Amazon S3 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 2013-06-30

AWS Storage Gateway: Amazon S3 ファイルゲートウェイユーザーガイド

Table of Contents

Amazon S3 ファイルゲートウェイとは

Amazon S3 ファイルゲートウェイ– Amazon S3 ファイルゲートウェイでは、Amazon Simple Storage Service (Amazon S3) へのファイルインターフェイスを提供し、サービスと仮想ソフトウェアアプライアンスを組み合わせたものです。この組み合わせを使用すると、ネットワークファイルシステム (Amazon S3にオブジェクトを保存および取得できます。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 にデプロイすることも AWS、Amazon EC2 の AMI としてデプロイすることもできます。ゲートウェイは、S3 内のオブジェクトへのアクセスをファイルまたはファイル共有のマウントポイントとして提供します。S3 ファイルゲートウェイでは、次のことを実行できます。

- NFS バージョン 3 または 4.1 プロトコルを使用して、ファイルを直接保存し取得できます。
- SMB ファイルシステムのバージョン 2 および 3 のプロトコルを使用してファイルを直接保存および取得できます。
- Amazon S3 のデータには、任意の AWS クラウドアプリケーションまたはサービスから直接アクセスできます。
- ライフサイクルポリシー、クロスリージョンレプリケーション、およびバージョニングを使用して S3 のデータを管理できます。S3 ファイルゲートウェイは、Amazon S3 上にマウントされたファイルシステムと考えることができます。

S3 ファイルゲートウェイは Amazon S3 のファイルストレージを簡素化し、既存のアプリケーションを業界標準ファイルシステムプロトコルと統合して、オンプレミスのストレージに代わるコスト効率の高い選択肢を提供します。また、透過的なローカルキャッシュを通じてデータへの低レイテンシーアクセスを提供します。S3 File Gateway は、との間のデータ転送を管理し AWS、ネットワークの輻輳からアプリケーションをバッファし、データを並行して最適化してストリーミングし、帯域幅の消費を管理します。

S3 File Gateway は、次のような他の AWS サービスと統合されます。

- AWS Identity and Access Management (IAM) を使用した一般的なアクセス管理
- AWS Key Management Service (AWS KMS) を使用した暗号化
- Amazon CloudWatch (CloudWatch) を使用したモニタリング
- AWS CloudTrail (CloudTrail) を使用した監査

- AWS マネジメントコンソール および AWS Command Line Interface (AWS CLI) を使用したオペレーション
- 請求情報とコスト管理

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

- S3 ファイルゲートウェイを作成および使用方法について説明しています。ここでは、ファイル共有を作成する方法、ドライブを Amazon S3 バケットにマッピングする方法、ファイルとフォルダを Amazon S3 にアップロードする方法を確認できます。

- すべてのゲートウェイタイプおよびリソースに対する管理タスクの実行方法について説明しています。

このガイドでは、主に AWS マネジメントコンソールを使用したゲートウェイ操作の方法について参照できます。プログラムによってこれらのオペレーションを実行する場合は、AWS Storage Gateway API リファレンスを参照してください。

Amazon S3 ファイルゲートウェイの仕組み

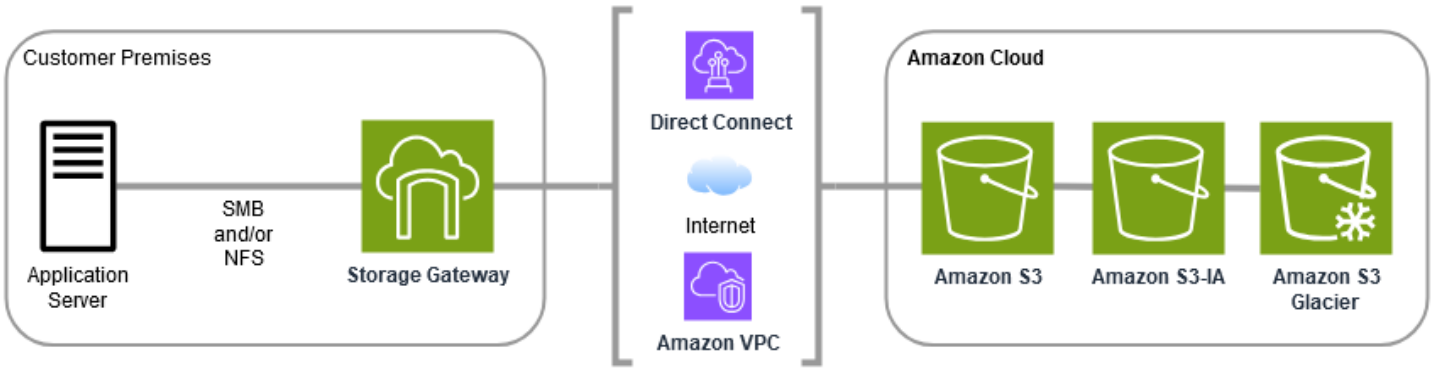
S3 ファイルゲートウェイを使用する際には、最初に、ファイルゲートウェイの VM イメージをダウンロードします。次に、 または Storage Gateway API AWS マネジメントコンソール を使用してゲートウェイをアクティブ化します。S3 ファイルゲートウェイは、Amazon EC2 イメージを使用して作成することもできます。

S3 ファイルゲートウェイを有効化した後、ファイル共有を作成および設定し、この共有を Amazon Simple Storage Service (Amazon S3) バケットに関連付けます。これにより、NFS (Network File System) または SMB (Server Message Block) プロトコルを使用して、クライアントからファイル共有にアクセスできるようになります。ファイル共有に書き込まれたファイルは Amazon S3 内のオブジェクトになり、そのパスがキーになります。ファイルとオブジェクトの間には 1 対 1 のマッピングがあり、ファイルを変更するたびに、ゲートウェイは Amazon S3 のオブジェクトを非同期的に更新します。Amazon S3 バケット内の既存のオブジェクトは、ファイルシステム内のファイルとして表示され、そのキーがパスになります。オブジェクトは、Amazon S3 のサーバー側暗号化キー (SSE-S3) により暗号化されます。すべてのデータ転送は、HTTPS 経由で実行されます。

Amazon S3 に HTTPS データアップロードリクエストを送信すると、ファイルゲートウェイは Content-MD5 ヘッダーにアップロードされるデータの MD5 チェックサムを入力します。このヘッダーを使用すると、Amazon S3 によって計算された MD5 チェックサムとファイルゲートウェイから受信した値が一致しない場合、Amazon S3 は失敗を返します。このような障害が返された場合、ファイルゲートウェイはリクエストを再送信します。

このサービスは、ゲートウェイ間のデータ転送を最適化し、マルチパート並列アップロードまたはバイト範囲のダウンロード AWS を使用して、使用可能な帯域幅をより適切に使用します。ローカルキャッシュの目的は、最近アクセスしたデータへの低レイテンシーなアクセスを提供し、データ出力にかかる料金を削減することです。CloudWatch メトリクスからは、VM でのリソースの使用状況と、 AWSとの間のデータ転送に関するインサイトが得られます。CloudTrail はすべての API コールを追跡します。

S3 ファイルゲートウェイストレージを使用すると、クラウド ワークロードの Amazon S3 への取り込み、バックアップとアーカイブの実行、 AWS クラウドへのストレージデータの階層化と移行などのタスクを行うことができます。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。



ファイルを Amazon S3 にアップロードする際、S3 ファイルゲートウェイは、対象のファイルを S3 オブジェクトに変換します。S3 ファイルゲートウェイと S3 オブジェクトの間で、ファイル共有に対し相互的なファイル操作を実行する場合、ファイルとオブジェクトの変換時に実行される特定の処理には慎重な検討が必要となります。

一般的なファイル操作では、ファイルのメタデータが変更されることで現在の S3 オブジェクトが削除され、新しい S3 オブジェクトが作成されます。次の表に、ファイル操作の例と、それらが S3 オブジェクトに与える影響を示します。

ファイル操作	S3 オブジェクトに対する影響	ストレージクラスの関係性
ファイルの名前変更	ファイルごとに新しい S3 オブジェクトを作成し、既存の S3 オブジェクトを置き換える	早期削除および取り出しには、料金が発生する場合があります
フォルダの名前変更	フォルダ構造内のフォルダとファイルごとに新しい S3 オブジェクトを作成し、既存の S3 オブジェクトをすべて置き換える	早期削除および取り出しには、料金が発生する場合があります
ファイル/フォルダーのアクセス許可の変更	ファイルまたはフォルダごとに新しい S3 オブジェクトを作成し、既存の S3 オブジェクトを置き換える	早期削除および取り出しには、料金が発生する場合があります
ファイル/フォルダーの所有権の変更	ファイルまたはフォルダごとに新しい S3 オブジェクトを作成し、既存の S3 オブジェクトを置き換える	早期削除および取り出しには、料金が発生する場合があります
ファイルへの追加	ファイルごとに新しい S3 オブジェクトを作成し、既存の S3 オブジェクトを置き換える	早期削除および取り出しには、料金が発生する場合があります

NFS または SMB クライアントによってS3 ファイルゲートウェイにファイルが書き込まれると、ファイルゲートウェイによりファイルデータが Amazon S3 にアップロードされます。その後、メタデータ (所有権、タイムスタンプなど) がアップロードされます。ファイルデータがアップロードされると S3 オブジェクトが作成され、ファイルのメタデータをアップロードされると S3 オブジェクトのメタデータが更新されます。このプロセスにより、別のバージョンのオブジェクトが作成され、オブジェクトのバーションが 2 つになります。S3 バージョニングがオンである場合、両方のバージョンが保存されます。

