Amazon FSx ファイルゲートウェイユーザーガイド

AWS Storage Gateway

API バージョン 2021-03-31

AWS Storage Gateway: Amazon FSx ファイルゲートウェイユーザーガイド

Table of Contents

新規のお客様へのAmazon FSx ファイルゲートウェイの提供は終了しました。FSx ファイルゲートウェイの既存のお客様は、引き続き通常どおりサービスを使用できます。FSx ファイルゲートウェイに似た機能については、このブログ記事を参照してください。

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。

Amazon FSx ファイルゲートウェイとは

Amazon FSx ファイルゲートウェイ(FSx ファイルゲートウェイ) は、お使いのオンプレミスの施設から、クラウド内の FSx for Windows File Server ファイル共有へ低レイテンシーで効率的なアクセスを実現できる、新しいタイプのファイルゲートウェイです。レイテンシーまたは帯域幅の要件があるためにオンプレミスで維持しているファイルストレージの代わりに、FSx ファイルゲートウェイを使用することで、AWS Cloud by FSx for Windows File Server で、フルマネージドで信頼性が高く事実上無制限の Windows ファイル共有に対するシームレスなアクセスが実現します。

Amazon FSx ファイルゲートウェイを使用する利点

FSx ファイルゲートウェイには以下の利点があります。

- オンプレミスのファイルサーバーが不要になり、すべてのデータを AWS に集約して、クラウドストレージの規模と経済性を活用できます。
- オンプレミスからクラウドデータへのアクセスが必要なワークロードを含め、あらゆるファイルワークロードで利用できるオプションを提供します。
- オンプレミスにとどまる必要があるアプリケーションでも、ネットワークに負荷をかけたり、最も高い要求を持つアプリケーションのレイテンシーに影響を及ぼしたりすることなく、AWS と同じ低レイテンシーと高パフォーマンスを実現できるようになります。

Amazon FSx ファイルゲートウェイの仕組み

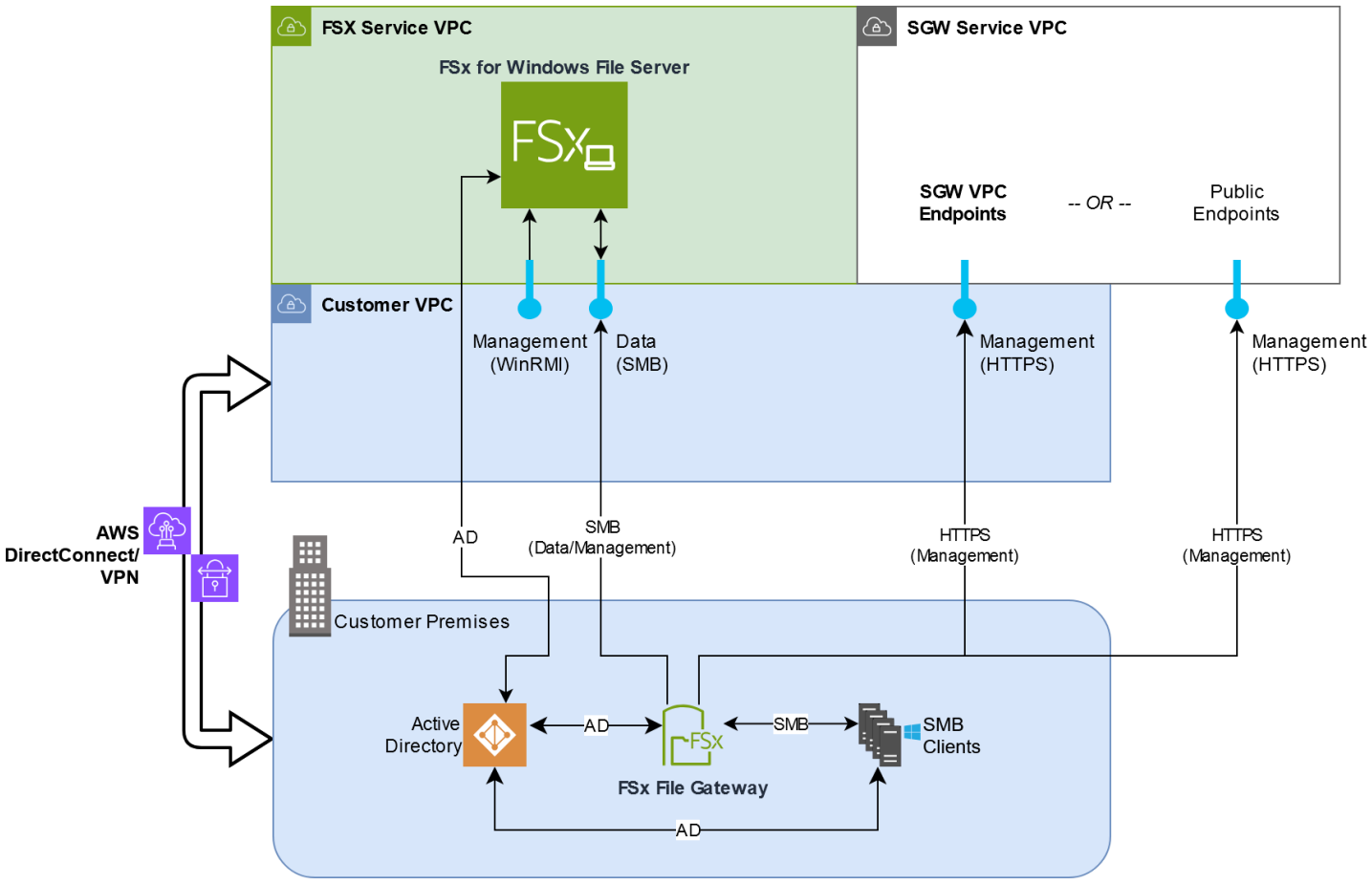
Amazon FSx ファイルゲートウェイ(FSx ファイルゲートウェイ) を使用するには、少なくとも 1 つの Amazon FSx for Windows File Server ファイルシステムが必要です。VPN または Direct Connect 接続で、FSx for Windows File Server へのオンプレミスアクセスも必要です。Amazon FSx ファイルシステムの使用の詳細については、「Amazon FSx for Windows File Server とは」を参照してください。

ゲートウェイは、VMware ESXi、Microsoft Hyper-V、または Linux カーネルベース仮想マシン (KVM) で実行されている仮想マシン (VM) として、または任意のリセラーに発注されたハードウェアアプライアンスとしてオンプレミス環境にデプロイされます。Storage Gateway VM は、VMware Cloud on AWS にデプロイすることも、Amazon EC2 の AMI としてデプロイすることもできます。アプライアンスをデプロイしたら、Storage Gateway コンソールまたは Storage Gateway API を使用して FSx ファイルゲートウェイをアクティベートします。

Amazon FSx ファイルゲートウェイがアクティブになり、FSx for Windows File Server にアクセスできるようになったら、Storage Gateway コンソールを使用して Microsoft Active Directory ドメインに参加させます。ゲートウェイがドメインに正常に参加したら、Storage Gateway コンソールを使用して、ゲートウェイを既存の FSx for Windows File Server にアタッチします。FSx for Windows File Server により、サーバー上のすべての共有を Amazon FSx ファイルゲートウェイ上の共有として利用できるようになります。その後、クライアントを使用して、選択した FSx ファイルゲートウェイに対応する FSx ファイルゲートウェイ上のファイル共有を参照して接続できます。

ファイル共有が接続されると、FSx for Windows File Server で利用可能なすべての機能を利用しながら、ファイルをローカルで読み書きできます。FSx ファイルゲートウェイを使用すると、FSx for Windows File Server にリモートで保存されているファイル共有に対して、ローカルのファイル共有とその内容をマッピングできます。リモートのファイルとローカルに表示されるファイルおよび共有は 1 対 1 で対応しています。

次の図は、Storage Gateway のファイルストレージのデプロイの概要を示しています。



図では、次の点に注意してください。

- Direct Connect または VPN は、FSx ファイルゲートウェイが SMB を使用して Amazon FSx ファイル共有にアクセスし、FSx for Windows File Server がオンプレミスの Active Directory ドメインに参加できるようにするために必要です。
- プライベートエンドポイントを使って FSx for Windows File Server サービス VPC や Storage Gateway サービス VPC に接続するには、Amazon Virtual Private Cloud (Amazon VPC) が必要です。FSx ファイルゲートウェイは、パブリックエンドポイントにも接続できます。

Amazon FSx ファイルゲートウェイは、FSx for Windows File Server が利用可能なすべての AWS リージョンで利用できます。

の開始方法 AWS Storage Gateway

このセクションでは、 の使用を開始する手順について説明します AWS。の使用を開始する前に、AWS アカウントが必要です AWS Storage Gateway。既存の AWS アカウントを使用するか、新しいアカウントにサインアップできます。また、Storage Gateway タスクを実行するために必要な管理権限を持つグループに属する AWS アカウントの IAM ユーザーも必要です。適切な権限を持つユーザーは、Storage Gateway コンソールと Storage Gateway API にアクセスして、ゲートウェイのデプロイ、設定、メンテナンスタスクを実行できます。初めて使用する場合は、Storage Gateway を使用する前に、サポートされている AWS リージョンとファイルゲートウェイのセットアップ要件セクションを確認することをお勧めします。 https://docs.aws.amazon.com/filegateway/latest/filefsxw/Requirements.html

このセクションには、 AWS Storage Gatewayの使用開始に関する追加情報を提供する以下のトピックが含まれています。

トピック

- Amazon Web Services へのサインアップ - にサインアップ AWS して AWS アカウントを作成する方法について説明します。
- 管理者権限を持つ IAM ユーザーの作成 - AWS アカウントの管理者権限を持つ IAM ユーザーを作成する方法について説明します。
- アクセス AWS Storage Gateway - Storage Gateway コンソール AWS Storage Gateway または AWS SDKs を使用してプログラムで にアクセスする方法について説明します。
- AWS リージョン Storage Gateway をサポートする - Storage Gateway でゲートウェイをアクティブ化するときにデータを保存するために使用できる AWS リージョンについて説明します。

Amazon Web Services へのサインアップ

AWS アカウント は、 AWS サービスにアクセスするための基本的な要件です。 AWS アカウント は、 ユーザーとして作成するすべての AWS リソースの基本的なコンテナです AWS 。 AWS アカウント は、 AWS リソースの基本的なセキュリティ境界でもあります。アカウントで作成したリソースは、そのアカウントに対する認証情報を持つユーザーが使用できます。の使用を開始する前に AWS Storage Gateway、 にサインアップする必要があります AWS アカウント。

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

1. https://portal.aws.amazon.com/billing/signup 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、電話またはテキストメッセージを受け取り、電話キーパッドで検証コードを入力します。

   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。セキュリティベストプラクティスとして、ユーザーに管理アクセス権を割り当て、ルートユーザーアクセスが必要なタスクの実行にはルートユーザーのみを使用するようにしてください。

また、ユーザーが AWSにアクセスする場合には、一時的な認証情報の使用を推奨します。一時的な認証情報を提供するには、フェデレーションと IAM Identity Center などの ID AWS プロバイダーを使用できます。会社が既に ID プロバイダーを使用している場合は、フェデレーションで使用して、AWS アカウント内のリソースへのアクセスを提供する方法を簡素化できます。

管理者権限を持つ IAM ユーザーの作成

AWS アカウントを作成したら、次のステップを使用して、自分用の AWS Identity and Access Management (IAM) ユーザーを作成し、そのユーザーを管理権限を持つグループに追加します。AWS Identity and Access Management サービスを使用して Storage Gateway リソースへのアクセスを制御する方法の詳細については、「」を参照してくださいAWS Storage Gatewayの Identity and Access Management。

管理者ユーザーを作成するには、以下のいずれかのオプションを選択します。

管理者を管理する方法を 1 つ選択します	目的	方法	以下の操作も可能
IAM アイデンティティセンター内 (推奨)	短期の認証情報を使用して AWSにアクセスします。 これはセキュリティのベストプラクティスと一致しています。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「IAM でのセキュリティのベストプラクティス」を参照してください。	AWS IAM アイデンティティセンター ユーザーガイドの「開始方法」の手順に従います。	AWS Command Line Interface ユーザーガイドの を使用する AWS CLI ように を設定 AWS IAM アイデンティティセンターして、プログラムによるアクセスを設定します。
IAM 内 (非推奨)	長期認証情報を使用して AWSにアクセスします。	IAM ユーザーガイドの「緊急アクセス用の IAM ユーザーを作成する」の手順に従います。	IAM ユーザーガイドの「IAM ユーザーのアクセスキーを管理する」の手順に従って、プログラムによるアクセスを設定します。

> **Warning**
>
> IAM ユーザーは長期認証情報を持っているため、セキュリティリスクがあります。このリスクを軽減するために、これらのユーザーにはタスクの実行に必要な権限のみを付与し、不要になったユーザーを削除することをお勧めします。

アクセス AWS Storage Gateway

AWS Storage Gateway コンソールを使用して、さまざまなゲートウェイの設定およびメンテナンス作業を実行できます。たとえば、Storage Gateway ハードウェアアプライアンスのデプロイからの有効化や削除、各種ゲートウェイの作成・管理・削除、ファイルシステムの・アタッチ・・デタッチ、さらにStorage Gateway サービス内の各要素のヘルスとステータスのモニタリングなどを実行できます。わかりやすさと使いやすさのために、このガイドでは、Storage Gateway コンソールのウェブインターフェイスを使用してタスクを実行することに焦点を当てています。Storage Gateway コンソールには、ウェブブラウザから https://console.aws.amazon.com/storagegateway/home/ でアクセスできます。

プログラムによるアプローチが必要な場合は、 AWS Storage Gateway Application Programming Interface (API) または コマンドラインインターフェイス (CLI) を使用して、Storage Gateway デプロイのリソースを設定および管理できます。Storage Gateway API のアクション、データ型、必要な構文の詳細については、「Storage Gateway API リファレンス」を参照してください。Storage Gateway CLI の詳細については、「AWS CLI コマンドリファレンス」を参照してください。

AWS SDKs を使用して、Storage 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。 AWS SDK for Java、.NET、PHP により、基盤となる Storage Gateway API がラッピングされるので、プログラミングの作業が簡素化されます。SDK ライブラリのダウンロードについては、「AWS デベロッパーセンター」を参照してください。

料金については、「AWS Storage Gateway の料金」を参照してください。

AWS リージョン Storage Gateway をサポートする

AWS リージョン は、 に複数のアベイラビリティーゾーン AWS がある世界の物理的な場所です。アベイラビリティーゾーンは、1 つ以上の個別の AWS データセンターで構成され、それぞれが冗長な電源、ネットワーク、および接続を備え、別々の施設に収容されています。つまり、それぞれ AWS リージョン が物理的に分離され、他のリージョンから独立しています。リージョンでは耐障害性や安定性が提供され、レイテンシーを低減することもできます。1 つのリージョンで作成したリソースは、 AWS サービスが提供するレプリケーション機能を明示的に使用しない限り、他のリージョンには存在しません。たとえば、Amazon S3 と Amazon EC2 はクロスリージョンのレプリケーションをサポートしています。などの一部のサービスには AWS Identity and Access Management、リージョンリソースがありません。ビジネス要件を満たす場所で AWS リソースを起動できます。例えば、Amazon EC2 インスタンスを起動して、欧州 AWS リージョン のユーザーの近くにある でアプライアンスをホスト AWS Storage Gateway したり、法的要件を満たすことができます。は、特定の

サービスでサポートされているリージョンのうち、どのリージョンを使用できるか AWS アカウントを決定します。

Amazon FSx File Gateway は、Amazon FSx ファイルシステムがある AWS リージョンにファイルデータを保存します。ゲートウェイのデプロイを始める前に、Storage Gateway コンソールの右上隅にあるリージョンを選択します。

- Amazon FSx File Gateway — サポートされている AWS リージョンと Amazon FSx File 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「Amazon FSx File 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 — 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 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対象のリージョンについては、「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。

ファイルゲートウェイのセットアップ要件

特に明記されていない限り、次の要件は AWS Storage Gatewayのすべてのファイルゲートウェイタイプに共通です。セットアップはこのセクションの要件を満たしている必要があります。ゲートウェイをデプロイする前に、ゲートウェイのセットアップに適用される要件を確認してください。

トピック

前提条件

Amazon FSx ファイルゲートウェイ (FSx ファイルゲートウェイ) を設定する前に、次の前提条件を満たす必要があります:

- FSx for Windows File Server ファイルシステムを作成および設定する。手順については、「Amazon FSx for Windows File Server ユーザーガイド」の「ステップ 1: ファイルシステムを作成する」を参照してください。
- Microsoft Active Directory (AD) を設定し、必要なアクセス許可を持つ Active Directory サービスアカウントを作成します。詳細については、Active Directory サービスアカウントのアクセス許可要件を参照してください。
- ゲートウェイと AWSの間に十分なネットワーク帯域幅があることを確認します。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。
- AWS とゲートウェイをデプロイするオンプレミス環境との間のネットワークトラフィックに使用する接続を設定します。パブリックインターネット、プライベートネットワーク、VPN、または を使用して接続できます Direct Connect。Amazon Virtual Private Cloud へのプライベート接続 AWS を介してゲートウェイと通信する場合は、ゲートウェイを設定する前に Amazon VPC を設定します。

- ゲートウェイが Active Directory ドメインコントローラーの名前を解決できることを確認します。Active Directory ドメインの DHCP を使用して解決を処理するか、ゲートウェイローカルコンソールのネットワーク設定メニューから DNS サーバーを手動で指定できます。

ハードウェアとストレージの要件

次のセクションでは、ゲートウェイに必要な最小限のハードウェアとストレージの構成、および必要なストレージに割り当てる最小限のディスクスペースについて説明します。

オンプレミス VM のハードウェア要件

ゲートウェイをオンプレミスでデプロイする前に必ず、ゲートウェイ仮想マシン (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 4 つの仮想プロセッサ
- ファイルゲートウェイ用に 16 GiB の予約済みの RAM
- 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)

Amazon EC2 インスタンスタイプでの要件

Amazon Elastic Compute Cloud (Amazon EC2) でゲートウェイをデプロイする場合、このゲートウェイが機能するためには、インスタンスサイズとして少なくとも **`xlarge`** を使用する必要があります。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、サイズは少なくとも **`2xlarge`** 以上である必要があります。

> **Note**
>
> Storage Gateway AMI は、Intel または AMD プロセッサを使用する x86 ベースのインスタンスとのみ互換性があります。Graviton プロセッサを使用する ARM ベースのインスタンスはサポートされていません。

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。

ファイルゲートウェイの種類に応じた推奨

- 汎用インスタンスファミリー – m5、m6、または m7 インスタンスタイプ。Storage Gateway プロセッサと RAM の要件を満たすには、xlarge インスタンスサイズ以上を選択します。

- コンピューティング最適化インスタンスファミリー — c5、c6、または c7 インスタンスタイプ。Storage Gateway プロセッサと RAM の要件を満たすには、2xlarge インスタンスサイズ以上を選択します。
- メモリ最適化インスタンスファミリー – r5、r6、または r7 インスタンスタイプ。Storage Gateway プロセッサと RAM の要件を満たすには、xlarge インスタンスサイズ以上を選択します。
- ストレージ最適化インスタンスファミリー – i3、i4、または i7 インスタンスタイプ。Storage Gateway プロセッサと RAM の要件を満たすには、xlarge インスタンスサイズ以上を選択します。

> **Note**
>
> Amazon EC2 でゲートウェイを起動し、選択したインスタンスタイプがエフェメラルストレージをサポートしている場合には、自動的にディスクの一覧が表示されます。Amazon EC2 インスタンスストレージの詳細については、Amazon EC2 ユーザーガイドのインスタンスストレージを参照してください。

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。

ゲートウェイタイプ	キャッシュ (最小)	キャッシュ (最大)			
ファイルゲートウェイ	150 GiB	64 TiB			

> **Note**
>
> キャッシュ用として、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を追加する場合、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。ディスクが以前にキャッシュとして割り当てられている場合は、既存のディスクのサイズを変更しないでください。

ネットワークとファイアウォールの要件

ゲートウェイには、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、ルーターなどへのアクセスが必要です。

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。

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、 AWS の 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を使用して、Amazon EC2 にゲートウェイをデプロイするか、または他のタイプのデプロイ (オンプレミスを含む) を行うことがあります。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リージョンの Amazon AWS 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してください。

トピック

ポート要件

FSx ファイルゲートウェイでは、デプロイとオペレーションを成功させるために、ネットワークセキュリティを介して特定のポートを許可する必要があります。一部のポートはすべてのゲートウェイに必要ですが、他のポートは VPC エンドポイントに接続するときなど、特定の設定にのみ必要です。

FSx ファイルゲートウェイでは、ドメイン ユーザーがサーバー メッセージ ブロック (SMB) ファイル共有にアクセスできるようにするために、Microsoft Active Directory を使用する必要があります。ファイルゲートウェイは、任意の有効な (かつ DNS が解決可能な) Microsoft Windows ドメインに参加させることができます。

を使用して Directory Service 、Amazon Web Services クラウドAWS Managed Microsoft ADで を作成することもできます。ほとんどの AWS Managed Microsoft AD デプロイでは、VPC の Dynamic Host Configuration Protocol (DHCP) サービスを設定する必要があります。DHCP オプションセットの作成については、AWS Directory Service 管理ガイドの「DHCP オプションセットの作成」を参照してください。

次の表に、必要なポートと、[注] 列の条件付き要件を示します。

FSx ファイルゲートウェイのポート要件

ネットワーク要素	から	まで	プロトコル	ポート	インバウンド	アウトバウンド	必須	注意事項
ウェブブラウザ	ウェブブラウザ	Storage Gateway VM	TCP HTTP	80	✓	✓	✓	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

ネットワーク要素	から	まで	プロトコル	ポート	インバウンド	アウトバウンド	必須	注意事項
								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

ネットワーク要素	から	まで	プロトコル	ポート	インバウンド	アウトバウンド	必須	注意事項
								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。

ネットワーク要素	から	まで	プロトコル	ポート	インバウンド	アウトバウンド	必須	注意事項
ウェブブラウザ	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓	AWS マネジメントコンソール (その他すべてのオペレーション)
DNS	Storage Gateway VM	ドメインネームサービス (DNS) サーバー	TCP & UDP DNS	53	✓	✓	✓	ストレージゲートウェイ VMとDNSサーバー間の通信に使用され、IP 名解決を行います。

ネットワーク要素	から	まで	プロトコル	ポート	インバウンド	アウトバウンド	必須	注意事項
NTP	Storage Gateway VM	Network Time Protocol (NTP) サーバー	TCP & UDP NTP	123	✓	✓	✓	VM 時間をホスト時間に同期するためにオンプレミスシステムで使用されます。Storage Gateway VM は、以下の 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

ネットワーク要素	から	まで	プロトコル	ポート	インバウンド	アウトバウンド	必須	注意事項
								• 2.amazon.pool.ntp.org • 3.amazon.pool.ntp.org Note Amazon EC2 でホストされているゲートウェイには必要ありま

ネットワーク要素	から	まで	プロトコル	ポート	インバウンド	アウトバウンド	必須	注意事項
								せん。

ネットワーク要素	から	まで	プロトコル	ポート	インバウンド	アウトバウンド	必須	注意事項
Storage Gateway	Storage Gateway VM	サポート エンドポイント	TCP SSH	22	✓	✓	✓	サポート 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

ネットワーク要素	から	まで	プロトコル	ポート	インバウンド	アウトバウンド	必須	注意事項
								シューティングでは必要です。サポートエンドポイントのリストについては、サポートエンドポイントを参照してください。
Storage Gateway	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓	管理コントロール
Amazon CloudFront	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓	アクティベーション用

ネットワーク要素	から	まで	プロトコル	ポート	インバウンド	アウトバウンド	必須	注意事項
VPC	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓*	管理コントロール *VPC エンドポイントを使用する場合にのみ必須
VPC	Storage Gateway VM	AWS	TCP HTTPS	1026		✓	✓*	コントロールプレーンエンドポイント *VPC エンドポイントを使用する場合にのみ必須

ネットワーク要素	から	まで	プロトコル	ポート	インバウンド	アウトバウンド	必須	注意事項
VPC	Storage Gateway VM	AWS	TCP HTTPS	1027		✓	✓*	Anon コントロールプレーン (アクティベーション用) *VPC エンドポイントを使用する場合にのみ必須
VPC	Storage Gateway VM	AWS	TCP HTTPS	1028		✓	✓*	プロキシエンドポイント *VPC エンドポイントを使用する場合にのみ必須

ネットワーク要素	から	まで	プロトコル	ポート	インバウンド	アウトバウンド	必須	注意事項
VPC	Storage Gateway VM	AWS	TCP HTTPS	1031		✓	✓*	データプレーン *VPC エンドポイントを使用する場合にのみ必須
VPC	Storage Gateway VM	AWS	TCP HTTPS	2222		✓	✓*	VPCe の SSH サポートチャネル *VPC エンドポイントを使用しサポートチャネルを開く場合にのみ必須

ネットワーク要素	から	まで	プロトコル	ポート	インバウンド	アウトバウンド	必須	注意事項
VPC	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓*	管理コントロール *VPC エンドポイントを使用する場合にのみ必須
ファイル共有クライアント	SMB クライアント	Storage Gateway VM	TCP または UDP SMBv3	445	✓	✓	✓	ファイル共有データ転送セッションサービス。 Microsoft Windows NT 以降のポート 137 ~ 139 を置き換えます。

ネットワーク要素	から	まで	プロトコル	ポート	インバウンド	アウトバウンド	必須	注意事項
Microsoft Active Directory	Storage Gateway VM	Active Directory サーバー	UDP NetBIOS	137	✓	✓	✓	サービス名
Microsoft Active Directory	Storage Gateway VM	Active Directory サーバー	UDP NetBIOS	138	✓	✓	✓	データグラムサービス
Microsoft Active Directory	Storage Gateway VM	Active Directory サーバー	TCP および UDP LDAP	389	✓	✓	✓	ディレクトリシステムエージェント (DSA) クライアント接続
Microsoft Active Directory	Storage Gateway VM	Active Directory サーバー	TCP および UDP Kerberos	88	✓	✓	✓	Kerberos

ネットワーク要素	から	まで	プロトコル	ポート	インバウンド	アウトバウンド	必須	注意事項
Microsoft Active Directory	Storage Gateway VM	Active Directory サーバー	TCP 分散コンピューティング環境/エンドポイント マッパー (DCE/EMAP)	135	✓	✓	✓	RPC
Amazon FSx 接続	Storage Gateway VM	FSx for Windows File Server	TCP または UDP SMBv3	445	✓	✓	✓	ファイル共有データ転送セッションサービス

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。

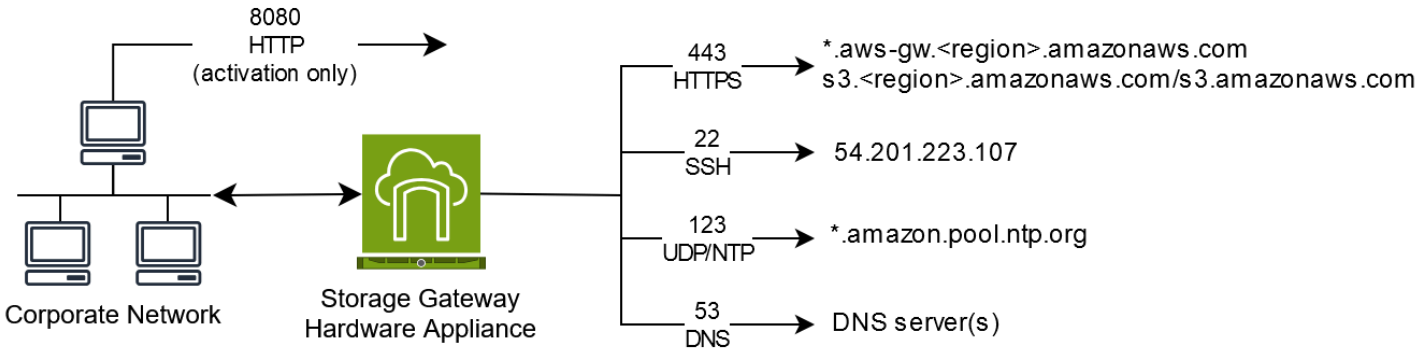
- インターネットアクセス – サーバー上の任意のネットワークインターフェイスを介した、インターネットへの常時接続のネットワーク接続。
- DNS サービス – ハードウェアアプライアンスと DNS サーバー間の通信のための DNS サービス。
- 時刻同期 – 自動的に設定された Amazon NTP タイムサービスへのアクセス。

- IP アドレス – 割り当てられた DHCP または静的 IPv4 アドレス。IPv6 アドレスを割り当てることはできません。

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

iDRAC ポートをリモートサーバー管理に使用できます。



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	ソース	目的地	使用方法
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

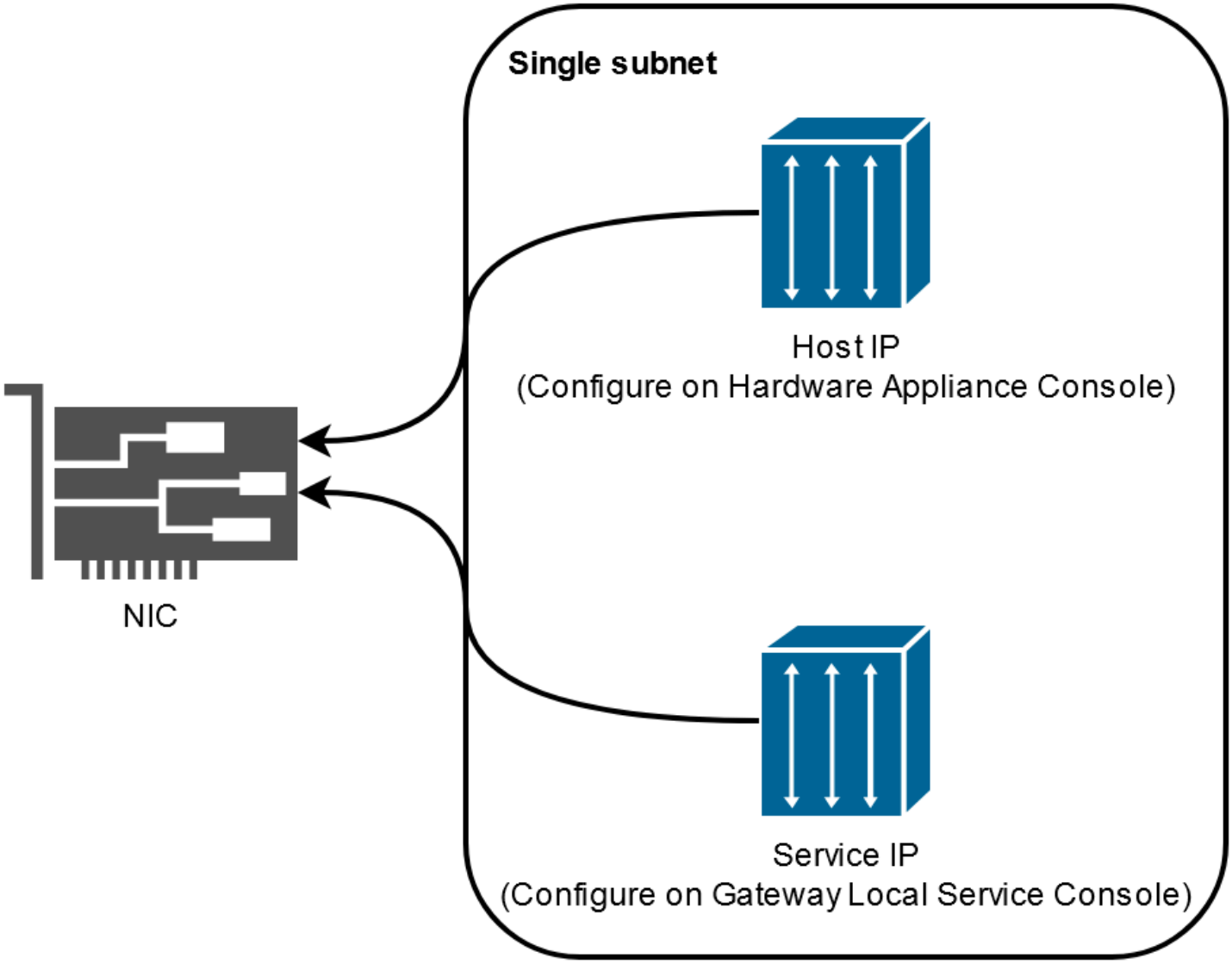
プロトコル	ポート	Direction	ソース	目的地	使用方法
UDP/NTP	123	アウトバウンド	ハードウェアアプライアンス	`*.amazon.pool.ntp.org`	時刻同期
HTTPS	443	アウトバウンド	ハードウェアアプライアンス	`*.amazonaws.com`	データ転送
HTTP	8080	インバウンド	AWS	ハードウェアアプライアンス	アクティベーション (短時間のみ)

設計どおりに動作させるには、ハードウェア アプライアンスで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 インターフェイスに、前の図にリストされているエンドポイントへの送信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、ハードウェアアプライアンスの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どちらであっても、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ブ化と設定の詳細については、AWS 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

ゲートウェイが通信するには、次の Storage Gateway 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。ゲートウェイのセットアップ時に、ネットワーク環境に基づいてゲートウェイのエンドポイントタイプを選択します。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必要があります。

> **Note**
>
> Storage Gateway との接続とデータ転送に使用するように Storage Gateway のプライベート VPC エンドポイントを設定する場合 AWS、ゲートウェイはパブリックインターネットへのアクセスを必要としません。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**
>
> 次のエンドポイント例の *region* を、 などのゲートウェイの正しい AWS リージョン 文字列に置き換えますus-west-2。
> *amzn-s3-demo-bucket* を、デプロイメント内の実際の Amazon S3 バケット名に置き換えます。*amzn-s3-demo-bucket* の代わりにアスタリスク (*) を使用して、ファイアウォールルールにワイルドカードエントリを作成することもできます。これにより、すべてのバケット名のサービスエンドポイントを一覧表示できます。
> ゲートウェイが米国またはカナダ AWS リージョン の にデプロイされており、連邦情報処理規格 (FIPS) 準拠のエンドポイント接続が必要な場合は、*s3* を に置き換えますs3-fips。

エンドポイントタイプ

標準エンドポイント

これらのエンドポイントは、ゲートウェイアプライアンスと 間の IPv4 トラフィックをサポートします AWS。

ヘッドバケット 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。

```
bucket-name.s3.region.amazonaws.com:443
```

以下のサービスエンドポイントは、すべてのゲートウェイが制御パス (anon-cp、client-cp、proxy-app)およびデータパス (dp-1) 操作のために必要とするものです。

```
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
```

次のゲートウェイサービスエンドポイントは、API コールを行うために必要です。

```
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
```

Storage Gateway および Amazon S3 サービスエンドポイントに加えて、Storage Gateway VMs次の NTP サーバーへのネットワークアクセスも必要です。

```
time.aws.com
0.amazon.pool.ntp.org
1.amazon.pool.ntp.org
2.amazon.pool.ntp.org
3.amazon.pool.ntp.org
```

サポートされているエンドポイント AWS リージョン とサービスエンドポイントの詳細については、のStorage Gateway」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でのセキュリティグループの設定

では AWS Storage Gateway、セキュリティグループが 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 80 (アクティベーション用) でのみ接続を許可することをお勧めします。
- ゲートウェイのセキュリティグループに属さない Amazon EC2 ホストからゲートウェイをアクティベートする場合は、そのホストの IP アドレスからの着信接続をポート 80 で許可します。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 サポート 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、「Amazon EC2 ゲートウェイ サポート 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。

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、仮想マシン (VM) アプライアンスまたは物理ハードウェアアプライアンスとしてオンプレミスで実行することも、Amazon EC2 インスタンス AWS として で実行することもできます。

> **Note**
>
> ファイルゲートウェイ 2.x、ボリュームゲートウェイ 3.x、テープゲートウェイ 3.x には、セキュアブートが無効 (loader_secure=no) の UEFI ブートモードが必要です。XML ファイルは、クイックセットアップ設定として各 qcow ダウンロードに付属しています。

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) – このセットアップには、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 ハイパーバイザー (2019、2022、または 2025) – このセットアップでは、ホストに接続するために Microsoft Windows クライアント コンピューターに Microsoft Hyper-V マネージャーが必要です。
- Linux カーネルベース仮想マシン (KVM) – これは無料のオープンソースの仮想化テクノロジーです。KVM は、Linux バージョン 2.6.20 以降のすべてのバージョンに同梱されています。Storage Gateway は、CentOS/RHEL 7.7、RHEL 8.6、Ubuntu 16.04 LTS、および Ubuntu 18.04 LTS の各ディストリビューションでテストされ動作が確認されています。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。既に KVM 環境が稼働しており、KVM の仕組みに精通している場合は、このオプションをお勧めします。推奨される起動設定については、提供されている aws-storage-gateway.xml ファイルを参照してください。ファイルゲートウェイ 2.x、ボリュームゲートウェイ 3.x、テープゲートウェイ 3.x には、セキュアブートが無効 (loader_secure=no) の UEFI ブートモードが必要です。
- バージョン 10.0.1.1 から始まる Nutanix AHV (アクロポリスハイパーバイザー) – Nutanix ハイパーコンバージドインフラストラクチャ (HCI) ソリューションに統合されている KVM ベースの仮想化プラットフォーム。

- Amazon EC2 インスタンス – Storage Gateway では、ゲートウェイ の VM イメージを含む Amazon マシンイメージ (AMI) を提供します。Amazon EC2 にゲートウェイをデプロイする方法については、FSx ファイルゲートウェイ用のデフォルトの Amazon EC2 ホストをデプロイするを参照してください。
- 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 では、スナップショットから作成された VM、または別のゲートウェイ VM のクローン、または Amazon EC2 AMI からのゲートウェイ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。

ファイルゲートウェイでサポートされている SMB クライアント

ファイルゲートウェイは以下のサービスメッセージブロック (SMB) クライアントをサポートしています。

- Microsoft Windows Server 2008 R2 以降
- Windows デスクトップバージョン: 10、8、7
- Windows Server 2008 以降で実行される Windows ターミナル サーバー

> **Note**
>
> サーバーメッセージブロックの暗号化には、SMB v3.x のダイアレクトをサポートするクライアントが必要です。

ファイルゲートウェイでサポートされているファイルシステムオペレーション

SMB クライアントは、ファイルの書き込み、読み取り、削除、切り捨てを行うことができます。クライアントが Storage Gateway に書き込みを送信すると、同期的にローカルキャッシュに書き込みます。次に、最適化された転送を介して非同期的に Amazon FSx に書き込まれます。読み取りはまずローカルキャッシュから行われます。データが利用できない場合は、Amazon FSx を通じてリードスルーキャッシュとして取得されます。

