートウェイを設定する個別の手順に進むことができます。詳細については、「テープゲートウェイの作成」を参照してください。	2014 年 5 月 19 日
Symantec Backup Exec 2012 との互換性	テープゲートウェイが Symantec Backup Exec 2012 に対応しました。Symantec Backup Exec 2012 を使用してデータを Amazon S3 にバックアップし、オフラインストレージ (S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive) に直接アーカイブできるようになりました。詳細については、「Veritas Backup Exec を使用したセットアップのテスト」を参照してください。	2014 年 4 月 28 日

変更	説明	変更日
Windows Server Failover Clustering のサポート VMware ESX イニシエータのサポート Storage Gateway ローカルコンソールでの設定タスクの実行のサポート	• Windows Server フェイルオーバークラスタリング () を使用してホストがアクセスを調整する場合、Storage Gateway は複数のホストを同じボリュームに接続できるようになりましたWSFC。ただし、 を使用せずに複数のホストを同じボリュームに接続することはできませんWSFC。 • Storage Gateway で、ESXホスト経由でストレージ接続を直接管理できるようになりました。これにより、 のゲスト OS に常駐するイニシエータを使用する代わりに使用できますVMs。 • Storage Gateway では、Storage Gateway ローカルコンソールでの設定タスクの実行を行えるようになりました。オンプレミスにデプロイされたゲートウェイでの設定タスクの実行については、「VM ローカルコンソールでのタスクの実行」または「VM ローカルコンソールでのタスクの実行」を参照してください。EC2 インスタンスにデプロイされたゲートウェイで設定タスクを実行する方法については、Amazon EC2 Local Console でのタスクの実行「」または「」を参照してくださいAmazon EC2 Local Console でのタスクの実行。	2014 年 1 月 31 日

変更	説明	変更日
仮想テープライブラリ (VTL) のサポートとAPIバージョン 2013-06-30 の導入	Storage Gateway は、オンプレミスのソフトウェアアプライアンスをクラウドベースのストレージに接続して、オンプレミスの IT 環境を AWS ストレージインフラストラクチャと統合します。Storage Gateway では、ボリュームゲートウェイ (キャッシュ型ボリュームとストアド型ボリューム) に加えて、ゲートウェイ仮想テープライブラリ () がサポートされるようになりましたVTL。ゲートウェイごとに最大 10 個の仮想テープドライブを使用して、テープゲートウェイを構成できます。各仮想テープドライブはSCSIコマンドセットに応答するため、既存のオンプレミスバックアップアプリケーションは変更なしで動作します。詳細については、AWS Storage Gateway ユーザーガイドの次のトピックを参照してください。 • アーキテクチャの概要については、「テープゲートウェイの仕組み (アーキテクチャ)」を参照してください。 • テープゲートウェイを使い始めるには、「テープゲートウェイの作成」を参照してください。	2013 年 11 月 5 日
Microsoft Hyper-V のサポート	Storage Gateway で、Microsoft Hyper-V 仮想プラットフォームにオンプレミスゲートウェイをデプロイできるようになりました。Microsoft Hyper-V にデプロイされたゲートウェイには、既存のオンプレミスストレージゲートウェイと同じ機能と特徴がすべてあります。Microsoft Hyper-V を使ってゲートウェイのデプロイを開始するには、サポートされているハイパーバイザーとホストの要件 を参照してください。	2013 年 4 月 10 日

変更	説明	変更日
Amazon でのゲートウェイのデプロイのサポート EC2	Storage Gateway で、Amazon Elastic Compute Cloud (Amazon) にゲートウェイをデプロイできるようになりましたEC2。でAMI利用可能な Storage Gateway EC2を使用して、Amazon でゲートウェイインスタンスを起動できますAWS Marketplace。Storage Gateway を使用してゲートウェイのデプロイを開始するにはAMI、「」を参照してくださいAmazon EC2インスタンスをデプロイしてボリュームゲートウェイをホストする。	2013 年 1 月 15 日