Amazon S3 にアップロードされたファイルが、NFS または SMB クライアントによって S3 ファイルゲートウェイ内で変更されると、ファイルゲートウェイはファイル全体をアップロードするの

ではなく、新しいデータまたは変更されたデータのみをアップロードします。ファイルの変更により、S3 オブジェクトの新しいバージョンが作成されます。

S3 ファイルゲートウェイが大きなファイルをアップロードする際は、クライアントが S3 ファイルゲートウェイへの書き込みを実行する間に、ファイルを小さなチャンクに分割しアップロードする場合があります。これは、キャッシュ領域が解放されることや、ファイル共有への書き込み率が高くなることなどが理由です。この処理では、S3 バケットで複数バージョンのオブジェクトが作成されることがあります。

オブジェクトを異なるストレージクラスに移動するライフサイクルポリシーを設定する前に、S3 バケットをモニタリングして、オブジェクトのバージョン数を確認する必要があります。S3 バケット内のオブジェクトのバージョン数を最小限に抑えるには、過去のバージョンのライフサイクルに有効期限を設定する必要があります。S3 バケット間で、同一リージョンでのレプリケーション (SRR) またはクロスリージョンでのレプリケーション (CRR) を使用すると、使用されるストレージが増加します。

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/files3/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

- アクセスAWS Storage Gateway - 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。
- アクセスAWS Storage Gateway - 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AWSSDKs 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。

にサインアップするAWS アカウント

の使用を開始するにはAWS、 が必要ですAWS アカウント。の作成の詳細についてはAWS アカウント、 AWS アカウント管理リファレンスガイドの「 の開始方法AWS アカウント」を参照してください。

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、ファイル共有の作成・・削除・、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 GatewayApplication 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。

AWSSDKs 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、それぞれに冗長電源、ネットワーク、および接続があり、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。たとえば、Amazon EC2 インスタンスを起動して欧州AWS リージョンの AWS Storage Gatewayでアプライアンスをホストし、欧州のユーザーの近くにいるか、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。

- 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 S3 ファイルゲートウェイ (S3 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:

- 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。

ファイルゲートウェイのパフォーマンスのベストプラクティスについては、「S3 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」を参照してください。

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)

詳細については、S3 ファイルゲートウェイスループットの最大化を参照してください。ハードウェアがゲートウェイ VM のパフォーマンスにどのように影響を与えるかについては、ファイル共有のクォータを参照してください。

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。
> アプリケーションによる書き込みは同期的にキャッシュに保存され、その後、Amazon S3 の永続的なストレージに非同期的にアップロードされます。アップロードが完了する前にインスタンスが停止したために一時ストレージが失われた場合、キャッシュ内に残っていて Amazon Simple Storage Service (Amazon S3) にまだ書き込まれていないデータが失われる可能性があります。ゲートウェイをホストするインスタンスを停止する前に、`CachePercentDirty` CloudWatch のメトリクスが `0` であることを確認してください。エフェメラルストレージの詳細については、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。ストレージゲートウェイのメトリクスのモニタリングの詳細についてはS3 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。
> S3 バケットに 500 万個を超えるオブジェクトがあり、gp2 EBS ボリュームを使用している場合、ゲートウェイの起動時に許容できるパフォーマンスを確保するには、ルート EBS ボリュームを最小 350 GiB にする必要があります。新しく作成された Amazon EC2 ファイルゲートウェイインスタンスはデフォルトで gp3 ルートボリュームを使用しますが、この要件はありません。ボリュームサイズを引き上げる方法については、「Elastic Volumes を使用して EBS ボリュームを変更する (コンソール)」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。

ゲートウェイクォータの詳細については、ファイル共有のクォータを参照してください。

ネットワークとファイアウォールの要件

ゲートウェイには、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
- 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
- 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
- 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

ポート要件

S3 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 NFS または SMB クライアント、VPC エンドポイント、Microsoft Active Directory に接続するときなど、特定の設定にのみ必要です。

S3 ファイルゲートウェイでは、ドメイン ユーザーにサーバー メッセージ ブロック (SMB) ファイル共有へのアクセスを許可する場合にのみ、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。

S3 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 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、

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
								ポート 80 へのパブリックアクセスは不要です。ポート 80 へのアクセスに必要なレベルはネットワークの設定によって決まります。Storage Gateway マネジメントコンソールからゲートウェイをアクティブ化する場

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
								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。
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)

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
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

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
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。 *SMB にのみ必要。
Microsoft Active Directory	Storage Gateway VM	Active Directory サーバー	UDP NetBIOS	137	✓	✓	✓*	サービス名 *SMBv1 にのみ必要です。

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
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 *SMBv1 にのみ必要です。
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 *SMB にのみ必要。
Microsoft Active Directory	Storage Gateway VM	Active Directory サーバー	TCP および UDP Kerberos	88	✓	✓	✓*	Kerberos *SMB にのみ必要。

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 *SMB にのみ必要。

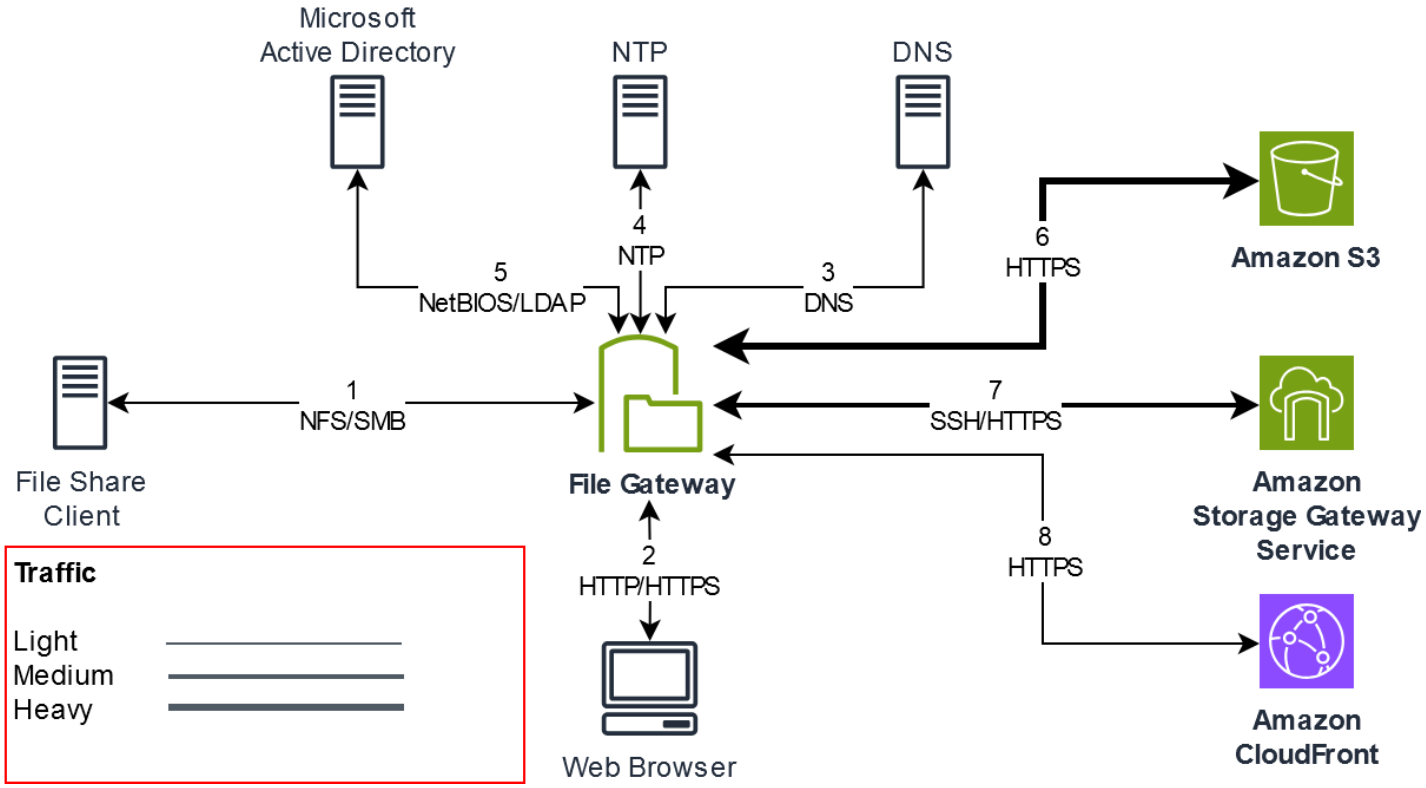
ネットワーク要素	から	まで	プロトコル	ポート	インバウンド	アウトバウンド	必須	注意事項
Microsoft Active Directory	Storage Gateway VM	Active Directory サーバー	TCP 分散コンピューティング環境/エンドポイント マッパー (DCE/EMAP)	49152-65535	✓	✓	✓*	RPC または、AD ドメインコントローラーが専用 RPC ポートを使用している場合は、代わりにそれらを開きます。 *SMB にのみ必要。

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
ファイル共有クライアント	NFS クライアント	Storage Gateway VM	TCP または UDP データ NFSv3	111	✓	✓	✓*	ファイル共有データ転送 (NFS v3 のみ) *NFS にのみ必要です。
ファイル共有クライアント	NFS クライアント	Storage Gateway VM	TCP または UDP NFS	2049	✓	✓	✓*	ファイル共有データ転送 *NFS v3 および v4 にのみ必要です。
ファイル共有クライアント	NFS クライアント	Storage Gateway VM	TCP または UDP NFSv3	20048	✓	✓	✓*	ファイル共有データ転送 *NFSv3 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
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 SMBv2	139	✓	✓	✓*	ファイル共有データ転送セッションサービス *SMB にのみ必要。