読み込みと書き込みは、変更された部分またはリクエストされた部分だけがゲートウェイ経由で転送されるように最適化されます。Amazon FSx からファイルを削除します。

ゲートウェイ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 インスタンス上に作成するファイルゲートウェイは、Amazon EBS ボリュームをローカルディスクとして使用します。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。ゲートウェイは、割り当てたキャッシュストレージを使用して、最近アクセスしたデータへの低遅延アクセスを提供します。キャッシュストレージは、Amazon FSx へのアップロードが保留中のデータのオンプレミスの耐久性の高いストアとして機能します。ファイルゲートウェイでは、キャッシュとして使用するために少なくとも 150 GiB のディスクが 1 台必要です。ゲートウェイの初期設定とデプロイが完了したら、ワークロードの需要の増加に応じてキャッシュストレージ用のディスクを追加できます。このセクションでは、ローカルディスクの管理に関連する概念と手順について説明する以下のトピックについて説明します。

トピック

- ローカルディスクストレージの容量の決定 - ファイルゲートウェイに割り当てるローカルキャッシュディスクの数とサイズを決定する方法について説明します。
- 追加の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 ファイルゲートウェイのキャッシュストレージ容量を増やす方法について説明します。
- EC2 ゲートウェイでのエフェメラルストレージの使用 - ファイルゲートウェイでエフェメラルディスクストレージを使用する場合にデータ損失を防ぐ方法について説明します。

ローカルディスクストレージの容量の決定

FSx ファイルゲートウェイをデプロイするときは、割り当てるキャッシュディスクの量を考慮してください。FSx ファイルゲートウェイは、最も最近使用されたアルゴリズムを使用して、キャッシュからevictデータを自動的に削除します。FSx ファイルゲートウェイのキャッシュは、そのゲートウェイ上のすべてのファイル共有間で共有されます。アクティブな共有が複数ある場合、1 つの共有で使用率が高いと、別の共有がアクセスできるキャッシュリソースの量に影響し、パフォーマンスに影響する可能性があることに注意してください。

特定のワークロードに必要なキャッシュディスクの量を決定するときは、常にキャッシュディスクをゲートウェイに追加できますが (FSx ファイルゲートウェイの現在のクォータまで)、特定のゲートウェイのキャッシュを減らすことはできません。データセットに対して基本的な分析を実行して適切な量のキャッシュディスクを決定できますが、「ホット」でローカルに保存する必要があるデータの量と「コールド」でクラウドに階層化できるデータの量を正確に判断する方法はありません。ワークロードは時間の経過とともに変化し、FSx ファイルゲートウェイは、使用できるリソースの量に関連する柔軟性と伸縮性を提供します。キャッシュの量はいつでも増やすことができるため、小規模から始めて必要に応じて増やすことが最も費用対効果の高いアプローチであることがよくあります。

ゲートウェイのセットアップ中にキャッシュストレージのディスクをプロビジョニングするには、150 GiB の初期近似値を使用できます。その後、Amazon CloudWatch オペレーションメトリクスを使用して、キャッシュストレージの使用率をモニタリングできます。そして、必要に応じて、コンソールを使用して、追加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、パフォーマンスと最適化を参照してください。

> **Note**
>
> 基になる物理ストレージリソースは、VMware で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。たとえば、キャッシュストレージ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、キャッシュストレージ用に1つのデータストアを選択することを強く推奨します。基になる物理ディスクが 1 つのみのデータストアを、両方のキャッシュストレージに使用すると、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 RAID1 などの低パフォーマンス RAID 設定である場合にも該当します。

追加の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。キャッシュとして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。

ゲートウェイ用の追加キャッシュストレージを設定するには

1. ゲートウェイホストのハイパーバイザーまたは Amazon EC2 インスタンスで 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 インスタンス用の Amazon EBS ボリュームのプロビジョニングについては、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、このディスクをキャッシュストレージとして設定します。
2. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
3. ナビゲーションペインで、ゲートウェイを選択します。
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 [キャッシュストレージの設定] を選択します。
6. [キャッシュストレージの設定] 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。各ディスクについて、[割り当て先]ドロップダウンメニューから[キャッシュ]を選択してください。

> **Note**
>
> キャッシュは、ファイル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。

EC2 ゲートウェイでのエフェメラルストレージの使用

FSx ファイルゲートウェイのキャッシュストレージにエフェメラルディスクを使用することはお勧めしません。

エフェメラルディスクは、Amazon EC2 インスタンス用のブロックレベルストレージとして使用できます。Amazon EC2 Amazon マシンイメージを使用してゲートウェイを起動し、選択したインスタンスタイプが一時ストレージをサポートしている場合、一時ディスクは自動的に一覧表示されます。いずれかのディスクを選択して、ゲートウェイのキャッシュデータを保存できます。詳細については、「Amazon EC2 ユーザーガイド」の「Amazon EC2 インスタンスストア」を参照してください。

アプリケーションがゲートウェイに書き込むデータは、エフェメラルディスクのキャッシュに同期的に保存され、FSx for Windows File Server の耐久性のあるストレージに非同期的にアップロードされます。データがエフェメラルストレージに書き込まれた後、非同期アップロードが発生する前に Amazon EC2 インスタンスが停止した場合、FSx for Windows File Server にまだアップロードされていないデータは失われる可能性があります。

> **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した場合、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。

AWS Storage Gateway ハードウェアアプライアンスの使用

> **Note**
>
> 可用性の終了通知: 2025 年 5 月 12 日をもって、 AWS Storage Gateway ハードウェアアプライアンスは提供されなくなります。 AWS Storage Gateway ハードウェアアプライアンスの既存のお客様は、2028 年 5 月まで引き続き を使用し、サポートを受けることができます。別の方法として、 AWS Storage Gateway サービスを使用して、オンプレミスおよびクラウド内のアプリケーションに事実上無制限のクラウドストレージへのアクセスを許可することもできます。

AWS Storage Gatewayハードウェアアプライアンスは、検証済みのサーバー設定に Storage Gateway ソフトウェアがプリ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。デプロイ内の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てアクティブ化を行うと、アクティブ化プロセスによって、ハードウェアアプライアンスは AWS アカウントに関連付けられます。アクティブ化が完了すると、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] ページに表示されます。ハードウェアアプライアンスは、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する手順は、仮想プラットフォームでの手順と同じです。

AWS Storage Gatewayハードウェアアプライアンス AWS リージョン のアクティベーションと使用が可能なサポートされている のリストについては、 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AWS 全般のリファレンス。

以下のセクションでは、 AWS Storage Gatewayハードウェアアプライアンスのセットアップ、ラックマウント、電源、設定、アクティブ化、起動、使用、削除の手順について説明します。

トピック

- AWS Storage Gatewayハードウェアアプライアンスのセットアップ
- ハードウェアアプライアンスの物理的なインストール

- ハードウェアアプライアンスコンソールへのアクセス
- ハードウェアアプライアンスのネットワークパラメータの設定
- AWS Storage Gateway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でゲートウェイを作成する
- ハードウェアアプライアンスのゲートウェイ IP アドレスの設定
- 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
- AWS Storage Gatewayハードウェアアプライアンスの削除

AWS Storage Gatewayハードウェアアプライアンスのセットアップ

> **Note**
>
> 可用性の終了通知: 2025 年 5 月 12 日をもって、 AWS Storage Gateway ハードウェアアプライアンスは提供されなくなります。 AWS Storage Gateway ハードウェアアプライアンスの既存のお客様は、2028 年 5 月まで引き続き を使用し、サポートを受けることができます。別の方法として、 AWS Storage Gateway サービスを使用して、オンプレミスおよびクラウド内のアプリケーションに事実上無制限のクラウドストレージへのアクセスを許可することもできます。

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のローカルコンソールを使用して、 への常時オン接続を提供し AWS 、アプライアンスを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は、アプライアンスをアクティベーションプロセス中に使用される AWS アカウントと関連付けます。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、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起動できます。

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) のインターネットプロトコルバージョン 4 (IPv4) アドレスを設定します。詳細については、「ハードウェアアプライアンスの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、「AWS Storage Gateway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. ハードウェアアプライアンスでゲートウェイを作成します。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。

   ハードウェアアプライアンスへのゲートウェイのセットアップは、VMware ESXi、Microsoft Hyper-V、Linux カーネルベース仮想マシン (KVM)、または Amazon EC2 でのセットアップと同じ方法で行います。

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は、5 個の 1.92 TB SSD (ソリッドステートドライブ) を購入することで、使用可能なストレージを 12 TB に増やすことができます。

次にそれを、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、 AWS サポートにお問い合わせください。
2. 5 個の 1.92 TB SSD をアプライアンスに追加します。

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 RJ45 銅線または 10G DA/SFP+ ネットワークカードが付属します。

- 10G-Base-T NIC の構成:
  - 10G には CAT6 のケーブルを使用し、1G には CAT5(e) を使用
- 10G DA/SFP+ NIC の構成:
  - 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 互換の SFP+ 光モジュール (SR または LR)
  - 1G-Base-T または 10G-Base-T 向け SFP/SFP+ 銅線トランシーバ

ハードウェアアプライアンスの物理的なインストール

> **Note**
>
> 可用性の終了通知: 2025 年 5 月 12 日をもって、 AWS Storage Gateway ハードウェアアプライアンスは提供されなくなります。 AWS Storage Gateway ハードウェアアプライアンスの既存のお客様は、2028 年 5 月まで引き続き を使用し、サポートを受けることができます。別の方法として、 AWS Storage Gateway サービスを使用して、オンプレミスおよびクラウド内のアプリケーションに事実上無制限のクラウドストレージへのアクセスを許可することもできます。

アプライアンスは 1U フォームファクタで、International Electrotechnical Commission (IEC) に準拠した標準の 19 インチラックに適合します。

前提条件

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。

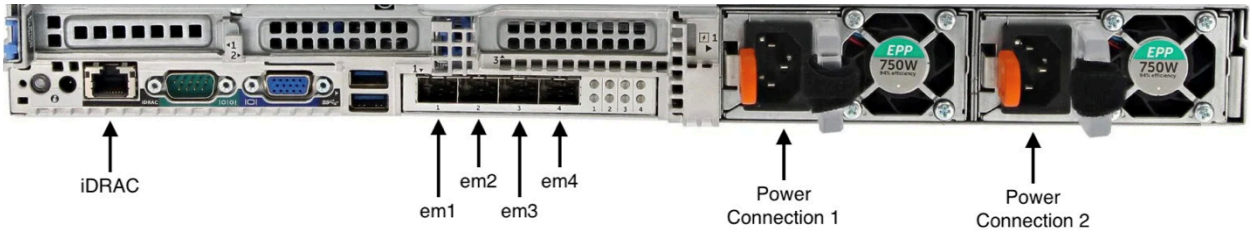
- 電源ケーブル: 1 つは必須です。2 つを推奨します。
- サポートされているネットワークケーブル (ハードウェアアプライアンスに組み込まれているネットワークインターフェイスカード (NIC) によって異なります)。Twinax 銅線 DAC、SFP+ 光モジュール (Intel 互換)、または Base-T 向け SFP 銅線トランシーバ。
- キーボードとモニター、またはキーボード、ビデオ、マウス (KVM) スイッチソリューション。

> **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。

ハードウェアアプライアンスを物理的にインストールするには

1. ハードウェアアプライアンスを開梱し、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。

次の画像は、電源、イーサネット、モニター、USB キーボード、iDRAC を接続するポートを備えたハードウェアアプライアンスの背面を示しています。
ハードウェアアプライアンス 1 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 1 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. 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、冗長性を確保するために両方の電源への接続を推奨します。
3. 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、VLAN ト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は、非トランキング VLAN ポートとして設定します。

4. キーボードとモニターを接続します。
5. 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。

次のステップ

ハードウェアアプライアンスコンソールへのアクセス

ハードウェアアプライアンスコンソールへのアクセス

> **Note**
>
> 可用性の終了通知: 2025 年 5 月 12 日をもって、 AWS Storage Gateway ハードウェアアプライアンスは提供されなくなります。 AWS Storage Gateway ハードウェアアプライアンスの既存のお客様は、2028 年 5 月まで引き続き を使用し、サポートを受けることができます。別の方法として、 AWS Storage Gateway サービスを使用して、オンプレミスおよびクラウド内のアプリケーションに事実上無制限のクラウドストレージへのアクセスを許可することもできます。

ハードウェアアプライアンスの電源を入れると、ハードウェアアプライアンスコンソールがモニタに表示されます。ハードウェアアプライアンスコンソールには、管理者パスワードの設定、初期ネットワークパラメータの設定、サポートチャネルのオープン 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 AWS。

ハードウェアアプライアンス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。

ハードウェアアプライアンスコンソールが初めて表示されると、[ようこそ] ページが表示され、コンソールにアクセスする前に管理者ユーザーアカウントのパスワードを設定するように求められます。

管理者パスワードを設定するには

- [ログインパスワードを設定してください] というプロンプトが表示されたら、以下を実行してください。

  a. [パスワードを設定] でパスワードを入力し、Down arrow を押します。

  b. 確認のためにパスワードを再入力し、[パスワードを保存] を選択します。

パスワードを設定すると、ハードウェアコンソールの [ホーム] ページが表示されます。[ホーム] ページには、[em1]、[em2]、[em3]、[em4] ネットワークインターフェイスのネットワーク情報が表示され、次のメニューオプションがあります。

- ネットワークの設定
- サービスコンソールを開く
- パスワードの変更
- ログアウト
- サポートコンソールを開く

次のステップ

ハードウェアアプライアンスのネットワークパラメータの設定

ハードウェアアプライアンスのネットワークパラメータの設定

> **Note**
>
> 可用性の終了通知: 2025 年 5 月 12 日をもって、 AWS Storage Gateway ハードウェアアプライアンスは提供されなくなります。 AWS Storage Gateway ハードウェアアプライアンスの既存のお客様は、2028 年 5 月まで引き続き を使用し、サポートを受けることができます。別の方法として、 AWS Storage Gateway サービスを使用して、オンプレミスおよびクラウド内のアプリケーションに事実上無制限のクラウドストレージへのアクセスを許可することもできます。

ハードウェアアプライアンスが起動し、「ハードウェアアプライアンスコンソールへのアクセス」の説明に従ってハードウェアコンソールで管理者ユーザーのパスワードを設定したら、次の手順を使用してネットワークパラメータを設定して、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. [ホーム] ページから、[ネットワークを設定] を選択し、`Enter` を押します。[ネットワークを設定] ページが表示されます。[ネットワークを設定] ページには、ハードウェアアプライアンス上の 4 つのネットワークインターフェイスの IP と DNS 情報が表示され、それぞれに [DHCP] または [静的] アドレスを設定するメニューオプションが含まれています。
2. [em1] インターフェイス内で、次のいずれかを実行します。

   - [DHCP] を選択し、`Enter` を押すと、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 アドレスが使用されます。

このアドレスを記録し、それを後のアクティベーション手順で使用します。

- [静的] を選択し、Enter を押して、静的 IPv4 アドレスを設定します。

  IP アドレス、サブネットマスク、ゲートウェイ、および DNS サーバーアドレスを、em1 ネットワークインターフェイスに対して入力します。

  完了したら、[保存] を選択し、Enter を押して設定を保存します。

> **Note**
>
> この手順を使用して、[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、要件に記載されている AWS エンドポイントへの同じ常時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 Link Aggregation Control Protocol (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。
> ルーティングの問題が発生する可能性があるため、同じ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。

ハードウェアコンソールからログアウトするには

1. [戻る] を選択して Enter を押すと、[ホーム] ページに戻ります。
2. [ログアウト] を選択し、Enter を押して [ようこそ] ページに戻ります。

次のステップ

AWS Storage Gatewayハードウェアアプライアンスのアクティブ化

AWS Storage Gatewayハードウェアアプライアンスのアクティブ化

> **Note**
>
> 可用性の終了通知: 2025 年 5 月 12 日をもって、 AWS Storage Gateway ハードウェアアプライアンスは提供されなくなります。 AWS Storage Gateway ハードウェアアプライアンスの既存のお客様は、2028 年 5 月まで引き続き を使用し、サポートを受けることができま

す。別の方法として、 AWS Storage Gateway サービスを使用して、オンプレミスおよびクラウド内のアプリケーションに事実上無制限のクラウドストレージへのアクセスを許可することもできます。

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は、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 のいずれか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。

AWS Storage Gateway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**
   >
   > アクティブ化のみを行う場合は、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、アプライアンスへインバウンドトラフィックのためのポート 8080 への 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. [アプライアンスのアクティブ化] 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することです。

次のステップ

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

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

> **Note**
>
> 可用性の終了通知: 2025 年 5 月 12 日をもって、 AWS Storage Gateway ハードウェアアプライアンスは提供されなくなります。 AWS Storage Gateway ハードウェアアプライアンスの既存のお客様は、2028 年 5 月まで引き続き を使用し、サポートを受けることができます。別の方法として、 AWS Storage Gateway サービスを使用して、オンプレミスおよびクラウド内のアプリケーションに事実上無制限のクラウドストレージへのアクセスを許可することもできます。

デプロイ内の任意の AWS Storage Gateway ハードウェアアプライアンスに、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 マネジメントコンソール し、https://console.aws.amazon.com/storagegateway/home で Storage Gateway コンソールを開きます。

2. 「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、デプロイする Storage Gateway の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。Dynamic Host Configuration Protocol (DHCP) を使用する場合、ゲートウェイがコンソールでオンラインとして表示されるまでに 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には、「ゲートウェイの IP アドレスの設定」を参照してください。

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

ハードウェアアプライアンスのゲートウェイ IP アドレスの設定

ハードウェアアプライアンスのゲートウェイ IP アドレスの設定

> **Note**
>
> 可用性の終了通知: 2025 年 5 月 12 日をもって、 AWS Storage Gateway ハードウェアアプライアンスは提供されなくなります。 AWS Storage Gateway ハードウェアアプライアンスの既存のお客様は、2028 年 5 月まで引き続き を使用し、サポートを受けることができます。別の方法として、 AWS Storage Gateway サービスを使用して、オンプレミスおよびクラウド内のアプリケーションに事実上無制限のクラウドストレージへのアクセスを許可することもできます。

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ゲートウェイ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 クライアントなど) は、この IP アドレスに接続します。[オープンサービスコンソール] オプションを使用して、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、[オープンサービスコンソール] を選択し、Enter を押して、ゲートウェイのローカルコンソールのログインページを開きます。
2. AWS Storage Gateway ローカルコンソールのログインページでは、ログインしてネットワーク設定やその他の設定を変更するように求められます。

   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。

   > **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 アプライアンスのアクティベーション - 設定] メインメニューで [ゲートウェイコンソール] 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。パスワードは、Storage Gateway コンソールから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。

3. [AWS アプライアンスのアクティベーション - 設定] ページには、次のメニューオプションが含まれています。

   - HTTP/SOCKS プロキシ設定
   - ネットワーク構成
   - ネットワーク接続のテスト
   - システムリソースチェックの表示
   - システム時刻の管理
   - ライセンス情報
   - コマンドプロンプト

   > **Note**
   >
   > 一部のオプションは、特定のゲートウェイタイプまたはホストプラットフォームにのみ表示されます。

対応する番号を入力して [ネットワーク構成] を選択します。

4. ゲートウェイ IP アドレスを設定するには、次のいずれかを実行します。

   - Dynamic Host Configuration Protocol (DHCP) サーバーによって割り当てられた IP アドレスを使用するには、[DHCP の設定] に対応する数値を入力し、次のページで有効な DHCP 設定情報を入力します。
   - 静的 IP アドレスを割り当てるには、[静的 IP の設定] に対応する数値を入力し、次のページで有効な IP アドレスと DNS 情報を入力します。

   > **Note**
   >
   > ここで指定する 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。

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。これで、Storage Gateway コンソールでゲートウェイのセットアップと設定手順を続行できます。手順については、「Amazon FSx ファイル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からゲートウェイソフトウェアを削除する

> **Note**
>
> 可用性の終了通知: 2025 年 5 月 12 日をもって、 AWS Storage Gateway ハードウェアアプライアンスは提供されなくなります。 AWS Storage Gateway ハードウェアアプライアンスの既存のお客様は、2028 年 5 月まで引き続き を使用し、サポートを受けることができます。別の方法として、 AWS Storage Gateway サービスを使用して、オンプレミスおよびクラウド内のアプリケーションに事実上無制限のクラウドストレージへのアクセスを許可することもできます。

ハードウェアアプライアンスにデプロイした特定の Storage Gateway が不要になった場合は、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できます。ゲートウェイソフトウェアを削除したら、新しいゲートウェイをその場所にデプロイするか、ハードウェアアプライアンス自体を Storage Gateway コンソールから削除するかを選択できます。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。

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 (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. コンソールページの左側にあるナビゲーションペインから [ハードウェア] を選択し、ゲートウェイソフトウェアを削除する [アプライアンスのハードウェアアプライアンス名] 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。
4. 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`」と入力します。
5. [削除] を選択して、ゲートウェイソフトウェアを完全に削除します。

   > **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、「ゲートウェイおよび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。

AWS Storage Gatewayハードウェアアプライアンスの削除

> **Note**
>
> 可用性の終了通知: 2025 年 5 月 12 日をもって、 AWS Storage Gateway ハードウェアアプライアンスは提供されなくなります。 AWS Storage Gateway ハードウェアアプライアンスの既存のお客様は、2028 年 5 月まで引き続き を使用し、サポートを受けることができます。別の方法として、 AWS Storage Gateway サービスを使用して、オンプレミスおよびクラウド内のアプリケーションに事実上無制限のクラウドストレージへのアクセスを許可することもできます。

既にアクティブ化した AWS 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、 サポート 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、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 サポート アクセスをオンにする」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ゲートウェイソフトウェアを削除する」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

このページの概要セクションでは、Storage Gateway の作成プロセスがどのように機能するか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手順については、以下のトピックを参照してください。

- Amazon S3 ファイルゲートウェイを作成してアクティブ化する
- Amazon FSx ファイルゲートウェイを作成してアクティブ化する
- テープゲートウェイを作成してアクティブ化する
- ボリュームゲートウェイを作成してアクティブ化する

> **Important**
>
> 新規のお客様へのAmazon FSx ファイルゲートウェイの提供は終了しました。FSx ファイルゲートウェイの既存のお客様は、引き続き通常どおりサービスを使用できます。FSx ファイルゲートウェイに似た機能については、このブログ記事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、ゲートウェイの接続 AWS、設定の確認と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した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アクセスできます。または、ネットワークのセキュリティ設定を完全に制御できる Amazon VPC 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するための設定を行い、必要に応じてゲートウェイの識別に役立つタグを追加します。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、ゲートウェイに関連付けるボリューム、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。

Amazon FSx for Windows File Server ファイルシステムを作成する

で Amazon FSx File Gateway を作成するには AWS Storage Gateway、まず Amazon FSx for Windows File Server ファイルシステムを作成します。Amazon FSx ファイルシステムをすでに作成している場合は、次のステップ Amazon FSx ファイルゲートウェイを作成してアクティブ化するに進みます。

Note

FSx ファイルゲートウェイから Amazon FSx ファイルシステムに書き込む場合、次の制限が適用されます。

- Amazon FSx ファイルシステムと FSx ファイルゲートウェイは、同じ AWS アカウントによって所有され、同じ AWS リージョンにある必要があります。
- 各ゲートウェイは 5 つのアタッチされたファイルシステムをサポートできます。ファイルシステムをアタッチすると、選択したゲートウェイが容量に達している場合、Storage Gateway コンソールに通知が表示されます。この場合、別のゲートウェイをアタッチする前に、別のゲートウェイを選択するか、ファイルシステムをデタッチする必要があります。
- FSx ファイルゲートウェイは、ソフトストレージクォータ (ユーザーがデータ制限を超えたときに警告を発行) をサポートしていますが、ハードクォータ (書き込みアクセスを拒否してデータ制限を適用する) はサポートしていません。ソフトクォータは、Amazon FSx 管理者ユーザーを除くすべてのユーザーでサポートされています。ストレージクォータの設定の詳細については、「Amazon FSx for Windows File Server ユーザーガイド」の「ストレージクォータ」を参照してください。
- Microsoft 分散ファイルシステム (DFS) を使用して、FSx ファイルゲートウェイ経由でユーザーを Amazon FSx ファイルシステムにリダイレクトすることはお勧めしません。代わりに、「Amazon FSx for Windows File Server ユーザーガイド」の「DFS 名前空間を使用した複数のファイルシステムのグループ化」で説明されているように、 AWS クラウドの Amazon FSx ファイルシステムに直接リダイレクトするように DFS を設定します。
- FSx ファイルゲートウェイでの一部のファイル操作 (トップレベルフォルダの名前変更や権限変更など) は、複数のファイル操作を引き起こし、FSx for Windows File Server ファイルシステムに高い I/O 負荷をもたらす可能性があります。ファイルシステムにワークロードに十分なパフォーマンスリソースがない場合、ファイルシステムはシャドウコピーの保持履歴よりも継続的な I/O の可用性を優先するため、シャドウコピーを削除する可能性があります。

  Amazon FSx コンソールで、「モニタリングとパフォーマンス」ページを見て、ファイルシステムがプロビジョニング不足かどうかを確認します。その場合は、SSD ストレージに切り替えるか、スループット容量を増やすか、または SSD IOPS を増やしてワークロードを処理することができます。

FSx for Windows File Server ファイルシステムを作成するには

1. https://console.aws.amazon.com/fsx/home/ AWS マネジメントコンソール で を開き、ゲートウェイを作成するリージョンを選択します。
2. 詳細については、「Amazon FSx for Windows File Server ユーザーガイド」の「Amazon FSxの使用開始」を参照してください。

Amazon FSx ファイルゲートウェイを作成してアクティブ化する

このセクションでは、 AWS Storage Gatewayでファイルゲートウェイを作成、デプロイ、アクティブ化する方法について説明します。

トピック

- Amazon FSx ファイルゲートウェイのセットアップ
- Amazon FSx ファイルゲートウェイを に接続する AWS
- 設定を確認し、Amazon FSx ファイルゲートウェイをアクティブ化
- Amazon FSx ファイルゲートウェイの設定

Amazon FSx ファイルゲートウェイのセットアップ

新しい FSx ファイル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 マネジメントコンソール 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。ゲートウェイが作成されると、この名前を検索して、 AWS 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、[Amazon FSx ファイルゲートウェイ] を選択します。
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、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ます。次に、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手順に従って、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 カーネルベース仮想マシン (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。推奨される起動設定については、提供されている aws-storage-gateway.xml ファイルを参照してください。ファイルゲートウェイ 2.x、ボリュームゲートウェイ 3.x、テープゲートウェイ 3.x には、セキュアブートが無効 (loader_secure=no) の UEFI ブートモードが必要です。
- 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。
- ハードウェアアプライアンス – ゲートウェイをホスト AWS するには、 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. ゲートウェイがセットアップされたので、ゲートウェイの接続方法と通信方法を選択する必要があります AWS。次へ をクリックして先に進みます。

Amazon FSx ファイルゲートウェイを に接続する AWS

新しい FSx ファイルゲートウェイを に接続するには AWS

1. まだ行っていない場合は、「Amazon FSx ファイルゲートウェイのセットアップ」で説明されている手順を完了してください。完了したら、次へ を選択して、 AWS Storage Gateway コンソールで Connect to AWS 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「AWS Storage Gateway エンドポイントとクォータ」を参照してください。

- VPC ホスト – ゲートウェイは Virtual Private Cloud (VPC) とのプライベート接続 AWS を介して 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した場合は、ドロップダウンリストから VPC エンドポイント ID を選択して、既存の VPC エンドポイントを指定する必要があります。VPC エンドポイントのドメインネームシステム (DNS) 名または IP アドレスを指定することもできます。

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. ゲートウェイの接続方法を選択したら AWS、ゲートウェイをアクティブ化する必要があります。次へ をクリックして先に進みます。

設定を確認し、Amazon FSx ファイルゲートウェイをアクティブ化

新しいFSxファイルゲートウェイをアクティブ化するには

1. まだ実行していない場合は、次のトピックで説明されている手順を完了してください:

   - Amazon FSx ファイルゲートウェイのセットアップ
   - Amazon FSx ファイルゲートウェイを に接続する AWS

   終了したら、次へ を選択して、 AWS 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。

   > **Important**
   >
   > ゲートウェイをアクティブ化した後で、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. 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。次へ をクリックして先に進みます。

Amazon FSx ファイルゲートウェイの設定

新しい FSx ファイルゲートウェイで初回設定を実行する

1. まだ実行していない場合は、次のトピックで説明されている手順を完了してください:

   - Amazon FSx ファイルゲートウェイのセットアップ
   - Amazon FSx ファイルゲートウェイを に接続する AWS
   - 設定を確認し、Amazon FSx ファイルゲートウェイをアクティブ化

   終了したら、次へ を選択して、 AWS 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、ドロップダウンリストを使用して、少なくとも 150 ギビバイト (GiB) の容量を持つ少なくとも 1 つのローカルディスクをキャッシュに割り当てます。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ための Amazon CloudWatch Logs の設定方法を選択します。次のオプションから選択できます:

   - 新しいロググループを作成 - 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リストから既存のロググループを選択します。
   - ログの無効化 - ゲートウェイのモニタリングに Amazon CloudWatch Logs を使用しません。

   > **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:*"
   > ```
   >
   > 個々のロググループに明示的にアクセス許可を適用する場合にのみ、「リソース」要素が必要です。

4. [CloudWatch アラーム] セクションで、定義されている制限からゲートウェイのメトリクスが逸脱したときに通知する Amazon CloudWatch アラームの設定方法を選択します。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 — ゲートウェイの作成時に、CloudWatch の推奨アラームをすべて自動的に作成します。推奨アラームの詳細については、「CloudWatch アラームの説明」を参照してください。

     > **Note**
     >
     > この機能を使用するには、CloudWatch ポリシーのアクセス権限が必要です。この権限は、事前設定済みの Storage Gateway のフルアクセスポリシーの一部として自動的に付与されるものではありません。CloudWatch の推奨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権限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

   - カスタムアラームを作成 — ゲートウェイのメトリクスについて通知する新しい CloudWatch アラームを設定します。[アラームを作成] 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 CloudWatch ユーザーガイド」の「Amazon CloudWatch でのアラームの使用」を参照してください。
   - アラームなし – CloudWatch アラームを使用してゲートウェイのメトリクスについて通知しないでください。

5. (オプション) タグセクションで 新しいタグの追加 を選択し、大文字と小文字を区別するキーと値のペアを入力して、 AWS Storage Gateway 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ー処理できるようにします。この手順を繰り返し、必要な数だけタグを追加します。

6. (オプション) VMware High Availability 設定の検証セクションで、ゲートウェイが VMware High Availability (HA) クラスターの一部である VMware ホストにデプロイされている場合は、VMware HA の検証を選択して、HA 設定が正しく動作しているかどうかをテストします。

> **Note**
>
> このセクションは、VMware ホストプラットフォームで実行されているゲートウェイにのみ表示されます。
> このステップは、ゲートウェイ設定プロセスを完了するためには必要ありません。
> ゲートウェイの HA 設定はいつでもテストできます。検証には数分かかり、Storage Gateway 仮想マシン (VM) を再起動します。

7. [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、 AWS Storage Gateway コンソールのゲートウェイの概要ページでゲートウェイを検索します。

ゲートウェイを作成したので、使用するファイルシステムをアタッチする必要があります。手順については、Amazon FSx for Windows File Serverファイルシステムをアタッチするを参照してください。

アタッチする既存の Amazon FSx ファイルシステムがない場合は、作成する必要があります。手順については、「Amazon FSxの使用開始」 を参照してください。

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 AWS ストレージサービスにデータを転送するように設定できます。Amazon VPC サービスを使用すると、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 リソースをカスタム仮想プライベートクラウド (VPC) で起動できます。VPC では、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。VPC の詳細については、Amazon VPC 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、Amazon VPC コンソールを使用して し、その VPC エンドポイント ID を取得します。ゲートウェイを作成およびアクティブ化するときに、この VPC エンドポイント ID を指定してください。詳細については、 Amazon FSx ファイルゲートウェイを接続する AWS」を参照してください。

VPC を介してデータを転送するように FSx File Gateway を設定するには、Amazon FSx for Windows File Server VPC とゲートウェイがデプロイされているネットワークとの間に VPN または AWS DirectConnect リンクを確立する必要があります。

> **Note**
>
> Storage Gateway 用の VPC エンドポイントを作成したのと同じリージョンで、ゲートウェイをアクティブ化する必要があります。

Storage Gateway 用の VPC エンドポイントを作成するには

これらの手順に従って、VPC エンドポイントを作成します。Storage Gateway 用に VPC エンドポイントがすでに用意されている場合には、それを使用することができます。

Storage Gateway 用の VPC エンドポイントを作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/vpc/ で 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、[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 `com.amazonaws.us-east-2.storagegateway`。
5. [VPC] で、VPC を選択し、そのアベイラビリティーゾーン (AZ) とサブネットをメモします。
6. プライベート DNS 名を有効にする 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、VPC に使用するセキュリティグループを選択します。デフォルトのセキュリティグループを使用できます。次の TCP ポートがすべてセキュリティグループで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保留中です。エンドポイントが作成された場合は、作成した VPC エンドポイントの ID をメモしておきます。
9. エンドポイントが作成されたら、エンドポイント を選択後、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 DNS 名 で、アベイラビリティーゾーン (AZ) を指定していない最初の DNS 名を使用します。DNS 名は次の例のようになります:`vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

これで VPC エンドポイントを作成したので、ゲートウェイを作成およびアクティブ化できます。詳細については、Amazon FSx ファイルゲートウェイを作成してアクティブ化するを参照してください。

アクティベーションキーの取得については、ゲートウェイのアクティベーションキーの取得を参照してください。

Microsoft Active Directory のドメイン設定の構成

このステップでは、Amazon FSx ファイルゲートウェイを、Microsoft Active Directory ドメインに参加させるために、ファイルゲートウェイのアクセス設定を構成します。

Active Directory 設定の構成

1. Storage Gateway コンソールで、ナビゲーションメニューから FSx ファイルシステムを選択します。
2. [FSx ファイルシステムのアタッチ] を選択します。
3. [ゲートウェイの確認] ページで、ドロップダウンメニューから Active Directory ドメインに参加させるゲートウェイを選択します。

   ゲートウェイがない場合は、作成します。ゲートウェイが Active Directory ドメインコントローラーの名前を解決できることを確認します。詳細については、「前提条件」を参照してください。
4. [Active Directory 設定] の値を入力します。

   > **Note**
   >
   > ゲートウェイが既にドメインに参加している場合は、再度参加する必要はありません。次のステップに進みます。

   - [ドメイン名] には、使用する Active Directory のドメイン名を入力します。
   - [ドメインユーザー] には、ゲートウェイをドメインに参加させるために使う Active Directory ユーザーのユーザー名を入力します。このユーザーは必要なアクセス許可を備えている必要があります。詳細については、「Active Directory サービスアカウントのアクセス許可要件」を参照してください。
   - [ドメインパスワード] に、ユーザーのパスワードを入力します。
   - [組織単位 - オプション] で、Active Directory が属する組織単位を指定できます。

     > **Note**
     >
     > このフィールドを空白のままにして、ドメインに参加させると、ゲートウェイのゲートウェイ ID をアカウント名 (SGW-1234ADE など) として使用して、デフォルトのコ

ンピュータコンテナ (OU ではない) に Active Directory コンピュータアカウントが作成されます。このアカウントの名前をカスタマイズすることはできません。
Active Directory 環境で、ドメイン結合プロセスを容易にするためにアカウントを事前ステージングする必要がある場合は、事前にこのアカウントを作成する必要があります。
Active Directory 環境に新しいコンピュータオブジェクト用に指定された OU がある場合は、ドメインに参加するときにその OU を指定する必要があります。

- [ドメインコントローラー (複数可)] の値を入力します。これは選択可能なオプションです。

5. [次へ] を選択して、[FSx ファイルシステムのアタッチ] ページを開きます。

次のステップ

Amazon FSx for Windows File Server ファイルシステムのアタッチ

Amazon FSx for Windows File Server ファイルシステムのアタッチ

FSx ファイルゲートウェイに接続する前に、FSx for Windows File Server ファイルシステムが必要です。ファイルシステムがない場合は作成する必要があります。手順については、「Amazon FSx for Windows File Server ユーザーガイド」の「ステップ 1: ファイルシステムを作成する」を参照してください。

次のステップでは、Amazon FSx ファイルシステムをゲートウェイにアタッチします。Amazon FSx ファイルシステムをアタッチすると、ファイルシステム上のすべてのファイル共有が Amazon FSx ファイルゲートウェイ (FSx ファイルゲートウェイ) でマウントできるようになります。

> **Note**
>
> Amazon FSx ファイルゲートウェイから Amazon FSx ファイルシステムに書き込む際には、次の制限が適用されます。
>
> - Amazon FSx ファイルシステムと FSx ファイルゲートウェイは、同じ AWS アカウント によって所有され、同じ AWS リージョン内にある必要があります。
> - 各ゲートウェイは最大 5 つのアタッチされたファイルシステムをサポートできます。ファイルシステムをアタッチすると、選択したゲートウェイが容量に達している場合、Storage Gateway コンソールに通知が表示されます。この場合、別のゲートウェイをアタッチする前に、別のゲートウェイを選択するか、ファイルシステムをデタッチする必要があります。
> - FSx ファイルゲートウェイは、ソフトストレージクォータ (ユーザーがデータ制限を超えたときに警告) をサポートしていますが、ハードクォータ (書き込みアクセスを拒否してデータ制限を適用) はサポートしていません。ソフトクォータは、Amazon FSx 管理者ユーザーを除くすべてのユーザーでサポートされています。ストレージクォータの設定の詳細については、「Amazon FSx ユーザーガイド」の「ストレージクォータ」を参照してください。
> - Microsoft 分散ファイルシステム (DFS) を使用して、FSx ファイルゲートウェイ経由でユーザーを Amazon FSx ファイルシステムにリダイレクトすることはお勧めしません。代わりに、「Amazon FSx for Windows File Server ユーザーガイド」の「DFS 名前空間を使用した複数のファイルシステムのグループ化」で説明 AWS クラウド されているよ

うに、 の Amazon FSx ファイルシステムに直接リダイレクトするように DFS を設定します。 https://docs.aws.amazon.com/fsx/latest/WindowsGuide/group-file-systems.html FSx