変更	説明	変更日
キャッシュ型ボリュームのサポートとAPIバージョン 2012-06-30 の導入	このリリースでは、Storage Gateway でキャッシュ型ボリュームのサポートが導入されました。キャッシュ型ボリュームは、オンプレミスストレージを拡張する必要性を最小限に抑えます。同時に、アプリケーションからは引き続き、アクティブデータへの低レイテンシーなアクセスが可能になります。最大 32 TiB のサイズのストレージボリュームを作成し、オンプレミスのアプリケーションサーバーから iSCSI デバイスとしてマウントできます。キャッシュ型ボリュームに書き込まれたデータは Amazon Simple Storage Service (Amazon S3) に保管され、オンプレミスのストレージハードウェアには、最近読み書きされたキャッシュのみがローカルに保存されます。キャッシュ型ボリュームでは、古くてあまり頻繁にアクセスされないデータなど、取得時に高レイテンシーが許容されるデータには Amazon S3 を使用し、低レイテンシーアクセスが必要なデータにはオンプレミスストレージを使用できます。 このリリースでは、Storage Gateway に、現在のオペレーションをサポートするだけでなく、キャッシュ型ボリュームをサポートする新しいオペレーションを提供する新しいAPIバージョンも導入されました。 これら 2 つの Storage Gateway ソリューションの詳細については、ボリュームゲートウェイの仕組み (アーキテクチャ) を参照してください。 また、テストのセットアップもお試しください。手順については、「テープゲートウェイの作成」を参照してください。	2012 年 10 月 29 日

変更	説明	変更日
API と IAM サポート	このリリースでは、Storage Gateway で AWS Identity and Access Management() API のサポートと のサポートが導入されていますIAM。 • API サポート — Storage Gateway リソースをプログラムで設定および管理できるようになりました。の詳細についてはAPI、「 ユーザーガイド」の API Storage Gateway のリファレンスAWS Storage Gateway 「」を参照してください。 • IAM サポート – AWS Identity and Access Management （ IAM) では、 IAMポリシーを使用してユーザーを作成し、Storage Gateway リソースへのユーザーアクセスを管理できます。IAM ポリシーの例については、「Identity and Access Management for AWS Storage Gateway」を参照してください。の詳細についてはIAM、AWS Identity and Access Management 「 (IAM) の詳細ページ」を参照してください。	2012 年 5 月 9 日
静的 IP のサポート	ローカルゲートウェイに対して、静的 IP を指定できるようになりました。詳細については、「ゲートウェイのネットワークの設定」を参照してください。	2012 年 3 月 5 日
新規ガイド	これは『AWS Storage Gateway ユーザーガイド』の最初のリリースです。	2012 年 1 月 24 日

Volume Gateway アプライアンスソフトウェアのリリースノート

これらのリリースノートでは、ボリュームゲートウェイアプライアンスの各バージョンに含まれる新機能および更新機能、改善点、修正点について説明します。各ソフトウェアバージョンは、リリース日と一意のバージョン番号によって識別されます。

ゲートウェイのソフトウェアバージョン番号を確認するには、Storage Gateway コンソールで詳細ページを確認するか、次のような AWS CLI コマンドを使用して DescribeGatewayInformationAPI アクションを呼び出します。

```
aws storagegateway describe-gateway-information --gateway-arn
 "arn:aws:storagegateway:us-west-2:123456789012:gateway/sgw-12A3456B"
```

バージョン番号はAPIレスポンスの `SoftwareVersion`フィールドで返されます。

> **Note**
>
> ゲートウェイは、以下の状況ではソフトウェアバージョン情報を報告しません。
>
> - ゲートウェイはオフラインです。
> - ゲートウェイは、バージョンレポートをサポートしていない古いソフトウェアを実行しています。
> - ゲートウェイタイプはFSxファイルゲートウェイです。

ゲートウェイのデフォルトの自動メンテナンスおよび更新スケジュールを変更する方法など、ボリュームゲートウェイの更新の詳細については、」を参照してくださいAWS Storage Gateway。

リリース日	ソフトウェアバージョン	リリースノート
2024-07-29	2.10.0	• 新規および既存のゲートウェイのオペレーティングシステムの更新 • その他のバグ修正と機能強化

リリース日	ソフトウェアバージョン	リリースノート
2024-06-17	2.9.2	• 新規および既存のゲートウェイのオペレーティングシステムの更新
2024-05-28	2.9.0	• ソフトウェア更新中のゲートウェイの再起動時間を短縮 • ネットワーク帯域幅を推定するために転送されるデータ量を削減
2024-05-08	2.8.3	• SOCKS5 プロキシを使用する際のクラウド接続の問題に対処
2024-04-10	2.8.1	• 2.8.0 で発生したメモリ使用量の問題に対応しました • セキュリティパッチの更新 • ソフトウェア更新プロセスの改善 • 新しいゲートウェイのネットワークタイムプロトコル (NTP) コンポーネントが見つからない場合に対処しました
2024-03-06	2.8.0	• 新しいゲートウェイのオペレーティングシステムの更新 • セキュリティパッチの更新
2023-12-19	2.7.0	• 新しいゲートウェイのオペレーティングシステムの更新

リリース日	ソフトウェアバージョン	リリースノート
2023-12-14	2.6.6	• メンテナンスリリース