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
Amazon S3	Storage Gateway VM	Amazon S3 サービスエンドポイント	TCP HTTPS	443	✓	✓	✓	Storage Gateway VM から AWS サービスエンドポイントへの通信用。サービスエンドポイントの詳細については、「ファイアウォールとルーターを介した Allowing AWS Storage Gateway アクセス」を参照してください。

次の図は、基本的な S3 ファイルゲートウェイデプロイのネットワークトラフィックフローを示しています。



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。

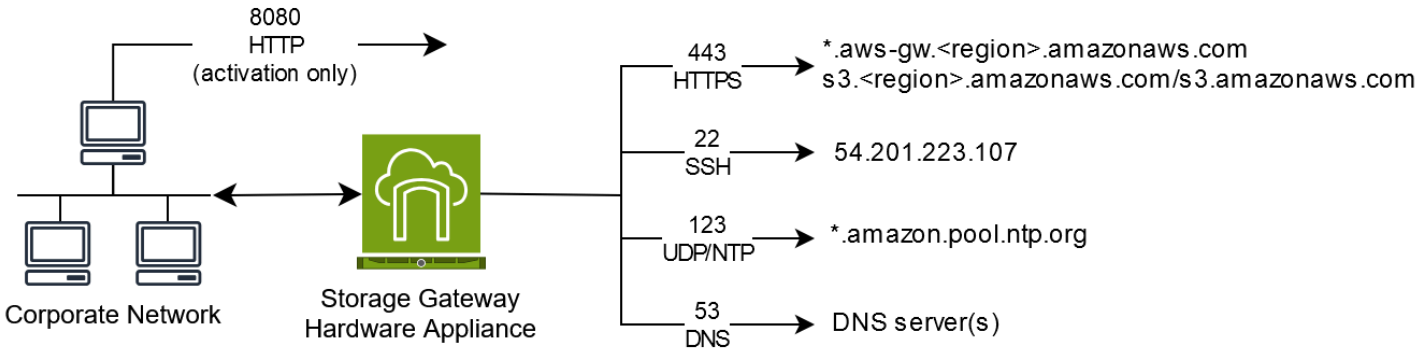
- インターネットアクセス – サーバー上の任意のネットワークインターフェイスを介した、インターネットへの常時接続のネットワーク接続。
- DNS サービス – ハードウェアアプライアンスと DNS サーバー間の通信のための DNS サービス。
- 時刻同期 – 自動的に設定された Amazon NTP タイムサービスへのアクセス。
- IP アドレス – 割り当てられた DHCP または静的 IPv4 アドレス。IPv6 アドレスを割り当てることはできません。

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
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

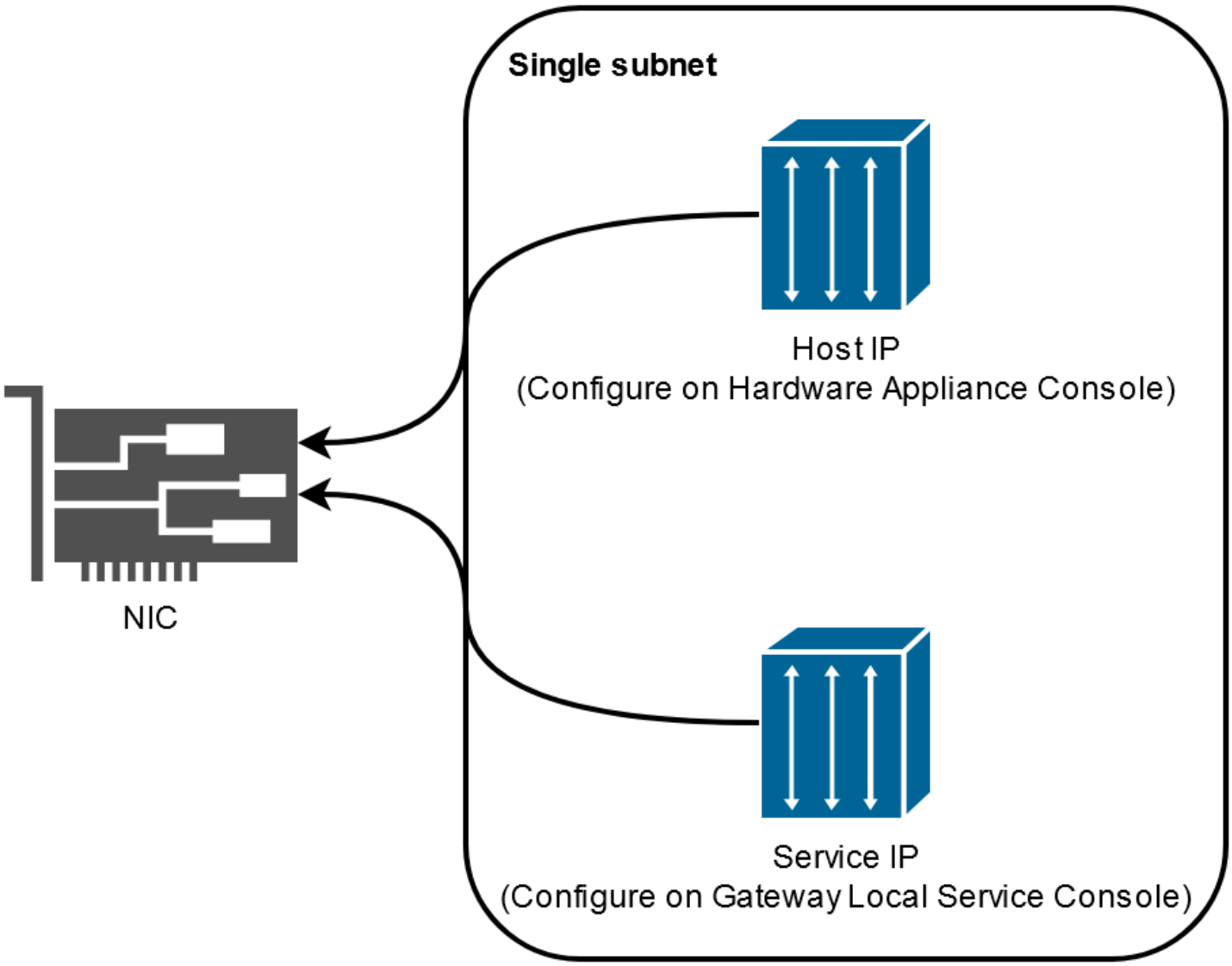
プロトコル	ポート	Direction	ソース	目的地	使用方法
					ン (短時間のみ)

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
```

デュアルスタックのエンドポイント

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 AWSの間の IPv4 および IPv6 トラフィックをサポートします。

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デュアルスタックサービスエンドポイントが必要です。

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

コントロールパス (アクティベーション、コントロールプレーン、プロキシ) およびデータパス (データプレーン) オペレーションには、すべてのゲートウェイで次のデュアルスタックサービスエンドポイントが必要です。

```
activation-storagegateway.region.api.aws:443
controlplane-storagegateway.region.api.aws:443
proxy-storagegateway.region.api.aws:443
dataplane-storagegateway.region.api.aws: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.api.aws: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.api.aws:443
```

Amazon S3 サービスエンドポイント

Amazon S3 ファイルゲートウェイでは、Amazon S3 サービスに接続するために次の 3 種類のエンドポイントが必要です。

Amazon S3 サービスエンドポイント

> **Note**
>
> このエンドポイントの場合のみ、FIPS 準拠のデプロイでは s3 を s3-fips に置き換えないでください。

```
s3.amazonaws.com
```

Amazon S3 リージョンエンドポイント

```
s3.region.amazonaws.com (Standard)
s3.dualstack.region.amazonaws.com (Dual-stack)
```

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

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

次の例は、米国西部 (北カリフォルニア) リージョン(us-west-1) の標準およびデュアルスタックの FIPS 準拠の Amazon S3 リージョンエンドポイントを示しています。

```
s3-fips.us-west-1.amazonaws.com
s3-fips.dualstack.us-west-1.amazonaws.com
```

次の例は、リージョンで使用される標準およびデュアルスタック AWS GovCloud (US) の Amazon S3 リージョンエンドポイントを示しています。

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

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

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

Amazon S3 バケットエンドポイント

```
bucket-name.s3.region.amazonaws.com (Standard)
bucket-name.s3.dualstack.region.amazonaws.com (Dual-stack)
```

以下の例は、米国東部 (オハイオ) リージョン (us-east-2) にある *amzn-s3-demo-bucket* という名前のバケットに対する、標準およびデュアルスタックのAmazon S3 バケットエンドポイントを示しています。

```
amzn-s3-demo-bucket.s3.us-east-2.amazonaws.com (Standard)
amzn-s3-demo-bucket.s3.dualstack.us-east-2.amazonaws.com (Dual-stack)
```

次の例は、 AWS GovCloud (US-East) リージョン () *amzn-s3-demo-bucket1*の という名前のバケットの標準およびデュアルスタックの FIPS 準拠の Amazon S3 バケットエンドポイントを示していますus-gov-east-1。