Amazon FSx ファイルシステムをアタッチするには

1. Storage Gateway コンソールの [FSx ファイルシステム] > [FSx ファイルシステムのアタッチ] ページに移動し、[FSx ファイルシステム設定] セクションで次のフィールドに入力します。

   - [FSx ファイルシステム名] で、アタッチするファイルシステムをドロップダウンリストから選択します。
   - [ローカルエンドポイント IP アドレス] に、クライアントが FSx ファイルシステム上のファイル共有を参照するために使用するゲートウェイ IP アドレスを入力します。

   > **Note**
   >
   > - ゲートウェイにアタッチされたファイルシステムごとに IP アドレスを指定する必要があります。
   > - Amazon EC2 ゲートウェイの場合、EC2 インスタンスのプライベート IP アドレスを指定できます。ただし、別のファイルシステムで既に使用されている場合は除きます。この場合、ゲートウェイに新しいプライベートアドレスを追加してから再起動する必要があります。詳細については、「Amazon EC2 ユーザーガイド」の「複数の IP アドレス」を参照してください。
   > - オンプレミスゲートウェイの場合、プライマリネットワークインターフェイス (静的または DHCP) の IP アドレスを指定できます。ただし、別のファイルシステムで既に使用されている場合は、プライマリインターフェイスと同じサブネットから別の IP アドレスを指定する必要があります。この IP アドレスは仮想 IP として使用可能になります。プライマリ以外のネットワークインターフェイスに割り当てられた IP アドレスを使用しないでください。

2. [サービスアカウント設定] セクションで、Amazon FSx ファイルシステムに関連付けられているサービスアカウントのサインイン認証情報を指定します。

> **Note**
>
> このサービスアカウントには、Amazon FSx ファイルシステムに関連付けられている Active Directory サービスからの Backup Operators 権限、または同等のアクセス許可が必要です。

> **Important**
>
> ファイル、フォルダ、およびファイルメタデータに対する十分なアクセス許可を確保するために、このサービスアカウントをファイルシステム管理者グループのメンバーにすることをお勧めします。
> Amazon FSx AWS Directory Service for Windows File Server で for Microsoft Active Directory を使用している場合、サービスアカウントは委任 AWS FSx 管理者グループのメンバーである必要があります。
> Amazon FSx for Windows File Server でセルフマネージド Active Directory を使用している場合は、Amazon FSx ファイルシステムの作成時にファイルシステム管理用に指定した、カスタム委任ファイルシステム管理者グループのメンバーとしてサービスアカウントを使用することをお勧めします。
> Amazon FSx ファイルシステムの作成時にカスタム委任ファイルシステム管理者グループを作成しない場合、デフォルトのグループはドメイン管理者です。代わりにサービスアカウントをこのグループのメンバーにすることはできますが、ベストプラクティスとしてはお勧めしません。
> 詳細については、「Amazon FSx for Windows File Server ユーザーガイド」の「Amazon FSx サービスアカウントに権限を委任する」を参照してください。

3. [監査ログ] セクションで、[既存のロググループ] を選択し、Amazon FSx ファイルシステムへのアクセスをモニタリングするために使用するログを選択します。新しいログを作成できます。システムをモニタリングしない場合は、[ログ記録を無効にする] を選択します。
4. [自動キャッシュ更新設定] でキャッシュを自動的にリフレッシュする場合、[更新間隔を設定] を選択し、5 分～30 日の間隔を入力して、キャッシュを自動的に更新します。
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、1 つ以上のキーと設定にタグ付けするための値を追加します。
6. [次へ] をクリックして、設定を確認します。[編集] を選択して、設定を変更できます。
7. 完了したら、[終了] を選択します。

次のステップ

Amazon FSx ファイル共有をマウントして使用する

Amazon FSx ファイル共有をマウントして使用する

クライアントにファイル共有をマウントする前に、Amazon FSx ファイルシステムのステータスが Available (利用可能) に変わるのを待ちます。ファイル共有がマウントされたら、Amazon FSx ファイルゲートウェイ(FSx ファイルゲートウェイ) の使用できるようになります。

トピック

SMB ファイル共有をクライアントにマウントする

このステップでは、SMB ファイル共有をマウントして、クライアントからアクセスできるようにドライブにマッピングします。コンソールのファイルゲートウェイのセクションには、SMB クライアントで使用できるサポート対象のマウントのコマンドが表示されます。以下は、試すことができる追加オプションです。

SMB ファイル共有のマウントでは、以下を含むいくつかの異なるメソッドを使用できます。

- `net use` コマンド — `/persistent:(yes:no)` スイッチを使用する場合を除いて、システムの再起動後は保持されません。
- `CmdKey` コマンドラインユーティリティ — 再起動後にも保持される、マウントされた SMB ファイル共有への永続的な接続を作成します。
- File Explorer にマッピングされるネットワークドライブ — サインインで再接続し、ネットワーク認証情報の入力が必要になるようにマウントされたファイル共有を設定します。
- PowerShell スクリプト — 永続的で、マウント中にオペレーティングシステムで表示あるいは非表示にすることができます。

> **Note**
>
> Microsoft Active Directory ユーザーの場合は、ローカルシステムにファイル共有をマウントする前に、SMB ファイル共有にアクセスできることを管理者に確認します。
> Amazon FSx ファイルゲートウェイは、SMB ロックまたは SMB 拡張属性をサポートしていません。

net use コマンドを使用して、ゲストユーザーに SMB ファイル共有をマウントするには

1. ローカルシステムにファイル共有をマウントする前に、SMB ファイル共有へのアクセス権があることを確認します。
2. Microsoft Active Directory クライアントの場合は、コマンドプロンプトで次のコマンドを入力します。

   ```
   net use [WindowsDriveLetter]: \\[Gateway IP Address]\[Name of the share on the FSx file system]
   ```

CmdKey を使用して Windows に SMB ファイル共有をマウントするには

1. Windows キーを押して「**cmd**」と入力し、コマンドプロンプトメニューアイテムを表示します。
2. [コマンドプロンプト] でコンテキスト (右クリック) メニューを開き、[Run as administrator (管理者として実行)] を選択します。
3. 次のコマンドを入力します。

   ```
   C:\>cmdkey /add:[Gateway VM IP address] /user:[DomainName]\[UserName] /pass:[Password]
   ```

> **Note**
>
> ファイル共有をマウントする際に、クライアントの再起動後、ファイル共有の再マウントが必要になる場合があります。

Windows ファイルエクスプローラーを使用して SMB ファイル共有をマウントするには

1. Windows キーを押して [Search Windows (検索ウィンドウ)] ボックスに「**File Explorer**」と入力するか、**Win+E** を押します。
2. ナビゲーションペインで [この PC] を選択します。次に、[コンピュータ] タブで、[ネットワークドライブのマッピング] を選択します。
3. [ネットワークドライブのマッピング] ダイアログボックスで、[ドライブ] にドライブ文字を選択します。

4. [Folder (フォルダ)] に「***[File Gateway IP]**[SMB File Share Name]***」と入力するか、または [Browse (閲覧)] を選択して、ダイアログボックスから SMB ファイル共有を選択します。
5. (オプション) 再起動後にマウントポイントを持続させる場合には、[サインアップ時に再接続] を選択します。
6. (オプション) Active Directory ログオンあるいはゲストアカウントユーザーパスワードをユーザーが入力するようにする場合には、[Connect using different credentials (異なる認証情報を使用して接続)] を選択します。
7. [Finish (完了)] を選択して、マウントポイントを完了します。

FSx ファイルゲートウェイをテストする

ファイルとフォルダをマップ済みのドライブにコピーできます。ファイルは自動的に FSx for Windows File Server ファイルシステムにアップロードされます。

ファイルを Windows クライアントから Amazon FSx にアップロードするには

1. Windows クライアントで、ファイル共有をマウントしたドライブに移動します。ドライブ名の先頭にはファイルシステムの名前が付いています。
2. ファイルまたはディレクトリをドライブにコピーします。

> **Note**
>
> ファイルゲートウェイはファイル共有で、ハードリンクまたはシンボリックリンクの作成をサポートしていません。

Amazon FSx ファイルゲートウェイのリソースの管理

以下のセクションでは、Amazon FSx ファイルシステムのアタッチとデタッチ、Microsoft Active Directory 設定の設定など、Amazon FSx ファイルゲートウェイ(FSx ファイルゲートウェイ) リソースの管理方法について説明します。

トピック

ゲートウェイのステータスを理解する

AWS Storage Gatewayデプロイの各ゲートウェイには、ゲートウェイの状態が一目でわかるステータスが関連付けられています。ほとんどの場合、このステータスはゲートウェイが正常に機能しており、ユーザー側でアクションを実行する必要がないことを示します。場合によっては、ステータスによって問題があることが示され、お客様による操作が必要な場合と、必要ない場合があります。

デプロイメント内の各ゲートウェイのステータスは、Storage Gateway コンソールの ゲートウェイ ページで確認できます。ゲートウェイのステータスは、ゲートウェイの名前の横にあるステータス列に表示されます。正常に機能しているゲートウェイのステータスは RUNNING となります。

次の表では、各ゲートウェイのステータスの説明と、それに基づく対応の要否が示されています。ゲートウェイは、使用中の全時間またはほとんどの時間、RUNNING ステータスになっている必要があります。

ステータス	意味
RUNNING	ゲートウェイは適切に構成されており、使用可能です。

ステータス	意味
OFFLINE	ゲートウェイが OFFLINE ステータスになっているのは、次の 1 つ以上の理由による可能性があります。 • 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ているキャッシュディスクが切断されているか、変更されているか、または失敗しています。

ファイルシステムのステータスを理解する

ステータスを確認することで、ファイルシステムの正常性を一目で確認できます。ステータスがファイルシステムが正常に機能していることを示している場合は、ユーザー側で操作を行う必要はありません。ステータスに問題があることが示されている場合は、調査を行って、アクションが必要かどうかを判断できます。

ファイルシステムのステータスは、Storage Gateway コンソールの ステータス 列で表示できます。正常に機能しているファイルシステムのステータスは利用可能と表示されます。これはほとんどの場合、ステータスである必要があります。

次の表に、ファイル共有のステータス、意味、アクションが必要かどうかを示します。

ステータス	意味
利用可能	ファイルシステムは適切に設定され、使用可能です。これは、正常に動作しているファイルシステムの標準ステータスです。
作成中	ファイルシステムはまだ完全には作成されておらず、使用する準備ができていません。作成中ステータスは遷移します。アクションは必要ありません。ファイルシステムがこのステータスで停止した場合、ゲートウェイ VM の接続が失われた可能性があります AWS。
更新中	ファイルシステム設定は現在更新中です。更新中ステータスは推移的です。アクションは必要ありません。ファイルシステムがこのステータス

ステータス	意味
	で停止した場合、ゲートウェイ VM の接続が失われた可能性があります AWS。
削除中	ファイルシステムは削除中です。ファイルシステムは、すべてのデータがアップロードされるまで削除されません AWS。削除中ステータスは変化するので、アクションは必要ではありません。
FORCE_DELETING	ファイルシステムは強制的に削除されます。ファイルシステムはすぐに削除され、データはアップロードされません AWS。FORCE_DELETING ステータスは変化するため、必要なアクションはありません。
エラー	ファイルシステムが異常な状態にあります。アクションは必要ありません。考えられる原因には、アクセス認証情報や権限の問題、接続の問題、ファイルシステムのストレージ容量不足などがあります。異常な状態を引き起こしていた問題が解決すると、ファイルは使用可能な状態に戻ります。

FSx ファイルゲートウェイの基本情報を編集する

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. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) 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. 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。

> **Note**
>
> ゲートウェイ名は 2～255 文字で、スラッシュ (\ または /) を含めることはできません。
> ゲートウェイの名前を変更すると、ゲートウェイを監視するために設定されたすべての 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の GatewayName を更新します。

5. [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。
6. [ロググループのセットアップ方法の選択] では、ゲートウェイのヘルスをモニタリングするための Amazon CloudWatch Logs の設定方法を選択します。次のオプションから選択できます:
   - 新しいロググループを作成 - 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リストから既存のロググループを選択します。
   - ログの無効化 - ゲートウェイのモニタリングに Amazon CloudWatch Logs を使用しません。
7. 変更する設定の変更が完了したら、変更を保存 を選択します。

ゲートウェイのセキュリティレベル設定

FSx ファイル ゲートウェイの SMB セキュリティ レベルを構成して、ゲートウェイでサーバー メッセージ ブロック (SMB) 署名または SMB 暗号化が必要かどうかを指定できます。

セキュリティレベルを設定するには

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. [ゲートウェイ] を選択し、SMB 設定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 [SMB 設定の編集] を選択し、[SMB セキュリティ設定] を選択します。
4. [セキュリティレベル] で、以下のいずれかを選択します。

> **Note**
>
> AWS API を使用してこの設定を設定する方法については、 API AWS Storage Gateway リファレンスのUpdateSMBSecurityStrategy」を参照してください。
> セキュリティ レベルを高くすると、ゲートウェイのパフォーマンスに影響する可能性があります。

- 必須暗号化 – このオプションを選択した場合、FSx ファイルゲートウェイは 256 ビット AES 暗号化アルゴリズムを使用する SMBv3 クライアントからの接続のみを許可します。128 ビットアルゴリズムは許可されません。このオプションは、機密データを扱う環境で推奨されます。Microsoft Windows 8、Windows Server 2012 以降の SMB クライアントで動作します。
- 暗号化の適用 – このオプションを選択すると、FSx ファイル ゲートウェイは暗号化が有効になっている SMBv3 クライアントからの接続のみを許可します。256 ビットと 128 ビットの両方のアルゴリズムを使用できます。このオプションは、機密データを扱う環境で推奨されます。Microsoft Windows 8、Windows Server 2012 以降の SMB クライアントで動作します。
- 署名の適用 — このオプションを選択した場合、FSx ファイルゲートウェイは、署名が有効になっている SMBv2 または SMBv3 クライアントからの接続のみを許可します。このオプションは、Microsoft Windows Vista、Windows Server 2008 以降の SMB クライアントで作動します。

> **Note**
>
> S3 ファイルゲートウェイのデフォルトのセキュリティレベルは [暗号化の適用] です。

5. 保存を選択します。

FSx ファイルゲートウェイのActive Directory設定の編集

企業の Microsoft Active Directory または Amazon FSx ファイルシステムへの AWS Managed Microsoft AD ユーザー認証アクセスを使用するには、ゲートウェイの SMB 設定を編集し、Active Directory ドメイン認証情報を指定します。これにより、ゲートウェイが Active Directory ドメインに参加し、ドメインのメンバーが SMB ファイルシステムにアクセスできるようになります。

> **Note**
>
> を使用すると Directory Service、 でホストされた Active Directory ドメインサービスを作成できます AWS クラウド。
> Amazon EC2 ゲートウェイ AWS Managed Microsoft AD で を使用するには、 と同じ VPC に Amazon EC2 インスタンスを作成し AWS Managed Microsoft AD、_workspaceMembers セキュリティグループを Amazon EC2 インスタンスに追加し、 の管理者認証情報を使用して AD ドメインに参加する必要があります AWS Managed Microsoft AD。
> 詳細については AWS Managed Microsoft AD、「AWS Directory Service 管理ガイド」を参照してください。
> Amazon EC2 の詳細については、Amazon Elastic Compute Cloud ドキュメントを参照してください。

Active Directory 認証を有効化するには

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. [ゲートウェイ] を選択し、SMB 設定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SMB 設定の編集を選択し、Active Directory 設定を選択します。
4. ドメイン名には、ゲートウェイを結合する Active Directory ドメインの名前を入力します。

> **Note**
>
> ゲートウェイがドメインに参加したことがない場合、Active Directory のステータスは切断と表示されます。
> Active Directory サービスアカウントには、必要なアクセス許可が必要です。詳細については、」「Active Directory サービスアカウントのアクセス許可要件」を参照してください。
> ドメインに加入すると、ゲートウェイのゲートウェイ ID をアカウント名 (SGW-1234ADE など) として使用して、デフォルトのコンピュータコンテナ (OU ではない) に Active Directory コンピュータアカウントが作成されます。このアカウントの名前をカスタマイズすることはできません。
> Active Directory 環境で、ドメイン結合プロセスを容易にするためにアカウントを事前ステージングする必要がある場合は、事前にこのアカウントを作成する必要があります。

Active Directory 環境に新しいコンピュータオブジェクト用に指定された OU がある場合は、ドメインに参加するときにその OU を指定する必要があります。
ゲートウェイが Active Directory ディレクトリと結合できない場合には、JoinDomain API オペレーションを使用して、ディレクトリの IP アドレスとの結合をお試しください。

5. ドメインユーザーとドメインパスワード には、ゲートウェイがドメインに参加するために使用する Active Directory サービスアカウントの認証情報を入力します。
6. (オプション) [組織単位 (OU)] には、Active Directory が新しいコンピュータオブジェクトに使用する指定された OU を入力します。
7. (オプション) ドメインコントローラー (DC)には、ゲートウェイが Active Directory に接続する 1 つ以上の DC の名前を入力します。複数の DC カンマ区切りのリストとして入力できます。このフィールドを空白のままにすると、DNS が DC を自動的に選択できるようになります。
8. 変更の保存 を選択します。

Amazon FSx ファイルシステムの設定の編集

Amazon FSx for Windows File Server ファイルシステムを作成したら、CloudWatch ログ、自動キャッシュ更新、Amazon FSx サービスアカウントの認証情報の設定を編集できます。

Amazon FSx ファイルシステム設定を編集するには

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 ファイルシステム を選択し、設定を編集したいファイルシステムを選択します。
3. アクション で、ファイルシステム設定の編集を選択します。
4. ファイルシステム設定セクションで、ゲートウェイ、Amazon FSx の場所、および IP アドレス情報を確認します。

Note

ゲートウェイにアタッチされたファイルシステムの IP アドレスは編集できません。IP アドレスを変更するには、ファイルシステムをデタッチして再アタッチする必要があります。

5. 監査ログセクションで、CloudWatch ロググループを使用して Amazon FSx ファイルシステムへのアクセスをモニタリングするオプションを選択します。既存のロググループを使用できます。
6. 自動キャッシュ更新設定で、オプションを選択します。更新間隔の設定を選択した場合は、Time To Live (TTL) を使用してファイルシステムのキャッシュを更新する間隔を、日・時・分単位で設定します。

   TTL は、最後に実行された更新からの時間的長さです。その時間が経過した後にディレクトリにアクセスすると、ファイルゲートウェイはそのディレクトリの内容を Amazon FSx ファイルシステムから更新します。

   > **Note**
   >
   > 有効な更新間隔の値は 5 分から 30 日の範囲です。

7. サービスアカウント設定 - オプションセクションで、ユーザー名とパスワードを入力します。これらの認証情報は、Amazon FSx ファイルシステムに関連付けられた Active Directory サービスのバックアップ管理者ロールを持つユーザーを対象としています。
8. 変更の保存 を選択します。

Amazon FSx ファイルシステムのデタッチ

ファイルシステムをデタッチしても、FSx for Windows ファイルサーバーのデータは削除されません。デタッチする前にこれらのファイルシステムに書き込まれたデータは、引き続き FSx for Windows ファイル サーバーにアップロードされます。

Amazon FSx ファイルシステ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. FSx ファイルシステムを選択し、デタッチするファイルシステムを 1 つ以上選択します。
3. アクション で、ファイルシステ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. 指定したファイルシステムをデタッチすることを確認し、確認ボックスにデタッチと入力してデタッチ を選択します。

Storage Gateway のモニタリング

このセクションでは、Amazon CloudWatch を使用して Storage Gateway 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リソースのモニタリングが含まれます。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。たとえば、読み取りおよび書き込みオペレーションで使用されるバイト数、読み取りおよび書き込みオペレーションに費やされた時間、 AWS クラウドからデータを取得するのにかかる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 では CloudWatch メトリクスを追加料金なしで提供しています。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、ゲートウェイのパフォーマンスをより的確に把握できます。Storage Gateway では、高精度アラームを除く CloudWatch アラームも追加料金なしで提供します。CloudWatch の料金の詳細については、「Amazon CloudWatch の料金」を参照してください。CloudWatch の詳細については、「Amazon CloudWatch ユーザーガイド」を参照してください。

トピック

- CloudWatch アラームの説明 - アラーム状態や推奨設定など、CloudWatch アラームに関する基本情報について説明します。
- CloudWatch 推奨アラームの作成 - ファイルゲートウェイの初期セットアッププロセスの一環として、推奨されるすべての CloudWatch アラームを迅速かつ自動的に設定する方法について説明します。
- カスタム CloudWatch アラームの作成 - カスタム CloudWatch アラームを作成して、特定の評価基準を使用して特定のメトリクスをモニタリングし、アラーム状態をトリガーして通知を送信する方法について説明します。
- FSx ファイルゲートウェイのモニタリング - CloudWatch ログと監査ログを表示し、ゲートウェイによってレポートされる特定のゲートウェイとファイル共有ファイルシステムメトリクスに関する情報を検索する方法について説明します。

CloudWatch アラームの説明

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。ゲートウェイ用の 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。FSx ファイル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「」「ファイルシステ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、ALARM 状態がアクティブ化する条件を指定します。ALARM 状態になると、Storage Gateway コンソールのアラーム状態のインジケータが赤に変わるため、先を見越した状態のモニタリングがしやすくなります。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 アラームの使用の詳細については、Amazon CloudWatch 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。

> **Note**
>
> CloudWatch を表示するアクセス許可がない場合は、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
- アップロードに失敗したファイル: `FilesFailingUpload` >= 5 分以内に1対1のデータポイント
- ファイルシステムエラー: `FileSystem-ERROR` >= 1、 1 つのデータポイント、5 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、[欠落データの処理] を [notBreaching] に設定してください。

> **Note**
>
> ヘルス通知アラームを設定できるのは、CloudWatch で以前にゲートウェイのヘルス通知を処理した場合のみです。

VMware High Availability クラスターの一部である 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、[欠落データの処理] を [notBreaching] に設定してください。

次の表に、CloudWatch アラームの状態を示します。

State	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。

ゲートウェイ用の CloudWatch 推奨アラームの作成

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、CloudWatch の推奨アラームをすべて自動的に作成することを選択できます。詳細については、Amazon FSx ファイルゲートウェイを設定するを参照してください。初回設定を完了した既存のゲートウェイに対して、推奨されるCloudWatchアラームを追加または更新する場合は、次の手順を実行してください。

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

> **Note**
>
> この機能を使用するには、CloudWatch ポリシーのアクセス権限が必要です。この権限は、事前設定済みの Storage Gateway のフルアクセスポリシーの一部として自動的に付与されるものではありません。CloudWatch の推奨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権限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. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home/) を開きます。
2. ページの左側にあるナビゲーションペインで [ゲートウェイ] を選択し、CloudWatch の推奨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 CloudWatch アラームがすべて一覧表示されます。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 では、アラームの状態が変化したときにアラーム通知を送信するために Amazon Simple Notification Service (Amazon SNS) を使用します。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 トピックを作成することができます。Amazon SNS の詳細については、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. 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 [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 [アラームを作成] 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、必要なタイプのアラームを作成します。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。指定した評価期間数にわたってメトリクスがしきい値を超えると、アラームが ALARM 状態に移行します。

     静的しきい値アラームを作成するには、Amazon CloudWatch ユーザーガイドの「静的しきい値に基づいて CloudWatch アラームを作成する」を参照してください。
   - 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、CloudWatch は、このしきい値をモデルで使用して、メトリクスの「正常」な値の範囲を決定します。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。

     メトリクスの数式アラームを作成するには、Amazon CloudWatch ユーザーガイドの「メトリクスの数式に基づく 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 CloudWatch 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。
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 CloudWatch アラームがすべて一覧表示されます。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には、「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、そのゲートウェイに関連付けられている CloudWatch アラームもすべて自動的に削除されます。

FSx ファイルゲートウェイのモニタリング

Amazon CloudWatch メトリクスと監査ログ AWS Storage Gateway を使用して、 で FSx File Gateway と関連するリソースをモニタリングできます。CloudWatch Events を使用して、ファイルオペレーションが完了したときに通知を受け取ることもできます。

トピック

- CloudWatch ロググループを使用した FSx ファイルゲートウェイヘルスログの取得
- Amazon CloudWatch メトリクスを使用する
- ゲートウェイメトリクスについて
- ファイルシステムメトリクスについて
- FSx ファイルゲートウェイ監査ログについて

CloudWatch ロググループを使用した FSx ファイルゲートウェイヘルスログの取得

Amazon CloudWatch Logs を使用して、FSx ファイルゲートウェイおよび関連リソースのヘルスに関する情報を取得できます。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の処理を自動化できます。詳細については、Amazon CloudWatch Logs 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。

たとえば、CloudWatch ロググループを設定してゲートウェイを監視し、FSx ファイルゲートウェイがファイルを Amazon FSx ファイルシステムにアップロードできなかった場合に通知を受け取るこ

とができます。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際、または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。ゲートウェイのアクティブ化時に CloudWatch ロググループを設定する方法については、「Amazon FSx ファイルゲートウェイの設定」を参照してください。CloudWatch ロググループの一般的情報については、Amazon CloudWatch ユーザーガイドの「ロググループとログストリームの操作」を参照してください。

FSx ファイルゲートウェイによって報告される可能性のあるエラーのトラブルシューティング方法については、「トラブルシューティング: ファイルゲートウェイに関する問題」を参照してください。

ゲートウェイをアクティブ化した後の CloudWatch ロググループの設定

次の手順では、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。

FSx ファイルゲートウェイと連携するように CloudWatch ロググループを設定するには

1. にサインイン AWS マネジメントコンソール し、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、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] を選択します。
4. [ロググループの設定方法を選択する] で、次のいずれかを選択します。

   - [Create a new log group] (新しいロググループの作成) 新しい CloudWatch ロググループを作成する場合。
   - [Use an existing log group] (既存のロググループの使用) 既に存在している CloudWatch ロググループを使用する場合。

     [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。
   - [ログの無効化] CloudWatch 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。
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. ナビゲーションペインで、[ゲートウェイ] を選択してから、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. [Details] (詳細) タブを選択し、[Health logs] (ヘルスログ) で、[CloudWatch Logs] を選択します。CloudWatch コンソールに、[Log group details] (ロググループの詳細) ページが開きます。

Amazon CloudWatch メトリクスを使用する

AWS マネジメントコンソール または CloudWatch API を使用してFSx File Gateway 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 raw データに基づいて一連のグラフが表示されます。CloudWatch API は、各種 AWS SDK や Amazon CloudWatch API ツールを通じても使用できます。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` および `GatewayName` です。CloudWatch コンソールでは、`Gateway Metrics` ビューを使用して、ゲートウェイ固有のディメンションを選択できます。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「Dimensions」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。

Amazon 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ます。FSx ファイルゲートウェイを特定して操作するには、両方の`GatewayId` と`GatewayName` のディメンションを指定します。 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ファイル共有に基づきます。

Amazon CloudWatch 名前空間	ディメンション	説明
		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ファイルのメトリクスの使用は、他のサービスの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。

- 使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

ゲートウェイメトリクスについて

次の表は、FSx ファイルゲートウェイを対象とするメトリクスを示しています。各ゲートウェイには、一連のメトリクスが関連付けられています。一部のゲートウェイ固有のメトリクスには、特定のファイルシステム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値を表していますが、ファイルシステムではなくゲートウェイを対象としています。

特定のメトリクスを扱う際は、ゲートウェイで作業するのか、ファイルシステムで作業するのかを必ず指定してください。具体的には、ゲートウェイメトリクスを使用する場合は、メトリクスデータを表示するゲートウェイの `Gateway Name` を指定する必要があります。詳細については、「Amazon CloudWatch メトリクスを使用する」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。

以下の表は、FSx ファイルゲートウェイに関する情報を取得するために使用できるメトリクスについて説明しています。

メトリクス	説明
AvailabilityNotifications	このメトリクスは、報告期間中にゲートウェイによって生成された可用性に関連するヘルス通知の数を報告します。 単位: カウント
CacheDirectorySize	このメトリクスは、ゲートウェイキャッシュ内のフォルダサイズを追跡します。フォルダのサイズは、最初のレベルのファイルとサブフォルダの数によって決まります。これはサブフォルダに再帰的にカウントされません。 このメトリクスを Average 統計で使用して、ゲートウェイキャッシュ内のフォルダの平均サイズを測定します。このメトリクスを Max 統計で使用して、ゲートウェイキャッシュ内のフォルダの最大サイズを測定します。 単位: カウント
CacheFileSize	このメトリクスは、ゲートウェイキャッシュ内のファイルサイズを追跡します。 このメトリクスを Average 統計で使用して、ゲートウェイキャッシュ内のファイルの平均サイズを測定します。このメトリクスを Max 統計で使用して、ゲートウェイキャッシュ内のファイルの最大サイズを測定します。 単位: バイト
CacheFree	このメトリクスは、ゲートウェイキャッシュ内の使用可能なバイト数を報告します。 単位: バイト

メトリクス	説明
CacheHitPercent	キャッシュから提供されるゲートウェイからのアプリケーション読み取り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。 ゲートウェイ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	永続化されていないゲートウェイキャッシュの全体的な割合 AWS。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
CachePercentUsed	使用されているゲートウェイキャッシュストレージの全体的な割合。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
CacheUsed	このメトリクスは、ゲートウェイキャッシュ内の使用中のバイト数を報告します。 単位: バイト
CloudBytesDownloaded	AWS レポート期間中にゲートウェイが からダウンロードした合計バイト数。 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 統計で使用して IOPS を測定します。 単位: バイト

メトリクス	説明
CloudBytesUploaded	AWS レポート期間中にゲートウェイが にアップロードした合計バイト数。 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 統計で使用して、1 秒あたりの入力/出力オペレーション (IOPS) を測定します。 単位: バイト
FilesFailingUpload	このメトリクスは、 AWSへのアップロードに失敗しているファイルの数を追跡します。これらのファイルは、問題に関する詳細情報を含むヘルス通知を生成します。 このメトリクスを Sum 統計で使用して、現在 AWSへのアップロードに失敗したファイルの数を表示します。 単位: カウント
FileShares	このメトリクスは、ゲートウェイ上のファイル共有の数を報告します。 単位: カウント

メトリクス	説明
FileSystem-ERROR	このメトリクスは、ERROR 状態にあるこのゲートウェイのファイルシステム関連付けの数を示します。 このメトリクスがファイルシステムの関連付けが ERROR 状態であると報告した場合、ゲートウェイに問題がある可能性があり、ワークフローが中断される可能性があります。このメトリクスがゼロ以外の値をレポートする場合は、アラームを作成することをお勧めします。 単位: カウント
HealthNotifications	このメトリクスは、報告期間中にこのゲートウェイによって生成されたヘルス通知の数を報告します。 単位: カウント
IndexEvictions	このメトリクスは、新しいエントリ用にスペースを確保するために、ファイルメタデータのキャッシュされたインデックスからメタデータが削除されたファイルの数を報告します。ゲートウェイはこのメタデータインデックスを維持し、オンデマンドで AWS クラウドから入力されます。 単位: カウント
IndexFetches	このメトリクスは、メタデータを取得したファイルの数を報告します。ゲートウェイは、オンデマンドで AWS クラウドから入力されるファイルメタデータのキャッシュされたインデックスを維持します。 単位: カウント

メトリクス	説明
IoWaitPercent	このメトリクスは、CPU がローカルディスクからの応答を待っている時間の割合を報告します。 単位: パーセント
MemTotalBytes	このメトリクスは、ゲートウェイ上のメモリの合計量を報告します。 単位: バイト
MemUsedBytes	このメトリクスは、ゲートウェイで使用されているメモリの量を報告します。 単位: バイト
RootDiskFreeBytes	このメトリクスは、ゲートウェイのルートディスクで使用可能なバイト数を報告します。 このメトリクスのレポートが 20 GB 未満であれば、ルートディスクのサイズを増やす必要があります。 ルートディスクのサイズを増やすには、VM 上の既存のルートディスクのサイズを増やすことができます。VM を再起動すると、ゲートウェイはルートディスクのサイズの増加を認識します。 単位: バイト

メトリクス	説明
SmbV2Sessions	このメトリクスは、ゲートウェイでアクティブな SMBv2 セッションの数を報告します。このメトリクスは、ゲートウェイに関連付けられたファイルシステムごとに 1 回発行されます。SUM 統計を使用して、すべてのファイルシステム全体でアクティブな SMBv2 セッションの合計数を計算します。 単位: カウント
SmbV3Sessions	このメトリクスは、ゲートウェイでアクティブな SMBv3 セッションの数を報告します。このメトリクスは、ゲートウェイに関連付けられたファイルシステムごとに 1 回発行されます。SUM 統計を使用して、すべてのファイルシステム全体でアクティブな SMBv3 セッションの合計数を計算します。 単位: カウント
TotalCacheSize	このメトリクスは、キャッシュの合計サイズを報告します。 単位: バイト
UserCpuPercent	このメトリクスは、ゲートウェイ処理に費やされた時間の割合を報告します。 単位: パーセント

ファイルシステムメトリクスについて

ファイルシステムに関する Storage Gateway のメトリクスについて、以下に説明します。各ファイルシステムには、一連の関連付けられたメトリクスがあります。一部のファイルシステム固有のメトリクスには、ゲートウェイ固有の特定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値を表していますが、代わりにファイルシステムにスコープされています。

メトリクスを使用する前に、ゲートウェイで作業するのか、ファイルシステムメトリクスで作業するのかを必ず指定してください。特に、ファイルシステムメトリクスを使用する場合は、メトリクスを表示するファイルシステムを識別する `File system ID` を指定する必要があります。詳細については、「Amazon CloudWatch メトリクスを使用する」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、ファイル共有の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
`CacheHitPercent`	キャッシュから提供されるファイル共有からのアプリケーション読み取り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。 ファイル共有からのアプリケーション読み取りオペレーションがない場合、このメトリクスのレポートは 100 パーセントになります。 単位: パーセント
`CachePercentDirty`	AWSに保持されていなかったゲートウェイのキャッシュの全体的な割合全体に対するファイル共有の割合。サンプリングは、レポート期間の最後に行われます。 このメトリクスを `Sum` 統計で使用します。 理想的には、このメトリクスを低く維持する必要があります。

メトリクス	説明
	Note ゲートウェイの CachePercentDirty メトリクスを使用して、AWSに保持されていなかったゲートウェイのキャッシュの全体的な割合を表示します。 単位: パーセント
CachePercentUsed	ゲートウェイ全体で使用されているデータキャッシュの割合。サンプリングは、レポート期間の最後に行われます。このファイル共有固有のメトリクスは、対応するゲートウェイ固有のメトリクスと同じ値を報告します。 単位: パーセント
CloudBytesUploaded	AWS レポート期間中にゲートウェイが にアップロードした合計バイト数。 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 統計で使用して IOPS を測定します。 単位: バイト
CloudBytesDownloaded	AWS レポート期間中にゲートウェイが からダウンロードした合計バイト数。 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 統計で使用して、1 秒あたりの入力/出力オペレーション (IOPS) を測定します。 単位: バイト

メトリクス	説明
FilesFailingUpload	このメトリクスは、 AWSへのアップロードに失敗しているファイルの数を追跡します。これらのファイルは、問題に関する詳細情報を含むヘルス通知を生成します。 このメトリクスを Sum 統計で使用して、現在AWSへのアップロードに失敗したファイルの数を表示します。 単位: カウント
ReadBytes	ファイル共有の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 統計で使用してスループットを測定し、Samples 統計で使用して IOPS を測定します。 単位: バイト
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 統計で使用してスループットを測定し、Samples 統計で使用して IOPS を測定します。 単位: バイト

FSx ファイルゲートウェイ監査ログについて

Amazon FSx ファイルゲートウェイ(FSx ファイルゲートウェイ) 監査ログは、ファイルシステムの関連付け内のファイルとフォルダへのユーザーアクセスに関する詳細を提供します。監査ログを使用して、ユーザーのアクティビティをモニタリングし、不適切なアクティビティパターンが検出された場合に対処できます。ログは、Windows Server のセキュリティログイベントと同様の形式で作成さ

れており、既存の Windows セキュリティイベント用ログ処理ツールとの互換性をサポートしています。

オペレーション

次の表は、FSx ファイルゲートウェイの監査ログにおけるファイルアクセス操作について説明しています。

オペレーション名	定義
データの読み取り	ファイルの内容を読み取ります。
データの書き込み	ファイルの内容を変更します。
作成	新しいファイルまたはフォルダを作成します。
名前を変更	既存のファイルまたはフォルダの名前を変更します。
Delete	ファイルまたはフォルダを削除します。
属性の書き込み	ファイルまたはフォルダのメタデータ (ACL、所有者、グループ、アクセス許可) を更新します。

属性

次の表では、FSx ファイルゲートウェイの監査ログファイルのアクセス属性について説明します。

属性	定義
`securityDescriptor`	オブジェクトに設定された随意アクセスコントロールリスト (DACL) を SDDL 形式で示します。
`sourceAddress`	ファイル共有クライアントマシンの IP アドレス。

属性	定義
SubjectDomainName	クライアントのアカウントが属する Active Directory (AD) ドメイン。
SubjectUserName	クライアントのアクティブディレクトリユーザー名。
source	監査対象の Storage Gateway FileSystemAssociation の ID。
mtime	オブジェクトのコンテンツが変更された時刻 (クライアントが設定します)。
version	監査ログ形式のバージョン。
ObjectType	オブジェクトがファイルまたはフォルダであるかどうかを定義します。
locationDnsName	FSx ファイルゲートウェイシステムの DNS 名。
objectName	オブジェクトへのフルパス。
ctime	オブジェクトの内容またはメタデータが変更された時刻 (クライアントが設定します)。
shareName	アクセスされている共有の名前。
operation	オブジェクトのアクセスオペレーションの名前。
newObjectName	名前を変更した後の新しいオブジェクトへのフルパス。
gateway	Storage Gateway ID。
status	オペレーションのステータス。成功のみがログに記録されます (失敗は、アクセス許可の拒否に伴う失敗を除き、ログに記録されます)。

属性	定義
fileSizeInBytes	ファイルの作成時にクライアントによって設定されたファイルのサイズ (バイト単位)。

オペレーションごとにログに記録される属性

次の表は、FSx ファイルゲートウェイの監査ログで、各ファイルアクセス操作時に記録される属性について説明しています。

	データの読み取り	データの書き込み	フォルダの作成	ファイルの作成	ファイル/フォルダの名前変更	ファイル/フォルダの削除	属性の書き込み (ACLの変更)	属性の書き込み (chown)	属性の書き込み (chmod)	属性の書き込み (chgrp)
securi escrip							X			
source ress	X	X	X	X	X	X	X	X	X	X
Subjec mainNa	X	X	X	X	X	X	X	X	X	X
Subjec erName	X	X	X	X	X	X	X	X	X	X
source	X	X	X	X	X	X	X	X	X	X
mtime			X	X						
versic	X	X	X	X	X	X	X	X	X	X

	データの読み取り	データの書き込み	フォルダの作成	ファイルの作成	ファイル/フォルダの名前変更	ファイル/フォルダの削除	属性の書き込み (ACLの変更)	属性の書き込み (chown)	属性の書き込み (chmod)	属性の書き込み (chgrp)
object	X	X	X	X	X	X	X	X	X	X
locatinsName	X	X	X	X	X	X	X	X	X	X
object	X	X	X	X	X	X	X	X	X	X
ctime			X	X						
shareN	X	X	X	X	X	X	X	X	X	X
operat	X	X	X	X	X	X	X	X	X	X
newObjName					X					
gatewa	X	X	X	X	X	X	X	X	X	X
status	X	X	X	X	X	X	X	X	X	X
fileSinBytes				X						

ゲートウェイの維持

Amazon FSx ファイルゲートウェイ のメンテナンスには、ゲートウェイのパフォーマンスを最適化するための一般的なメンテナンス作業が含まれます。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。

このセクションには、Amazon FSx ファイルゲートウェイ のメンテナンスに関連する概念と手順について説明する以下のトピックが含まれています。

トピック

- ゲートウェイアップデートの管理 - メンテナンス更新をオンまたはオフにする方法、およびファイルゲートウェイの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。
- 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 – ゲートウェイのローカルコンソールを使用してメンテナンス作業を実行する方法について説明します。
- ゲートウェイ VM のシャットダウン - ハイパーバイザーへのパッチ適用などのメンテナンス時に、ゲートウェイの仮想マシンをシャットダウンまたは再起動する必要がある場合の対処方法について説明します。
- 既存の FSx ファイルゲートウェイを新しいインスタンスに置き換える – パフォーマンスを向上させたい場合や、ゲートウェイ移行の通知に対応する必要がある場合に、FSx ファイルゲートウェイを新しいインスタンスに置き換える方法について説明します。
- ゲートウェイおよび関連リソースの削除 – AWS Storage Gateway コンソールを使用してゲートウェイを削除し、関連するリソースをクリーンアップして、継続的な使用に対して課金されないようにする方法について説明します。

ゲートウェイアップデートの管理

Storage Gateway は、マネージド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されます。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、デプロイ内のゲートウェイで更新関連の設定を行う方法について説明します。

> **Important**
>
> Storage Gateway アプライアンスは、管理された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以外の方法 (SSM やハイパーバイザーツールなど) を使用してソフトウェアパッケージをインストール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。
> Storage Gateway は、セキュリティと安定性を維持するために、アプライアンスへ自動的かつ定期的にパッチを適用します。Storage Gateway アプライアンスは、ベースのオペレーティングシステムとして Amazon Linux を使用しています。Amazon Linux セキュリティセンターで検出された共通脆弱性識別子 (CVE) の問題のステータスを確認できます。CVE パッチは、Amazon Linux セキュリティセンターに表示されているように、リリースされてから 30 日以内に自動的に適用されます。パッチは、ゲートウェイがオンラインである限り、ゲートウェイのメンテナンススケジュール中にインストールされます。
> Storage Gateway では、cloud-init 指示を使用して Amazon EC2 ゲートウェイを手動で更新することはサポートされていません。この方法でゲートウェイを更新すると、ゲートウェイアプライアンスのアクティベーションや使用を妨げる相互運用性の問題が発生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、次のタイプの更新を受け取ります。

- メンテナンス – オペレーティングシステムやソフトウェアのアップグレード、安定性・パフォーマンス・セキュリティの修正、新機能へのアクセスを含む定期的な更新。
- 緊急 – ゲートウェイのセキュリティ、パフォーマンス、耐久性に直ちに影響する問題に対する必須の修正を含む重要な更新。緊急更新は、通常の月次メンテナンスや機能更新のスケジュールとは別に、いつでもリリースされる可能性があります。

すべての更新は累積的であり、適用時にゲートウェイを現在のバージョンにアップグレードします。各更新に含まれる具体的な変更内容については、を参照してください。

すべてのゲートウェイアプライアンスの更新では、短時間のサービス中断が発生する可能性があります。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が更新および再起動している間は、ゲートウェイが短期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きに、デフォルト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スケジュールはいつでも変更できます。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推奨します。

> **Note**
>
> 緊急更新は、通常のメンテナンス更新がオフになっている場合でも、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の送信先の 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

更新が利用可能な場合は、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。また、[詳細] タブには、最後に更新が正常に適用された日時が表示されます。

メンテナンスアップデートをオンまたはオフにする

メンテナンスアップデートがオンになっている場合、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アップデートを自動的に適用します。詳細については、「ゲートウェイメンテナンスウィンドウスケジュールの変更」を参照してください。

メンテナンスアップデートがオフになっている場合、ゲートウェイはこれらのアップデートを自動的に適用しませんが、Storage Gateway コンソール、API、または CLI を使用していつでも手動で適用できます。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オンまたはオフにする方法について説明します。API を使用してプログラムでこの設定を変更するには、「Storage Gateway API リファレンス」の「UpdateMaintenanceStartTime」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アップデートをオンまたはオフにするには:

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、[ゲートウェイ] を選択してから、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、[メンテナンス設定を編集] を選択します。
4. [メンテナンスアップデート] では、[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。

ゲートウェイの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。緊急更新は、メンテナンス更新の設定に関係なく、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。API を使用してプログラムでこの設定を変更するには、「Storage Gateway API リファレンス」の「UpdateMaintenanceStartTime」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. 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、[ゲートウェイ] を選択してから、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、[メンテナンス設定を編集] 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] では、[毎週] または [毎月] を選択してメンテナンスウィンドウの頻度を設定します。

b. [毎週] 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始ま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、[日付] と [時刻] の値を変更して、メンテナンスウィンドウが始まる各月の特定のポイントを設定します。

> **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 日目から 31 日目に開始するように設定することはできません。
> この設定を構成中にエラーが表示された場合は、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。

更新を手動で適用する

ゲートウェイのソフトウェア更新が利用可能な場合は、以下の手順に従って手動で適用できます。この手動更新プロセスは、メンテナンスウィンドウのスケジュールを無視し、メンテナンスの更新がオフになっていても、すぐに更新を適用します。

> **Note**
>
> 次の手順では、Storage Gateway コンソールを使用して更新を手動で適用する方法について説明します。API を使用してこのアクションをプログラムで実行するには、「Storage Gateway API リファレンス」の「UpdateGatewaySoftwareNow」を参照してください。

Storage Gateway コンソールを使用してゲートウェイソフトウェアの更新を手動で適用するには:

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 [ゲートウェイ] を選択してから、更新するゲートウェイを選択します。

   更新が利用可能な場合、コンソールはゲートウェイの [詳細] タブに青い通知バナーを表示します。これには、更新を適用するオプションが含まれます。

3. [アップデートを今すぐ適用する] を選択して、ゲートウェイをすぐに更新します。

> **Note**
>
> この操作により、更新のインストール中にゲートウェイ機能が一時的に中断されます。この間、ゲートウェイステータスは Storage Gateway コンソールに [OFFLINE] と表示されます。更新のインストールが完了すると、ゲートウェイは通常のオペレーションを再開し、ステータスは [RUNNING] に変わります。

Storage Gateway コンソールで、選択したゲートウェイの [詳細] タブを確認することで、ゲートウェイソフトウェアが最新バージョンに更新されたことを確認できます。

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

このセクションでは、ゲートウェイアプライアンスのローカルコンソールを使用してメンテナンスタスクを実行する方法に関する情報を提供する次のトピックが含まれています。これらのタスクは、オンプレミスの仮想マシンまたはゲートウェイアプライアンスをホストする Amazon EC2 インスタンスを介してローカルコンソールにアクセスすることで実行できます。ほとんどのタスクはさまざまなホストプラットフォーム間で共通していますが、異なる点もいくつかあります。

トピック

- ゲートウェイローカルコンソールへのアクセス - Linux のカーネルベース仮想マシン (KVM)、VMware ESXi、または Microsoft Hyper-V Manager プラットフォームでホストされているオンプレミスゲートウェイのローカルコンソールにログインする方法について説明します。
- 仮想マシンのローカルコンソールでタスクの実行 - ローカルコンソールを使用して、HTTP プロキシの設定、システムリソースのステータスの表示、ターミナルコマンドの実行など、オンプレミスゲートウェイの基本的なセットアップタスクと高度な設定タスクを実行する方法について説明します。
- Amazon EC2 ローカルコンソールでのタスクの実行 - ローカルコンソールにログインして、HTTP プロキシの設定、システムリソースのステータスの表示、ターミナルコマンドの実行な

ど、Amazon EC2 ゲートウェイの基本的なセットアップタスクと高度な設定タスクを実行する方法について説明します。

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 カーネルベース仮想マシン (KVM)、VMware ESXi、および Microsoft Hyper-V マネージャーを使用して VM 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 KVM でゲートウェイのローカルコンソールにアクセスする
- VMware ESXi でゲートウェイのローカルコンソールにアクセスする
- 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 KVM でゲートウェイのローカルコンソールにアクセスする

KVM で実行する仮想マシンを構成する方法は、使用する Linux ディストリビューションによって異なります。コマンドラインから KVM 構成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 の実装によって異なる場合があります。

KVM で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

1. 次のコマンドを使用して、KVM で現在利用可能な VM を一覧表示します。

   ```
   # virsh list
   ```

   コマンドは、それぞれの [Id]、[名前]、[状態] 情報を持つ VM のリストを返します。ゲートウェイローカルコンソールを起動する VM の `Id` に注意してください。
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 Id
   ```

   `[Id]` を、以前の手順で書き留めた VM の [Id] に置き換えます。

   AWS アプライアンスゲートウェイのローカルコンソールでは、ログインしてネットワーク設定やその他の設定を変更するように求められます。

3. ユーザー名とパスワードを入力して、ゲートウェイローカルコンソールにログインします。詳細については、ファイルゲートウェイのローカルコンソールへのログインを参照してください。

   ログインすると、[AWS アプライアンスのアクティベーション - 設定] メニューが表示されます。メニューオプションから選択して、ゲートウェイ設定タスクを実行できます。詳細については、「仮想マシンの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。

VMware ESXi でゲートウェイのローカルコンソールにアクセスする

VMware ESXi で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

1. VMware vSphere クライアントで、ゲートウェイの VM を選択します。
2. ゲートウェイ VM 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 がオンになっている場合、アプリケーションウィンドウの左側にある VM ブラウザパネルに、VM アイコンと共に緑色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、アプリケーションウィンドウの上部にある [ツールバー] の緑の [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. アプリケーションウィンドウの右側にあるメイン情報パネルの [コンソール] タブを選択します。

   しばらくすると、 AWS アプライアンスゲートウェイのローカルコンソールにログインしてネットワーク設定やその他の設定を変更するよう求められます。

   > **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. ユーザー名とパスワードを入力して、ゲートウェイローカルコンソールにログインします。詳細については、ファイルゲートウェイのローカルコンソールへのログインを参照してください。

   ログインすると、[AWS アプライアンスのアクティベーション - 設定] メニューが表示されます。メニューオプションから選択して、ゲートウェイ設定タスクを実行できます。詳細については、「仮想マシンの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。

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 アプリケーションウィンドウの左側にある [仮想マシン] パネルからゲートウェイアプライアンス 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 がオンになっている場合、Running はアプリケーションウィンドウの左側にある [仮想マシン] パネルの VM の [状態] 列に表示されます。ゲートウェイ VM がオンになっていない場合は、アプリケーションウィンドウの左側にある [アクション] ペインの [起動] を選択してオンにすることができます。

3. [アクション] パネルから [接続] 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、 AWS アプライアンスゲートウェイのローカルコンソールにログインしてネットワーク設定やその他の設定を変更するよう求められます。
4. ユーザー名とパスワードを入力して、ゲートウェイローカルコンソールにログインします。詳細については、ファイルゲートウェイのローカルコンソールへのログインを参照してください。

   ログインすると、[AWS アプライアンスのアクティベーション - 設定] メニューが表示されます。メニューオプションから選択して、ゲートウェイ設定タスクを実行できます。詳細については、「仮想マシンの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。

仮想マシンのローカルコンソールでタスクの実行

ファイル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、Microsoft Hyper-V、Linux カーネルベース仮想マシン (KVM) ハイパーバイザーに共通です。

トピック

- ファイルゲートウェイローカルコンソールへのログイン - ゲートウェイネットワーク設定を構成し、デフォルトのパスワードを変更できるゲートウェイローカルコンソールにログインする方法について説明します。
- HTTP プロキシの設定 - プロキシサーバーを介してすべての AWS エンドポイントトラフィックをルーティングするように Storage Gateway を設定する方法について説明します。
- ゲートウェイネットワークの設定 - DHCP を使用するようにゲートウェイを設定する方法、または静的 IP アドレスを割り当てる方法について説明します。
- ゲートウェイのネットワーク接続をテストする - ゲートウェイローカルコンソールを使用してゲートウェイネットワーク接続をテストする方法について説明します。
- ゲートウェイシステムリソースのステータスの表示 - ゲートウェイで使用できる仮想 CPU コア、ルートボリュームサイズ、RAM を確認する方法について説明します。
- ゲートウェイの Network Time Protocol (NTP) サーバーの設定 - ネットワークタイムプロトコル (NTP) サーバー設定を表示および編集し、ゲートウェイの時刻をハイパーバイザーホストと同期する方法について説明します。
- ローカルコンソールでの Storage Gateway コマンドの実行 - ローカルコンソールコマンドを実行して、ルーティングテーブルの保存、 への接続などのタスクを実行する方法について説明しますサポート。

ファイルゲートウェイ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。VM のローカルコンソールに初めてログインする場合は、一時的なサインイン認証情報を使用してログインします。これらの仮発行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。初期ユーザー名は `admin` で、仮パスワードは `password` です。最初のログイン時にパスワードを変更する必要があります。

一時パスワードを変更するには

1. [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。
2. `passwd` コマンドを実行します。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。

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

Storage Gateway ウェブベースのコンソールからローカルコンソールのパスワードを管理することもできます。ウェブベースのコンソールでパスワードが正常に更新されると、ゲートウェイ VM のローカルコンソールで使用されるパスワードが上書きされます。これには、ローカルでログインしたことがない場合の一時パスワードが含まれます。ゲートウェイに現在ネットワーク経由でアクセスできない場合、パスワードの更新プロセスは失敗します。

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. 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、[ゲートウェイ] 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、[保存] を選択します。

   新しいパスワードを設定すると、現在のパスワードが置き換えられます。Storage Gateway サービスはパスワードを保存・記録したりすることはなく、暗号化されたチャネルを通じて仮想マシンに安全に送信され、そこで安全に保管されます。

   > **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。

HTTP プロキシの設定

ファイルゲートウェイは HTTP プロキシの設定をサポートします。

> **Note**
>
> ファイルゲートウェイでサポートされるプロキシ設定は、HTTP のみです。

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、HTTP プロキシをゲートウェイ用に設定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。これを行うと、Storage Gateway はプロキシサーバーを介してすべての AWS エンドポイントトラフィックをルーティングします。HTTP プロキシを使用している場合でも、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。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。

ファイルゲートウェイの HTTP 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 ローカルコンソールへのログインの詳細については、「VMware ESXi 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。
   - 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 カーネルベース仮想マシン (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、「Linux KVM 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. [AWS Appliance Activation - Configuration] メインメニューから、対応する番号を入力して [Configure HTTP Proxy] を選択します。
3. [AWS Appliance Activation HTTP Proxy Configuration] 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。
   - Configure HTTP proxy - 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。
   - View current HTTP proxy configuration - HTTP プロキシが設定されていない場合、メッセージ「`HTTP Proxy not configured`」が表示されます。HTTP 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。
   - Remove an HTTP proxy configuration - メッセージ「`HTTP Proxy Configuration Removed`」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、動的ホスト構成プロトコル (DHCP) です。DHCP を使用すると、ゲートウェイには 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 ローカルコンソールへのログインの詳細については、「VMware ESXi 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。
   - 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、「Linux KVM 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. [AWS Appliance Activation - 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. [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に関する情報を取得する	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、例えば「**eth0**」のような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 有効ステータス

このタスクを実行するには	操作
	静的 IP アドレスを設定する場合や、ゲートウェイのデフォルトアダプターを設定する場合には、ここに記載されているアダプター名を使用します。
DHCP ルーティングを構成する	対応する番号を入力して [Configure DHCP] 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。

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する場合、すべてのアクティブ

このタスクを実行するには	操作
	なインターフェイスを DHCP または静的 IP アドレスで設定する必要があります。 たとえば、ゲートウェイ VM で DHCP として設定された 2 つのインターフェイスを使用するとします。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。 最初に両方のインターフェイスが静的 IP アドレスを使用するように設定されている場合、DHCP を使用するようにゲートウェイを設定すると、どちらのインターフェイスも DHCP を使用するようになります。

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。 指定した静的ホスト名をゲートウェイで使用するか、DCHP または RDN を通じて自動的に取得するかを選択するように求められます。 [静的] を選択すると、`testgateway.example.com` などの静的ホスト名を指定するように求められます。y を入力して設定を適用します。 **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。
ゲートウェイのホスト名設定を表示する	対応する番号を入力して [View Hostname Configuration] を選択します。 ゲートウェイのホスト名、取得モード、ドメイン、Active Directory 領域が表示されます。

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 DHCP にリセットする	対応する番号を入力して [Reset all to 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が、DHCP を使用するように設定されます。 **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。
ゲートウェイの DNS 設定を編集する	対応する番号を入力して [Edit DNS Configuration] を選択します。 プライマリとセカンダリの DNS サーバーの使用可能なアダプタが表示されます。新しい IP アドレスを指定するよう求められます。

このタスクを実行するには	操作
ゲートウェイの DNS 設定を表示する	対応する番号を入力して [View DNS Configuration] を選択します。 プライマリとセカンダリの DNS サーバーの使用可能なアダプタが表示されます。 **Note** VMware ハイパーバイザの一部のバージョンでは、このメニューでアダプタ設定を編集できます。
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。

ゲートウェイのネットワーク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 ローカルコンソールへのログインの詳細については、「VMware ESXi 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。
   - 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、「Linux KVM 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. [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。サポートされているサービスエンドポイント 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。

テストが進むに従い、各エンドポイントに [PASSED] または [FAILED] と表示されます。それぞれ、次の接続状態を表しています。

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

ゲートウェイの開始時に、その仮想 CPU コア、ルートボリュームサイズ、RAM がチェックされます。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、「VMware ESXi 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。

- 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、「Linux KVM 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. [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 [OK]、[WARNING]、[FAIL] と表示されます。それぞれ、リソースの次の状態を表しています。

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 Network Time Protocol (NTP) サーバーの設定

ネットワークタイムプロトコル (NTP) サーバー設定を表示および編集し、ゲートウェイの VM の時刻をハイパーバイザーホストと同期できます。

システム時刻を管理するには

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、「VMware ESXi 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。
   - 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、「Linux KVM 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. [AWS Appliance Activation - Configuration] メインメニューで、対応する番号を入力して [System Time Management] を選択します。

3. System Time Management 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
VM の時刻を表示して NTP サーバーの時刻と同期します。	対応する番号を入力して、システム時刻の表示と同期を選択します。 VM の現在の時刻が表示されます。ファイルゲートウェイによりゲートウェイ VM との時刻の差が判別され、NTP サーバーの時刻により VM の時刻と NTP の時刻を同期するように求められます。 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とします。この場合、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。

このタスクを実行するには	操作
	VMware ESXi にデプロイされたゲートウェイの場合、時刻のずれを防ぐには、ハイパーバイザーホストの時刻を設定して、VM の時刻をホストと同期するだけで十分です。詳細については、「VM の時刻と VMware ホストの時刻を同期する」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、「VM の時刻を Hyper-V または Linux KVM ホストの時刻と同期する」を参照してください。 KVM にデプロイされたゲートウェイの場合、KVM の `virsh` コマンドラインインターフェイスを使用して VM の時間を確認および同期できます。
NTP サーバー設定の編集	対応する番号を入力して [Edit NTP Configuration] を選択します。 優先およびセカンダリ NTP サーバーを指定するように求められます。
NTP サーバー設定の表示	対応する番号を入力して [View NTP Configuration] を選択します。 NTP サーバー設定が表示されます。

ローカルコンソールでの Storage Gateway コマンドの実行

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すると、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 サポート。

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、「VMware ESXi 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。
   - 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、「Linux KVM 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. [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。

   [AVAILABLE COMMANDS] メニューがコンソールに表示されます。このメニューには、利用できるコマンドが表示されています。

コマンド	関数
dig	DNS のトラブルシューティング用に、dig からの出力を収集します。
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

コマンド	関数
	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。 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および NAT の管理ツール。
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。 AWS サポートアクセスを有効にする方法については、「ECEC2 ゲートウェイのトラブルシューティングに役立つ AWS サポートが必要」を参照してください。
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。

コマンド	関数
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。
tcptraceroute	送信先への TCP トラフィックに関する traceroute 出力を収集します。
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 検査を実行する可能性があります。この場合、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。

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。

コマンドの機能を調べるには、コマンドプロンプトで「**man** + *#####*」を入力してください。

Amazon EC2 ローカルコンソールでのタスクの実行

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 ゲートウェイの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 インスタンス上のゲートウェイのローカルコンソールに接続し、ログインする方法について説明します。

- Amazon EC2 にデプロイされたゲートウェイを HTTP プロキシ経由でルーティングする - AWS と Amazon EC2 インスタンスにデプロイされたゲートウェイとの間で Socket Secure version 5 (SOCKS5) プロキシを設定する方法について説明します。
- ゲートウェイのネットワーク接続をテストする - ゲートウェイローカルコンソールを使用して、ゲートウェイとさまざまなネットワークリソース間のネットワーク接続をテストする方法について説明します。
- ゲートウェイシステムリソースのステータスの表示 - ゲートウェイのローカルコンソールを使用して、ゲートウェイの仮想 CPU コア数、ルートボリュームサイズ、および RAM を確認する方法を学びます。
- Amazon EC2 上のゲートウェイで、ローカルコンソールから Storage Gateway コマンドを実行する - ルーティングテーブルの保存、 サポートへの接続などの追加のタスクを実行できるようにするローカルコンソールコマンドを実行する方法について説明します。
- Amazon EC2 上のゲートウェイのネットワーク設定の構成 - Amazon EC2 インスタンス上のゲートウェイで、ローカルコンソールを使用して DNS やホスト名などのネットワーク設定を表示および構成する方法を学びます。

Amazon EC2 ゲートウェイの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 インスタンス上のゲートウェイローカルコンソールに接続できます。詳細については、Amazon EC2 Linux インスタンス用 ユーザーガイドの「Linux インスタンスへの接続」を参照してください。この方法で接続するには、インスタンスを起動したときに指定した SSH キーペアが必要です。Amazon EC2 キーペアについては、Amazon EC2 Linux インスタンス用 ユーザーガイドの「Amazon EC2 のキーペアと Linux インスタンス」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. SSH を使用して Amazon EC2 インスタンスに接続し、管理者ユーザーとしてログインします。
2. ログインすると、[AWS Appliance Activation - 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 HTTP プロキシを設定する	Amazon EC2 にデプロイされたゲートウェイを HTTP プロキシ経由でルーティングする

実行するタスク	参照先のトピック
ゲートウェイのネットワーク設定を設定する	Amazon EC2 上のゲートウェイのネットワーク設定の構成
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
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.
Storage Gateway コンソールコマンドを実行する	Amazon EC2 上のゲートウェイで、ローカルコンソールから Storage Gateway コマンドを実行する

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。

Amazon EC2 にデプロイされたゲートウェイを HTTP プロキシ経由でルーティングする

Storage Gateway では、Amazon EC2 にデプロイされたゲートウェイと AWSとの間の Socket Secure バージョン (SOCKS5) プロキシの設定をサポートします。

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、HTTP プロキシをゲートウェイ用に設定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。これを行うと、Storage Gateway はプロキシサーバーを介してすべての AWS エンドポイントトラフィックをルーティングします。HTTP プロキシを使用している場合でも、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 ゲートウェイの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 [Configure HTTP Proxy] を選択します。

3. [AWS Appliance Activation HTTP Proxy Configuration] 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。

   - Configure HTTP proxy - 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。
   - View current HTTP proxy configuration - HTTP プロキシが設定されていない場合、メッセージ「`HTTP Proxy not configured`」が表示されます。HTTP 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。
   - Remove an HTTP proxy configuration - 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 ゲートウェイの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。サポートされているサービスエンドポイント 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。

テストが進むに従い、各エンドポイントに [PASSED] または [FAILED] と表示されます。それぞれ、次の接続状態を表しています。

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

ファイルゲートウェイの開始時に、その仮想 CPU コア、ルートボリュームサイズ、RAM がチェックされます。その後、利用可能なシステムリソースがゲートウェイの正常な動作に十分かどうかを判断します。ゲートウェイのローカルコンソールを使用して、システムリソースチェックの結果を確認できます。

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. Amazon EC2 ファイルゲートウェイのローカルコンソールへのログイン。手順については、「Amazon EC2 ゲートウェイの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。

   ゲートウェイローカルコンソールに [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]	リソースは推奨要件を満たしていませんが、ゲートウェイは引き続き動作可能です。ゲートウェイのローカルコンソールには、リソースチェックの結果を示すメッセージが表示されます。

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。ゲートウェイのローカルコンソールには、リソースチェックの結果を示すメッセージが表示されます。

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。

Amazon EC2 上のゲートウェイで、ローカルコンソールから Storage Gateway コマンドを実行する

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します。コンソールコマンドを使用すると、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 サポート。

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 ゲートウェイの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。

   [AVAILABLE COMMANDS] メニューがコンソールに表示されます。このメニューには、利用できるコマンドが表示されています。

コマンド	関数
dig	DNS のトラブルシューティング用に、dig からの出力を収集します。
exit	コンソール設定メニューに戻ります。

コマンド	関数
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。 **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および NAT の管理ツール。
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。

コマンド	関数
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。
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。
tcptraceroute	送信先への TCP トラフィックに関する 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。

コマンドの機能を調べるには、コマンドプロンプトで「**man** + *#####*」を入力してください。

Amazon EC2 上のゲートウェイのネットワーク設定の構成

ゲートウェイのローカルコンソールを使用して、Amazon EC2 上のファイルゲートウェイのネットワーク設定を表示および構成できます。

ネットワーク設定を構成するには

1. Amazon EC2 ファイルゲートウェイのローカルコンソールへのログイン。手順については、「Amazon EC2 ゲートウェイの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 [Network Configuration] を選択します。
3. [AWS Appliance Activation - Network Configuration] 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。

   - DNS 設定の編集 - ゲートウェイのローカルコンソールには、プライマリおよびセカンダリ DNS サーバー用の利用可能なアダプターが表示されます。その後、コンソールが新しい IP アドレスの入力を求めます。
   - DNS 設定の表示 - ゲートウェイのローカルコンソールには、プライマリおよびセカンダリ DNS サーバーで使用できるアダプターが表示されます。

- ホスト名の設定 - ゲートウェイのローカルコンソールでは、ゲートウェイに指定した静的ホスト名を使用するか、DCHP または rDNS を通じて自動的にホスト名を取得するかを選択するよう求められます。

  > **Note**
  >
  > ゲートウェイに静的ホスト名を設定する場合は、ゲートウェイの IP アドレスをその静的ホスト名に紐付ける A レコードを DNS システムに作成する必要があります。

- ホスト名設定の表示 - ゲートウェイのローカルコンソールには、Amazon EC2 ファイルゲートウェイのホスト名、取得モード、ドメイン、Active Directory 領域が表示されます。

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。オンプレミスのゲートウェイ VM はハイパーバイザーのインターフェイスを使用してシャットダウンし、Amazon EC2 インスタンスは Amazon EC2 コンソールを使用してシャットダウンします。

> **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した場合、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。

既存の FSx ファイルゲートウェイを新しいインスタンスに置き換える

既存の FSx File Gateway は、データとパフォーマンスのニーズが増えるにつれて、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に、新しいインスタンスに置き換えることができます。ゲートウェイをより優れたホストプラットフォームや新しい Amazon EC2 インスタンスに移行したい場合、または基盤となるサーバーハードウェアを更新したい場合に、この操作が必要になることがあります。

> **Important**
>
> これらの手順は、バージョン 1.x を実行しているゲートウェイアプライアンスを移行する場合にのみ使用します。これらを使用して、下位バージョンを実行しているゲートウェイアプライアンスを移行することはできません。

> **Note**
>
> 移行は、同じタイプのゲートウェイ間でのみ実行できます。たとえば、設定やデータを FSx ファイルゲートウェイから S3 ファイルゲートウェイに移行することはできません。

FSx ファイルゲートウェイゲートウェイを空のキャッシュディスクと新しい Gateway ID を持つ新しいインスタンスに置き換えるには:

1. 既存の FSx ファイルゲートウェイに書き込むアプリケーションをすべて停止します。新しいゲートウェイでファイルシステム関連付けを設定する前に、[モニタリング] タブの `CachePercentDirty` メトリクスが `0` であることを確認してください。
2. AWS Command Line Interface (AWS CLI) を使用して、既存の FSx ファイルゲートウェイおよび関連するファイルシステムに関する設定情報を収集して保存します。

   a. FSx ファイルゲートウェイのゲートウェイ設定情報を保存します。

   ```
   aws storagegateway describe-gateway-information --gateway-arn
    "arn:aws:storagegateway:us-east-2:123456789012:gateway/sgw-12A3456B"
   ```

   このコマンドは、名前、ネットワークインターフェイス、設定したタイムゾーン、および状態 (ゲートウェイが実行中かどうか) など、ゲートウェイに関するメタデータを含む JSON ブロックを出力します。

   b. FSx ファイルゲートウェイのサーバーメッセージブロック (SMB) 設定を保存します。

   ```
   aws storagegateway describe-smb-settings --gateway-arn
    "arn:aws:storagegateway:us-east-2:123456789012:gateway/sgw-12A3456B"
   ```

   このコマンドは、ゲートウェイが結合されている Microsoft Active Directory のドメイン名を含む JSON ブロックを出力します。

c. FSx ファイルゲートウェイに関連付けられた各ファイルシステムのファイル共有情報を保存します:

関連付けられたファイルシステムごとに次のコマンドを使用します。