```
amzn-s3-demo-bucket1.s3-fips.us-gov-east-1.amazonaws.com (FIPS)
amzn-s3-demo-bucket1.s3-fips.dualstack.us-gov-east-1.amazonaws.com (FIPS dual-stack)
```

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 AWS リージョン および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 ゲートウェイのトラブルシューティングを支援 サポート したい」を参照してください。

ゲートウェイで開くポートについては、ポート要件を参照してください。

サポートされているハイパーバイザーとホストの要件

Storage Gateway は、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、qcow のダウンロードごとにクイックセットアップ設定として提供されます。

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、S3 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 NFS および SMB クライアント

ファイルゲートウェイは次のクライアントをサポートしています。

オペレーティングシステムのバージョン	カーネルバージョン	サポートされるプロトコル
Amazon Linux 2023	6.1 LTS	NFSv4.1,NFSv3
Amazon Linux 2	5.10 LTS	NFSv4.1,NFSv3
RHEL 9	5.14	NFSv4.1,NFSv3
RHEL 8.10	4.18	NFSv4.1,NFSv3
SUSE 15	6.4	NFSv4.1,NFSv3
Ubuntu 24.04 LTS	6.8 LTS	NFSv4.1,NFSv3
Ubuntu 22.04 LTS	5.15 LTS	NFSv4.1,NFSv3
Microsoft Windows Server 2025		SMBv2、SMBv3、NFSv3
Microsoft Windows Server 2022		SMBv2、SMBv3、NFSv3
Microsoft Windows 11		SMBv2、SMBv3、NFSv3

オペレーティングシステムのバージョン	カーネルバージョン	サポートされるプロトコル
Microsoft Windows 10		SMBv2、SMBv3、NFSv3

> **Note**
>
> サーバーメッセージブロック (SMB) 暗号化には、SMB v3 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

NFS または SMB クライアントは、ファイルの書き込み、読み取り、削除、切り捨てができます。クライアントが書き込みを に送信すると AWS Storage Gateway、ローカルキャッシュに同期的に書き込みます。次に、最適化された転送を介して非同期的に Amazon S3 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。データがない場合は、リードスルーキャッシュとして S3 から取得されます。

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。削除は Amazon S3 からオブジェクトを削除します。ディレクトリは、Amazon S3 コンソールと同じ構文を使用して、S3 のフォルダオブジェクトとして管理されます。

GET、PUT、UPDATE、及びDELETE などの HTTP オペレーションでは、ファイル共有内のファイルを変更できます。これらのオペレーションはアトミックな作成、読み取り、更新、削除 (CRUD) 機能に従っています。

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 S3 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

S3 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。S3 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。S3 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 (S3 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、S3 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

このセクションでは、ゲートウェイのキャッシュストレージとしてエフェメラルディスクを選択した場合に、データ損失を防ぐために必要な手順について説明します。

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。エフェメラルディスクは、ゲートウェイのキャッシュストレージなど、頻繁に変更されるデータを一時的に保存するのに理想的です。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、Amazon S3 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、Amazon S3 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。このようなデータ損失を防ぐには、ゲートウェイをホストする EC2 インスタンスを再起動または停止する前に、次の手順に従います。

> **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。

以下の手順のステップは、ファイルゲートウェイに固有です。

エフェメラルディスクを使用するファイルゲートウェイのデータ損失を防ぐ方法

1. Amazon S3 に書き込んでいるすべてのプロセスを停止します。
2. CloudWatch Events からの通知を受信するにはサブスクライブします。詳細については、ファイルオペレーションについての通知を受信するを参照してください。
3. NotifyWhenUploaded API を呼び出し、書き込まれたデータが、エフェメラルストレージが失われるまでに、恒久的に Amazon S3 に保存されたときに、通知を受け取るようにします。
4. API が完了するのを待って、通知 ID を受け取ります。

   同じ通知 ID を持つ CloudWatch イベントを受け取ります。
5. ファイル共有の `CachePercentDirty` メトリクスが 0 であることを確認します。これにより、すべてのデータが Amazon S3 に書き込まれたことが確認できます。ファイル共有のメトリクスの詳細については、ファイル共有メトリクスについてを参照してください。
6. これでデータを失うリスクなく、ファイルゲートウェイを再起動または停止できるようになりました。

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 が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、および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。

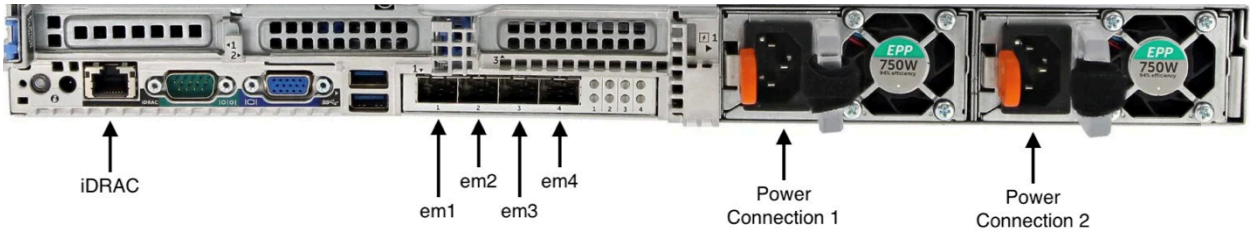
- 電源ケーブル: 1 つは必須です。2 つを推奨します。
- サポートされているネットワークケーブル (ハードウェアアプライアンスに組み込まれているネットワークインターフェイスカード (NIC) によって異なります)。Twinax 銅線 DAC、SFP+ 光モジュール (Intel 互換)、または Base-T 向け SFP 銅線トランシーバ。
- キーボードとモニター、またはキーボード、ビデオ、マウス (KVM) スイッチソリューション。

> **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。

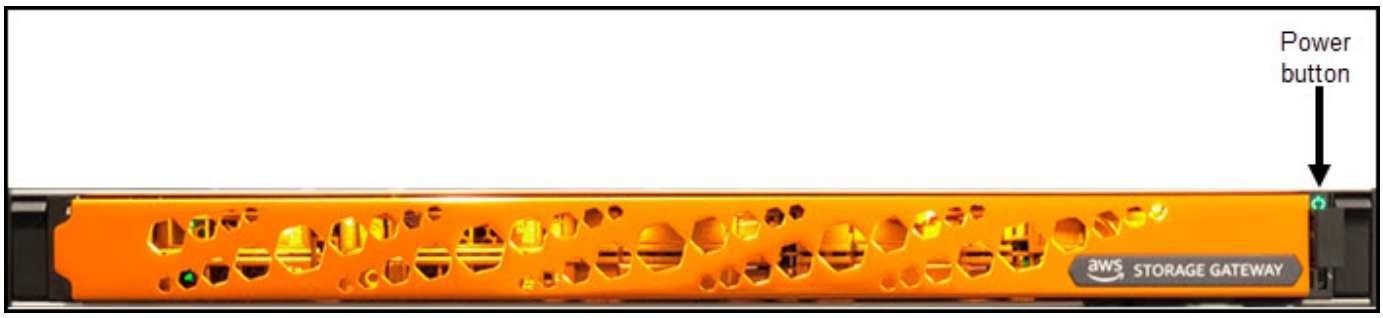


ハードウェアアプライアンス 1 の背面。ネットワークや電源のコネクタのラベルが表示されています。

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、要件にリストされている AWS エンドポイントへの同じ常時オン接続を提供する必要があります。
> ネットワークボンディングと 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から、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 S3 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、「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オンプレミス」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

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 S3 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 S3 ファイルゲートウェイのセットアップ
- Amazon S3 ファイルゲートウェイを に接続する AWS
- 設定を確認し、Amazon S3 ファイルゲートウェイをアクティブ化
- Amazon S3 ファイルゲートウェイの設定

Amazon S3 ファイルゲートウェイのセットアップ

新しい S3 ファイルゲートウェイを設定する

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 S3 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。
      - Nutanix AHV – Linux カーネルベースの仮想マシン (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。同じイメージは、Linux KVM 環境と Nutanix AHV ハイパーバイザー環境の両方で機能します。
      - Amazon EC2 - ゲートウェイをホストするように Amazon EC2 インスタンスを設定し、起動します。

- 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] では、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ため、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 S3 ファイルゲートウェイを に接続する AWS

新しい S3 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 S3 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. [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。詳細については、「ゲートウェイ IP アドレスの取得」を参照してください。
   - 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。
3. [エンドポイントオプション] セクションで、次の操作を行います。

   a. 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 検証済みの暗号化モジュールが必要な場合は、FIPS 準拠のエンドポイントを使用します。詳細については、連邦情報処理規格 (FIPS) 140-2 を参照してください。
> FIPS のサービスエンドポイントは、一部の AWS リージョンでのみ使用できます。詳細については、AWS 全般のリファレンスの「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。

> **Note**