```
aws storagegateway describe-file-system-associations --file-system-
association-arn-list "arn:aws:storagegateway:us-east-2:123456789012:fs-
association/fsa-987A654B"
```

このコマンドは、場所 ARN、監査ログの送信先、キャッシュ更新属性、設定済み IP アドレス、タグなど、ファイルシステムに関するメタデータを含む JSON ブロックを出力します。

3. 古いゲートウェイと同じ設定と設定で新しい FSx ファイルゲートウェイを作成します。必要に応じて、ステップ 2 で保存した情報を参照してください。
4. 古いゲートウェイで設定されたファイルシステムと同じ設定と設定で、新しいゲートウェイの新しいファイルシステムの関連付けを作成します。必要に応じて、ステップ 2 で保存した情報を参照してください。
5. 新しいゲートウェイが正しく動作していることを確認し、環境に最適な方法で、古いファイルシステムから新しいファイルシステムにクライアントを再マッピング/カットオーバーします。
6. 新しいゲートウェイが正しく動作していることを確認し、Storage Gateway コンソールから古いゲートウェイを削除します。

> **Important**
>
> FSx ファイルゲートウェイを削除する前に、現在そのゲートウェイのキャッシュ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。

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

7. 古いゲートウェイ VM または Amazon EC2 インスタンスを削除します。

ゲートウェイおよび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、ファイルシステム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。プログラムによってゲートウェイを削除する場合は、「AWS Storage Gateway API Reference」を参照してください。

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ているゲートウェイの場合、そのインスタンスは削除するまで引き続き存在します。
> 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。仮想マシンを削除するには、VMware vSphere クライアント、Microsoft Hyper-V マネージャー、または Linux カーネルベース仮想マシン (KVM) クライアントを使用してホストに接続し、仮想マシンを削除します。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. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) 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するとソフトウェア料金の支払いは不要になりますが、Amazon S3 バケットや Amazon EC2 インスタンスなどのリソースは引き続き存在します。ファイルゲートウェイが削除された後、ゲートウェイ Amazon EC2 インスタンスを削除できます。

パフォーマンスと最適化

このセクションでは、ファイルゲートウェイのパフォーマンスを最適化するためのガイダンスとベストプラクティスについて説明します。

トピック

FSx ファイルゲートウェイの基本的なパフォーマンスガイダンス

このセクションでは、FSx ファイルゲートウェイVM 用にハードウェアをプロビジョニングするためのガイダンスを説明します。表に示されているインスタンスのサイズとタイプは例ですので、参考までにご覧ください。

最高のパフォーマンスを得るには、キャッシュディスクのサイズをアクティブな作業セットのサイズ合わせる必要があります。キャッシュに複数のローカルディスクを使用すると、データへのアクセスを並列処理することで書き込みパフォーマンスが上がり、IOPS が向上します。

> **Note**
>
> エフェメラルストレージの使用はお勧めしません。エフェメラルストレージの使用については、「EC2 ゲートウェイでのエフェメラルストレージの使用」を参照してください。
> ファイルゲートウェイに接続するファイルシステム内の個々のディレクトリの推奨サイズ制限は、ディレクトリあたり 10,000 ファイルです。ファイルゲートウェイは、ファイル数が 10,000 個を超えるディレクトリでも使用できますが、パフォーマンスに影響する可能性があります。

以下の表で、キャッシュヒットの読み取りオペレーションは、キャッシュから提供されるファイルデータの読み取りです。キャッシュミスの読み取りオペレーションは、Amazon FSx for Windows File Server から提供されるファイルデータの読み取りです。

次の表は、FSx ファイルゲートウェイの構成の例を示しています。

Windows クライアントでの FSx ファイルゲートウェイのパフォーマンス

構成例	プロトコル	書き込みスループット (ファイルサイズ 1 GB)	キャッシュヒット読み取りスループット	キャッシュミス読み取りスループット
ルートディスク: 80 GB、io1 SSD、4,000 IOPS キャッシュディスク: 2 x 2 TiB NVME 最小ネットワークパフォーマンス: 10 Gbps CPU: 32 vCPU | RAM: 244 GB	SMBv3 - 1 スレッド	162 MiB/秒 (1.4 Gbps)	403 MiB/秒 (3.4 Gbps)	288 MiB/秒 (2.4 Gbps)
	SMBv3 - 8 スレッド	511 MiB/秒 (4.3 Gbps)	571 MiB/秒 (4.8 Gbps)	567 MiB/秒 (4.8 Gbps)

> **Note**
>
> パフォーマンスは、ホストプラットフォーム設定とネットワーク帯域幅によって異なる場合があります。書き込みスループットのパフォーマンスはファイルサイズとともに低下し、小さなファイル (32MiB 未満) で達成可能なスループットは最大 1 秒あたり 16 ファイルです。

ゲートウェイのパフォーマンスの最適化

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方法について説明します。ガイダンスは、ゲートウェイへのリソースの追加およびアプリケーションサーバーへのリソースの追加に基づいています。

ゲートウェイへのリソースの追加

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

ゲートウェイのパフォーマンスを最適化するために、Solid State Drive (SSD) や NVMe コントローラーなどの高性能のディスクを追加できます。また、Microsoft Hyper-V NTFS ではなく、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できます。通常、ディスクパフォーマンスが向上すると、スループットおよび 1 秒あたりの入力/出力操作数 (IOPS) が改善します。ディスクの追加については、追加のキャッシュストレージの設定 を参照してください。

スループットを測定するには、`ReadBytes` および `WriteBytes` メトリクスを `Samples` Amazon 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` 統計を 300 秒で割ると、IOPS がわかります。一般的なルールとして、ゲートウェイのこれらのメトリクスを確認する場合は、ディスク関連のボトルネックを示す低いスループットおよび低い IOPS トレンドを探します。

> **Note**
>
> CloudWatch メトリクスは、すべてのゲートウェイに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、「FSx ファイルゲートウェイのモニタリング」を参照してください。

ゲートウェイホストへの CPU リソースの追加

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 に割り当てられている 4 つの仮想プロセッサが 4 つのコアによってサポートされることを確認します。さらに、ホストサーバーの CPU をオーバー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に CPU 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保存と、同時に FSx for Windows File Server へのデータアップロードの両方を並行して処理できるようになります。また、CPU を追加すると、ホストが他の VM と共有される場合に、ゲートウェイで十分な

CPU リソースを利用できます。十分な CPU リソースを提供することによって、スループットを向上させる一般的な効果があります。

Storage Gateway では、ゲートウェイホストサーバーで 24 個の CPU を使用することができます。24 個の CPU を使用すると、ゲートウェイのパフォーマンスを大幅に向上できます。ゲートウェイホストサーバーのゲートウェイ設定は次のように設定することを推奨します:

- 24 個の CPU。
- ファイルゲートウェイ用に 16 GiB の予約済みの RAM
  - 16 TiB までのキャッシュ容量が使用可能な、ゲートウェイ用に予約された 16 GiB の RAM 領域
  - 16 TiB ~ 32 TiB のキャッシュ容量が使用可能な、ゲートウェイ用に予約された 32 GiB の RAM 領域
  - 32 TiB ~ 64 TiB のキャッシュ容量が使用可能な、ゲートウェイ用に予約された 48 GiB の RAM 領域
- 準仮想化コントローラー 1 にアタッチされているディスク 1 (ゲートウェイのキャッシュとして次のように使用する) :
  - NVMe コントローラーを使用する SSD。
- 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) を追加する。
- 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、 AWSへの接続に使用する VMXnet3 (10 Gbps) を追加する。

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

ゲートウェイディスクをプロビジョニングする際は、ローカルストレージ用にローカルディスクをプロビジョニングする際、同じ基盤となる物理ストレージディスクを使用しないことを強く推奨します。たとえば、VMware ESXi の場合、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推奨します。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、RAID 1 のようなパフォーマンスの低い RAID 構成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。

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の増大

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` および `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る場合には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への CPU リソースの追加

アプリケーションが追加の CPU リソースを使用できる場合、CPU の追加はアプリケーションの I/O 負荷の調整に役立つことがあります。

FSx ファイルゲートウェイでの一部のファイル操作 (トップレベルフォルダの名前変更や権限変更など) は、複数のファイル操作を引き起こし、FSx for Windows File Server ファイルシステムに高い I/O 負荷をもたらす可能性があります。ファイルシステムにワークロードに十分なパフォーマンスリソースがない場合、ファイルシステムはシャドウコピーの保持履歴よりも継続的な I/O の可用性を優先するため、シャドウコピーを削除する可能性があります。

Amazon FSx コンソールで、「モニタリングとパフォーマンス」ページを見て、ファイルシステムがプロビジョニング不足かどうかを確認します。その場合は、SSD ストレージに切り替えるか、スループット容量を増やすか、または SSD IOPS を増やしてワークロードを処理することができます。

S3 ファイルゲートウェイスループットの最大化

次のセクションでは、NFS および SMB クライアント、S3 ファイルゲートウェイ、Amazon S3 間のスループットを最大化するためのベストプラクティスについて説明します。各セクションで提供されるガイダンスは、全体的なスループットの段階的な向上に有用です。これらの推奨事項は必須ではな

く、相互に依存しませんが、 サポート が S3 File Gateway 実装のテストとチューニングに使用する論理的な方法で選択および順序付けされています。これらの提案を実装してテストするときは、S3 ファイルゲートウェイの各デプロイはそれぞれ固有であるため、結果は異なる場合があります。

S3 ファイルゲートウェイは、業界標準の NFS または SMB ファイルプロトコルを使用して Amazon S3 オブジェクトを保存および取得するためのファイルインターフェイスを提供し、ファイルとオブジェクトの間にネイティブな 1:1 のマッピングを備えています。S3 File Gateway は、VMware、Microsoft Hyper-V、Linux KVM 環境でオンプレミスの仮想マシンとしてデプロイするか、Amazon EC2 インスタンスとして AWS クラウドにデプロイします。S3 ファイルゲートウェイは、完全なエンタープライズ NAS の代役として動作するようには設計されていません。S3 ファイルゲートウェイはファイルシステムを エミュレートしますが、ファイルシステムそのものではありません。Amazon S3 を耐久性のあるバックエンドストレージとして使用すると、I/O オペレーションごとに追加のオーバーヘッドが発生します。そのため、既存の NAS やファイルサーバーと S3 ファイルゲートウェイのパフォーマンスを比較して評価しても、同等の比較にはなりません。

クライアントと同じ場所へのゲートウェイのデプロイ

S3 ファイルゲートウェイの仮想アプライアンスは、NFS または SMB クライアントとの間のネットワークレイテンシーができるだけ小さい物理ロケーションにデプロイすることを推奨します。ゲートウェイの場所を選択するときは、次の点を考慮してください。

- ゲートウェイへのネットワークレイテンシーを低くすると、NFS または SMB クライアントのパフォーマンスを向上させることができます。
- S3 ファイルゲートウェイは、ゲートウェイとクライアント間よりもゲートウェイと Amazon S3 間のネットワークレイテンシーが高くなるように設計されています。
- Amazon EC2 にデプロイされた S3 ファイルゲートウェイインスタンスの場合、ゲートウェイと NFS クライアントまたは SMB クライアントを同じプレイスメントグループに保持することをお勧めします。詳細については、Amazon Elastic Compute Cloud ユーザーガイドの「Amazon EC2 インスタンスの配置グループ」を参照してください。

低速ディスクによるボトルネックの軽減

`IoWaitPercent` CloudWatch メトリクスをモニタリングして、S3 ファイルゲートウェイの低速ストレージディスクが原因で発生するパフォーマンスのボトルネックを特定することを推奨します。ディスク関連のパフォーマンス問題を最適化する場合は、次の点を考慮してください。

- `IoWaitPercent` は、CPU がルートディスクまたはキャッシュディスクからの応答を待っている時間の割合を報告します。

- `IoWaitPercent` が 5～10% を超えると、通常、パフォーマンスの低いディスクが原因でゲートウェイパフォーマンスのボトルネックが発生していることを示します。このメトリクスはできるだけ 0% に近い値 (つまり、ゲートウェイのディスク待機時間がない状態) にする必要があります。これにより、CPU リソースを最適化できます。
- Storage Gateway コンソールの[モニタリング] タブで `IoWaitPercent` を確認するか、あるいはメトリクスが特定のしきい値を超えた場合に自動的に通知するように推奨 CloudWatch アラームを設定できます。詳細については、「ゲートウェイの推奨 CloudWatch アラームの作成」を参照してください。
- `IoWaitPercent` を最小限に抑えるには、ゲートウェイのルートディスクとキャッシュディスクに NVMe または SSD を使用することを推奨します。

CPU、RAM、キャッシュディスクの仮想マシンリソースの割り当ての調整

S3 ファイルゲートウェイのスループットを最適化しようとするときは、CPU、RAM、キャッシュディスクなど、ゲートウェイ VM に十分なリソースを割り当てることが重要です。4 CPU、16GB RAM、150GB キャッシュストレージの最小仮想リソース要件は、通常、小規模なワークロードにのみ適しています。大規模なワークロードに仮想リソースを割り当てる場合は、次のことを推奨します。

- S3 ファイルゲートウェイによって生成される一般的な CPU 使用率に応じて、割り当てられた CPU の数を 16～48 に増やします。`UserCpuPercent` メトリクスを使用して CPU 使用率をモニタリングできます。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。
- 割り当てる RAM 数を 32～64 GB に増やします。

> **Note**
>
> S3 ファイルゲートウェイは 64 GB を超える RAM を使用できません。

- ルートディスクとキャッシュディスクに NVMe または SSD を使用し、ゲートウェイに書き込む予定のピーク作業データセットに合わせてキャッシュディスクのサイズを設定します。詳細については、公式 Amazon Web Services YouTube チャンネルの「S3 ファイルゲートウェイキャッシュサイジングのベストプラクティス」を参照してください。
- 1 つの大きなディスクを使用するのではなく、少なくとも 4 つの仮想キャッシュディスクをゲートウェイに追加します。複数の仮想ディスクは、基盤となる同じ物理ディスクを共有していてもパフォーマンスを向上させることができますが、仮想ディスクが異なる基盤となる物理ディスクに配置されると、通常は改善点が大きくなります。

たとえば、12TB のキャッシュをデプロイする場合は、次のいずれかの設定を使用できます。

- 4 x 3 TB キャッシュディスク
- 8 x 1.5 TB キャッシュディスク
- 12 x 1 TB キャッシュディスク

これにより、パフォーマンスに加えて、時間の経過とともに仮想マシンをより効率的に管理できます。ワークロードの変化に応じて、個々の仮想ディスクの元のサイズを維持しながら、キャッシュディスクの数と全体的なキャッシュ容量を段階的に増やして、ゲートウェイの整合性を維持できます。

詳細については、「ローカルディスクストレージの量の決定」を参照してください。

S3 ファイルゲートウェイを Amazon EC2 インスタンスとしてデプロイする場合は、次の点を考慮してください:

- 選択したインスタンスタイプは、ゲートウェイのパフォーマンスに大きな影響を与える可能性があります。Amazon EC2 は、S3 ファイルゲートウェイインスタンスのリソース割り当てを柔軟に調整できます。
- S3 ファイルゲートウェイに推奨される Amazon EC2 インスタンスタイプについては、Amazon EC2 インスタンスタイプの要件を参照してください。
- アクティブな S3 ファイルゲートウェイをホストする Amazon EC2 インスタンスタイプを変更できます。これにより、Amazon EC2 ハードウェアの生成とリソースの割り当てを簡単に調整して、最適な費用対効果比を見つけることができます。インスタンスタイプを変更するには、Amazon EC2 コンソールで次の手順を使用します。

  1. Amazon EC2 インスタンスを停止します。
  2. Amazon EC2 インスタンスタイプを変更します。
  3. Amazon EC2 インスタンスの電源を入れます。

> **Note**
>
> S3 ファイルゲートウェイをホストするインスタンスを停止すると、ファイル共有アクセスが一時的に中断されます。必要に応じて、メンテナンスウィンドウの予定を必ず設定してください。

- Amazon EC2 インスタンスの費用対効果比は、支払う料金に対してどれだけのコンピューティング能力を得られるかを示します。一般的に、より新しい世代の Amazon EC2 インスタンスのほうが、最高レベルの費用対効果比を実現できます。つまり、旧世代と比べて比較的低コストで、より新しいハードウェアを使用することで、パフォーマンスが向上します。インスタンスタイプ、リージョン、使用パターンなどの要因がこの比率に影響するため、コスト効率を最適化するには、そのワークロードに適したインスタンスを選択することが重要です。

SMB セキュリティレベルの調整

SMBv3 プロトコルにより、SMB の署名と SMB の暗号化が可能になりますが、パフォーマンスとセキュリティはトレードオフの関係にあります。スループットを最適化するために、ゲートウェイの SMB セキュリティレベルを調整して、クライアント接続にどのセキュリティ機能を適用するかを指定できます。詳細については、「ゲートウェイのセキュリティレベルを設定する」を参照してください。

SMB セキュリティレベルを調整するときは、次の点を考慮してください。

- S3 ファイルゲートウェイのデフォルトのセキュリティレベルは [暗号化の適用] です。この設定では、ゲートウェイファイル共有への SMB クライアント接続の暗号化と署名の両方が適用されます。つまり、クライアントからゲートウェイへのすべてのトラフィックが暗号化されます。この設定は AWS、ゲートウェイから へのトラフィックには影響しません。このトラフィックは常に暗号化されます。

  ゲートウェイは、暗号化された各クライアント接続を 1 つの vCPU に制限します。たとえば、暗号化されたクライアントが 1 つしかない場合、4 つ以上の vCPU がゲートウェイに割り当てられていても、そのクライアントは 1 つの vCPUs に制限されます。このため、単一のクライアントから S3 ファイルゲートウェイへの暗号化された接続のスループットは通常、40 ~ 60 MB/秒の間でボトルネックになります。
- セキュリティ要件でより緩やかな体制が許されている場合には、セキュリティレベルをクライアントネゴシエートに変更できます。これにより、SMB 暗号化は無効になり、SMB 署名のみが適用されます。この設定では、ゲートウェイへのクライアント接続で複数の vCPU を利用できるため、通常、スループットパフォーマンスが向上します。

> **Note**
>
> S3 ファイルゲートウェイの SMB セキュリティレベルを変更します。その後、Storage Gateway コンソールでファイル共有ステータスが [更新] から [使用可能] に変わるまで待ち

ます。次に、SMB クライアントを切断してから再接続すると、新しい設定が有効になります。

複数のスレッドとクライアントを使用して、書き込みオペレーションを並列化

S3 ファイルゲートウェイで、1 つの NFS または SMB クライアントが 1 回に 1 ファイルずつ書き込む場合、単一クライアントからの連続書き込みはシングルスレッドの操作となるため、最大スループット性能を達成するのは困難です。代わりに、各 NFS または SMB クライアントで複数のスレッドを使用して複数のファイルを並列に書き込み、さらに複数の NFS または SMB クライアントを同時に S3 ファイルゲートウェイに接続して、ゲートウェイのスループットを最大化することを推奨します。

複数のスレッドを使うと、パフォーマンスを大幅に向上できます。ただし、より多くのスレッドを使うにはより多くのシステムリソースが必要であるため、負荷の増加に対応するようにゲートウェイのサイズを設定していない場合は、パフォーマンスに悪影響を及ぼす可能性があります。一般的なデプロイでは、ゲートウェイの最大ハードウェアと帯域幅の制限に達するまで、スレッドとクライアントを追加するとスループットのパフォーマンスが向上します。さまざまなスレッド数を試して、特定のハードウェアとネットワーク設定の速度とシステムリソースの使用状況の最適なバランスを見つけることをお勧めします。

スレッドとクライアント設定のテストに役立つ一般的なツールについては、次の情報を考慮してください。

- マルチスレッド書き込みパフォーマンスをテストするには、Robocopy などのツールを使用して、一連のファイルをゲートウェイ上のファイル共有にコピーします。デフォルトでは Robocopy はファイルのコピーに 8 スレッドを使用しますが、最大 128 スレッドを指定できます。

  Robocopy で複数のスレッドを使うには、 コマンドに `/MT:n` スイッチを追加します。ここで、n は使うスレッドの数です。例えば、次のようになります。

  ```
  robocopy C:\source D:\destination /MT:64
  ```

  このコマンドは、コピーの処理に 64 スレッドを使用します。

> **Note**
>
> 最大スループットのテスト時に Windows Explorer を使ってファイルをドラッグアンドドロップすることはお勧めしません。この方法ではスレッドが 1 つに制限され、ファイルが順番にコピーされるからです。

詳細については、Microsoft Learn ウェブサイトの「Robocopy」を参照してください。

- DISKSPD や FIO などの一般的なストレージベンチマークツールを使用してテストを実行することもできます。これらのツールには、特定のワークロード要件に合わせてスレッド数、I/O 深度、およびその他のパラメータを調整するオプションがあります。

  DiskSpd では、`-t`パラメータを使用してスレッドの数を制御できます。例えば、次のようになります。

  ```
  diskspd -c10G -d300 -r -w50 -t64 -o32 -b1M -h -L C:\testfile.dat
  ```

  このコマンド例では、次の操作を行います。

  - 10GB のテストファイルを作成します (`-c1G`)
  - 300 秒間実行 (`-d300`)
  - 読み取り 50%、書き込み 50% でランダム I/O テストを実行します (`-r -w50`)
  - 64 スレッドを使用 (`-t64`)
  - キューの深さをスレッドあたり 32 に設定します (`-o32`)
  - 1MB のブロックサイズを使用する (`-b1M`)
  - ハードウェアおよびソフトウェアのキャッシュを無効にします (`-h -L`)

  詳細については、Microsoft Learn ウェブサイトの「DISKSPD を使用してワークロードストレージのパフォーマンスをテストする」を参照してください。

- FIO は `numjobs` パラメータを使用して並列スレッドの数を制御します。例えば、次のようになります。

  ```
  fio --name=mixed_test --rw=randrw --rwmixread=70 --bs=1M -- iodepth=64
  --size=10G --runtime=300 --numjobs=64 --ioengine=libaio --direct=1 --
  group_reporting
  ```

  このコマンド例では、次の操作を行います。

- ランダム I/O テストを実行する (`--rw=randrw`)
- 70% の読み取りと 30% の書き込みを実行する (`--rwmixread=70`)
- 1MB のブロックサイズを使用する (`--bs=1M`)
- I/O 深度を 64 に設定 (`--iodepth=64`)
- 10 GB ファイルのテストをします (`--size=10G`)
- 5 分間実行 (`--runtime=300`)
- 64 の並列ジョブ (スレッド) を作成する (`--numjobs=64`)
- 非同期 I/O エンジンを使用します (`--ioengine=libaio`)
- 結果をグループ化して分析を容易にする (`--group_reporting`)

詳細については「fio Linux man」ページを参照してください。

-

自動キャッシュ更新の無効化

自動キャッシュ更新機能により、S3 ファイルゲートウェイはメタデータを自動的に更新できます。これにより、ユーザーやアプリケーションがゲートウェイを通さずに直接 Amazon S3 バケットに書き込んだファイルセットの変更を反映させることが可能になります。詳細については、Amazon S3 バケットオブジェクトキャッシュの更新」を参照してください。

ゲートウェイのスループットを最適化するために、Amazon S3 バケットへのすべての読み取りと書き込みが S3 ファイルゲートウェイを介して実行されるデプロイでは、この機能をオフにすることをお勧めします。

自動キャッシュ更新を設定する際は、以下の点を考慮してください。

- デプロイ内のユーザーまたはアプリケーションが Amazon S3 に直接書き込むことがあるため、自動キャッシュ更新を使用する必要がある場合は、更新間隔をできるだけ長く (業務ニーズに合理的な間隔で) 設定することを推奨します。キャッシュ更新間隔を長くすると、ディレクトリを参照したりファイルを変更したりするときにゲートウェイが実行する必要があるメタデータオペレーションの数を減らすことができます。

  例えば、自動キャッシュ更新を 5 分ではなく 24 時間に設定します (ワークロードに許容できる範囲で)。
- 最小更新間隔は 5 分です。最大間隔は 30 日間です。

- 非常に短いキャッシュ更新間隔を設定する場合は、NFS および SMB クライアントのディレクトリブラウジングエクスペリエンスをテストすることをお勧めします。ゲートウェイキャッシュの更新にかかる時間は、Amazon S3 バケット内のファイル数とサブディレクトリ数によってかなり長くなる可能性があります。

Amazon S3 アップローダースレッドの数の増大

デフォルトでは、S3 ファイルゲートウェイは Amazon S3 データアップロード用に 8 つのスレッドを使用し、ほとんどの一般的なデプロイに十分なアップロード容量を提供します。ただし、ゲートウェイが標準の 8 スレッド容量で Amazon S3 にアップロードできるよりも高いレートで NFS および SMB クライアントからデータを受信する可能性があります。これにより、ローカルキャッシュがストレージ制限に達する可能性があります。

特定の状況では、ゲートウェイの Amazon S3 アップロードスレッドプールの数を 8 から 40 に サポート 増やすことができます。これにより、より多くのデータを並行してアップロードできます。帯域幅やその他のデプロイに固有の要因によっては、アップロードパフォーマンスが大幅に向上し、ワークロードのサポートに必要なキャッシュストレージの量を減らすことができます。

`CachePercentDirty` CloudWatch メトリクスを使用して、Amazon S3 にまだアップロードされていないローカルゲートウェイキャッシュディスクに保存されているデータ量をモニタリングし、 サポート に連絡して、アップロードスレッドプール数を増やすことで S3 File Gateway のスループットが向上するかどうかを判断することをお勧めします。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。

> **Note**
>
> この設定では、追加のゲートウェイ CPU リソースを消費します。ゲートウェイの CPU 使用率をモニタリングし、必要に応じて割り当てられた CPU リソースを増やすことを推奨します。

SMB タイムアウト設定の増大

S3 ファイルゲートウェイが大きなファイルを SMB ファイル共有にコピーする場合、長時間経過すると SMB クライアント接続がタイムアウトすることがあります。

ファイルのサイズとゲートウェイの書き込み速度に応じて、SMB クライアントの SMB セッションタイムアウト設定を 20 分以上に延長することを推奨します。デフォルトは 300 秒 (5 分) です。詳細

については、「ゲートウェイのバックアップジョブが失敗する、またはゲートウェイへの書き込み時にエラーが発生する」を参照してください。

互換性のあるアプリケーションの日和見ロックの有効化

日和見ロック (オプロック) は、新しい S3 ファイルゲートウェイごとにデフォルトで有効になっています。互換性のあるアプリケーションで日和見ロックを使用する場合、クライアントは複数の小さなオペレーションをまとめてより大きなオペレーションとしてバッチ処理します。これはクライアント、ゲートウェイ、ネットワークにとって効率的です。Microsoft Office、Adobe Suite など、クライアント側のローカルキャッシュを活用するアプリケーションを使用する場合は、日和見ロックを有効にしておくことを推奨します。これにより、パフォーマンスが大幅に向上する可能性があります。

日和見ロックを無効にすると、日和見ロックをサポートするアプリケーションは通常、大きなファイル (50 MB 以上) をよりゆっくりと開きます。この遅延は、ゲートウェイが 4 KB のパートでデータを送信するために発生します。これにより、I/O が高くなり、スループットが低くなります。

作業ファイルセットのサイズに応じたゲートウェイ容量の調整

ゲートウェイ容量パラメータは、ゲートウェイがローカルキャッシュにメタデータを保存するファイルの最大数を指定します。デフォルトでは、ゲートウェイ容量は 小 に設定されています。つまり、ゲートウェイは最大 500 万個のファイルのメタデータを保存できます。デフォルト設定は、Amazon S3 に数億または数十億のオブジェクトがある場合でも、ほとんどのワークロードでうまく機能します。これは、通常のデプロイで特定の時間にアクティブにアクセスされるファイルのサブセットがごくわずかであるためです。このファイルのグループは、「ワーキングセット」と呼ばれます。

ワークロードが 500 万を超えるファイルのワーキングセットに定期的にアクセスする場合、ゲートウェイは頻繁にキャッシュエビクションを実行する必要があります。これは、RAM に保存され、ルートディスクに保持される小さな I/O オペレーションです。これは、ゲートウェイが Amazon S3 から新しいデータを取得するときに、ゲートウェイのパフォーマンスに悪影響を及ぼす可能性があります。

`IndexEvictions` メトリクスをモニタリングして、メタデータがキャッシュから削除されたファイルの数を決定し、新しいエントリのスペースを確保できます。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。

`UpdateGatewayInformation` API アクションを使用して、一般的なワーキングセット内のファイル数に対応するようにゲートウェイ容量を増やすことをお勧めします。詳細については、「UpdateGatewayInformation」を参照してください。

> **Note**
>
> ゲートウェイ容量を増やすには、追加の RAM とルートディスク容量が必要です。
>
> - 小 (500 万ファイル) には、少なくとも 16 GB RAM と 80 GB ルートディスクが必要です。
> - 中 (1,000 万ファイル) には、少なくとも 32 GB RAM と 160 GB ルートディスクが必要です。
> - 大 (2,000 万ファイル) の場合、64 GB RAM と 240 GB ルートディスクが必要です。

> **Important**
>
> ゲートウェイ容量を減らすことはできません。

ワークロードの増大用の複数のゲートウェイのデプロイ

1 つの大きなゲートウェイに多数のファイル共有を統合するのではなく、可能であればワークロードを複数のゲートウェイに分割することをお勧めします。たとえば、頻繁に使用するファイル共有を 1 つのゲートウェイで分離し、使用頻度の低いファイル共有を別のゲートウェイでグループ化できます。

複数のゲートウェイとファイル共有を使用してデプロイを計画する場合は、次の点を考慮してください。

- 1 つのゲートウェイでのファイル共有の最大数は 50 ですが、ゲートウェイによって管理されるファイル共有の数はゲートウェイのパフォーマンスに影響を与える可能性があります。詳細については、「複数のファイル共有を持つゲートウェイのパフォーマンスガイダンス」を参照してください。
- 各 S3 ファイルゲートウェイのリソースは、パーティション化することなく、すべてのファイル共有で共有されます。
- 使用量が多い単一のファイル共有は、ゲートウェイ上の他のファイル共有のパフォーマンスに影響を与える可能性があります。

> **Note**
>
> 少なくとも 1 つのゲートウェイを読み取り専用にしない限り、複数のゲートウェイから同じ Amazon S3 の場所にマッピングされた複数のファイル共有を作成することはお勧めしません。
> 複数のゲートウェイから同じファイルへの同時書き込みは、マルチライターシナリオと見なされ、データ整合性の問題が発生する可能性があります。

SQL Server データベースバックアップ用の S3 ファイルゲートウェイの最適化

データベースのバックアップは、S3 ファイルゲートウェイの一般的で推奨されるユースケースです。S3 ファイルゲートウェイは、データベースのバックアップを Amazon S3 に保存することで、コスト効率の高い短期および長期の保持を提供し、必要に応じてライフサイクル管理により低コストのストレージ階層へ移行することができます。このソリューションを使用すると、SQL Server Management Studio や Oracle RMAN などの組み込みツールを使用して、エンタープライズバックアップアプリケーションの必要性を減らすことができます。

次のセクションでは、S3 ファイルゲートウェイのデプロイを最適化し、数百テラバイト規模の SQL データベースバックアップをコスト効率よくサポートするためのベストプラクティスについて説明します。各セクションで提供されるガイダンスは、全体的なスループットの段階的な向上に有用です。これらの推奨事項は必須ではなく、相互に依存しませんが、 サポート が S3 File Gateway 実装のテストとチューニングに使用する論理的な方法で選択および順序付けされています。これらの提案を実装してテストするときは、S3 ファイルゲートウェイの各デプロイはそれぞれ固有であるため、結果は異なる場合があります。

S3 ファイルゲートウェイは、業界標準の NFS または SMB ファイルプロトコルを使用して Amazon S3 オブジェクトを保存および取得するためのファイルインターフェイスを提供し、ファイルとオブジェクトの間にネイティブな 1:1 のマッピングを備えています。S3 File Gateway は、VMware、Microsoft Hyper-V、Linux KVM 環境でオンプレミスの仮想マシンとしてデプロイするか、Amazon EC2 インスタンスとして AWS クラウドにデプロイします。S3 ファイルゲートウェイは、完全なエンタープライズ NAS の代役として動作するようには設計されていません。S3 ファイルゲートウェイはファイルシステムをエミュレートしますが、ファイルシステムそのものではありません。Amazon S3 を耐久性のあるバックエンドストレージとして使用すると、I/O オペレーションごとに追加のオーバーヘッドが発生します。そのため、既存の NAS やファイルサーバーと S3 ファイルゲートウェイのパフォーマンスを比較して評価しても、同等の比較にはなりません。

SQL Server と同じ場所へのゲートウェイのデプロイ

S3 ファイルゲートウェイの仮想アプライアンスは、SQL Server との間のネットワークレイテンシーができるだけ小さい物理ロケーションにデプロイすることを推奨します。ゲートウェイの場所を選択するときは、次の点を考慮してください。

- ゲートウェイへのネットワークレイテンシーを低くすると、SQL サーバーなどの SMB クライアントのパフォーマンスを向上させることができます。
- S3 ファイルゲートウェイは、ゲートウェイとクライアント間よりもゲートウェイと Amazon S3 間のネットワークレイテンシーが高くなるように設計されています。
- Amazon EC2 にデプロイされた S3 ファイルゲートウェイインスタンスの場合、ゲートウェイと SQL サーバーを同じプレイスメントグループに保持することをお勧めします。詳細については、Amazon Elastic Compute Cloud ユーザーガイドの「Amazon EC2 インスタンスの配置グループ」を参照してください。

低速ディスクによるボトルネックの軽減

`IoWaitPercent` CloudWatch メトリクスをモニタリングして、S3 ファイルゲートウェイの低速ストレージディスクが原因で発生するパフォーマンスのボトルネックを特定することを推奨します。ディスク関連のパフォーマンス問題を最適化する場合は、次の点を考慮してください。

- `IoWaitPercent` は、CPU がルートディスクまたはキャッシュディスクからの応答を待っている時間の割合を報告します。
- `IoWaitPercent` が 5 ~ 10% を超えると、通常、パフォーマンスの低いディスクが原因でゲートウェイパフォーマンスのボトルネックが発生していることを示します。このメトリクスはできるだけ 0% に近い値 (つまり、ゲートウェイのディスク待機時間がない状態) にする必要があります。これにより、CPU リソースを最適化できます。
- Storage Gateway コンソールの[モニタリング] タブで `IoWaitPercent` を確認するか、あるいはメトリクスが特定のしきい値を超えた場合に自動的に通知するように推奨 CloudWatch アラームを設定できます。詳細については、「ゲートウェイの推奨 CloudWatch アラームの作成」を参照してください。
- `IoWaitPercent` を最小限に抑えるには、ゲートウェイのルートディスクとキャッシュディスクに NVMe または SSD を使用することを推奨します。

CPU、RAM、キャッシュディスクの S3 ファイルゲートウェイ仮想マシンリソース割り当ての調整

S3 ファイルゲートウェイのスループットを最適化しようとするときは、CPU、RAM、キャッシュディスクなど、ゲートウェイ VM に十分なリソースを割り当てることが重要です。4 CPU、16GB RAM、150GB キャッシュストレージの最小仮想リソース要件は、通常、小規模なワークロードにのみ適しています。大規模なワークロードに仮想リソースを割り当てる場合は、次のことを推奨します。

- S3 ファイルゲートウェイによって生成される一般的な CPU 使用率に応じて、割り当てられた CPU の数を 16～48 に増やします。`UserCpuPercent` メトリクスを使用して CPU 使用率をモニタリングできます。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。
- 割り当てる RAM 数を 32～64 GB に増やします。

> **Note**
>
> S3 ファイルゲートウェイは 64 GB を超える RAM を使用できません。

- ルートディスクとキャッシュディスクに NVMe または SSD を使用し、ゲートウェイに書き込む予定のピーク作業データセットに合わせてキャッシュディスクのサイズを設定します。詳細については、公式 Amazon Web Services YouTube チャンネルの「S3 ファイルゲートウェイキャッシュサイジングのベストプラクティス」を参照してください。
- 1 つの大きなディスクを使用するのではなく、少なくとも 4 つの仮想キャッシュディスクをゲートウェイに追加します。複数の仮想ディスクは、基盤となる同じ物理ディスクを共有していてもパフォーマンスを向上させることができますが、仮想ディスクが異なる基盤となる物理ディスクに配置されると、通常は改善点が大きくなります。

  たとえば、12TB のキャッシュをデプロイする場合は、次のいずれかの設定を使用できます。

  - 4 x 3 TB キャッシュディスク
  - 8 x 1.5 TB キャッシュディスク
  - 12 x 1 TB キャッシュディスク

  これにより、パフォーマンスに加えて、時間の経過とともに仮想マシンをより効率的に管理できます。ワークロードの変化に応じて、個々の仮想ディスクの元のサイズを維持しながら、キャッシュディスクの数と全体的なキャッシュ容量を段階的に増やして、ゲートウェイの整合性を維持できます。

詳細については、「ローカルディスクストレージの量の決定」を参照してください。

S3 ファイルゲートウェイを Amazon EC2 インスタンスとしてデプロイする場合は、次の点を考慮してください:

- 選択したインスタンスタイプは、ゲートウェイのパフォーマンスに大きな影響を与える可能性があります。Amazon EC2 は、S3 ファイルゲートウェイインスタンスのリソース割り当てを柔軟に調整できます。
- S3 ファイルゲートウェイに推奨される Amazon EC2 インスタンスタイプについては、Amazon EC2 インスタンスタイプの要件を参照してください。
- アクティブな S3 ファイルゲートウェイをホストする Amazon EC2 インスタンスタイプを変更できます。これにより、Amazon EC2 ハードウェアの生成とリソースの割り当てを簡単に調整して、最適な費用対効果比を見つけることができます。インスタンスタイプを変更するには、Amazon EC2 コンソールで次の手順を使用します。

  1. Amazon EC2 インスタンスを停止します。
  2. Amazon EC2 インスタンスタイプを変更します。
  3. Amazon EC2 インスタンスの電源を入れます。

  > **Note**
  >
  > S3 ファイルゲートウェイをホストするインスタンスを停止すると、ファイル共有アクセスが一時的に中断されます。必要に応じて、メンテナンスウィンドウの予定を必ず設定してください。

- Amazon EC2 インスタンスの費用対効果比は、支払う料金に対してどれだけのコンピューティング能力を得られるかを示します。一般的に、より新しい世代の Amazon EC2 インスタンスのほうが、最高レベルの費用対効果比を実現できます。つまり、旧世代と比べて比較的低コストで、より新しいハードウェアを使用することで、パフォーマンスが向上します。インスタンスタイプ、リージョン、使用パターンなどの要因がこの比率に影響するため、コスト効率を最適化するには、そのワークロードに適したインスタンスを選択することが重要です。

S3 ファイルゲートウェイのセキュリティレベルを調整して SMB クライアントのスループットを向上

SMBv3 プロトコルにより、SMB の署名と SMB の暗号化が可能になりますが、パフォーマンスとセキュリティはトレードオフの関係にあります。スループットを最適化するために、ゲートウェイの SMB セキュリティレベルを調整して、クライアント接続にどのセキュリティ機能を適用するかを指定できます。詳細については、「ゲートウェイのセキュリティレベルを設定する」を参照してください。

SMB セキュリティレベルを調整するときは、次の点を考慮してください。

- S3 ファイルゲートウェイのデフォルトのセキュリティレベルは [暗号化の適用] です。この設定では、ゲートウェイファイル共有への SMB クライアント接続の暗号化と署名の両方が適用されます。つまり、クライアントからゲートウェイへのすべてのトラフィックが暗号化されます。この設定は AWS、ゲートウェイから へのトラフィックには影響しません。このトラフィックは常に暗号化されます。

  ゲートウェイは、暗号化された各クライアント接続を 1 つの vCPU に制限します。たとえば、暗号化されたクライアントが 1 つしかない場合、4 つ以上の vCPU がゲートウェイに割り当てられていても、そのクライアントは 1 つの vCPUs に制限されます。このため、単一のクライアントから S3 ファイルゲートウェイへの暗号化された接続のスループットは通常、40 ~ 60 MB/秒の間でボトルネックになります。
- セキュリティ要件でより緩やかな体制が許されている場合には、セキュリティレベルをクライアントネゴシエートに変更できます。これにより、SMB 暗号化は無効になり、SMB 署名のみが適用されます。この設定では、ゲートウェイへのクライアント接続で複数の vCPU を利用できるため、通常、スループットパフォーマンスが向上します。

> **Note**
>
> S3 ファイルゲートウェイの SMB セキュリティレベルを変更します。その後、Storage Gateway コンソールでファイル共有ステータスが [更新] から [使用可能] に変わるまで待ちます。次に、SMB クライアントを切断してから再接続すると、新しい設定が有効になります。

SQL バックアップを複数のファイルに分割して SMB クライアントのスループットを向上

- 単一の SQL サーバーからのシーケンシャル書き込みはシングルスレッドの処理となるため、一度に 1 つの SQL サーバーのみを使用して 1 つのファイルを書き込む構成では、S3 ファイルゲートウェイのスループットを最大限に引き出すことは困難です。代わりに、各 SQL サーバーで複数のスレッドを使用して複数のファイルを並列に書き込み、さらに複数の SQL サーバーを同時に S3 ファイルゲートウェイに接続して、ゲートウェイのスループットを最大化することを推奨します。SQL バックアップでは、バックアップを複数のファイルに分割することで、各ファイルで個別のスレッドを使用できます。これにより、複数のファイルが同時に S3 ファイルゲートウェイファイル共有に書き込まれます。スレッドが多いほど、ゲートウェイの制限まで達成できるスループットが向上します。
- SQL Server は、1 回のバックアップ処理中に複数のファイルへの書き込みを同時にサポートします。例えば、T-SQL コマンドまたは SQL Server Management Studio (SSMS) を使用して、複数のファイル送信先を指定できます。各ファイルは、個別のスレッドを使用して SQL Server からゲートウェイファイル共有にデータを送信します。この方法により、I/O スループットが向上し、バックアップの速度と効率を大幅に向上できます。

SQL Server バックアップを設定するときは、次の点を考慮してください。

- バックアップを複数のファイルに分割することで、SQL Server 管理者はバックアップ時間を最適化し、大規模なデータベースバックアップをより効果的に管理できます。
- 使用するファイル数は、サーバーのストレージ設定とパフォーマンス要件によって異なります。大規模なデータベースでは、バックアップをそれぞれ 10 GB から 20 GB までのいくつかの小さなファイルに分割することを推奨します。
- SQL Server がバックアップ中に書き込むことができるファイルの数には厳密な制限はありませんが、ストレージアーキテクチャやネットワーク帯域幅などの実用的な検討事項が指針となるでしょう。

詳細については、以下を参照してください。

- 複数のファイルに書き込むことで SQL Server を 43 ~ 67% 高速化
- ファイルゲートウェイを使用して SQL Server のバックアップを Amazon S3 に簡単に保存

SMB タイムアウト設定を増やして大きなファイルコピーの失敗を防止

S3 ファイルゲートウェイが大きな SQL バックアップファイルを SMB ファイル共有にコピーすると、SMB クライアント接続は長期間経過するとタイムアウトする可能性があります。ファイルのサイズとゲートウェイの書き込み速度に応じて、SQL サーバー SMB クライアントの SMB セッションタイムアウト設定を 20 分以上に延長することを推奨します。デフォルトは 300 秒 (5 分) です。詳細については、「ゲートウェイのバックアップジョブが失敗する、またはゲートウェイへの書き込み時にエラーが発生する」を参照してください。

Amazon S3 アップローダースレッドの数の増大

デフォルトでは、S3 ファイルゲートウェイは Amazon S3 データアップロード用に 8 つのスレッドを使用し、ほとんどの一般的なデプロイに十分なアップロード容量を提供します。ただし、ゲートウェイが標準の 8 スレッド容量で Amazon S3 にアップロードできる速度を超えて SQL サーバーからデータを受信する場合があります。これにより、ローカルキャッシュがストレージの上限に達する可能性があります。

特定の状況では、ゲートウェイの Amazon S3 アップロードスレッドプールの数を 8 から 40 に サポート 増やすことができます。これにより、より多くのデータを並行してアップロードできます。帯域幅やその他のデプロイに固有の要因によっては、アップロードパフォーマンスが大幅に向上し、ワークロードのサポートに必要なキャッシュストレージの量を減らすことができます。

`CachePercentDirty` CloudWatch メトリクスを使用して、Amazon S3 にまだアップロードされていないローカルゲートウェイキャッシュディスクに保存されているデータ量をモニタリングし、 サポート に連絡して、アップロードスレッドプール数を増やすことで S3 File Gateway のスループットが向上するかどうかを判断することをお勧めします。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。

> **Note**
>
> この設定では、追加のゲートウェイ CPU リソースを消費します。ゲートウェイの CPU 使用率をモニタリングし、必要に応じて割り当てられた CPU リソースを増やすことを推奨します。

自動キャッシュ更新の無効化

自動キャッシュ更新機能により、S3 ファイルゲートウェイはメタデータを自動的に更新できます。これにより、ユーザーやアプリケーションがゲートウェイを通さずに直接 Amazon S3 バケットに書

き込んだファイルセットの変更を反映させることが可能になります。詳細については、Amazon S3 バケットオブジェクトキャッシュの更新」を参照してください。

ゲートウェイのスループットを最適化するために、Amazon S3 バケットへのすべての読み取りと書き込みが S3 ファイルゲートウェイを介して実行されるデプロイでは、この機能をオフにすることをお勧めします。

自動キャッシュ更新を設定する際は、以下の点を考慮してください。

- デプロイ内のユーザーまたはアプリケーションが Amazon S3 に直接書き込むことがあるため、自動キャッシュ更新を使用する必要がある場合は、更新間隔をできるだけ長く (業務ニーズに合理的な間隔で) 設定することを推奨します。キャッシュ更新間隔を長くすると、ディレクトリを参照したりファイルを変更したりするときにゲートウェイが実行する必要があるメタデータオペレーションの数を減らすことができます。

  例えば、自動キャッシュ更新を 5 分ではなく 24 時間に設定します (ワークロードに許容できる範囲で)。
- 最小更新間隔は 5 分です。最大間隔は 30 日間です。
- 非常に短いキャッシュ更新間隔を設定する場合は、SQL サーバーのディレクトリ閲覧エクスペリエンスをテストすることをお勧めします。ゲートウェイキャッシュの更新にかかる時間は、Amazon S3 バケット内のファイル数とサブディレクトリ数によってかなり長くなる可能性があります。

ワークロードをサポートするために複数のゲートウェイをデプロイする

Storage Gateway は、ワークロードを複数のゲートウェイに分割することで、数百の SQL データベース、複数の SQL Server、数百テラバイトのバックアップデータを持つ大規模な環境の SQL バックアップをサポートできます。

複数のゲートウェイと SQL サーバーを使用してデプロイを計画する場合は、次の点を考慮してください。

- 通常、1 つのゲートウェイで 1 日あたり最大 20 TB のハードウェアリソースと帯域幅をアップロードできます。Amazon S3 アップローダースレッドの数を増やすことで、この制限を 1 日あたり 40 TB まで増やすことができます。
- 概念実証テストを実施してパフォーマンスを測定し、デプロイ内のすべての変数を考慮することをお勧めします。SQL バックアップワークロードのピークスループットを決定したら、要件を満たすようにゲートウェイの数をスケールできます。

- データベースの数とデータベースのサイズは時間の経過とともに増加する可能性があるため、成長を念頭に置いてソリューションを設計することをお勧めします。増加するワークロードを引き続きスケーリングしてサポートするために、必要に応じて追加のゲートウェイをデプロイできます。

データベースバックアップワークロードの追加リソース

- を使用して SQL Server バックアップを Amazon S3 に保存 AWS Storage Gateway
- ファイルゲートウェイを使用して SQL Server のバックアップを Amazon S3 に簡単に保存できる
- AWS Storage Gateway を使用して Oracle データベースのバックアップを Amazon S3 に保存
- Oracle データベースを Amazon S3 に大規模にバックアップ
- を使用して SAP ASE データベースを Amazon S3 に統合する AWS Storage Gateway
- 1 人の AWS HERO がクラウド内バックアップ AWS Storage Gateway に を使用する方法
- S3 ファイルゲートウェイキャッシュサイジングのベストプラクティス

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を活用できます。

セキュリティは、 AWS とお客様の間の責任共有です。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 — クラウドで AWS 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 AWS 責任があります。 AWS また、 では、安全に使用できるサービスも提供しています。サードパーティーの監査者は、AWS コンプライアンスプログラムコンプライアンスプログラムの一環として、当社のセキュリティの有効性を定期的にテストおよび検証。 AWS Storage Gateway「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、ユーザーは、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 サービスの使用方法についても説明します。

In 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。ユーザーは、このインフラストラクチャでホストされ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に関するよくある質問を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿された「AWS 責任共有モデルおよび GDPR」のブログ記事を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント 、 AWS IAM アイデンティティセンターまたは AWS Identity and Access Management (IAM) 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。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。TLS 1.2 は必須ですが、TLS 1.3 を推奨します。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「 AWS CloudTrail ユーザーガイド」のCloudTrail 証跡の使用」を参照してください。
- 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 などの高度な管理された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 API AWS を介して にアクセスするときに FIPS 140-3 検証済み暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な 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を、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含めないことを強くお勧めします。これは、コンソール、API、または SDK を使用して Storage Gateway AWS CLIまたは他の AWS のサービス を使用する場合も同様です。 AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL 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

Amazon FSx ファイルゲートウェイは、AES 128 CCM や AES 128 GCM など、最新の SMB v3.1.1 仕様までの SMB 暗号化をサポートしています。互換性のあるクライアントは、暗号化を使用して自動的に接続します。さらに、FSx ファイルゲートウェイは、 AWSで FSx for Windows File Server と通信するときに SMB 暗号化を使用します。SMB トラフィックと管理トラフィックが に渡すことができるように AWS、 Direct Connect へのリンクを設定し、適切なポリシーを設定する必要があります AWS。

ファイルシステムの暗号化

詳細については、Amazon FSx for Windows File Server ユーザーガイドの「Amazon FSx でのデータ暗号化」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、データはAmazon FSx で暗号化されます。
- IAM ユーザーには、 AWS KMS API オペレーションを呼び出すために必要なアクセス許可が必要です。詳細については、「AWS Key Management Service 開発者ガイド」の「AWS KMSで IAM ポリシーを使用する」を参照してください。

> **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。

詳細については AWS KMS、「 とは」を参照してください AWS Key Management Service。

AWS Storage Gatewayの Identity and Access Management

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 SGW AWS リソースの使用を許可する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで使用できる AWS のサービス です。

トピック

- オーディエンス
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- How AWS Storage Gateway と IAM の連携
- AWS Storage Gatewayのアイデンティティベースのポリシーの例
- Troubleshooting AWS Storage Gateway のアイデンティティとアクセス
- タグを使用してゲートウェイとリソースへのアクセスをコントロールする

オーディエンス

AWS Identity and Access Management (IAM) の使用方法は、ロールによって異なります。

- サービスユーザー - 機能にアクセスできない場合は、管理者にアクセス許可をリクエストします (「Troubleshooting AWS Storage Gateway のアイデンティティとアクセス」を参照)。
- サービス管理者 - ユーザーアクセスを決定し、アクセス許可リクエストを送信します (「How AWS Storage Gateway と IAM の連携」を参照)
- IAM 管理者 - アクセスを管理するためのポリシーを作成します (「AWS Storage Gatewayのアイデンティティベースのポリシーの例」を参照)

アイデンティティを使用した認証

認証は、ID 認証情報 AWS を使用して にサインインする方法です。、IAM ユーザー 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で認証される必要があります。

AWS IAM アイデンティティセンター (IAM Identity Center)、シングルサインオン認証、Google/Facebook 認証情報などの ID ソースからの認証情報を使用して、フェデレーティッド ID としてサインインできます。サインインの詳細については、「AWS サインイン ユーザーガイド」の「AWS アカウントにサインインする方法」を参照してください。

プログラムによるアクセスの場合、 は SDK と CLI AWS を提供してリクエストを暗号化して署名します。詳細については、「IAM ユーザーガイド」の「API リクエストに対するAWS 署名バージョン 4」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、すべての AWS のサービス および リソースへの完全なアクセス権を持つ AWS アカウント ルートユーザーと呼ばれる 1 つのサインインアイデンティティから始めます。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。ルートユーザー認証情報を必要とするタスクについては、「IAM ユーザーガイド」の「ルートユーザー認証情報が必要なタスク」を参照してください。

フェデレーテッドアイデンティティ

ベストプラクティスとして、人間のユーザーが一時的な認証情報 AWS のサービス を使用して にアクセスするには、ID プロバイダーとのフェデレーションを使用する必要があります。

フェデレーティッド ID は、エンタープライズディレクトリ、ウェブ ID プロバイダー、または ID Directory Service ソースの認証情報 AWS のサービス を使用して にアクセスするユーザーです。フェデレーテッドアイデンティティは、一時的な認証情報を提供するロールを引き受けます。

アクセスを一元管理する場合は、 AWS IAM アイデンティティセンターをお勧めします。詳細については、「AWS IAM アイデンティティセンター ユーザーガイド」の「IAM アイデンティティセンターとは」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、特定の個人やアプリケーションに対する特定のアクセス許可を持つアイデンティティです。長期認証情報を持つ IAM ユーザーの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。詳細については、IAM ユーザーガイドの「ID プロバイダーとのフェデレーションを使用して にアクセスする必要がある AWS」を参照してください。

IAM グループは、IAM ユーザーの集合を指定し、大量のユーザーに対するアクセス許可の管理を容易にします。詳細については、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」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を持つアイデンティであり、一時的な認証情報を提供します。ユーザーから IAM ロール (コンソール) に切り替えるか、 または API オペレーションを呼び出すことで、ロールを引き受けることができます。 AWS CLI AWS 詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールは、フェデレーションユーザーアクセス、一時的な IAM ユーザーのアクセス許可、クロスアカウントアクセス、クロスサービスアクセス、および Amazon EC2 で実行するアプリケーションに役立ちます。詳細については、IAM ユーザーガイド の IAM でのクロスアカウントリソースアクセス 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、ID AWS 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場合のアクセス許可を定義します。 は、プリンシパル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。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詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は、ポリシーを使用して、どのプリンシパルがどのリソースに対して、どのような条件でアクションを実行できるかを定義することで、誰が何にアクセスできるかを指定します。

デフォルトでは、ユーザーやロールにアクセス許可はありません。IAM 管理者は IAM ポリシーを作成してロールに追加し、このロールをユーザーが引き受けられるようにします。IAM ポリシーは、オペレーションの実行方法を問わず、アクセス許可を定義します。

アイデンティティベースのポリシー

アイデンティティベースのポリシーは、アイデンティティ (ユーザー、グループ、またはロール) 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、アイデンティティがどのリソースに対してどのような条件下でどのようなアクションを実行できるかを制御します。アイデンティティベースポリシーの作成方法については、IAM ユーザーガイド の カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する 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、インラインポリシー (単一の ID に直接埋め込む) または管理ポリシー (複数の ID にアタッチされたスタンドアロンポリシー) にすることができます。管理ポリシーとインラインポリシーのいずれ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いずれかを選択する」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、リソースに添付する JSON ポリシードキュメントです。例としては、IAM ロール信頼ポリシーや 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制御できます。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。

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では、IAM の AWS マネージドポリシーを使用できません。

その他のポリシータイプ

AWS は、より一般的なポリシータイプによって付与されるアクセス許可の上限を設定できる追加のポリシータイプをサポートしています。

- アクセス許可の境界 – アイデンティティベースのポリシーで IAM エンティティに付与することのできるアクセス許可の数の上限を設定します。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 (SCP) - AWS Organizations内の組織または組織単位の最大のアクセス許可を指定します。詳細については、「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。
- リソースコントロールポリシー (RCP) – は、アカウント内のリソースで利用できる最大数のアクセス許可を定義します。詳細については、「AWS Organizations ユーザーガイド」の「リソースコントロールポリシー (RCP)」を参照してください。
- セッションポリシー – ロールまたはフェデレーションユーザーの一時セッションを作成する際にパラメータとして渡される高度なポリシーです。詳細については、「IAM ユーザーガイド」の「セッションポリシー」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アクセス許可を理解するのがさらに難しくなります。が複数のポリシータイプが関与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、「IAM ユーザーガイド」の「ポリシー評価ロジック」を参照してください。

How AWS Storage Gateway と IAM の連携

IAM を使用して SGW AWS へのアクセスを管理する前に、SGW で使用できる IAM AWS 機能を確認してください。

AWS Storage Gatewayで使用できる IAM 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)	はい
ACL	なし

IAM 機能	AWS SGW サポート
ABAC (ポリシー内のタグ)	部分的
一時認証情報	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	はい

AWS SGW 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の概要については、「IAM ユーザーガイド」のAWS 「IAM と連携する のサービス」を参照してください。

SGW AWS のアイデンティティベースのポリシー

アイデンティティベースのポリシーのサポート: あり

アイデンティティベースポリシーは、IAM ユーザー、ユーザーグループ、ロールなど、アイデンティティにアタッチできる JSON 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ポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」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、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。JSON ポリシーで使用できるすべての要素について学ぶには、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

SGW AWS 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。

SGW AWS 内のリソースベースのポリシー

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、リソースに添付する 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には例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。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、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、全体のアカウント、または別のアカウントの IAM エンティティを、リソースベースのポリシーのプリンシパルとして指定します。詳細については、IAM ユーザーガイドのIAM でのクロスアカウントリソースアクセスを参照してください。

SGW AWS のポリシーアクション

ポリシーアクションのサポート: あり

管理者は JSON AWS ポリシーを使用して、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` 要素にはポリシー内の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が記述されます。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アクセス許可を付与するポリシーで使用されます。

AWS SGW アクションのリストを確認するには、「サービス認可リファレンス」の「Actions Defined by AWS Storage Gateway」を参照してください。

SGW AWS の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"
         ]
```