>
> ゲートウェイの作成に現在使用している AWS アカウント 以外の に属する VPC エンドポイントを指定するには、その DNS 名または IP アドレスを指定する必要があります。

b. IP バージョンの場合は、ゲートウェイが AWSとの通信に使用するプロトコルバージョンとエンドポイントを選択します。

> **Note**
>
> ゲートウェイの IP アドレスは、ここで指定した IP バージョンと一致する必要があります。デュアルスタックエンドポイントは IPv4 および IPv6 接続を受け入れますが、選択した IP バージョンを使用してのみゲートウェイと通信します。

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 S3 ファイルゲートウェイをアクティブ化

設定を確認して新しい S3 ファイルゲートウェイをアクティブ化する

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 S3 ファイルゲートウェイのセットアップ
   - Amazon S3 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 S3 ファイルゲートウェイの設定

新しい S3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 S3 ファイルゲートウェイのセットアップ
   - Amazon S3 ファイルゲートウェイを に接続する AWS
   - 設定を確認し、Amazon S3 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 — ゲートウェイのメトリクスに関する CloudWatch の通知を受信しません。

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。

ゲートウェイの作成はこれで完了です。次は、ゲートウェイで使用するファイル共有を作成する必要があります。手順については、「ファイル共有の作成」 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 Storage Gateway 用の VPC エンドポイントを作成し、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 S3 ファイルゲートウェイを接続して 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 S3 ファイルゲートウェイを設定するには、Amazon S3 用に別の VPC エンドポイントを作成し、ゲートウェイのファイル共有を作成するときにこの VPC エンドポイントを指定する必要があります。

> **Note**
>
> Storage Gateway の VPC エンドポイントを作成するリージョン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、ファイル共有用に設定した Amazon S3 ストレージはAmazon S3 の VPC エンドポイントを作成するリージョンと同じリージョンにある必要があります。

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 S3 ファイルゲートウェイの作成とアクティブ化を参照してください。

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。

> **Important**
>
> VPC を介してデータを転送するように S3 ファイルゲートウェイを設定するには、Amazon S3 用に別の VPC エンドポイントを作成し、ゲートウェイのファイル共有を作成するときにこの VPC エンドポイントを指定する必要があります。
> これを行うには、上記と同じ手順に従いますが、サービス名で`com.amazonaws.region.s3`を選択し、サブネット/セキュリティグループの代わりに S3 エンドポイントを関連付けるルートテーブルを選択します。手順については、ゲートウェイエンドポイントの作成を参照してください。

ファイル共有の作成

このセクション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) プロトコルを使用してアクセスできるファイル共有を作成できます。

NFS 共有を作成すると、デフォルトでは、NFS サーバーにアクセスできるすべてのユーザーが NFS ファイル共有にアクセスできます。IP アドレスでクライアントへのアクセスを制限することができます。

SMB ファイル共有を作成するときは、次の 3 つの認証モードのいずれかを使用できます。

- Microsoft Active Directory (AD) アクセスによるファイル共有。認証された Microsoft AD ユーザーはこのファイル共有タイプへのアクセスを取得します。
- アクセスが制限された SMB ファイル共有。指定した特定のドメインユーザーとグループのみにアクセスが許可されます (許可リスト経由)。ユーザーおよびグループはアクセスを拒否される場合もあります (拒否リスト経由)。
- ゲストアクセスによる SMB ファイル共有。ゲストパスワードを使用できるすべてのユーザーは、このファイル共有にアクセスできます。

> **Note**
>
> ゲートウェイを介して NFS ファイル共有にエクスポートされたファイル共有は、POSIX のアクセス許可をサポートします。SMB ファイル共有の場合は、アクセスコントロールリスト (ACL) を使用して、ファイル共有内のファイルおよびフォルダに対するアクセス許可を管理できます。詳細については、「Windows ACL を使用して SMB ファイル共有へのアクセスを制限する」を参照してください。

ファイルゲートウェイでは、さまざまなタイプの 1 つ以上のファイル共有をホストできます。ファイルゲートウェイには複数の NFS および SMB ファイル共有を作成できます。

> **Important**
>
> ファイル共有を作成するには、ファイルゲートウェイで AWS Security Token Service() をアクティブ化する必要がありますAWS STS。ファイルゲートウェイを作成する で AWS リージョンがアクティブ化されていない場合AWS STSは、アクティブ化します。アクティブ化する方法の詳細についてはAWS STS、「 AWS Identity and Access Managementユーザーガイ

ド」の「 AWSリージョンAWS Security Token Serviceでのアクティブ化と非アクティブ化」を参照してください。

トピック

ゲートウェイデータをアップロードする際の予期しないコストを回避する

NFS クライアントによってファイルゲートウェイにファイルが書き込まれると、ファイルゲートウェイによりファイルデータに続いてメタデータが Amazon S3 にアップロードされます。ファイルデータがアップロードされると S3 オブジェクトが作成され、ファイルのメタデータをアップロードされると S3 オブジェクトのメタデータが更新されます。このプロセスでは、オブジェクトの追加バージョンが作成されます。S3 バージョニングが有効になっている場合、両方のバージョンが保存されます。

ファイルゲートウェイに保存されているファイルのメタデータを変更すると、新しい S3 オブジェクトが作成され、既存の S3 オブジェクトに置き換わります。この動作は、ファイルを編集しても新しいファイルが作成されないファイルシステム内のファイルの編集とは異なります。AWSStorage Gatewayで使用する予定のすべてのファイルオペレーションをテストして、各ファイルオペレーションが Amazon S3 ストレージとどのように相互作用するかを理解します。

Amazon S3 を用いてファイルゲートウェイからデータをアップロードされる際には、S3 バージョニングおよびクロスリージョンレプリケーション（CRR）のご利用について、十分にご検討ください。S3 バージョニングが有効になっている場合にファイルゲートウェイから Amazon S3 にファイルをアップロードすると、一般的に S3 オブジェクトの複数のバージョンが生成されます。

いくつかの手順で実行するファイルアップロードなど、大きなファイルおよびファイルの書き込みパターンを含む特定のワークフローでは、保存される S3 オブジェクトのバージョン数が増える可能性があります。ファイルの書き込みレートが高いためにファイルゲートウェイのキャッシュを解放する

必要がある場合、複数の S3 オブジェクトバージョンが作成される可能性があります。これらのシナリオでは、S3 バージョニングが有効になっている場合 S3 ストレージが増加し、CRR に関連する転送コストが増加します。Storage Gateway で使用する予定のすべてのファイルオペレーションをテストして、各ファイルオペレーションが Amazon S3 ストレージとどのように相互作用するかを理解する必要があります。

ファイルゲートウェイで Rsync ユーティリティを使用すると、キャッシュにファイル、Amazon S3 に S3 オブジェクトが一時的に作成されます。この状況により、S3 Standard-Infrequent Access (S3 Standard-IA) ストレージクラスにおいて早期削除料金が発生します。

Amazon S3 のファイルゲートウェイによって保存されているオブジェクトを暗号化する

S3 ファイルゲートウェイは、Amazon S3 に保存するデータのサーバー側の暗号化に次の方法をサポートしています。

- SSE-S3 - デフォルトでは、Amazon S3 バケットにアップロードされるすべての新しいオブジェクトは、Amazon S3 マネージドキーを使用して、サーバー側の暗号化を使用します。詳細については、「Amazon Simple Storage Service ユーザーガイド」の「Amazon S3 マネージドキーによるサーバー側の暗号化の使用」を参照してください。
- SSE-KMS — AWS Key Management Service(AWS KMS) マネージドキーでサーバー側の暗号化を使用するようにファイル共有を設定できます。AWS KMS は、安全で可用性の高いハードウェアとソフトウェアを組み合わせて、クラウド向けにスケーリングされたキー管理システムを提供するサービスです。詳細については、AWS「 Key Management Service とは」を参照してください。「 AWS Key Management Serviceデベロッパーガイド」の「
- DSSE-KMS — AWS KMSキーによる二層式サーバー側の暗号化は、オブジェクトが Amazon S3 にアップロードされると 2 つの暗号化レイヤーをオブジェクトに適用します。これは、マルチレイヤー暗号化のコンプライアンス基準を満たすのに役立ちます。詳細については、「Amazon Simple Storage Service ユーザーガイド」のAWS KMS「キーによる二層式サーバー側の暗号化の使用」を参照してください。

> **Note**
>
> DSSE-KMS および AWS KMSキーの使用には追加料金がかかります。詳細については、「AWS KMS 料金表」を参照してください。

Storage Gateway コンソールまたは Storage Gateway API を使用して、新しいファイル共有を作成するときに暗号化方法を指定できます。コンソールの手順については、「カスタム設定を使用して NFS ファイル共有を作成する」または「カスタム設定で SMB ファイル共有を作成する」を参照してください。対応する API コマンドの詳細については、AWSStorage Gateway API リファレンスの「CreateNFSFileShare」または「CreateSMBFileShare」を参照してください。

Storage Gateway コンソールまたは Storage Gateway API を使用して、既存のファイル共有の暗号化設定を更新することもできます。コンソールの手順については、「既存のファイル共有のサーバー側の暗号化方法を変更する」を参照してください。対応する API コマンドの詳細については、AWSStorage Gateway API リファレンスの「UpdateNFSFileShare」または「UpdateSMBFileShare」を参照してください。

> **Note**
>
> 暗号化方法を更新すると、ゲートウェイは Amazon S3 で作成するすべての新しいオブジェクトと、今後更新または変更される保存済みオブジェクトに対して新しい方法を使用します。既存の Amazon S3 オブジェクトは、ゲートウェイによって更新または変更された場合にのみ、新しい暗号化方法を受け取ります。

> **Important**
>
> ファイル共有が、データを保存する Amazon S3 バケットと同じ暗号化タイプを使用していることを確認してください。
> 暗号化に SSE-KMS または DSSE-KMS を使用するようにファイルゲートウェイを設定する場合は、ファイル共有に関連付けられた IAM ロールに `kms:Encrypt`、`kms:Decrypt`、`kms:ReEncrypt*`、`kms:GenerateDataKey`、`kms:DescribeKey` のアクセス許可を手動で追加する必要があります。詳細については、「Storage Gateway でアイデンティティベースのポリシー (IAM ポリシー) を使用する」を参照してください。

NFS ファイル共有を作成する

Network File System (NFS) プロトコルは、Unix ベースのシステム用のステートフルファイル共有プロトコルです。NFS 対応クライアントと NFS サーバーが通信する際、クライアントはリモートプロシージャコール (RPC) を使用してサーバーにファイルまたはディレクトリを要求します。サーバーは、そのファイルまたはディレクトリが利用可能であること、そしてクライアントが必要なアクセス

許可を持っていることを確認します。その後、サーバーはファイルまたはディレクトリをクライアント側にリモートでマウントし、仮想接続を通じてアクセスを共有します。クライアントの操作において、NFS はリモートサーバー上のファイルを、ローカルファイルにアクセスするのと同じように扱えるようにします。

> **Note**
>
> NFS プロトコルは、ユーザーごとに最大 16 個のグループをサポートしています。ユーザーが 16 個を超えるグループに所属している場合、NFS ファイル共有をマウントできない問題が発生する可能性があります。マウントの問題を避けるために、NFS ファイル共有へアクセスする際は、ユーザーが所属するグループ数を 16 以下にしておいてください。

以下のトピックでは、ファイルゲートウェイの NFS ファイル共有を作成するさまざまな方法について説明します。

目次

デフォルト設定を使用して NFS ファイル共有を作成する

このセクションでは、事前設定されたデフォルト設定を使用して新しいネットワークファイルシステム (NFS) ファイル共有を作成する方法について説明します。この方法は、基本的なデプロイ、個人使用、テスト、または後で編集およびカスタマイズする予定の複数のファイル共有をすばやくデプロイする方法として使用します。この手順を使用して作成するファイル共有のデフォルト設定のリストについては、「NFS ファイル共有のデフォルト設定」を参照してください。より詳細な制御が必要な場合、またはファイル共有に高度な設定を使用する場合は、「カスタム設定を使用して NFS ファイル共有を作成する」を参照してください。

> **Note**
>
> 仮想プライベートクラウド (VPC)を介してファイル共有を Amazon S3 に接続する必要がある場合は、カスタム設定手順に従う必要があります。ファイル共有の作成後に VPC 設定を編集することはできません。

> **Important**
>
> ファイルゲートウェイからデータをアップロードするときに S3 バージョニング、クロスリージョンレプリケーション、または Rsync ユーティリティを使用すると、コストに大きな影響が生じる可能性があります。詳細については、「ファイルゲートウェイからデータをアップロードする際の予期しないコストを回避する」を参照してください。

デフォルト設定を使用して NFS ファイル共有を作成するには。

1. https://console.aws.amazon.com/storagegateway/home/ で AWS Storage Gatewayコンソールを開き、左側のナビゲーションペインからファイル共有を選択します。
2. [ファイル共有の作成] を選択します。
3. ゲートウェイ で、リストから Amazon S3 ファイルゲートウェイを選択します。
4. ファイル共有プロトコルで、NFS を選択します。
5. S3 バケットで、次のいずれかを実行します。

   - ドロップダウンリストからアカウント内の既存の Amazon S3 バケットを選択します。
   - ドロップダウンリストから別のアカウントのバケットを選択し、クロスアカウントバケット名にバケットの名前を入力します。
   - [新しい S3 バケットの作成] を選択し、新しいバケットの Amazon S3 エンドポイントがある AWS リージョン を選択し、一意の S3 バケット名を入力します。完了したら、[S3 バケットの作成] を選択します。

     新しいバケットの作成についての詳細は、Amazon S3 ユーザーガイドの「S3 バケットを作成するには」を参照してください。

> **Note**
>
> S3 ファイルゲートウェイは、バケット名にピリオド (.) を使った Amazon S3 バケットをサポートしていません。
> バケット名が Amazon S3 のバケット命名ルールに準拠していることを確認します。詳細については、「Amazon Simple Storage Service ユーザーガイド」で「バケットの命名規則」を参照してください。

6. [デフォルト設定] で設定を確認し、[ファイル共有の作成] を選択して、デフォルト設定を使用して新しい NFS ファイル共有を作成します。

NFS ファイル共有を作成したら、ファイル共有の詳細タブの AWS Storage Gateway コンソールでその設定を表示できます。ファイル共有のマウントの詳細については、「クライアントに NFS ファイル共有をマウントする」を参照してください。

NFS ファイル共有のデフォルト構成設定

以下の設定は、デフォルト設定を使用して作成するすべての新しい NFS ファイル共有に適用されます。ファイル共有を作成したら、 AWS Storage Gateway コンソールのファイル共有ページから選択して、その設定の詳細を表示できます。

> **Important**
>
> デフォルトの NFS ファイル共有設定は、バケットが別の AWS アカウントによって所有されていても、ファイル共有にマッピングされている S3 バケットの所有者に完全なファイル制御とアクセス許可を提供します。ファイル共有を使用して、別のアカウントが所有するバケット内のオブジェクトにアクセスする方法についての詳細は、「クロスアカウントアクセスでのファイル共有の使用」を参照してください。

設定	デフォルトの値	注意事項
Amazon S3 の場所	ファイル共有は Amazon S3 バケットに直接接続され、バケットと同じ名前になります。ゲートウェイでファイルを保存し取得するために、このバケットが使用されます。	名前にはプレフィックスは含まれません。
AWS S3 用 PrivateLink	ファイル共有は、仮想プライベートクラウド (VPC) のインターフェイスエンドポイントを介して Amazon S3 に接続されません。	

設定	デフォルトの値	注意事項
ファイルのアップロード通知	オフ	
新しいオブジェクトのストレージクラス	Amazon S3 Standard	これにより、頻繁にアクセスされるオブジェクト データを、地理的に離れた複数のアベイラビリティーゾーン (AZ) に冗長的に保存できるようになります。Amazon S3 Standard ストレージクラスの詳細については、「Amazon Simple Storage Service ユーザーガイドの「アクセス頻度の高いオブジェクトのストレージクラス」を参照してください。
暗号化	S3 マネージドキーを用いたサーバー側の暗号化 (SSE-S3)	S3 ファイルゲートウェイがアップロード、更新、または変更するすべての Amazon S3 オブジェクトは、Amazon S3 マネージドキーを使用したサーバー側の暗号化によってデフォルトで暗号化されます。

設定	デフォルトの値	注意事項
オブジェクトメタデータ	Guess MIME タイプ	これにより、Storage Gatewayはアップロードされたオブジェクトのファイル拡張子に基づいて、多目的インターネットメール拡張 (MIME) タイプを推測できます。 このオプションを使用するには、ファイル共有に関連付けられている Amazon S3 バケットのアクセスコントロールリスト (ACL) をオンにする必要があります。ACL がオフになっている場合、ファイル共有は Amazon S3 バケットにアクセスできず、無期限に使用不可の状態のままになります。
リクエスタ支払いを有効にする	オフ	詳細については、リクエスタ支払いバケットを参照してください。
監査ログ	オフ	Amazon CloudWatch グループへの口グ記録は、デフォルトでオフになっています。

設定	デフォルトの値	注意事項
S3 バケットへのアクセス	新しい IAM ロールを作成する	デフォルト オプションでは、ファイルゲートウェイがユーザーに代わって新しい IAM ロールとアクセス ポリシーを作成できます。すべての NFS クライアントにアクセスが許可されます。サポートされている NFS クライアントの詳細については、ファイルゲートウェイでサポートされている NFS および SMB クライアントを参照してください。
マウントオプション	• Squash レベル – ルートスカッシュ • エクスポート – 読み取り-書き込み	Squash レベルのデフォルト値では、リモートのスーパーユーザー (root) へのアクセスがユーザー識別子 (UID) 65534およびグループ識別子 (GID) 65534 にマッピングされます。
ファイルメタデータのデフォルト	• ディレクトリ権限 – 0777 • ファイル権限 – 0666 • ユーザー識別子 (UID) – 65534 • グループ識別子 (GID) – 65534	

カスタム設定を使用して NFS ファイル共有を作成する

カスタム設定でネットワークファイルシステム (NFS) ファイル共有を作成するには、次の手順に従います。デフォルト設定を使用して NFS ファイル共有を作成するには、「デフォルト設定を使用して NFS ファイル共有を作成する」を参照してください。

> **Important**
>
> ファイルゲートウェイからデータをアップロードするときに S3 バージョニング、クロスリージョンレプリケーション、または Rsync ユーティリティを使用すると、コストに大きな影響が生じる可能性があります。詳細については、「ファイルゲートウェイからデータをアップロードする際の予期しないコストを回避する」を参照してください。

カスタマイズされた設定で NFS ファイル共有を作成するには

1. https://console.aws.amazon.com/storagegateway/home/ で AWS Storage Gatewayコンソールを開き、左側のナビゲーションペインからファイル共有を選択します。
2. [ファイル共有の作成] を選択します。
3. [設定をカスタマイズ] を選択します。このページの他のフィールドは無視できます。以降のステップで、ゲートウェイ、プロトコル、ストレージの設定を行うように求められます。
4. ゲートウェイで、新しいファイル共有用にドロップダウンリストから Amazon S3 ファイルゲートウェイを選択してください。
5. CloudWatch ロググループでは、ドロップダウンリストから次のいずれかを選択します。

   - [ログの無効化] をクリックして、ログ記録をオフにします。
   - このファイル共有の新しいロググループを自動的に作成するには、[Storage Gateway で作成] を選択します。
   - このファイル共有のヘルスとリソースの通知を既存のロググループに送信するには、リストから目的のグループを選択します。

   監査ログの詳細については、S3 ファイルゲートウェイ監査ログについて」を参照してください。
6. (オプション) [タグ - オプション] で [新しいタグの追加] を選択し、ファイル共有のキーと値を入力します。