AWS SGW アイデンティティベースのポリシーの例を表示するには、「」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。

SGW AWS のポリシーリソース

ポリシーリソースのサポート: あり

管理者は JSON AWS ポリシーを使用して、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。

`Resource` JSON ポリシー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。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。リソースレベルのアクセス許可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": "*"
```

SGW リソースタイプとその ARN AWS のリストを確認するには、「サービス認可リファレンス」のAWS Storage Gatewayで定義されるリソース」を参照してください。 ARNs 各リソースの ARN を指定できるアクションについては、「Actions Defined by AWS Storage Gateway」を参照してください。

AWS SGW アイデンティティベースのポリシーの例を表示するには、「」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。

SGW AWS のポリシー条件キー

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 JSON AWS ポリシーを使用して、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` 要素は、定義された基準に基づいてステートメントが実行される時期を指定します。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して、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。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「グローバル条件コンテキストキー」を参照してください。

AWS SGW 条件キーのリストを確認するには、「サービス認可リファレンス」の「Condition Keys for AWS Storage Gateway」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、「Actions Defined by AWS Storage Gateway」を参照してください。

AWS SGW アイデンティティベースのポリシーの例を表示するには、「」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。

SGW AWS ACLs

ACL のサポート: なし

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするためのアクセス許可を持つかを制御します。ACL 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は使用しません。

SGW AWS での ABAC

ABAC (ポリシー内のタグ) のサポート: 一部

属性ベースのアクセスコントロール (ABAC) は、タグと呼ばれる属性に基づいてアクセス許可を定義する認可戦略です。IAM エンティティと AWS リソースにタグをアタッチし、プリンシパルのタグがリソースのタグと一致するときにオペレーションを許可するように ABAC ポリシーを設計できます。

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。

ABAC の詳細については、「IAM ユーザーガイド」の「ABAC 認可でアクセス許可を定義する」を参照してください。ABAC をセットアップする手順を説明するチュートリアルについては、「IAM 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」を参照してください。

SGW AWS での一時的な認証情報の使用

一時的な認証情報のサポート: あり

一時的な認証情報は、 AWS リソースへの短期的なアクセスを提供し、フェデレーションまたは切り替えロールを使用する場合に自動的に作成されます。 AWS では、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お勧めします。詳細については、「IAM ユーザーガイド」の「IAM の一時的な認証情報」および「AWS のサービス と IAM との連携」を参照してください。

SGW AWS の転送アクセスセッション

転送アクセスセッション (FAS) のサポート: あり

転送アクセスセッション (FAS) は、 を呼び出すプリンシパルのアクセス許可と AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストをリクエストする を使用します。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。

SGW AWS のサービスロール

サービスロールのサポート: あり

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、IAM ユーザーガイドの AWS のサービスに許可を委任するロールを作成する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、SGW AWS 機能が破損する可能性があります。SGW AWS が指示する場合にのみ、サービスロールを編集します。

SGW AWS のサービスにリンクされたロール

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、「IAM と提携するAWS のサービス」を参照してください。表の「サービスリンクロール」列に Yes と記載されたサービスを見つけます。サービスにリンクされた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 SGW AWS リソースを作成または変更するアクセス許可はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。

これらのサンプルの JSON ポリシードキュメントを使用して IAM 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、「IAM ユーザーガイド」の「IAM ポリシーを作成する (コンソール)」を参照してください。

各リソースタイプの ARN の形式など、SGW AWS 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、「サービス認可リファレンス」の「Actions, Resources, and Condition Keys for AWS Storage Gateway」を参照してください。 ARNs

トピック

- ポリシーに関するベストプラクティス
- SGW AWS コンソールの使用
- 自分の権限の表示をユーザーに許可する

ポリシーに関するベストプラクティス

ID ベースのポリシーは、アカウント内で誰かが SGW AWS リソースを作成、アクセス、または削除できるかどうかを決定します。これらのアクションでは、 AWS アカウントに費用が発生する場合があります。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の付与を開始するには、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することで、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、IAM ユーザーガイド の AWS マネージドポリシー または ジョブ機能のAWS マネージドポリシー を参照してください。

- 最小特権を適用する – 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 を使用して許可を適用する方法の詳細については、IAM ユーザーガイド の IAM でのポリシーとアクセス許可 を参照してください。
- IAM ポリシーで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、アクションやリソースへのアクセスを制限できます。たとえば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、サービスアクションが などの特定の を通じて使用されている場合に 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 CloudFormation。詳細については、IAM ユーザーガイド の IAM JSON ポリシー要素:条件 を参照してください。
- IAM アクセスアナライザー を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM アクセスアナライザー は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、IAM ユーザーガイド の IAM Access Analyzer でポリシーを検証する を参照してください。
- 多要素認証 (MFA) を要求する – 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、MFA をオンにしてセキュリティを強化します。API オペレーションが呼び出されるときに MFA を必須にするには、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 を使用した安全な API アクセス を参照してください。

IAM で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 IAM でのセキュリティのベストプラクティス を参照してください。

SGW AWS コンソールの使用

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のセットが必要です。これらのアクセス許可により、 の SGW AWS リソースの詳細を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 AWS API 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。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が許可されます。

ユーザーとロールが引き続き SGW AWS コンソール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、「IAM ユーザーガイド」の「ユーザーへのアクセス許可の追加」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、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI または AWS API 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。

```
{
    "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": "*"
        }
    ]
}
```

Troubleshooting AWS Storage Gateway のアイデンティティとアクセス

次の情報は、 AWS SGW と IAM の使用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。

トピック

- SGW AWS でアクションを実行する権限がない
- iam:PassRole を実行する権限がありません
- 自分の 以外のユーザーに SGW AWS リソース AWS アカウント へのアクセスを許可したい

SGW AWS でアクションを実行する権限がない

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、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。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用して、ある *my-example-widget* リソースに関する詳細情報を表示しようとしたことを想定して、その際に必要な sgw:*GetWidget* アクセス許可を持っていない場合に発生するものです。

```
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:PassRole を実行する権限がありません

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 SGW AWS 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。

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アクセス許可が必要です。

以下の例のエラーは、 `marymajor` という IAM ユーザーがコンソールを使用して AWS SGW でアクションを実行しようする場合に発生します。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アクセス許可が必要です。Mary には、ロールをサービスに渡すアクセス許可がありません。

```
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。サインイン資格情報を提供した担当者が管理者です。

> **Important**
>
> Storage Gateway は、`iam:PassRole` ポリシーアクションを使用して渡される既存のサービスロールを引き受けることができますが、`iam:PassedToService` コンテキストキーを使用してアクションを特定のサービスに制限するIAM ポリシーはサポートされていません。詳細については、「AWS Identity and Access Management ユーザーガイド」の以下のトピックを参照してください。
>
> - IAM: IAM ロールを特定の AWS サービスに渡す
> - AWS サービスにロールを渡すアクセス許可をユーザーに付与する
> - IAM で使用できるキー

自分の 以外のユーザーに SGW AWS リソース AWS アカウント へのアクセスを許可したい

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 (ACL) 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、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- SGW がこれらの機能をサポートしているかどうかを確認するには、 AWS 「」を参照してくださいHow AWS Storage Gateway と IAM の連携。
- 所有 AWS アカウント 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、「IAM 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」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、IAM 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」を参照してください。
- ID フェデレーションを介し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 外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可 を参照してください。
- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用方法の違いについては、IAM ユーザーガイド の IAM でのクロスアカウントのリソースへのアクセス を参照してください。

タグを使用してゲートウェイとリソースへのアクセスをコントロールする

ゲートウェイリソースとアクションへのアクセスを制御するには、タグに基づいて AWS Identity and Access Management (IAM) ポリシーを使用できます。コントロールは 2 つの方法で提供できます。

1. それらのリソースのタグに基づいて、ゲートウェイリソースへのアクセスをコントロールします。
2. IAM リクエストの条件でどのタグを渡せるかをコントロールする。

タグを使用してアクセスをコントロールする方法については、「タグを使用したアクセスのコントロール」を参照してください。

リソースのタグに基づいてアクセスをコントロールする

ユーザーまたはロールがゲートウェイリソースで実行できるアクションをコントロールするには、ゲートウェイリソースでタグを使用できます。たとえば、リソースのタグのキーと値のペアに基づいて、ファイルゲートウェイリソースに対する特定の API オペレーションを許可または拒否することが必要な場合があります。

以下の例では、ユーザーまたはロールに、すべてのリソースに対する `ListTagsForResource`、`ListFileShares`、および `DescribeNFSFileShares` アクションの実

行を許可しています。このポリシーは、リソースのタグのキーが allowListAndDescribe に設定され、値が yes に設定されている場合にのみ適用されます。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:ListTagsForResource",
                "storagegateway:ListFileShares",
                "storagegateway:DescribeNFSFileShares"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/allowListAndDescribe": "yes"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:*"
            ],
            "Resource": "arn:aws:storagegateway:us-east-1:111122223333:*/*"
        }
    ]
}
```

IAM リクエスト内のタグに基づいてアクセスをコントロールする

IAM ユーザーがゲートウェイリソースできることをコントロールするには、タグに基づく IAM ポリシーの条件を使用できます。たとえば、リソースの作成時に指定されたタグに基づいて特定の API オペレーションを実行する機能を許可または拒否するポリシーを作成できます。

以下の例の最初のステートメントでは、ゲートウェイの作成時に指定されたタグのキーと値のペアが **Department** と **Finance** の場合にのみ、ゲートウェイの作成をユーザーに許可しています。API オペレーションを使用するときに、このタグをアクティベーションリクエストに追加します。

2 番目のステートメントでは、ゲートウェイのタグのキーと値のペアが **Department** および **Finance** に一致する場合にのみ、ゲートウェイでネットワークファイルシステム (NFS) またはサーバーメッセージブロック (SMB) のファイル共有を作成することをユーザーに許可しています。さらに、ユーザーはファイル共有にタグを追加すること、そのタグのキーと値のペアが **Department** および **Finance** であることが必要です。ファイル共有を作成するときに、そのタグをファイル共有に追加します。AddTagsToResource または RemoveTagsFromResource オペレーションに対するアクセス許可がないため、ユーザーはゲートウェイまたはファイル共有でこれらのオペレーションを実行できません。

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "storagegateway:ActivateGateway"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/Department":"Finance"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":[
            "storagegateway:CreateNFSFileShare",
            "storagegateway:CreateSMBFileShare"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/Department":"Finance",
               "aws:RequestTag/Department":"Finance"
            }
         }
      }
   ]
```

```
}
```

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。これらには、SOC、PCI、ISO、FedRAMP、HIPAA、MTCS、C5、K-ISMS、ENS High、OSPAR、HITRUST CSF が含まれます。

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AWS プログラムによる対象範囲内のサービスコンプライアンス」を参照してください。一般的な情報については、AWS 「 Compliance ProgramsAssurance」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、「Downloading Reports in AWS Artifact」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デプロイする手順について説明します AWS。
- 「Architecting for HIPAA Security and Compliance」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」のルールを使用してリソースを評価する – この AWS Config サービスは、リソース設定が内部プラクティス、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 CSPM – 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 および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、データセンターがクラスター化されている世界中の物理的な場所です。論理的なデータセンターの各グループはアベイラビリティーゾーン (AZ) と呼ばれます。各 AWS リージョン は、1 つの地理的領域内にある、少なくとも 3 つの隔離され、物理的にも分かれている AZ で成り立っています。多くの場合、リージョンを単一のデータセンターとして定義する他のクラウドプロバイダーとは異なり、すべての の複数の AZ 設計 AWS リージョン には明確な利点があります。各 AZ には独立した電源、冷却、物理的セキュリティがあり、冗長で超低レイテンシーのネットワークを介して接続されます。デプロイで高可用性に重点を置く必要がある場合は、耐障害性を高めるために、複数の AZ でサービスとリソースを設定することができます。

AWS リージョン は、最高レベルのインフラストラクチャセキュリティ、コンプライアンス、データ保護を満たしています。AZ 間のトラフィックはすべて暗号化されます。AZ 間の同期レプリケーションを実行するために、十分なネットワークパフォーマンスが提供されます。AZ を使用すると、高可用性のためにサービスとリソースをパーティショニングすることが容易になります。デプロイを AZ 間でパーティショニングすると、リソースは停電、落雷、竜巻、地震などの問題から、より良く隔離され保護されます。AZ は他の AZ から物理的に意味のある距離で離れていますが、互いにすべて 100 km (60 マイル) 以内に配置されています。

AWS リージョン および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 は、 AWS グローバルインフラストラクチャに加えて、VMware vSphere High Availability (VMware HA) をサポートし、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、VMware vSphere High Availability と Storage Gateway の使用を参照してください。

インフラストラクチャセキュリティ in AWS Storage Gateway

マネージドサービスである AWS Storage Gateway は、Security Pillar - AWS Well-Architected Framework で説明されている AWS グローバルネットワークセキュリティ手順で保護されています。

AWS 公開された API コールを使用して、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。また、一時的ディフィー・ヘルマン Ephemeral Diffie-Hellman (DHE) や Elliptic Curve Ephemeral Diffie-Hellman

(ECDHE) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートもクライアントでサポートされている必要があります。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。

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

> **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能力に影響を与える可能性があります。
>
> AWS は CVEs を定期的にレビュー、分析、修復します。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 に組み込まれます。これらの修正は、通常スケジュールされたメンテナンス期間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、「コンソールを使用したゲートウェイの更新の管理」を参照してください AWS Storage Gateway。

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多く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 セキュリティベストプラクティス」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 のサービスによって実行されたアクションを記録する AWS サービスである と統合されています。CloudTrail は、Storage Gateway に対するすべての API コールをイベントとしてキャプチャします。キャプチャされる呼び出しには、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。証跡を作成すると、Storage Gateway のイベン

トなど、Amazon S3 バケットへの CloudTrail イベントの継続的デリバリーを有効にできます。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。CloudTrail で収集された情報により、Storage Gateway に対するリクエスト、リクエスト元の IP アドレス、リクエストの実行者、リクエストの日時などの詳細を特定できます。

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

CloudTrail での Storage Gateway の情報

CloudTrail は、 AWS アカウントの作成時に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 イベント履歴 で、その他の AWS サービスのイベントと共に CloudTrail イベントに記録されます。 AWS アカウントで最近のイベントを表示、検索、ダウンロードできます。詳細については、CloudTrail イベント履歴での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、 AWS アカウントのイベントの継続的な記録については、証跡を作成します。証跡を作成すれば、CloudTrail でログファイルを 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口グに記録し、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さらに分析して処理するように他の 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 がサポートするサービスと統合
- CloudTrail 用 Amazon SNS 通知の構成
- 複数のリージョンから CloudTrail ログファイルを受け取るおよび複数のアカウントから CloudTrail ログファイルを受け取る

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。たとえば、`ActivateGateway`、`ListGateways`、`ShutdownGateway` の各アクションを呼び出すと、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、リクエストの生成者に関する情報が含まれます。アイデンティティ情報は、以下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) ユーザー認証情報を使用して行われたかどうか。

- 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について

証跡とは、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 のログファイルは、単一か複数のログエントリを含みます。イベントは、任意の出典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。

以下の例は、 アクションを示す CloudTrail ログエントリです。

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

次は、ListGateways アクションを示す CloudTrail ログエントリの例です。

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

Storage Gateway のデプロイに関する問題のトラブルシューティング

以下は、ゲートウェイ、ホストプラットフォーム、ファイルシステム、高可用性、データ復旧、スナップショットに関連するベストプラクティスとトラブルシューティングの問題についての情報です。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、サポートされている仮想化プラットフォームにデプロイされたゲートウェイにつて述べています。高可用性の問題のトラブルシューティング情報には、VMware vSphere High Availability (HA) プラットフォームで実行されるゲートウェイが含まれます。

トピック

- トラブルシューティング: ゲートウェイのオフラインに関する問題 - Storage Gateway コンソールでゲートウェイがオフラインになる原因となる問題を診断する方法について説明します。
- トラブルシューティング: Active Directory に関する問題 - ファイルゲートウェイを Microsoft Active Directory ドメインに参加させようとする `NETWORK_ERROR`、`TIMEOUT`、`ACCESS_DENIED` などのエラーメッセージが表示された場合の対処方法について説明します。
- 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に関する問題 - Storage Gateway をアクティベートしようとして内部エラーメッセージが表示された場合の対処方法について説明します。
- トラブルシューティング: オンプレミスゲートウェイに関する問題 - オンプレミスゲートウェイの操作で発生する可能性がある一般的な問題と、 がゲートウェイに接続 サポート してトラブルシューティングを支援する方法について説明します。
- トラブルシューティング: Microsoft Hyper-V セットアップに関する問題 - 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について説明します。
- トラブルシューティング: Amazon EC2 ゲートウェイに関する問題 - Amazon EC2 にデプロイされたゲートウェイを操作するときに発生する可能性のある一般的な問題に関する情報を確認します。
- トラブルシューティング: ハードウェアアプライアンスに関する問題 - AWS Storage Gatewayハードウェアアプライアンスで発生する可能性のある問題を解決する方法について説明します。
- トラブルシューティング: ファイルゲートウェイに関する問題 - ファイルゲートウェイの CloudWatch Log に表示されたエラーの原因やヘルス通知について理解するのに役立つ情報が示されます。

- トラブルシューティング: 高可用性に関する問題 - VMware HA 環境にデプロイされているゲートウェイで問題が発生した場合の対処方法について説明します。

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となる

次のトラブルシューティング情報を使用して、 AWS Storage Gateway コンソールにゲートウェイがオフラインであると表示された場合にどう対処すべきかを判断します。

ゲートウェイは、次のいずれかの理由でオフラインと表示されている可能性があります。

- 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、あるいは失敗しました。

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の確認

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、またはファイアウォールの背後にゲートウェイを配置した場合は、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てください。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、「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。

ゲートウェイのトラフィックの継続的な SSL またはディープパケット検査の確認

ゲートウェイと の間のネットワークトラフィックに対して SSL またはディープパケット検査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。

再起動またはソフトウェア更新後の IOWaitPercent メトリクスの確認

再起動またはソフトウェアの更新後、ファイルゲートウェイの `IOWaitPercent` メトリクスが 10 以上であるかどうかを確認します。その場合、インデックスキャッシュを RAM に再構築している間、ゲートウェイの応答が遅くなる可能性があります。詳細については、「トラブルシューティング: CloudWatch メトリクスの使用」を参照してください。

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の確認

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、ゲートウェイが想定外にシャットダウンし、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アクセス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、「ベストプラクティス: データの復旧」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の問題の確認

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、またはサイズ変更された場合や、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。

ハイパーバイザーホストから動作キャッシュディスクが削除された場合:

1. ゲートウェイをシャットダウンします。
2. ディスクを再度追加します。

> **Note**
>
> ディスクは必ず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か、置き換えられたか、またはサイズが変更された場合:

- 「既存の S3 ファイルゲートウェイを新しいインスタンスに置き換える」で説明されている方法 2 の手順に従って、新しいゲートウェイを設定し、 AWS クラウドからキャッシュディスク情報を再ダウンロードします。

トラブルシューティング: ゲートウェイの Active Directory への参加に関する問題

ファイルゲートウェイを Microsoft Active Directory ドメインに参加させようとしたときに、NETWORK_ERROR、TIMEOUT、ACCESS_DENIED、などのエラーメッセージが表示された場合の対処方法を判断したいとき、次のトラブルシューティング情報を利用します。

これらのエラーを解決するには、次の確認事項と設定を実行します。

nping テストを実行して、ゲートウェイがドメインコントローラーに到達できることを確認する

nping テストを実行するには:

1. オンプレミスゲートウェイの場合はハイパーバイザー管理ソフトウェア (VMware、Hyper-V、または KVM) を使用するか、または Amazon EC2 ゲートウェイの場合は ssh を使用して、ゲートウェイローカルコンソールに接続します。
2. 対応する数字を入力して [ゲートウェイコンソール] を選択し、h を入力して使用可能なすべてのコマンドを一覧表示します。Storage Gateway 仮想マシンとドメイン間の接続をテストするには、次のコマンドを実行します。

   ```
   nping -d corp.domain.com -p 389 -c 1 -t tcp
   ```

   > **Note**
   >
   > corp.domain.com を Active Directory ドメイン DNS 名に置き換え、389 をご利用の環境の LDAP ポートに置き換えます。
   > ファイアウォール内で必要なポートが開放されていることを確認します。

以下は、ゲートウェイがドメインコントローラーに到達できた場合の nping テスト成功例です。

```
nping -d corp.domain.com -p 389 -c 1 -t tcp

Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2022-06-30 16:24 UTC
SENT (0.0553s) TCP 10.10.10.21:9783 > 10.10.10.10:389 S ttl=64 id=730 iplen=40
 seq=2597195024 win=1480
RCVD (0.0556s) TCP 10.10.10.10:389 > 10.10.10.21:9783 SA ttl=128 id=22332 iplen=44
 seq=4170716243 win=8192 <mss 8961>
```

```
Max rtt: 0.310ms | Min rtt: 0.310ms | Avg rtt: 0.310ms
Raw packets sent: 1 (40B) | Rcvd: 1 (44B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 1.09 seconds<br>
```

以下は、送信先corp.domain.comへの接続がない場合や、送信先から応答がない場合の nping テストの例です。

```
nping -d corp.domain.com -p 389 -c 1 -t tcp

Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2022-06-30 16:26 UTC
SENT (0.0421s) TCP 10.10.10.21:47196 > 10.10.10.10:389  S ttl=64 id=30318 iplen=40
 seq=1762671338 win=1480

Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Raw packets sent: 1 (40B) | Rcvd: 0 (0B) | Lost: 1 (100.00%)
Nping done: 1 IP address pinged in 1.07 seconds
```

Amazon EC2 ゲートウェイインスタンスの VPC に設定されている DHCP オプションを確認する

ファイルゲートウェイが Amazon EC2 インスタンスで実行されている場合は、DHCP オプションセットが正しく構成され、ゲートウェイインスタンスを含む Amazon 仮想プライベートクラウド (VPC) にアタッチされていることを確認する必要があります。詳細については、「Amazon VPC DHCP オプションセット」を参照してください。

dig クエリを実行して、ゲートウェイがドメインを解決できることを確認する

ドメインがゲートウェイによって解決されない場合、ゲートウェイはドメインに参加できません。

dig クエリを実行するには:

1. オンプレミスゲートウェイの場合はハイパーバイザー管理ソフトウェア (VMware、Hyper-V、または KVM) を使用するか、または Amazon EC2 ゲートウェイの場合は ssh を使用して、ゲートウェイローカルコンソールに接続します。
2. 対応する数字を入力して [ゲートウェイコンソール] を選択し、h を入力して使用可能なすべてのコマンドを一覧表示します。ゲートウェイがドメインを解決できるかどうかをテストするには、次のコマンドを実行します。

```
dig -d corp.domain.com
```

> **Note**
>
> corp.domain.com を Active Directory ドメイン DNS 名に置き換えます。

以下に、正常な応答の例を示します。

```
; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.amzn2.5.2 <<>> corp.domain.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24817
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;corp.domain.com.        IN    A

;; ANSWER SECTION:
corp.domain.com.    600    IN    A    10.10.10.10
corp.domain.com.    600    IN    A    10.10.20.10

;; Query time: 0 msec
;; SERVER: 10.10.20.228#53(10.10.20.228)
;; WHEN: Thu Jun 30 16:36:32 UTC 2022
;; MSG SIZE  rcvd: 78
```

ドメインコントローラーの設定とロールを確認する

ドメインコントローラーが読み取り専用に設定されていないこと、およびドメインコントローラーにコンピュータが参加するのに十分なロールがあることを確認します。これをテストするには、ゲートウェイ VM と同じ VPC サブネットの他のサーバーをドメインに参加させてみてください。

ゲートウェイが最寄りのドメインコントローラーに参加していることを確認する

ベストプラクティスとしては、ゲートウェイアプライアンスに地理的に近いドメインコントローラーにゲートウェイを参加させることを推奨します。ネットワークレイテンシーが原因でゲートウェイア

プライアンスが 20 秒以内にドメインコントローラーと通信できない場合、ドメイン参加プロセスはタイムアウトすることがあります。たとえば、ゲートウェイアプライアンスが米国東部 (バージニア北部) にあり、 AWS リージョン ドメインコントローラーがアジアパシフィック (シンガポール) にある場合、プロセスはタイムアウトすることがあります AWS リージョン。

> **Note**
>
> デフォルトのタイムアウト値を 20 秒に増やすには、 AWS Command Line Interface (AWS CLI) で join-domain コマンドを実行し、時間を増やす`--timeout-in-seconds`オプションを含めることができます。また、JoinDomain API コールを使用し、`TimeoutInSeconds` パラメータを含めてタイムアウト時間を増やすことができます。最大タイムアウト値は 3,600 秒です。
>
> AWS CLI コマンドの実行時にエラーが発生した場合は、最新バージョンを使用していることを確認してください AWS CLI 。

Active Directory がデフォルトの組織単位 (OU) に新しいコンピュータオブジェクトを作成することを確認する

Microsoft Active Directory に、デフォルトの OU 以外の場所に新しいコンピュータオブジェクトを作成するグループポリシーオブジェクトがないことを確認します。ゲートウェイを Active Directory ドメインに参加させる前に、新しいコンピュータオブジェクトがデフォルトの OU に存在している必要があります。一部の Active Directory 環境は、新しく作成されたオブジェクトに対して異なる OU を持つようにカスタマイズされています。ゲートウェイ VM の新しいコンピュータオブジェクトがデフォルトの OU に存在することを確認するには、ゲートウェイをドメインに参加させる前に、ドメインコントローラーでコンピュータオブジェクトを手動で作成してみてください。 AWS CLIを使用して join-domain コマンドを実行することもできます。その場合は、`--organizational-unit` のオプションを指定します。

> **Note**
>
> コンピュータオブジェクトを作成するプロセスは、事前ステージングと呼ばれます。

ドメインコントローラーのイベントログの確認

前のセクションで説明した他のすべての確認事項と設定を試した後にゲートウェイをドメインに参加させられない場合は、ドメインコントローラーのイベントログを調べることを推奨します。ドメイン

コントローラーのイベントビューワーにエラーがないか確認します。ゲートウェイクエリがドメインコントローラーに到達していることを確認します。

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。クライアントによって送信される受信アクティベーションリクエストは、ポート 80 経由で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。

AWS Storage Gatewayをアクティベート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は、次のトラブルシューティング情報を使用して対処方法を決定します。

> **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 AMI を使用するゲートウェイをアクティベートしようとすると、内部エラーが表示されます。
> - AMI をダウンロードする前に、デプロイする正しいゲートウェイタイプを選択していることを確認してください。各ゲートウェイタイプの .ova ファイルと AMI は異なっており、互換性がありません。

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ベート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ベート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。

必要なポートの確認

オンプレミスにデプロイされたゲートウェイの場合、ポートがローカルファイアウォールで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内にある必要があります。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の場合) 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 EC2 にデプロイされたゲートウェイの場合) に SSH 接続できます。次に、ネットワーク接続テストを実行します。テストで [PASSED] が返されることを確認します。詳細については、「ゲートウェイのネットワーク接続のテスト」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 admin で、デフォルトのパスワードは password です。

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た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に干渉する可能性があります。SSL 証明書がアクティベーションエンドポイントでの所定の内容から変更されると、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**
>
> *region* を に置き換えます AWS リージョン。

SSL 検査が進行中でない場合、コマンドは次のような応答を返します。

```
$ 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、応答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 証明書を認識した場合にのみ 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される必要があります。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の確認

過剰な時刻のずれがあると、SSL ハンドシェイクエラーを引き起こす可能性があります。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。時刻のずれは 60 秒以下にする必要があります。詳細については、「ゲートウェイ VM 時刻の同期」を参照してください。

[システム時刻管理] 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 と TCP 123 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。

- time.aws.com
- 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ベートする際のエラーの解決

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ベート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。

必要なポートの確認

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 EC2 にデプロイされたゲートウェイの場合) 内の必要なポートが開いていることを確認します。Storage Gateway VPC エンドポイントにゲートウェイを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、「Storage Gateway 用の VPC エンドポイントの作成」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 アドレス範囲からのトラフィックを必要なポート経由で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検証します。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 コマンドを実行できます。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 (AZ) を指定していない最初の DNS 名でテストを実行できます。例えば、次の telnet コマンドは、DNS 名 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 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がゲートウェイから Storage Gateway Amazon VPC エンドポイントに送信されたパケットを変更しないことの確認

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に干渉する可能性があります。SSL 証明書がアクティベーションエンドポイントでの所定の内容から変更されると、SSL ハンドシェイクは失敗します。SSL 検査が進行中で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
```

SSL 検査が進行中でない場合、コマンドは次のような応答を返します。

```
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、応答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 証明書を認識した場合にのみ 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。そのような検査には、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の確認

過剰な時刻のずれがあると、SSL ハンドシェイクエラーを引き起こす可能性があります。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。時刻のずれは 60 秒以下にする必要があります。詳細については、「ゲートウェイ VM 時刻の同期」を参照してください。

[システム時刻管理] 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 と TCP 123 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て関連するセキュリティグループ設定の確認

アクティベーションの前に、Amazon EC2 の HTTP プロキシがオンプレミスゲートウェイ VM でポート 3128 の Squid プロキシとして設定されているかどうかを確認します。この場合は次の点を確認します。

- Amazon EC2 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 上の Squid プロキシトラフィックを許可する必要があります。
- Amazon EC2 VPC 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 EC2 の HTTP プロキシの IP アドレスからポート 1026 ~ 1028、1031、2222、443 へのトラフィックを許可する必要があります。

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ベートし、同じ VPC に Storage Gateway VPC エンドポイントがある場合のエラーの解決

同じ VPC 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ベートする際の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。

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の確認

[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 VPC からパブリックエンドポイントへのゲートウェイをアクティベート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、[このエンドポイントを有効にする] を選択します。
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。

トラブルシューティング: オンプレミスゲートウェイに関する問題

オンプレミスゲートウェイの操作で発生する可能性がある一般的な問題と、トラブルシューティングに役立つゲートウェイへの接続を サポート に許可する方法については、以下を参照してください。

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起こりう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。

問題	実行するアクション
	• VMware ESXi の場合、VM の IP アドレスは vSphere クライアントの [概要] タブにあります。 • 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は、 • 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。 • 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。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。

問題	実行するアクション
Storage Gateway マネジメントコンソールで [アクティブ化に進む] 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。接続していない場合は、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、「ゲートウェイのネットワーク接続をテストする」を参照してください。 • ホストの時間が正しく、その時間を Network Time Protocol (NTP) サーバーに自動的に同期させるように設定されていて、ゲートウェイ VM の時間が正しいことを確認します。ハイパーバイザーホストと VM の時間の同期に関する詳細については、ゲートウェイの Network Time Protocol (NTP) サーバーの設定 を参照してください。 • 以上の手順を実行したら、Storage Gateway コンソールと [ゲートウェイのセットアップとアクティブ化] 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。 • VM に 16 GB 以上の RAM があることを確認します。16 GB 未満の RAM がある場合、ゲートウェイの割り当ては失敗します。詳細については、「ファイルゲートウェイのセットアップ要件」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の復元中に帯域幅の競合を回避 AWS 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、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、「パフォーマンスと最適化」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 [ゲートウェイ] 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。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 [ゲートウェイ] タブにある [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 ESXi の場合、VM の IP アドレスは vSphere クライアントの [概要] タブにあります。
	  • 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ネットワーク接続をテストする。
	• ハイパーバイザー管理クライアントでゲートウェイのネットワークアダプタ設定をチェックし、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。
	• ゲートウェイローカルコンソールでゲートウェイのネットワークアダプタ設定を確認します。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。
	
	Amazon CloudWatch コンソールにゲートウェイとの双方向のスループットを表示できます。ゲートウェイ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パフォーマンスと最適化。

問題	実行するアクション
Microsoft Hyper-V への Storage Gateway のインポート (デプロイ) に問題がある。	「トラブルシューティング: Microsoft Hyper-V セットアップ」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。
「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、 サポートにお問い合わせください。

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 サポート アクセスを有効にする

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 サポート へのアクセスの許可など、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 サポート へのアクセスはオフになっています。このアクセスは、ホストのローカルコンソールを通じて有効にできます。ゲートウェイ サポート 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、サポートサーバーに接続します。

ゲートウェイ サポート へのアクセスを有効にするには

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、「VMware ESXi 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。
   - 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。

- ゲートウェイでパブリックエンドポイントを使用している場合は、[AVAILABLE COMMANDS] (利用可能なコマンド) ウィンドウに「**open-support-channel**」と入力して、Storage Gateway のカスタマーサポートに接続します。 AWSへのサポートチャネルを開くことがでるように、TCP ポート 22 を許可します。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、[AVAILABLE COMMANDS (利用可能なコマンド)] ウィンドウで「**open-support-channel**」と入力します。ゲートウェイがアクティベートされていない場合は、Storage Gateway のカスタマーサポートに接続する VPC エンドポイントまたは IP アドレスを指定します。 AWSへのサポートチャネルを開くことがでるように、TCP ポート 22 を許可します。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**
>
> チャネル番号は Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ポート番号ではありません。代わりに、ゲートウェイが Storage Gateway サーバーへの Secure Shell (SSH) (TCP 22) 接続を作成し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、 サポート がトラブルシューティングのサポートを提供 サポート できるように、サポートサービス番号を に提供します。
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、Storage Gateway 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。

トラブルシューティング: Microsoft Hyper-V セットアップ

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、次のエ	このエラーは、次の原因で発生することがあります。

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。 「仮想マシンのインポート中にサーバーエラーが発生しました。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。Hyper-V を使用して仮想マシンを作成してエクスポートする場合にのみ、仮想マシンをインポートできます。」	• 解凍された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ない場合。[仮想マシンをインポート] ダイアログボックスで指定した場所の最後のパートは、`AWS-Storage-Gateway` となっている必要があります。例えば、次のようになります。 `C:\prod-gateway\unzippedSourceVM\AWS-Storage-Gateway\ .` • ゲートウェイを既にデプロイしていて、[仮想マシンのインポート] ダイアログボックスで、[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、[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、解凍した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。 1 つの解凍されたソースファイルの場所から複数のゲートウェイを作成する場合は、[仮想マシンをコピー] を選択し、[仮想マシンをインポート] ダイアログボックスで、[すべてのファイルを複製] チェックボックスをオンにする必要があります。
ゲートウェイをインポートしようとすると、次のエラーメッセージが表示されます。 「仮想マシンのインポート中にサーバーエラーが発生しました。インポートに失敗しました。インポートタスクは [...] からファイルをコピーできませんでした。ファイルが存在しています。(0x80070050)」	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。この問題を修正するには、[Hyper-V の設定] ダイアログボックスの左側にあるパネルで、[サーバー] の下に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、次のエラーメッセージが表示されます。 「仮想マシンのインポート中にサーバーエラーが発生しました。インポートに失敗しました。インポートが失敗したのは、仮想マシンには新しい識別子が必要だからです。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」。	ゲートウェイをインポートするときは、[仮想マシンをインポート] ダイアログボックスで、[仮想マシンをコピー] を選択し、[すべてのファイルを複製] ボックスをオンにしていることを確認して、VM の新しい固有の ID を作成します。
ゲートウェイ VM を起動しようとすると、次のエラーメッセージが表示されます。 「選択した仮想マシンを起動しようとしたときにエラーが発生しました。子パーティションのプロセッサの設定は、親パーティションと互換性がありません。「AWS-Storage-Gateway」を初期化できませんでした。(仮想マシン ID [...])」	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、「ファイルゲートウェイのセットアップ要件」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、次のエラーメッセージが表示されます。 「選択した仮想マシンを起動しようとしたときにエラーが発生しました。「AWS-Storage-Gateway」を初期化できませんでした。(仮想マシン ID [...]) パーティションの作成に失敗しました。リクエストされたサービスを完了するためのシステムリソースが不足しています。(0x800705AA)」	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、「ファイルゲートウェイのセットアップ要件」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、「ゲートウェイの Network Time Protocol (NTP) サーバーの設定」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。
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。

問題	実行するアクション
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) をオンにすると、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 のドキュメントの「Poor network performance on virtual machines on a Windows Server 2012 Hyper-V host if VMQ is turned on」を参照してください。

トラブルシューティング: Amazon EC2 ゲートウェイに関する問題

以下のセクションでは、Amazon EC2 にデプロイされているゲートウェイを操作しているときに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。オンプレミスのゲートウェイと Amazon EC2 にデプロイされているゲートウェイの違いに関する詳細については、「FSx ファイルゲートウェイ用のデフォルトの Amazon EC2 ホストをデプロイする」を参照してください。

トピック

- しばらくし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ない
- 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したい
- Amazon EC2 ゲートウェイ サポート のトラブルシューティングを支援したい

しばらくし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 が有効になっているか。セキュリティグループのルールの追加に関する詳細については、「Amazon EC2 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。
- 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、インスタンスの [状態] 値が RUNNING になっている必要があります。
- Amazon EC2 インスタンスタイプが「ストレージの要件」で説明されている最低要件を満たしていることを確認します。

問題を修正したら、ゲートウェイを再度アクティベートしてみてください。これを行うには、Storage Gateway コンソールを開き、[Deploy a new Gateway on Amazon 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 AMI を基礎とするインスタンスは、「**`aws-storage-gateway-ami`**」というテキストで始まります。
- Storage Gateway AMI を基礎とするインスタンスが複数ある場合、インスタンスの起動時間を確認してインスタンスを見分けます。

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したい

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、およびその他の問題のトラブルシューティングができます。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。

Amazon EC2 ゲートウェイ サポート 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 サポート へのアクセスの許可など、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 サポート へのアクセスはオフになっています。このアクセスを有効にするには、Amazon EC2 ローカルコンソールを使用します。Amazon EC2 ローカルコンソールは、Secure Shell (SSH) を使用してログインします。SSH を使用して正常にログインするために、インスタンスのセキュリティグループには、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の追加方法については、Amazon EC2 ユーザーガイドの「Amazon EC2 とは」を参照してください。

がゲートウェイ サポート 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の サポート 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 インスタンスを起動するために使用した 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 EC2 ユーザーガイド」の「キーペアのパブリックキーを取得する」を参照してください。*INSTANCE-PUBLIC-DNS-NAME* は、ゲートウェイが実行中の 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) 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て、[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、 サポート Channel コンソールを開きます。
3. 「**h**」と入力して [AVAILABLE COMMANDS (利用可能なコマンド)] ウィンドウを開きます。
4. 次のいずれかを行います。

   - ゲートウェイでパブリックエンドポイントを使用している場合は、[AVAILABLE COMMANDS] (利用可能なコマンド) ウィンドウに「**open-support-channel**」と入力して、Storage Gateway のカスタマーサポートに接続します。 AWSへのサポートチャネル

を開くことができるように、TCP ポート 22 を許可します。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、[AVAILABLE COMMANDS (利用可能なコマンド)] ウィンドウで「**open-support-channel**」と入力します。ゲートウェイがアクティベートされていない場合は、Storage Gateway のカスタマーサポートに接続する VPC エンドポイントまたは IP アドレスを指定します。 AWSへのサポートチャネルを開くことができるように、TCP ポート 22 を許可します。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**
>
> チャネル番号は Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ポート番号ではありません。代わりに、ゲートウェイが Storage Gateway サーバーへの Secure Shell (SSH) (TCP 22) 接続を作成し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、 サポート がトラブルシューティングのサポートを提供 サポート できるように、サポートサービス番号を に提供します。
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、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。

トラブルシューティング: ハードウェアアプライアンスに関する問題

> **Note**
>
> 可用性の終了通知: 2025 年 5 月 12 日をもって、 AWS Storage Gateway ハードウェアアプライアンスは提供されなくなります。 AWS Storage Gateway ハードウェアアプライアンスの既存のお客様は、2028 年 5 月まで引き続き を使用し、サポートを受けることができます。別の方法として、 AWS Storage Gateway サービスを使用して、オンプレミスおよびクラウド内のアプリケーションに事実上無制限のクラウドストレージへのアクセスを許可することもできます。

以下のトピックでは、 AWS Storage Gateway ハードウェアアプライアンスで発生する可能性のある問題と、それらのトラブルシューティングに関する提案について説明します。

トピック

サービスの IP アドレスを特定できない

ご利用の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、[サービスコンソールを開く] を選択します。

工場出荷時設定への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で説明されているように、 AWS Storage Gateway ハードウェアアプライアンスチームにサポートを依頼してください。

リモート再起動を実行するにはどうすればよいですか

アプライアンスをリモートで再起動する必要がある場合は、Dell iDRAC の管理インターフェイスを使用して実行できます。詳細については、Dell Technologies InfoHub 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。

Dell iDRAC のサポートを受けるにはどうすればよいですか

Dell PowerEdge サーバーには、Dell iDRAC 管理インターフェイスが搭載されています。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 - What is the default sign-in credentials for iDRAC?」を参照してください。
- セキュリティ違反を防ぐため、ファームウェアが最新であることを確認します。
- 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、アプライアンスの通常の機能を妨げたりす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

Storage AWS Storage Gateway Gateway ハードウェアアプライアンスのシリアル番号を確認できます。

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:

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
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. リストからハードウェアアプライアンスを選択します。
4. アプライアンスの [詳細] タブで [シリアル番号] フィールドを見つけます。

ハードウェアアプライアンスのサポートの依頼先

ハードウェアアプライアンスのテクニカルサポート AWS については、「」を参照してくださいサポート。

サポート 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ベート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. ハードウェアコンソールのメインページの下部にある [サポートチャネルを開く] を選択し、Enter を押します。

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。例えば、次のようになります。

ステータス: ポート 19599 で開く

3. ポート番号を書き留めて指定します サポート。

トラブルシューティング: ファイルゲートウェイに関する問題

Amazon CloudWatch ロググループにログエントリを書き込むようにファイルゲートウェイを設定できます。その場合は、ファイルゲートウェイのヘルスステータスと、ゲートウェイで発生したエラーに関する通知が表示されます。CloudWatch ログで、これらのエラーおよびヘルス通知に関する情報を参照できます。

以下のセクションでは、各エラーとヘルス通知の原因、およびその問題の修正方法を理解するのに役立つ情報が見つかります。

トピック

エラー: FileMissing

`FileMissing` エラーは `ObjectMissing` エラーに似ており、解決する手順は同じです。指定されたファイルゲートウェイ以外のライターが、指定ファイルを Amazon FSx から削除する

と、FileMissing エラーが発生する場合があります。以降、Amazon FSx へのオブジェクトのアップロード、または Amazon FSx からのオブジェクトの取得は失敗します。

FileMissing エラーを解決するには

1. ファイルの最新のコピーを SMB クライアントのローカルファイルシステムに保存します (ステップ 3 でこのファイルのコピーが必要です)。
2. SMB クライアントを使用して、ファイルゲートウェイからファイルを削除します。
3. SMB クライアントを使用して、ステップ 1 Amazon FSx で保存したファイルの最新バージョンをコピーします。この操作はファイルゲートウェイを介して行います。

エラー: FsxFileSystemAuthenticationFailure

ファイルシステムをアタッチする際に指定した認証情報の有効期限が切れている場合、またはその権限が取り消されている場合、FsxFileSystemAuthenticationFailure エラーが発生することがあります。

FsxFileSystemAuthenticationFailure エラーを解決するには

1. Amazon FSx ファイルシステムのアタッチ時に指定した認証情報がまだ有効であることを確認します。
2. 「Amazon FSx for Windows File Server ファイルシステムのアタッチ」で説明されているように、ユーザーにすべての必要なアクセス許可があることを確認します。

エラー: FsxFileSystemConnectionFailure

Amazon FSx サーバーがゲートウェイマシンからアクセスできない場合、FsxFileSystemConnectionFailure エラーが発生することがあります。

FsxFileSystemConnectionFailure エラーを解決するには

1. すべてのファイアウォールと VPC ルールで、ゲートウェイマシンと Amazon FSx サーバー間の接続が許可されていることを確認します。
2. Amazon FSx サーバーが実行中であることを確認します。

エラー: FsxFileSystemFull

Amazon FSx ファイルシステムに十分な空きディスク容量がない場合、FsxFileSystemFullエラーが発生することがあります。

FsxFileSystemFull エラーを解決するには

- Amazon FSx ファイルシステムのストレージ容量を増やします。

エラー: GatewayClockOutOfSync

ゲートウェイがローカルシステム時刻と AWS Storage Gatewayサーバーによって報告された時刻の差を 5 分以上検出すると、GatewayClockOutOfSyncエラーが発生することがあります。クロック同期の問題は、ゲートウェイと 間の接続に悪影響を及ぼす可能性があります AWS。ゲートウェイクロックが同期していない場合、NFS および SMB の接続で I/O エラーが発生し、SMB ユーザーに認証エラーが発生する可能性があります。

GatewayClockOutOfSync エラーを解決するには

- ゲートウェイと NTP サーバー間のネットワーク設定を確認します。ゲートウェイ VM 時刻の同期と NTP サーバー設定の更新の詳細については、「ゲートウェイのネットワークタイムプロトコル (NTP) サーバーの設定」を参照してください。

エラー: InvalidFileState

指定されたゲートウェイ以外のライターが、指定されたファイル共有内の指定されたファイルを変更すると、InvalidFileState エラーが発生する場合があります。その結果、ファイルゲートウェイのファイルの状態が Amazon FSx のファイルの状態と一致しなくなります。以降、Amazon FSx からのファイルのアップロードまたは取得は失敗する可能性があります。

InvalidFileState エラーを解決するには

1. ファイルの最新のコピーを SMB クライアントのローカルファイルシステムに保存します (ステップ 4 でこのファイルのコピーが必要です)。Amazon FSx 内のファイルのバージョンが最新の場合、そのバージョンをダウンロードします。これを行うには、任意の SMB クライアントを使用して Amazon FSx 共有に直接アクセスします。
2. Amazon FSx でファイルを直接削除します。
3. SMB クライアントを使用して、ゲートウェイからファイルを削除します。

4. SMB クライアントを使用して、ステップ 1 で保存したファイルの最新バージョンをファイルゲートウェイ経由で Amazon FSx にコピーします。

エラー: ObjectMissing

指定されたファイルゲートウェイ以外のライターが、指定ファイルを Amazon FSx から削除すると、`ObjectMissing` エラーが発生する場合があります。以降、Amazon FSx へのオブジェクトのアップロード、または Amazon FSx からのオブジェクトの取得は失敗します。

ObjectMissing エラーを解決するには

1. ファイルの最新のコピーを SMB クライアントのローカルファイルシステムに保存します (ステップ 3 でこのファイルのコピーが必要です)。
2. SMB クライアントを使用して、ファイルゲートウェイからファイルを削除します。
3. SMB クライアントを使用して、ステップ 1 Amazon FSx で保存したファイルの最新バージョンをコピーします。この操作はファイルゲートウェイを介して行います。

エラー: DroppedNotifications

ゲートウェイのルートディスクの空きストレージ容量が 1 GB 未満の場合や、1 分以内に 100 件を超えるヘルス通知が生成された場合、他の予想されるタイプの CloudWatch Log エントリの代わりに`DroppedNotifications` エラーが表示されることがあります。このような状況では、ゲートウェイは予防策として、詳細な CloudWatch ログ通知の生成を停止します。

DroppedNotifications エラーを解決するには

1. Storage Gateway コンソールのゲートウェイの [モニタリング] タブの `Root Disk Usage` メトリクスを確認して、使用可能なルートディスク容量が少ないかどうかを確認します。
2. 使用可能な容量が 1 GB 未満の場合は、ゲートウェイのルートストレージディスクのサイズを増やします。手順については、仮想マシン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 ゲートウェイのルートディスクサイズを増やすには、「Amazon Elastic Compute Cloud ユーザーガイド」の「EBS ボリュームの変更をリクエストする」を参照してください。

> **Note**
>
> AWS Storage Gateway ハードウェアアプライアンスのルートディスクサイズを増やすことはできません。

3. ゲートウェイを再起動します。

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、このイベントが引き起こされることがあります。

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: リブート

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。

再起動の時刻がゲートウェイで設定されたメンテナンス開始時刻から 10 分以内である場合、この再起動の発生はおそらく正常であり、問題の兆候ではありません。メンテナンスの大幅な期間外に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。

トラブルシューティング: Active Directory ドメインに関する問題

FSx ファイルゲートウェイは、Active Directory ドメインに関する問題についての特定のログメッセージを生成しません。ゲートウェイを Active Directory ドメインに参加させられない場合は、次の操作を行います。

- ゲートウェイが読み取り専用ドメインコントローラー (RODC) を使用してドメインに参加しようとしていないことを確認します。
- ゲートウェイが正しい DNS サーバーを使用するように設定されていることを確認します。

例えば、Amazon EC2 ゲートウェイインスタンスを AWSマネージド Active Directory に参加させる場合は、EC2 VPC の DHCP オプションセットが AWSマネージド Active Directory DNS サーバーを指定していることを確認します。

VPC DHCP オプションセットを使用して設定した DNS サーバーは、VPC 内のすべての EC2 インスタンスに提供されます。個々のゲートウェイに DNS サーバーを指定する場合は、そのゲートウェイの EC2 ローカルコンソールを使用して指定できます。

オンプレミスゲートウェイの場合は、VM ローカルコンソールを使用して DNS サーバーを指定します。

- ゲートウェイのローカルコンソールのコマンドプロンプトから次のコマンドを実行して、ゲートウェイのネットワーク接続を確認します。強調表示された変数を、デプロイの実際のドメイン名と IP アドレスに置き換えます。

```
dig -d ExampleDomainName
ncport -d ExampleDomainControllerIPAddress -p 445
ncport -d ExampleDomainControllerIPAddress -p 389
```

- Active Directory サービスアカウントに、必要なアクセス許可があることを確認します。詳細については、「Active Directory サービスアカウントのアクセス許可要件」を参照してください。
- ゲートウェイが正しい組織単位 (OU) に参加していることを確認します。

  ドメインに参加すると、ゲートウェイのゲートウェイ ID をアカウント名 (SGW-1234ADE など) として使用して、デフォルトのコンピュータコンテナ (OU ではない) に Active Directory コンピュータアカウントが作成されます。このアカウントの名前をカスタマイズすることはできません。

  Active Directory 環境に新しいコンピュータオブジェクト用に指定された OU がある場合は、ドメインに参加するときにその OU を指定する必要があります。

  指定された OU に参加しようとしたときにアクセス拒否エラーが発生した場合は、Active Directory ドメイン管理者に確認してください。管理者は、ドメインに参加する前にゲートウェイのコンピュータアカウントを事前にステージングしておく必要がある場合があります。詳細については、「Storage Gateway ファイルゲートウェイを Microsoft Active Directory 認証用のドメインに参加させる際の問題をトラブルシューティングするにはどうすればよいですか?」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のコマンドプロンプトから次のコマンドを実行して、ゲートウェイのホスト名が DNS で解決可能であることを確認します。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。

  ```
  dig -d ExampleHostName -r A
  ```

  ゲートウェイにカスタムホスト名を設定した場合は、IP アドレスを指す DNS A レコードを手動で追加する必要があります。
- ゲートウェイとドメインコントローラー間のネットワークレイテンシーが許容できる範囲で低いことを確認します。ゲートウェイが 20 秒以内にドメインコントローラーから応答を受信しない場合、ドメインに加入するクエリがタイムアウトすることがあります。

  JoinDomain CLI コマンドを使用してゲートウェイをドメインに参加させる場合は、`--timeout-in-seconds` フラグを追加してタイムアウトを最大 3,600 秒に増やすことができます。
- ゲートウェイをドメインに参加させるために使用する Active Directory ユーザーが、そのために必要な権限を持っていることを確認します。

トラブルシューティング: CloudWatch メトリクスの使用

Storage Gateway で Amazon CloudWatch メトリクスを使用する際の問題に対処するためのアクションについては、次を参照してください。

トピック

- ディレクトリの閲覧時にゲートウェイの反応が遅い
- ゲートウェイが応答しない
- Amazon FSx ファイルシステムにファイルが表示されない
- Amazon FSx ファイルシステムに古いスナップショットが表示されない
- ゲートウェイを介した Amazon FSx へのデータ転送速度が遅い
- ゲートウェイへの書き込み時にゲートウェイのバックアップジョブが失敗する、またはエラーが発生する

ディレクトリの閲覧時にゲートウェイの反応が遅い

ls コマンドの実行時またはディレクトリの閲覧時にファイルゲートウェイの反応が遅い場合は、`IndexFetch` および `IndexEviction` の CloudWatch メトリクスを確認します。

- ls コマンドの実行時またはディレクトリの閲覧時に IndexFetch メトリクスが 0 を超えている場合、ファイルゲートウェイは影響を受けるディレクトリの内容に関する情報なしで起動し、FSx for Windows File Server にアクセスする必要がありました。今後そのディレクトリの内容をリストする作業の速度は上がるはずです。
- IndexEviction メトリクスが 0 を超えている場合は、ファイルゲートウェイがその時点でキャッシュとして管理できる上限に達していることを意味します。この場合、ファイルゲートウェイでは、最近最もアクセスしていないディレクトリから一部のストレージ領域を解放して、新しいディレクトリをリストする必要があります。この問題が頻繁に発生し、パフォーマンスへの影響がある場合は、 にお問い合わせください サポート。

  関連する Amazon FSx ファイルシステム サポート の内容と、ユースケースに基づいてパフォーマンスを向上させるための推奨事項について説明します。

ゲートウェイが応答しない

ファイルゲートウェイが応答しない場合は、次の操作を行います。

- 最近再起動またはソフトウェアの更新を行った場合は、IOWaitPercent メトリクスを確認します。このメトリクスは、未処理のディスク I/O リクエストがある場合に、CPU がアイドル状態の時間の割合を示します。場合によっては、この値が高く (10 以上)、サーバーの再起動または更新後に増えていることがあります。このような場合、ファイルゲートウェイによりインデックスのキャッシュが RAM に再構築されるため、低速のルートディスクがゲートウェイのボトルネックになっている可能性があります。より高速な物理ディスクをルートディスクに使用することにより、この問題に対処できます。
- MemUsedBytes メトリクスが MemTotalBytes メトリクスと同じか、ほぼ同じ場合、ファイルゲートウェイで使用可能な RAM が不足しています。ファイルゲートウェイに最低限必要な RAM があることを確認してください。既にある場合は、ワークロードとユースケースに基づいて、ファイルゲートウェイに RAM を追加することを検討してください。

  ファイル共有が SMB の場合は、ファイル共有に接続されている SMB クライアントの数が問題の原因である可能性もあります。任意の時点で接続しているクライアントの数を確認するには、SMBV(1/2/3)Sessions メトリクスをチェックします。多くのクライアントが接続されている場合、ファイルゲートウェイに RAM の追加が必要になることがあります。

Amazon FSx ファイルシステムにファイルが表示されない

ゲートウェイ上のファイルが Amazon FSx ファイルシステムに反映されていない場合は、`FilesFailingUpload` メトリクスを確認してください。メトリクスが一部のファイルのアップロードに失敗したことを報告している場合は、ヘルス通知を確認します。ファイルのアップロードに失敗すると、ゲートウェイは問題の詳細を示したヘルス通知を生成します。

Amazon FSx ファイルシステムに古いスナップショットが表示されない

FSx ファイルゲートウェイでの一部のファイル操作 (トップレベルフォルダの名前変更や権限変更など) は、複数のファイル操作を引き起こし、FSx for Windows File Server ファイルシステムに高い I/O 負荷をもたらす可能性があります。ファイルシステムにワークロードに十分なパフォーマンスリソースがない場合、ファイルシステムはシャドウコピーの保持履歴よりも継続的な I/O の可用性を優先するため、シャドウコピーを削除する可能性があります。

Amazon FSx コンソールで、「モニタリングとパフォーマンス」ページを見て、ファイルシステムがプロビジョニング不足かどうかを確認します。その場合は、SSD ストレージに切り替えるか、スループット容量を増やすか、または SSD IOPS を増やしてワークロードを処理することができます。

ゲートウェイを介した Amazon FSx へのデータ転送速度が遅い

ファイルゲートウェイを介した Amazon FSx for Windows File Server へのデータ転送速度が遅い場合は、次の操作を行います。

- `CachePercentDirty` メトリクスが 80 以上の場合、ファイルゲートウェイでは、データが Amazon FSx for Windows File Server にアップロードされるよりも速くデータがディスクに書き込まれています。ファイルゲートウェイからのアップロードの帯域幅を増やしたり、1 つ以上のキャッシュディスクを追加したり、クライアントの書き込み速度を遅くしたり、Amazon FSx for Windows File Server に関連するスループット容量を増やしたりすることを検討してください。
- `CachePercentDirty` メトリクスが低い場合は、`IoWaitPercent` メトリクスを確認します。`IoWaitPercent` が 10 を超える場合、ファイルゲートウェイでローカルキャッシュディスクの速度がボトルネックになっている可能性があります。キャッシュには、ローカルソリッドステートドライブ (SSD) ディスク (できれば NVM Express (NVMe)) をお勧めします。このようなディスクが使用できない場合は、パフォーマンスを向上させるために、別々の物理ディスクから複数のキャッシュディスクを使用してみてください。

ゲートウェイへの書き込み時にゲートウェイのバックアップジョブが失敗する、またはエラーが発生する

ファイルゲートウェイへの書き込み時にゲートウェイのバックアップジョブが失敗する、またはエラーが発生する場合は、次の操作を行います。

- `CachePercentDirty` メトリクスが 90 パーセント以上の場合、キャッシュディスクに十分な空き領域がないため、ファイルゲートウェイではディスクへの新しい書き込みを受け付けることができません。ファイルゲートウェイでの FSx for Windows File Server へのアップロード速度を確認するには、`CloudBytesUploaded` メトリクスを表示します。そのメトリクスと、クライアントによるファイルゲートウェイへのファイルの書き込みの速さを示す `WriteBytes` メトリクスを比較します。SMB クライアントがファイルゲートウェイが、FSx for Windows File Server にアップロードできる速度よりも速く書き込みを行っている場合は、少なくともバックアップジョブのサイズに対応できるキャッシュディスクを追加します。または、アップロード帯域幅を増やします。
- バックアップジョブが失敗しているにもかかわらず、`CachePercentDirty` メトリクスが 80 パーセント未満の場合は、ファイルゲートウェイでクライアント側のセッションがタイムアウトしている可能性があります。SMB の場合は、PowerShell コマンド `Set-SmbClientConfiguration -SessionTimeout 300` を使用してこのタイムアウトを増やすことができます。このコマンドを実行すると、タイムアウトが 300 秒に設定されます。

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、「トラブルシューティング: 高可用性に関する問題」を参照してください。

トラブルシューティング: 高可用性に関する問題

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

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で、設定済みの Amazon CloudWatch ロググループに対して次のヘルス通知が生成されます。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: リブート

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。メンテナンスの大幅な期間外に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、このイベントが引き起こ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。さらにサポートが必要な場合は、 にお問い合わせください サポート。

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 ロググループを参照してください。

ファイルゲートウェイのベストプラクティス

このセクションには、ゲートウェイ、ファイル共有、バケット、およびデータの操作に関するベストプラクティスに関する情報を提供する次のトピックが含まれています。このセクションで説明されている情報を理解し、 AWS Storage Gatewayの問題を避けるためにこれらのガイドラインに従うことをお勧めします。デプロイで発生する可能性がある一般的な問題の診断と解決に関する追加のガイダンスについては、「Storage Gateway のデプロイ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。

トピック

ベストプラクティス: データの復旧

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。

予期しない仮想マシンのシャットダウンからの復旧

停電時など、VM が予期せずシャットダウンすると、ゲートウェイにアクセスできなくなります。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、「ゲートウェイのネットワーク接続をテストする」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。

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。

アクセス不能なデータセンターのファイルゲートウェイからデータを復旧するには

ファイルゲートウェイの場合、回復したいデータが格納されている FSx for Windows File Server に、新しいファイルシステムをマッピングします。

1. Amazon EC2 ホストで新しいファイル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、「FSx ファイルゲートウェイ用のデフォルトの Amazon EC2 ホストをデプロイする」を参照してください。
2. 作成した EC2 ゲートウェイに新しいファイルシステムを作成します。詳細については、「」「FSx for Windows ファイル サーバー ファイル システムの作成」を参照してください。
3. ファイルシステムをクライアントにマウントし、復旧するデータが含まれている FSx for Windows File Server にこれをマッピングします。詳細については、「ファイル共有をマウントして使用する」を参照してください。

Amazon FSx でバックアップまたはスナップショットから直接復元する

場合によっては、以前の時点からのバックアップまたはスナップショットを使用して、Amazon FSx ファイルシステム上のデータを直接復元する必要があります。このような場合、バックアップアプリケーションと FSx ファイルゲートウェイの間にデュアルライターシナリオを作成するリスクがあり、ファイルがスタックしたり、一致しない可能性があります。Amazon FSx ファイルシステムをバックアップまたはスナップショットから復元する際の問題を回避するには、次の手順を使用します。

> **Note**
>
> この手順を使用してバックアップまたはスナップショットから Amazon FSx ファイルシステムを復元した後、FSx ファイルゲートウェイに現在保存されているキャッシュされたデータは無効になります。

Amazon FSx ファイルシステムをバックアップまたはスナップショットから復元する際の問題を回避するには

1. Storage Gateway コンソールを使用して、FSx ファイルゲートウェイから Amazon FSx ファイルシステムをデタッチします。
2. Amazon FSx ファイルシステムに直接バックアップまたはスナップショットを復元します。
3. Storage Gateway コンソールを使用して、Amazon FSx ファイルシステムを FSx ファイルゲートウェイに再接続します。

不要なリソースのクリーンアップ

ベストプラクティスとして、予期しない料金や不要な料金が発生しないように、Storage Gateway リソースのクリーンアップを推奨します。たとえば、デモンストレーション演習やテストとしてゲートウェイを作成した場合は、デプロイからゲートウェイとその仮想アプライアンスを削除することを検討してください。リソースをクリーンアップするには、次の手順に従います。

不要なリソースをクリーンアップする

1. ゲートウェイの使用を継続する予定がない場合は、ゲートウェイを削除します。詳細については、「ゲートウェイおよび関連リソースの削除」を参照してください。

2. オンプレミスホストから Storage Gateway VM を削除します。Amazon EC2 インスタンスにゲートウェイを作成した場合、インスタンスを終了します。

Storage Gateway に関するその他のリソース

このセクションでは、 AWS Storage Gatewayのセットアップと使用に関する追加情報とリソースを提供する以下のトピックについて説明します。

トピック

- ホストセットアップ - ゲートウェイの仮想マシンホストをデプロイして設定する方法について説明します。
- VMware HA での Storage Gateway の使用 - VMware vSphere の高可用性機能を使用するように Storage Gateway を設定する方法について説明します。
- アクティベーションキーの取得 - 新しいゲートウェイをデプロイするときに提供する必要があるアクティベーションキーの確認場所について説明します。
- の使用 Direct Connect - オンプレミスゲートウェイと AWS クラウドの間に専用ネットワーク接続を作成する方法について説明します。
- Active Directory のアクセス許可 - サービスアカウントがゲートウェイを Active Directory ドメインに参加させるために必要なアクセス許可について説明します。
- ゲートウェイアプライアンスの IP アドレスの取得 - 新しいゲートウェイをデプロイするときに指定する必要があるゲートウェイの仮想マシンホスト IP アドレスの確認場所について説明します。
- リソースとリソース ID について - Storage Gateway によって作成されるリソースとサブリソース AWS を識別する方法について説明します。
- リソースのタグ付け - メタデータタグを使用してリソースを分類し、管理を容易にする方法について説明します。
- オープンソースコンポーネント - Storage Gateway 機能の配信に使用されるサードパーティのツールとライセンスについて説明します。
- クォータ - ファイル共有とローカルキャッシュディスクの最小および最大制限を含む、ファイルゲートウェイの制限とクォータについて説明します。

ゲートウェイ VM ホストのデプロイと設定

以下のトピックでは、ゲートウェイの仮想マシンホストプラットフォームの設定について説明します。

トピック

- FSx ファイルゲートウェイ用のデフォルトの Amazon EC2 ホストをデプロイする

- FSx ファイルゲートウェイ用にカスタマイズされた Amazon EC2 ホストをデプロイする
- Amazon EC2 インスタンスメタデータオプションの変更
- VM の時刻を Hyper-V または Linux KVM ホストの時刻と同期する
- VM の時刻と VMware ホストの時刻を同期する
- ゲートウェイのネットワークアダプタの設定
- Storage Gateway での VMware vSphere High Availability の使用

FSx ファイルゲートウェイ用のデフォルトの Amazon EC2 ホストをデプロイする

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) インスタンス上でとAmazon FSx ファイル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 AWS済みプロバイダー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、「」および「Amazon EC2 インスタンスをデプロイしてAmazon FSx ファイルゲートウェイをホストする」を参照してください。
2. インスタンスを起動を選択して 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 IP 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 ファイル共有 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。ファイル共有に 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				

[ポート]	[プロトコル]	ファイルシステムプロトコル
137	UDP	NetBIOS
138	UDP	NetBIOS
139	TCP、UDP	SMB
389	TCP	LDAP
445	TCP	SMB

- 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
デバイス名		'/dev/sdb'
サイズ	80 Gib	165 GiB
ボリュームタイプ	gp3	gp3
IOPS	3000	3000
終了時に削除	はい	はい
暗号化された	いいえ	いいえ

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				
スループット	125	125				

FSx ファイルゲートウェイ用にカスタマイズされた Amazon EC2 ホストをデプロイする

Amazon Elastic Compute Cloud (Amazon EC2) インスタンス上でとAmazon FSx ファイル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 AWS済みプロバイダーであることがわかります。
> FSx ファイルゲートウェイの AMI では、次の命名規則を使用します。AMI 名に追加されるバージョン番号は、バージョンリリースごとに変更されます。
> `aws-storage-gateway-FILE_FSX_SMB-2.2.3`

Amazon EC2 インスタンスをデプロイしてAmazon FSx ファイル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、「」「Amazon FSx ファイルゲートウェイのセットアップ」を参照してください。[プラットフォームオプション] セクションが表示されたら、[ホストプラットフォーム] として Amazon EC2 を選択し、その後の手順に従って、ファイル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。
2. インスタンスを起動を選択して Amazon EC2 AWS Storage Gateway コンソールで AMI テンプレートを開き、追加の設定を構成できます。

   Quicklaunch を使用して、Amazon EC2 インスタンスをデフォルト設定で起動します。Amazon EC2 Quicklaunch のデフォルト仕様の詳細については、「」および「Amazon EC2 の Quicklaunch 設定仕様」を参照してください。