   タグは、Storage Gateway リソースの分類に役立つ大文字と小文字を区別するキーと値のペアです。タグを追加すると、ファイル共有のフィルタリングや検索が簡単になります。この手順を繰り返して、最大 50 個のタグを追加できます。

   完了したら、[次へ] を選択します。

7. S3 バケットの場合は、ファイル共有がファイルを保存および取得する場所を指定するには、次のいずれかを実行してください：

   - ファイル共有を Amazon Web Services アカウントの既存の S3 バケットに直接接続するには、ドロップダウンリストからバケット名を選択します。
   - ファイル共有を作成するために使用するアカウント以外の Amazon Web Services アカウントが所有する既存の S3 バケットにファイル共有を接続するには、ドロップダウンリストから別のアカウントのバケットを選択し、クロスアカウントバケット名を入力します。
   - ファイル共有を新しい S3 バケットに接続するには、新しい S3 バケットの作成を選択し、新しいバケットの Amazon S3 エンドポイントがあるリージョンを選択し、一意の S3 バケット名を入力します。完了したら、[S3 バケットの作成] を選択します。Amazon S3 バケットの作成の詳細については、Amazon S3 ユーザーガイドの「バケットの作成」を参照してください。
   - アクセスポイント名を使用してファイル共有を S3 バケットに接続するには、ドロップダウンリストから Amazon S3 Access Points 名を選択し、アクセスポイント名を入力します。新しいアクセスポイントを作成する必要がある場合は、「S3 アクセスポイントの作成」を選択できます。詳細な手順については、Amazon S3 ユーザーガイドの「アクセスポイントの作成」を参照してください。アクセスポイントの詳細については、Amazon S3 ユーザーガイドの「Amazon S3 Access Points を使用したデータアクセスの管理」および「アクセスポイントへのアクセスコントロールの委任」を参照してください。
   - アクセスポイントエイリアスを使用してファイル共有を S3 バケットに接続するには、ドロップダウンリストから [Amazon S3 Access Points エイリアス] を選択し、アクセスポイントエイリアスを入力します。新しいアクセスポイントを作成する必要がある場合は、[S3 アクセスポイントの作成] を選択できます。詳細な手順については、Amazon S3 ユーザーガイドの「アクセスポイントの作成」を参照してください。アクセスポイントのエイリアスの詳細については、Amazon S3 ユーザーガイドの「アクセスポイントにバケット形式のエイリアスを使用する」を参照してください。

   > **Note**
   >
   > 各ファイル共有は 1 つの S3 バケットにのみ接続できますが、複数のファイル共有は同じバケットに接続できます。複数のファイル共有を同じバケットに接続する場合は、読み書きの競合を防ぐために、各ファイル共有で一意かつ重複しない S3 バケットプレフィックスを設定する必要があります。
   >
   > S3 ファイルゲートウェイは、バケット名にピリオド (.) を使った Amazon S3 バケットをサポートしていません。

バケット名が Amazon S3 のバケット命名ルールに準拠していることを確認します。詳細については、「Amazon Simple Storage Service ユーザーガイド」で「バケットの命名規則」を参照してください。

8. (オプション) S3 バケットプレフィックスには、Amazon S3 で作成するオブジェクトに適用するファイル共有のプレフィックスを入力します。プレフィックスは、従来のファイル構造のディレクトリと同様に、S3 でデータを整理する方法です。詳細については、「Amazon S3 ユーザーガイド」の「プレフィックスを使用してオブジェクトを整理する」を参照してください。

   Note

   - 同じバケットに複数のファイル共有を接続する場合、読み書きの競合を防ぐために、各ファイル共有で一意かつ重複しないプレフィックスを設定する必要があります。
   - このプレフィックスは、スラッシュ (/) で終わる必要があります。
   - ファイル共有の作成後に、プレフィックスを修正したり削除することはできません。

9. リージョンでは、ドロップダウンリストからバケットの S3 エンドポイント AWS リージョン がある を選択します。このフィールドは、S3 バケットの別のアカウントのアクセスポイントまたはバケットを指定する場合にのみ表示されます。
10. 新しいオブジェクトのストレージクラスで、ドロップダウンリストからストレージクラスを選択します。ストレージクラスの詳細については、「ファイルゲートウェイでのストレージクラスの使用」を参照してください。
11. IAM ロールの場合は、次のいずれかを実行して、ファイル共有の IAM ロールを設定します。

    - ファイル共有が正しく機能するために必要なアクセス許可を持つ新しい IAM ロールを自動的に作成するには、ドロップダウンリストから [Storage Gateway で作成] を選択します。
    - 既存の IAM ロールを使用するには、ドロップダウンリストからロール名を選択します。
    - 新しい IAM ロールを作成するには、[ロールの作成] を選択します。詳細については、「 AWS Identity and Access Management ユーザーガイド」の「 AWS サービスにアクセス許可を委任するロールの作成」を参照してください。

    IAM ロールがファイル共有と S3 バケット間のアクセスを制御する方法の詳細については、Amazon S3バケットへのアクセスの許可」を参照してください。
12. プライベートリンクの場合、Virtual Private Cloud (VPC) のプライベートエンドポイント AWS を使用して と通信するようにファイル共有を設定する必要がある場合にのみ、以下を実行しま

す。それ以外の場合は、この手順をスキップしてください。詳細については、PrivateLink ガイド」の「PrivateLink とは AWS」を参照してください。 AWS PrivateLink

a. VPC エンドポイントを選択します。

b. [VPC エンドポイントを識別する方法] では、次のいずれかを実行します。

- [VPC エンドポイント ID] を選択し、[VPC エンドポイント] のドロップダウンリストから使用するエンドポイントを選択します。
- DNS 名を選択し、使用するエンドポイントの DNS 名を入力します。

13. 暗号化では、ファイル共有が Amazon S3 に保存するデータに使用するサーバー側の暗号化のタイプを選択します。

- Amazon S3 で管理されるサーバーサイド暗号化 (SSE-S3) を使用するには、[S3 マネージドキー (SSE-S3)]を選択します。

  詳細については、「Amazon Simple Storage Service ユーザーガイド」の「Amazon S3 マネージドキーによるサーバー側の暗号化の使用」を参照してください。

- AWS Key Management Service (SSE-KMS) で管理されるサーバー側の暗号化を使用するには、KMS マネージドキー (SSE-KMS) を選択します。プライマリ KMS キーで、既存の AWS KMS キーを選択するか、新しい KMS キーの作成を選択して、Key Management Service (AWS KMS) コンソールで新しい KMS AWS キーを作成します。

  詳細については AWS KMS、「 AWS Key Management Service デベロッパーガイド」のAWS「 Key Management Service とは」を参照してください。

- AWS Key Management Service (DSSE-KMS) で管理される二層式サーバー側の暗号化を使用するには、 AWS Key Management Service キーによる二層式サーバー側の暗号化 (DSSE-KMS) を選択します。プライマリ KMS キーで、既存の AWS KMS キーを選択するか、新しい KMS キーの作成を選択して、Key Management Service (AWS KMS) コンソールで新しい KMS AWS キーを作成します。

  DSSE-KMS の詳細については、「Amazon Simple Storage Service ユーザーガイド」の AWS KMS 「キーによる二層式サーバー側の暗号化の使用」を参照してください。

> **Note**
>
> DSSE-KMS および AWS KMS キーの使用には追加料金がかかります。詳細については、「AWS KMS 料金表」を参照してください。

リストにないエイリアスで AWS KMS キーを指定するか、別の AWS アカウントの AWS KMS キーを使用するには、 を使用する必要があります AWS Command Line Interface。非対称 KMS キーはサポートされていません。詳細については、AWS Storage Gateway API リファレンスで「CreateNFSFileShare」を参照してください。

> **Important**
>
> ファイル共有が、データを保存する Amazon S3 バケットと同じ暗号化タイプを使用していることを確認してください。

14. Guess MIME typesで、[Guess media MIME type](メディアタイプの推測)を選択して、Storage Gateway がファイル拡張子に基づいてアップロードされたオブジェクトのメディアタイプを推測できるようにします。
15. [ファイル共有名] で、ファイル共有の名前を入力します。

> **Note**
>
> 有効な NFS ファイル共有名に使用できる文字は、`a-z`、`A-Z`、`0-9`、`-`、`.`、および`_`のみです。

16. [アップロードイベント]で、Amazon S3 にファイルが正常にアップロードされたときにゲートウェイが CloudWatch ログイベントを記録する場合は、[ゲートウェイによってファイルが正常にアップロードされたときにイベントを記録する] を選択します。[通知の遅延] は、最新のクライアント書き込み操作から `ObjectUploaded` ログ通知の生成までの最小の遅延を制御します。クライアントは短時間でファイルに多数の小さな書き込みを行うこともあるため、同じファイルに対して複数の通知が連続して生成されないように、このパラメータをできるだけ長く設定することをお勧めします。詳細については、「ファイルのアップロード通知の受け取り」を参照してください。

> **Note**
>
> この設定は、S3 へのオブジェクトのアップロードのタイミングには影響せず、通知のタイミングにのみ影響します。

この設定は、通知が送信される正確な時刻を指定することを目的としたものではありません。場合によっては、ゲートウェイが通知を生成して送信するために、指定された遅延時間よりも長い時間がかかることがあります。

完了したら、[次へ] を選択します。

17.

18. ファイル共有プロトコルで、NFS を選択します。
19. クライアントアクセスの場合は、次のいずれかを実行して、ファイル共有にアクセスできる NFS クライアントを指定します。

    - すべての受信クライアント接続を受け入れるには、すべての NFS クライアントを選択します。
    - 特定の IP アドレスからの受信クライアント接続のみを受け入れるには、[特定の NFS クライアント]を選択し、[クライアントの追加]を選択します。許可されたクライアントの場合、接続を受け入れる有効な IP アドレスまたは CIDR ブロックを指定します。追加の IP アドレスを指定する必要がある場合は、[別のクライアントを追加]を選択します。

    > **Note**
    >
    > 特定の NFS クライアントオプションを使用して、ファイル共有へのアクセスを制限するように設定することをお勧めします。変更しない場合、ネットワークのすべてのクライアントがファイル共有にマウントできます。

20. [アクセスタイプ] では、次のいずれかを選択します。

    - クライアントがファイル共有でファイルを読み書きできるようにするには、読み取り/書き込みを選択します。
    - クライアントがファイルを読み取ってもファイル共有に書き込めないようにするには、読み取り専用を選択します。

    > **Note**