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見つけることができます。
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での要件」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 EC2 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。

   > **Note**
   >
   > 特定のインスタンスタイプ (特に i3 EC2) では、NVMe SSD ディスクを使用します。これは、ファイルゲートウェイを起動または停止するときに問題を引き起こす可能性があります。たとえば、キャッシュからデータを失う可能性があります。Amazon CloudWatch メトリクス `CachePercentDirty` をモニタリングし、システムを起動または停止するのは、このパラメータが `0` の場合のみにします。ゲートウェイのメトリクスのモニタリングに関する詳細については、CloudWatch ドキュメントの「Storage Gateway Metrics and Dimensions」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] 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 VPC の仕組み」を参照してください。

   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. [自動割り当てパブリック IP] で、[有効] 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。Amazon EC2 インスタンス用に作成される新しいセキュリティグループのデフォル

トの名前と説明を必要に応じて変更するか、代わりに既存のセキュリティグループのファイアウォールルールを適用することができます。

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。およびAmazon FSx ファイル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**
>
> Amazon FSx ファイルゲートウェイでは、インバウンドトラフィックと、ゲートウェイのアクティブ化時の 1 回限りの HTTP アクセス用に、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、SMB アクセスの場合は TCP ポート 445、NetBIOS アクセスの場合は UDP ポート 137、NetBIOS 名アクセスの場合は UDP ポート 138、LDAP アクセスの場合は TCP ポート 389 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**
>
> 事前設定済みのルートボリュームに加えて、キャッシュストレージ用に容量が 150 GiB 以上の Amazon EBS 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ため、それぞれ 150 GiB 以上の容量がある複数の EBS ボリュームをキャッシュストレージ用に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、指定した設定内容で新しい 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 EC2 コンソールの [インスタンス] ページに移動し、新しいインスタンスを名前で検索します。[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 IP 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、Amazon FSx ファイル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 パラメータストアをクエリすることで、ファイル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、以下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、「」「Amazon FSx ファイルゲートウェイのセットアップ」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移動したら、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 AWS Storage Gateway AMI テンプレートを開きます。

  EC2 コミュニティ AMI ページにリダイレクトされ、URL に AWS リージョンの AMI ID が表示されます。

- 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 API を使用して、名前空間 の Systems Manager パブリックパラメータをクエリできます`/aws/service/storagegateway/ami/FILE_FSX_SMB/latest`。たとえば、次の CLI コマンドを使用すると、指定した で現在の AMI 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/
FILE_FSX_SMB/latest
```

  この CLI コマンドにより、以下のような出力が返されます。

```
{
    "Parameter": {
        "Type": "String",
        "LastModifiedDate": 1561054105.083,
        "Version": 18,
         "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/
FILE_FSX_SMB/latest",
         "Name": "/aws/service/storagegateway/ami/FILE_FSX_SMB/latest",,
        "Value": "ami-033d1edba5606cffb"
    }
}
```

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 EC2 インスタンスメタデータに安全にアクセスするために提供される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ように設定することも、すべてのメタデータリクエストで IMDS バージョン 2 (IMDSv2) の使用をリクエストするように設定することもできます。IMDSv2 はセッション指向のリクエストを使用し、IMDS へのアクセス試行に利用される可能性があるいくつかのタイプの脆弱性を軽減します。IMDSv2 の詳細については、「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 インスタンスに IMDSv2 をリクエストすることをお勧めします。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は、デフォルトで IMDSv2 が必要です。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、IMDSv2 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については、「Amazon Elastic Compute Cloud ユーザーガイド」の「IMDSv2 の使用を要求する」を参照してください。この変更を適用するために、インスタンスを再起動する必要はありません。

VM の時刻を Hyper-V または Linux KVM ホストの時刻と同期する

VMware ESXi にデプロイされたゲートウェイの場合、時刻のずれを防ぐには、ハイパーバイザーホストの時刻を設定して、仮想マシンの時刻をホストと同期するだけで十分です。詳細については、「VM の時刻と VMware ホストの時刻を同期する」を参照してください。Microsoft Hyper-V または Linux KVM にデプロイされたゲートウェイの場合、次に説明する手順を使用して、定期的に仮想マシンの時刻を確認することをお勧めします。

ハイパーバイザーゲートウェイ仮想マシンの時刻を表示してネットワークタイムプロトコル (NTP) サーバーと同期するには

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。

   - 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 カーネルベース仮想マシン (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、「Linux KVM 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. [Storage Gateway の設定] メインメニュー画面で、対応する数字を入力して、[システム時刻の管理] を選択します。
3. [システム時刻の管理] メニュー画面で、対応する数字を入力して、[システム時刻の表示と同期] を選択します。

   ゲートウェイローカルコンソールは、現在のシステム時刻を表示し、NTP サーバーによって報告された時刻と比較して、2 つの時刻の正確な差異を秒単位で報告します。
4. 時刻の差異が 60 秒を超える場合は、**y** を入力してシステム時刻を NTP 時刻と同期します。それ以外の場合は、「**n**」と入力します。

   時刻の同期には数分かかる場合があります。

VM の時刻と VMware ホストの時刻を同期する

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。続いて、ホストの時刻を確認し、必要であればホストの時刻を設定して、ホストの時刻がネットワークタイムプロトコル (NTP) サーバーに自動的に同期するように設定します。

> **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、アプリケーションウィンドウの左側にあるパネルでゲートウェイ VM の名前を右クリックして VM のコンテキストメニューを開き、[設定の編集] を選択します。

      [仮想マシンプロパティ] 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. [仮想マシンのプロパティ] ダイアログボックスの右側にある [アドバンスト] セクションで、[ゲスト時刻をホストと同期する] オプションをチェックし、[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。ホストの時計の設定が済んでいない場合は、次の手順に従って、時計を設定して NTP サーバーと同期します。

   a. VMware vSphere クライアントで、左側のパネル vSphere ホストノードを選択し、[設定] タブを選択します。
   b. [ソフトウェア] パネルで [時刻設定] を選択してから、[プロパティ] リンクを選択します。

      [時刻設定] ダイアログボックスが表示されます。
   c. [日付と時刻] で、vSphere ホストの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. [時刻設定] ダイアログボックスで [オプション] を選択してから、[NTP デーモン (ntpd) オプション] ダイアログボックスで、左ペインの [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 サーバーを追加] 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て、[OK] を選択します。

         ドメイン名として `pool.ntp.org` を使用できます。
      iv. [NTP デーモン (ntpd) オプション] ダイアログボックスで、左側のパネルの [全般] を選択します。
      v. [サービスコマンド] で、[開始] を選択してサービスを開始します。

         後でこの NTP サーバー参照を変更したり他の参照を追加した場合、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ります。
   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 [時刻設定] ダイアログボックスを閉じます。

ゲートウェイのネットワークアダプタの設定

Storage Gateway はデフォルトで単一の VMXNET3 (10 GbE) ネットワークアダプタを使用しますが、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て、複数の IP アドレスからアクセスできるようにします。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は、ゲートウェイへのスループットを最大化したいことがあります。
- 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によっては、ファイル共有と、それに接続するイニシエータを分離されたネットワークに置いておくことが必要な場合があります。このネットワークは、ゲートウェイが AWSへの通信に使用するネットワークとは異なります。

一般的な複数アダプタのユースケースでは、1 つのアダプタがゲートウェイが通信するルートとして設定されます AWS (つまり、デフォルトゲートウェイとして) 。このアダプタを除き、イニシエータは、接続するファイル共有を含むアダプタと同じサブネット内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、そのターゲットのファイル共有トラフィックと AWS トラフィックは同じアダプターを経由します。

場合によっては、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た後、2 つ目のアダプタを追加できます。そのような場合、Storage Gateway は 2 つ目のアダプタを優先ルートとして使用するようにルートテーブルを自動的に設定します。複数のアダプタを設定する手順については、以下のトピックを参照してください。

トピック

- VMware ESXi ホストの複数の NIC に対するゲートウェイの設定
- Microsoft Hyper-V ホストの複数の NIC に対するゲートウェイの設定

VMware ESXi ホストの複数の NIC 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 で 1 つのネットワークアダプタが定義済みであることを前提に、VMware ESXi でアダプタを設定する方法を説明します。

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、ゲートウェイの 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、[設定を編集] を選択します。
4. [仮想マシンのプロパティ] ダイアログボックスの [ハードウェア] タブで、[追加] を選択してデバイスを追加します。
5. [ハードウェアの追加] 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. [デバイスタイプ] ペインで [イーサネットアダプタ] を選択してアダプタを追加し、[次へ] を選択します。
   b. [ネットワークタイプ] ペインで、[タイプ]に [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、[次へ] をクリックします。

      Storage Gateway では 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。アダプタのリストに表示されるアダプタタイプの詳細については、ESXi and vCenter Server Documentation の Network Adapter Types を参照してください。
   c. [Ready to Complete] ペインで情報を確認し、[終了] を選択します。
6. VM の [概要] タブを選択し、[IP アドレス] ボックスの横にある [すべて表示] を選択します。[仮想マシン IP アドレス] 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 [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。

VMware、Hyper-V、KVM ホストに共通するローカルコンソールタスクについては、「仮想マシンのローカルコンソールでタスクの実行」を参照してください。

Microsoft Hyper-V ホストの複数の NIC 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 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 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. Storage Gateway コンソールでゲートウェイをオフにします。
2. Microsoft Hyper-V Manager で、[仮想マシン] パネルからゲートウェイ VM を選択します。
3. ゲートウェイ VM がオフになっていない場合は、VM 名を右クリックしてコンテキストメニューを開き、[オフにする] を選択します。
4. ゲートウェイ VM 名を右クリックしてコンテキストメニューを開き、[設定] を選択します。
5. [設定] ダイアログボックスの [ハードウェア] で、[ハードウェアの追加] を選択します。
6. [設定] ダイアログボックスの右側にある [ハードウェアの追加] パネルで、[ネットワークアダプタ] を選択し、[追加] 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、[適用する] を選択して設定を適用します。
8. [設定] ダイアログボックスの [ハードウェア] で、新しいネットワークアダプタがハードウェアリストに追加されたことを確認し、[OK] を選択します。
9. Storage Gateway コンソールを使用してゲートウェイをオンにします。
10. Storage Gateway コンソールの [ナビゲーション] パネルで、[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。

VMware、Hyper-V、KVM ホストに共通するローカルコンソールタスクについては、「仮想マシンのローカルコンソールでタスクの実行」を参照してください。

Storage Gateway での VMware vSphere High Availability の使用

Storage Gateway は、VMware vSphere High Availability (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を通じて VMware の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。

この統合により、オンプレミスの VMware 環境または の VMware クラウドにデプロイされたゲートウェイは、ほとんどのサービスの中断から AWS 自動的に回復します。これは通常、60 秒未満でデータ損失なしで行われます。

> **Note**
>
> Storage Gateway を VMware HA クラスターにデプロイする場合は、次の操作を行うことをお勧めします。
>
> - Storage Gateway VM を含む VMware ESX 用の .ova ダウンロード可能パッケージは、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、特定の 1 つのホスト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。
> - クラスタリングを使用して .ova パッケージをクラスターにデプロイする場合は、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。

次のトピックでは、Storage Gateway を VMware HA クラスターにデプロイする方法について説明します。

トピック

vSphere の VMware HA クラスターの設定

最初に、VMware クラスターをまだ作成していない場合は、作成します。VMware クラスターの作成方法については、VMware のドキュメントの「Create a vSphere HA Cluster」を参照してください。

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. VMware vSphere の [クラスター設定の編集] ページで、VM のモニタリングが VM とアプリケーションの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、オプションごとに次の値を設定します。

   - Host Failure Response: Restart VMs
   - Response for Host Isolation: Shut down and restart VMs
   - Datastore with PDL: Disabled
   - Datastore with APD: Disabled
   - VM Monitoring: VM and Application Monitoring
2. 次の値をファインチューニングして、クラスターの感度を微調整します。

   - 失敗の間隔 – 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。
   - 最小稼働時間 – 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。
   - VM あたりの最大リセット数 – 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。
   - 最大リセット時間枠 – 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。

   - 失敗の間隔: **30** 秒
   - 最小稼働時間: **120** 秒
   - VM あたりの最大リセット数: **3**
   - 最大リセット時間枠: **1** 時間

クラスターで他の VM が実行されている場合は、VM 専用にこれらの値を設定することもできます。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) クラスター上の他の VM に対する上書きオプションの追加」を参照してください。

ゲートウェイタイプをセットアップする

以下の手順に従って、ゲートウェイをセットアップします。

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

- ゲートウェイタイプの .ova イメージを、次のいずれかからダウンロードします。
  - ファイルゲートウェイ– Amazon FSx ファイルゲートウェイを作成してアクティブ化する

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。手順については、VMware vSphere オンラインドキュメントの「OVF または OVA テンプレートをデプロイする」を参照してください。

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。

(オプション) クラスター上の他の VM に対する上書きオプションの追加

クラスターで他の VM が実行されている場合は、各 VM 専用にクラスター値を設定することもできます。手順については、「VMware vSphere オンラインドキュメント」の「Customize an Individual Virtual Machine」を参照してください。

クラスター上の他の VM のオーバーライドオプションを追加するには

1. VMware vSphere の [Summary] ページで、クラスターを選択してクラスターページを開き、[Configure] 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。

[vSphere HA - VM モニタリング] の各オプションに次の値を設定します。

- [VM モニタリング]: [上書きが有効] - [VM およびアプリケーションのモニタリング]
- [VM モニタリングの機密性]: [上書きが有効] - [VM とアプリケーションのモニタリング]
- [VM モニタリング]: [カスタム]
- 失敗の間隔: **30** 秒
- 最小稼働時間: **120** 秒
- VM あたりの最大リセット数**5**:
- 最大リセット時間枠: **1** 時間以内

ゲートウェイのアクティブ化

.ova が VMware 環境にデプロイされたら、Storage Gateway コンソールを使用してゲートウェイをアクティブ化します。手順については、「」および「Amazon FSx ファイルゲートウェイの設定を確認してアクティブ化する」を参照してください。

VMware High Availability 設定のテスト

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. 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 [ゲートウェイ] を選択してから、VMware HA をテストするゲートウェイを選択します。
3. [アクション] で、[VMware HA の確認] を選択します。
4. 表示される [Verify VMware High Availability Configuration (VMware High Availability 設定の検証)] ページで、[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 ロググループで確認できます。詳細については、「CloudWatch ロググループを使用した FSx ファイルゲートウェイヘルスログの取得」を参照してください。

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」の「ActivateGateway」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「`http://`*`gateway_ip_address`*`/?activationRegion=`*`activation_region`*」のようになります。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**
>
> AWS 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、このページで説明されてい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、CACHED、VTL、FILE_S3、または FILE_FSX_SMB など、アクティブ化するゲートウェイのタイプ。
> - *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 応答を取得し、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

次の例では、Microsoft Windows PowerShell を使用して HTTP 応答を取得し、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-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 admin ユーザーとしてログインします。
2. ログイン後に [AWS アプライアンスのアクティベーション - 設定] メインメニューが表示されたら、0 を選択して [アクティベーションキーを取得] 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 エンドポイント] を入力します。
6. エンドポイントタイプとして「Standard」の場合は「1」、Federal Information Processing Standard (FIPS) の場合は「2」と入力します。

Storage Gateway Direct Connect での の使用

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 Direct Connect で を使用すると、高スループットのワークロードの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。 Direct Connect 接続を使用すると、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 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 Direct Connect 連携する方法の例を示しています。
AWS 直接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 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、Direct Connect ユーザーガイドの「使用の開始 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 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。詳細については、「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。

詳細については Direct Connect、 Direct Connect ユーザーガイドの「 とは Direct Connect」を参照してください。

Active Directory サービスアカウントのアクセス許可要件

Microsoft Active ディレクトリを使用して のファイルシステムへのユーザー認証アクセスを提供する場合は AWS Storage Gateway、Active Directory サービスアカウントがあり、サービスアカウントにコンピュータをドメインに結合する権限が委任されていることを確認する必要があります。サービスアカウントは、特定のタスクを実行する権限が委任されている Active Directory のユーザーアカウントです。Storage Gateway を Active Directory ドメインに参加させるときに、このアカウントのユーザー名とパスワードの認証情報を指定します。

Active Directory サービスアカウントには、ゲートウェイに参加する OU で次のアクセス許可を委任する必要があります。

- コンピュータオブジェクトを作成および削除する権限
- パスワードをリセットする機能
- アクセス許可を変更する機能

- アカウントのデータの読み取りと書き込みを制限する機能
- アカウントの検証を読み書きするための検証済みの機能
- サービスプリンシパル名への書き込みを許可
- DNS ホスト名への書き込みを検証する機能

これらは、コンピュータオブジェクトをアクティブディレクトリに参加させるために必要な最小限のアクセス許可セットを表します。詳細については、「Microsoft Windows Server のドキュメント」トピック「エラー: コントロールを付与された管理者以外のユーザーがコンピュータをドメインコントローラーに参加させようとすると、アクセスが拒否される」を参照してください。

ゲートウェイアプライアンスの IP アドレスの取得

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 ゲートウェイでは、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: VMware ESXi でゲートウェイのローカルコンソールにアクセスする
- 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 カーネルベース仮想マシン (KVM) ホスト: Linux KVM でゲートウェイのローカルコンソールにアクセスする
- EC2 ホスト: Amazon EC2 のホストから IP アドレスを取得する

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 のホストから IP アドレスを取得する

ゲートウェイをデプロイする 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、「」を参照してください。

また、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 アドレス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. Amazon EC2 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。
2. ナビゲーションペインで [インスタンス] を選択してから、ゲートウェイがデプロイする EC2 インスタンスを選択してください。
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. Amazon EC2 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。
2. ナビゲーションペインで [インスタンス] を選択してから、ゲートウェイがデプロイする EC2 インスタンスを選択してください。
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。

Storage Gateway のリソースとリソース ID の説明

Storage Gateway では、プライマリリソースはゲートウェイですが、他のリソースタイプはファイル共有です。ファイル共有は、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。

リソースとサブリソースには、この表に示すとおり、一意の Amazon リソースネーム (ARN) 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*
ファイル共有 ARN	arn:aws:storagegateway: *region*:*account-id* :share/*share-id*

リソース ID の使用

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 ARN の一部です。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。

Storage Gateway のリソース ID は大文字です。ただし、Amazon EC2 API でこれらのリソース ID を使用する場合、Amazon EC2 には小文字のリソース ID が必要です。リソース ID を EC2 API で使用するには、小文字に変更する必要があります。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 API で使用するには、vol-1122aabb に変更する必要があります。これを行わなければ、EC2 API が正常に動作しない場合があります。

> **Important**
>
> Storage Gateway ボリュームと、ゲートウェイボリュームから作成された Amazon EBS スナップショットの ID は、長い形式に変更されています。2016 年 12 月から、すべての新しいボリュームとスナップショットは、17 文字の文字列で作成されます。2016 年 4 月からこれらの長い ID を使用できるので、新しい形式でシステムをテストできます。詳細については、「長い EC2 および EBS リソース ID」を参照してください。
> たとえば、長いボリューム ID 形式のボリューム ARN は次のようになります。
> arn:aws:storagegateway:us-west-2:111122223333:gateway/sgw-12A3456B/volume/vol-1122AABBCCDDEEFFG.
> 長い ID 形式のスナップショット ID は「snap-78e226633445566ee」のようになります。
> 詳細については、「Announcement: Heads-up – Longer Storage Gateway volume and snapshot IDs coming in 2016」を参照してください。

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。

ファイルゲートウェイの場合、タグを使用してリソースへのアクセスをコントロールできます。これを行う方法については、「タグを使用してゲートウェイとリソースへのアクセスをコントロールする」を参照してください。

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。
- キープロパティに使用できる文字は、UTF-8 文字および数字、スペース、特殊文字 +、-、=、.、:、/、@ です。

タグの操作

Storage Gateway コンソール、Storage Gateway API、または Storage Gateway コマンドラインインターフェイス (CLI) を使用して、タグを使用した作業ができます。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. 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、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、[ゲートウェイ] 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. [タグ] を選択してから、[タグの編集/追加] を選択します。
4. [タグの編集/追加] ダイアログボックスで、[タグの作成] を選択します。
5. [キー] でキーを、[値] 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**
   >
   > [値] 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、[保存] を選択します。

タグを編集するには

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. タグを編集するリソースを選択します。
3. [タグ] を選択して、[タグの追加/編集] 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、[保存] を選択します。

タグを削除するには

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. タグを削除するリソースを選択します。

3. [タグ] を選択してから、[タグの追加/編集] を選択して [タグの追加/編集] 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、[保存] を選択します。

のオープンソースコンポーネントの使用 AWS Storage Gateway

このセクションでは、 AWS 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。

トピック

- Storage Gateway のオープンソースコンポーネント
- Amazon FSx ファイルゲートウェイのオープンソースコンポーネント

Storage Gateway のオープンソースコンポーネント

Volume Gateway、Tape Gateway、Amazon S3 ファイルゲートウェイの機能を提供するために、いくつかのサードパーティ製ツールとライセンスが使用されています。

以下のリンクを使用して、 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をダウンロードします。

- VMware ESXi にデプロイされた Storage Gateway アプライアンスの場合: sources.tar
- Microsoft Hyper-V にデプロイされた Storage Gateway アプライアンスの場合は、sources_hyperv.tar をダウンロードします。
- Linux カーネルベース仮想マシン (KVM) にデプロイされたStorage Gatewayの場合は、sources_KVM.tar をダウンロードします。

この製品には、OpenSSL ツールキット (http://www.openssl.org/) での使用を前提に OpenSSL プロジェクトにより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製ツールの関連ライセンスについては、サードパーティのライセンスを参照してください。

Amazon FSx ファイルゲートウェイのオープンソースコンポーネント

Amazon FSx ファイルゲートウェイ(FSx ファイルゲートウェイ) の機能を提供するために、いくつかのサードパーティ製ツールとライセンスが使用されています。

FSx ファイルゲートウェイ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、以下のリンクからダウンロードします。

- Amazon FSx ファイルゲートウェイ2021-07-07 リリースの場合：sgw-file-fsx-smb-open-source.tgz
- Amazon FSx ファイルゲートウェイ2021-04-06 リリースの場合：sgw-file-fsx-smb-20210406-open-source.tgz

この製品には、OpenSSL ツールキット (http://www.openssl.org/) での使用を前提に OpenSSL プロジェクトにより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製ツールの関連ライセンスについては、以下のリンクを参照してください。

- Amazon FSx ファイルゲートウェイ2021-07-07 リリースの場合: サードパーティライセンス。
- Amazon FSx ファイルゲートウェイ2021-04-06 リリースの場合: サードパーティライセンス。

およびAmazon FSx ファイルゲートウェイの制限とクォータ

Amazon FSx ファイルシステムのクォータ

次の表に、Amazon FSx ファイルシステムの最小制限と最大制限とクォータを示します。

[リソース]	Amazon FSx ファイルシステムあたりの制限
タグの最大数	タグ 50 個
自動バックアップの最大保持期間	90 日間
単一の宛先リージョンに対して同時に送信できるバックアップコピーリクエストの 1 アカウントあたりの最大数。	リクエスト 5 回
SSD ファイルシステムの最小ストレージ容量	32 GiB
HDD ファイルシステムの最小ストレージ容量	2,000 GiB
SSD および HDD ファイルシステムの最大ストレージ容量	64 TiB

[リソース]	Amazon FSx ファイルシステムあたりの制限
最小スループット容量	8 MBps
最大スループット容量	2,048 MBps
Amazon FSx ファイル共有の最大数	100,000

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 AWS Storage Gateway 内の各 のローカルディスクストレージのサイズを推奨しています。

ゲートウェイタイプ	キャッシュ (最小)	キャッシュ (最大)	
FSx ファイルゲートウェイ	150 GiB	64 TiB	

> **Note**
>
> キャッシュ用として、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 FSx ファイルゲートウェイにキャッシュを追加する場合は、仮想ホスト (ハイパーバイザーまたは Amazon EC2 インスタンス) 上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既に割り当てられている場合は、既存のディスクサイズを変更しないでください。

Storage Gateway の API リファレンス

コンソールの使用に加えて、 AWS Storage Gateway API を使用してプログラムでゲートウェイを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**
>
> Storage Gateway でアプリケーションを開発するときに、 AWS SDKs を使用することもできます。 AWS SDK for Java、.NET、PHP により、基盤となる Storage Gateway API がラッピングされるので、プログラミングの作業が簡素化されます。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

AWS Storage Gateway 必要なリクエストヘッダー

このセクションでは、 AWS Storage Gatewayへのすべての POST リクエストで送信しなければならない必須ヘッダーについて説明します。HTTP ヘッダーでは、呼び出すオペレーション、リクエストの日付、リクエストの送信者として認可されていることを示す情報など、リクエストに関する重要な情報を特定します。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。

次の例では、ActivateGateway オペレーションで使用されるヘッダーを示します。

```
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、 が POST リクエストに含める必要があるヘッダーです AWS Storage Gateway。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。それ以外のヘッダーはすべて、HTTP トランザクションで使用される共通のヘッダーです。

ヘッダー	説明
Authorization	認可ヘッダーには、リクエストがリクエスタの有効なアクションかどうかを が判断 AWS Storage Gateway できるようにする、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` この構文では、YourAccessKey、年、月、日 (yyyymmdd)、リージョン、および CalculatedSignature が指定されています。認可ヘッダーの形式は、 AWS V4 署名プロセスの要件によって指定されています。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	を、 へのすべてのリクエストのコンテンツタイプapplication/x-amz-json-1.1 として使用します AWS Storage Gateway。 `Content-Type: application/x-amz-json-1.1`
Host	ホストヘッダーを使用して、リクエストを送信する AWS Storage Gateway エンドポイントを指定します。例えば storagega

ヘッダー	説明
	teway.us-east-2.amazonaws.com は、米国東部 (オハイオ) リージョンのエンドポイントを表します。で利用可能なエンドポイントの詳細については AWS Storage Gateway、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。 `Host: storagegateway. region.amazonaws.com`
x-amz-date	HTTP Date ヘッダーまたは AWS x-amz-date ヘッダーにタイムスタンプを入力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 ヘッダーを設定することができません)。x-amz-date ヘッダーが存在する場合、 はリクエスト認証中にDateヘッダー AWS Storage Gateway を無視します。x-amz-date の形式は、ISO8601 Basic の YYYYMMDD'T'HHMMSS'Z' 形式でなければなりません。Date ヘッダーと x-amz-date ヘッダーの両方を使用する場合は、Date ヘッダーの形式は ISO8601 でなくてもかまいません。 `x-amz-date: YYYYMMDD'T'HHMMSS'Z'`
x-amz-target	このヘッダーでは、API のバージョンおよび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の値を作成するには、API のバージョンと API の名前を次のような形式で連結します。 `x-amz-target: StorageGateway_ APIversion .operationName` operationName 値 (例: ActivateGateway) は、API リスト (Storage Gateway の API リファレンス) で確認できます。

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変換します。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。シークレットアクセスキーから開始し、認証情報スコープの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 (HMAC) を作成することで、派生キーが計算されます。

署名の計算例

次の例で、ListGateways の署名を作成する詳細な手順を示します。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。

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" GMT」です。

- エンドポイントは、米国東部 (オハイオ) リージョンです。

リクエストの一般的な構文 (JSON の本体を含む) 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 (あるいは任意の Storage Gateway API)に、クエリパラメータがないためです。

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のアクセスキー AKIAIOSFODNN7EXAMPLE の場合、ヘッダーは次のとおりです (読みやすいように改行しています)。

```
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

- 例外
- オペレーションエラーコード
- エラーレスポンス

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、エラー例外 InvalidSignatureException は、リクエスト署名に問題がある場合に、API レスポンスによって返されます。ただし、オペレーションエラーコード ActivationKeyInvalid は、ActivateGateway API に対してのみ返されます。

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、 AWS Storage Gateway API の例外を示します。 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。

例外	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	指定された 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

例外	メッセージ	HTTP ステータスコード
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 証明書が含まれている必要があります。	403 Forbidden
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 ペイロードが正しく形成されていることを確認してください。	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 Too Many Requests
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 API アクション に示します。	400 Bad Request

例外	メッセージ	HTTP ステータスコード
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 間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

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
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 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

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
DuplicateCertificateInfo	指定された証明書情報が重複しています。	ActivateGateway
FileSystemAssociationEndpointConfigurationConflict	既存のファイルシステム関連付けエンドポイント設定が、指定された設定と競合しています。	AssociateFileSystem
FileSystemAssociationEndpointIpAddressAlreadyInUse	指定されたエンドポイント IP アドレスは既に使用されています。	AssociateFileSystem
FileSystemAssociationEndpointIpAddressMissing	ファイルシステムの関連付けエンドポイント IP アドレスがありません。	AssociateFileSystem
FileSystemAssociationNotFound	指定されたファイルシステムの関連付けが見つかりませんでした。	UpdateFileSystemAssociation DisassociateFileSystem DescribeFileSystemAssociations
FileSystemNotFound	指定されたファイルシステムが見つかりませんでした。	AssociateFileSystem

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、無効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 は無効です。	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。

- コンテンツタイプ: application/x-amz-json-1.1
- 適切な 4xx または 5xx HTTP 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"
        }
```

```
}
```

次の表では、前述の構文で表示される JSON エラーレスポンスフィールドを説明します。

__type

例外 からの例外の 1 つ。

タイプ：文字列

error

API 固有のエラー詳細が含まれています。特定の API に固有ではない一般的なエラーの場合、このような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。

タイプ：文字列

errorDetails

このフィールドは、API の現在のバージョンでは使われていません。

タイプ：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 。

タイプ：文字列

エラーレスポンスの例

DescribeStorediSCSIVolumes API を使用して、存在しないゲートウェイ ARN リクエスト入力を指定した場合、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 が計算した署名が、リクエストと一緒に送信された署名と一致しない場合、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 API アクション

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。

Amazon FSx ファイルゲートウェイユーザーガイドのドキュメント履歴

次の表に、2018 年 4 月以降の本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を受け取るには、RSS フィードにサブスクライブできます。

変更	説明	日付
FSx ファイルゲートウェイの可用性の変更通知	新規のお客様への Amazon FSx ファイルゲートウェイの提供は終了しました。FSx ファイルゲートウェイの既存のお客様は、引き続き通常どおりサービスを使用できます。FSx ファイルゲートウェイに似た機能については、このブログ記事を参照してください。	2024 年 10 月 28 日
FSx ファイルゲートウェイの可用性の変更通知	2024 年 10 月 28日以降、新規のお客様はAWS Storage Gatewayの FSx ファイルゲートウェイを利用できなくなります。サービスを使用するには、その日より前にサインアップする必要があります。FSx ファイルゲートウェイの既存のお客様は、引き続き通常どおりサービスを使用できます。FSx ファイルゲートウェイに似た機能については、このブログ記事を参照してください。	2024 年 9 月 26 日

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を含む定期的なメンテナンスの更新を受け取ります。デプロイ内の個々のゲートウェイごとにこれらの更新をオンまたはオフにするように設定を構成できるようになりました。詳細については、「コンソールを使用したゲートウェイの更新の管理」を参照してください AWS Storage Gateway。	2024 年 6 月 6 日
CloudWatch の推奨アラームを更新	CloudWatch `HealthNotifications` アラームが、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適用されるようになり、これらすべてに対して推奨されるようになりました。`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 アラームの説明」を参照してください。	2023 年 10 月 2 日

GatewayClockOutOfSync トラブルシューティングのヒントを追加	トラブルシューティング: ファイルゲートウェイの問題セクションに、ゲートウェイシステムクロックが AWS Storage Gatewayサーバー時刻と同期されていない場合に発生する可能性がある問題を診断するためのトラブルシューティングガイドラインが追加されました。詳細については、「エラー: GatewayClockOutOfSync」を参照してください。	2022 年 10 月 19 日
Active Directory ドメイン参加のトラブルシューティングのヒントを追加	「トラブルシューティング: ファイルゲートウェイに関する問題」セクションに、ゲートウェイを Active Directory ドメインに参加させようとするときに発生する可能性のある問題を診断するためのトラブルシューティングガイドラインを追加しました。詳細については、「トラブルシューティング: Active Directory ドメインに関する問題」を参照してください。	2022 年 10 月 19 日
ゲートウェイの作成手順を更新	Storage Gateway コンソールの変更を反映するために、新しいゲートウェイを作成する手順を更新しました。詳細については、「Amazon S3 ファイルゲートウェイを作成してアクティブ化する」を参照してください。	2021 年 10 月 12 日

複数のファイルシステムのサポート	Amazon FSx ファイルゲートウェイは、最大 5 つのアタッチされた Amazon FSx ファイルシステムをサポートするようになりました。詳細については、「Amazon FSx for Windows File Server ファイルシステムのアタッチ」を参照してください。	2021 年 7 月 7 日
Amazon FSx ソフトストレージクォータのサポート	Amazon FSx ファイルゲートウェイは、ストレージクォータが設定されている、アタッチされた Amazon FSx ファイルシステムに書き込むときに、ソフトストレージクォータ (ユーザーがデータ制限を超えたときに警告する) をサポートするようになりました。ハードクォータ (書き込みアクセスを拒否してデータ制限を適用する) はサポートされていません。ソフトクォータは、Amazon FSx 管理者ユーザーを除くすべてのユーザーに対して機能します。ストレージクォータの設定の詳細については、「Amazon FSx for Windows File Server ユーザーガイド」の「ストレージクォータ」を参照してください。	2021 年 7 月 7 日

新しいガイド	Storage Gateway は、元のファイルゲートウェイ(現在は Amazon S3 ファイルゲートウェイ) に加えて、Amazon FSx ファイルゲートウェイ(FSx ファイルゲートウェイ) を提供します。FSx ファイルゲートウェイは、オンプレミスの施設からクラウド内の FSx for Windows File Server ファイル共有への低レイテンシーで効率的なアクセスを提供します。詳細については、「Amazon FSx ファイルゲートウェイとは」を参照してください。	2021 年 4 月 27 日
FedRAMP 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、「Storage Gateway のコンプライアンス検証」を参照してください。	2020 年 11 月 24 日
ファイルゲートウェイの移行	ファイルゲートウェイは、既存のファイルゲートウェイを新しいファイルゲートウェイに置き換えるための、文書化されたプロセスを提供するようになりました。詳細については、「ファイルゲートウェイを新しいファイルゲートウェイに置き換える」を参照してください。	2020 年 10 月 30 日

ファイルゲートウェイのコールドキャッシュの読み取りパフォーマンスが 4 倍向上	Storage Gateway で、コールドキャッシュの読み取りパフォーマンスが 4 倍向上しました。詳細については、「ファイルゲートウェイのパフォーマンスガイダンス」を参照してください。	2020 年 8 月 31 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、「AWS 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)、およびカナダ (中部) の各リージョンで FIPS 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

ファイル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 のファイルゲートウェイで、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提供されることで、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、「Storage Gateway ユーザーガイド」の「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 7 月 7 日
Storage Gateway コンソールでの Amazon CloudWatch アラームの表示	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、「CloudWatch アラームの説明」を参照してください。	2020 年 5 月 29 日
連邦情報処理規格 (FIPS) エンドポイントのサポート	AWS GovCloud (US) リージョンで FIPS エンドポイントを持つゲートウェイをアクティブ化できるようになりました。ファイルゲートウェイの 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。	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

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。KVM にデプロイされたゲートウェイは、既存のオンプレミスのゲートウェイと同じ機能と特徴をすべて備えています。詳細については、「Storage Gateway ユーザーガイド」の「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。	2020 年 2 月 4 日

VMware vSphere High Availability のサポート	Storage Gateway で、VMware 上での高可用性がサポートされるようになりました。これは、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ワークロードを保護するのに役立ちます。詳細については、「Storage Gateway ユーザーガイド」の「Storage Gateway での VMware vSphere High Availability の使用」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
Amazon CloudWatch Logs のサポート	ファイルゲートウェイで Amazon CloudWatch ロググループを設定して、ゲートウェイとそのリソースのエラーと状態について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「Getting Notified About Gateway Health and Errors With Amazon CloudWatch Log Groups」を参照してください。	2019 年 9 月 4 日

New 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
New 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 (VPC) でゲートウェイをアクティブ化するためのサポート	VPC でゲートウェイをアクティベートできるようになりました。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

ファイルゲートウェイでのタグベースの認可のサポート	ファイルゲートウェイでタグベースの認可がサポートされるようになりました。ファイルゲートウェイリソースへのアクセスをリソースのタグに基づいてコントロールできます。このアクセスは、IAM リクエストの条件で渡すことのできるタグに基づいてコントロールすることもできます。詳細については、「ファイルゲートウェイリソースへのアクセスを制御する」を参照してください。	2019 年 3 月 4 日
欧州での AWS Storage Gatewayハードウェアアプライアンスの可用性	AWS Storage Gatewayハードウェアアプライアンスが欧州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 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、 AWS Storage Gateway ハードウェアアプライアンスの使用可能なストレージを 5 TB から 12 TB に増やし、インストールさ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置き換えることができます。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

AWS Storage Gatewayハードウェアアプライアンスのサポート	AWS 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 マネジメントコンソール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、「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。	2018 年 9 月 18 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
新規 AWS 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
新規 AWS 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
VMware ESXi Hypervisor バー	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。	2017 年 9 月 13 日

変更	説明	変更日
ジョン 6.5 のサポート	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。	
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
新規 AWS 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
Amazon EC2 のファイルゲートウェイのサポート	AWS Storage Gateway では、Amazon EC2 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。Storage Gateway Amazon マシンイメージ (AMI) をコミュニティ AMI として利用できるようになりました。この AMI を使用して、Amazon EC2 でファイルゲートウェイを起動できます。ファイルゲートウェイを作成し、EC2 インスタンスでデプロイする方法については、「Amazon FSx ファイルゲートウェイを作成してアクティブ化する」を参照してください。AMI にファイルゲートウェイを起動する方法についての詳細は、「FSx ファイルゲートウェイ用のデフォルトの Amazon EC2 ホストをデプロイする」を参照してください。 さらに、ファイルゲートウェイで HTTP プロキシ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、「Amazon EC2 にデプロイされたゲートウェイを HTTP プロキシ経由でルーティングする」を参照してください。	2017 年 2 月 08 日

変更	説明	変更日
新規 AWS 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
新規 AWS 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
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。ファイルゲートウェイでは、サービスおよび仮想ソフトウェアアプライアンスを組み合わせ、ネットワークファイルシステム (NFS) のような業界標準のファイルプロトコルを使用することで、Amazon S3 でオブジェクトを保存し、取得することができます。ゲートウェイでは、NFS マウントポイントのファイルとして、Amazon S3 のオブジェクトへのアクセスが提供されます。	2016 年 11 月 29 日