    >
    > Microsoft Windows クライアントにマウントされたファイル共有で、[読み取り専用] を選択した場合は、予期しないエラーによってフォルダを作成できないことを示すメッセージが表示される場合があります。このメッセージは無視できます。

21. [アクセスレベル] で、以下のいずれかを選択します。

    - ルートスカッシュ (デフォルト): リモートスーパーユーザー (ルート) のアクセスは UID (65534) および GID (65534) にマッピングされます。
    - All squash (すべてスカッシュ): すべてのユーザーアクセスはユーザー ID (UID) (65534) およびグループ ID (GID) (65534) にマッピングされます。
    - No root squash (ルートスカッシュなし): リモートスーパーユーザー (ルート) はルートとしてのアクセスを受け取ります。

22. (オプション)[S3 の自動キャッシュ更新] では、[キャッシュの更新間隔を設定] を選択し、ファイル共有のキャッシュを Time To Live (TTL) を使用して更新する時間を、[分] または [日] で指定します。TTL は、最後に実行された更新からの時間的長さです。TTL 間隔が経過すると、ディレクトリにアクセスしたときに、ゲートウェイは Amazon S3 バケットからそのディレクトリの内容を更新します。

    > **Note**
    >
    > この値を 30 分より短く設定すると、多数の Amazon S3 オブジェクトが頻繁に作成または削除される状況では、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。

23. ファイルメタデータのデフォルトでは、ゲートウェイが S3 バケットで検出した既存のオブジェクトにファイルメタデータ (Unix アクセス許可を含む) を適用する場合は、ゲートウェイによって作成または変更されなかった S3 オブジェクトのデフォルトメタデータを変更するを選択します。対応するフィールドに適用するディレクトリアクセス許可、ファイルアクセス許可、ユーザー ID、グループ ID を指定します。

24. ファイルの所有権とアクセス許可については、S3 バケットを所有するアカウントがファイル共有によってバケットに書き込まれたすべてのオブジェクトを完全に制御できるようにする場合は、読み取り、書き込み、編集、削除のアクセス許可など、ゲートウェイによって作成されたファイルの所有権を S3 バケット所有者に付与する を選択します。 AWS

    完了したら、[次へ] を選択します。

25. ファイル共有設定を確認します。設定を変更するには、変更するセクションの [編集] を選択します。終了したら、[作成] を選択します。

NFS ファイル共有を作成したら、ファイル共有の詳細タブの AWS Storage Gateway コンソールでその設定を表示できます。ファイル共有をマウントする手順については、「クライアントに NFS ファイル共有をマウントする」を参照してください。

SMB ファイル共有の作成

Server Message Block (SMB) プロトコルは Microsoft Windows 製品スイートに深く統合されており、Windows オペレーティングシステムの標準のファイル共有プロトコルです。クライアントとサーバーの通信プロセスは NFS と概ね類似していますが、詳細や動作メカニズムには相違があります。たとえば SMB では、ファイルシステムはローカルの SMB クライアントにマウントされません。代わりに、SMB サーバーでホストされているネットワーク共有には、ネットワークパス経由でアクセスします。

このセクションでは、ファイルゲートウェイの SMB ファイル共有を作成するための各種方法について説明します。

目次

デフォルト設定を使用して SMB ファイル共有を作成する

このセクションでは、事前設定されたデフォルト設定を使用して新しいサーバーメッセージブロック (SMB) ファイル共有を作成する方法について説明します。この方法は、基本的なデプロイ、個人使用、テスト、または後で編集およびカスタマイズする予定の複数のファイル共有をすばやくデプロイする方法として使用します。この手順を使用して作成するファイル共有のデフォルト設定のリストについては、「SMB ファイル共有のデフォルト設定」を参照してください。より詳細な制御が必要な場合、またはファイル共有に高度な設定を使用する場合は、「カスタム設定で SMB ファイル共有を作成する」を参照してください。

> **Note**
>
> 仮想プライベートクラウド (VPC) を介してファイル共有を Amazon S3 に接続する必要がある場合は、カスタム設定手順に従う必要があります。ファイル共有の作成後に VPC 設定を編集することはできません。

> **Important**
>
> ファイルゲートウェイからデータをアップロードするときに S3 バージョニング、クロスリージョンレプリケーション、または Rsync ユーティリティを使用すると、コストに大きな影響が生じる可能性があります。詳細については、「ファイルゲートウェイからデータをアップロードする際の予期しないコストを回避する」を参照してください。

前提条件

ファイル共有を作成する前に、次の作業を行います。

- ファイルゲートウェイの SMB セキュリティ設定を構成します。手順については、「ゲートウェイのセキュリティレベルの設定」を参照してください。
- 認証用に Microsoft Active Directory またはゲストアクセスも設定します。手順については、「Active Directory を使用してユーザーを認証する」または「ファイル共有へのゲストアクセスを提供する」を参照してください。
- セキュリティグループで必要なポートが開放されていることを確認します。詳細については、「ポート要件」を参照してください。

デフォルト設定を使用して SMB ファイル共有を作成するには:

1. https://console.aws.amazon.com/storagegateway/home/ で AWS Storage Gatewayコンソールを開き、左側のナビゲーションペインからファイル共有を選択します。
2. [ファイル共有の作成] を選択します。
3. [ゲートウェイ] では、ドロップダウンリストから Amazon S3 ファイルゲートウェイを選択します。
4. [ファイル共有プロトコル] で、SMB を選択します。
5. S3 バケットで、次のいずれかを実行します。
   - ドロップダウンリストからアカウント内の既存の Amazon S3 バケットを選択します。
   - ドロップダウンリストから別のアカウントのバケットを選択し、クロスアカウントバケット名にバケットの名前を入力します。
   - [新しい S3 バケットの作成] を選択し、新しいバケットの Amazon S3 エンドポイントがある AWS リージョン を選択し、一意の S3 バケット名を入力します。完了したら、[S3 バケットの作成] を選択します。

新しいバケットの作成についての詳細は、Amazon S3 ユーザーガイドの「S3 バケットを作成するには」を参照してください。

> **Note**
>
> S3 ファイルゲートウェイは、バケット名にピリオド (.) を使った Amazon S3 バケットをサポートしていません。
> バケット名が Amazon S3 のバケット命名ルールに準拠していることを確認します。詳細については、「Amazon Simple Storage Service ユーザーガイド」で「バケットの命名規則」を参照してください。

6. ユーザー認証 ドロップダウンリストから使用する認証方法を選択します。

- 企業の Microsoft Active Directory を使用するか、SMB ファイル共有へのユーザーアクセスを認証 AWS Managed Microsoft AD するには、Active Directory を選択します。この方法を使用するには、ゲートウェイがドメインに参加している必要があります。詳細については、「Active Directory を使用してユーザーを認証する」を参照してください。

> **Note**
>
> 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、Amazon EC2 インスタンスに`_workspaceMembers`セキュリティグループを追加し、 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。

Join ステータスがゲートウェイが既に Active Directory ドメインに参加していることを示している場合は、次のステップに進みます。それ以外の場合は以下の作業を行います。

1. [設定] を選択します。
2. Domain には、ゲートウェイを参加させる Active Directory ドメインの名前を入力します。

3. Username と Password を入力します。これらは、ゲートウェイがドメインに参加する際に使用されます。
4. (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。
5. (オプション) ドメインコントローラーには、ゲートウェイが Active Directory に接続する DC の名前を入力します。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。
6. [Active Directory に参加]を選択します。

> **Note**
>
> ドメインに参加すると、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、デフォルトのコンテナ (組織単位ではない) に Active Directory 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、ドメイン参加プロセスを容易にするためにアカウントを事前にステージングする必要がある場合は、このアカウントを事前に作成しておく必要があります。
> 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。

- 設定したゲストパスワードを提供するすべてのユーザーにパスワード保護されたアクセスを許可するには、[ゲストアクセス] を選択します。この方法を使用するには、お使いのファイルゲートウェイが Microsoft Active Directory ドメインの一部である必要はありません。[設定] を選択して [ゲストパスワード] を指定し、[保存] を選択します。

7. [デフォルト設定] で設定を確認し、[ファイル共有の作成] を選択して、デフォルト設定を使用して新しい SMB ファイル共有を作成します。

SMB ファイル共有を作成したら、そのファイル共有の [詳細] タブの AWS Storage Gateway コンソールで設定を表示できます。ファイル共有のマウントの詳細については、「クライアントに SMB ファイル共有をマウントする」を参照してください。

SMB ファイル共有のデフォルト設定

以下の設定は、デフォルト設定を使用して作成するすべての新しい SMB ファイル共有に適用されます。ファイル共有を作成したら、 AWS Storage Gateway コンソールのファイル共有ページから選択して、その設定の詳細を表示できます。

> **Important**
>
> デフォルトの SMB ファイル共有設定は、バケットが別の Amazon Web Services アカウントによって所有されている場合でも、ファイル共有にマッピングされている S3 バケットの所有者に完全なファイル制御とアクセス許可を提供します。別のアカウントが所有するバケット内のオブジェクトにアクセスするためにファイル共有を使用する方法の詳細については、「クロスアカウントアクセスにファイル共有を使用する」を参照してください。

設定	デフォルトの値	注意事項
Amazon S3 の場所	ファイル共有は Amazon S3 バケットに直接接続され、バケットと同じ名前になります。ゲートウェイでファイルを保存し取得するために、このバケットが使用されます。	名前にはプレフィックスは含まれません。
AWS S3 用 PrivateLink	ファイル共有は、仮想プライベートクラウド (VPC) のインターフェイスエンドポイントを介して Amazon S3 に接続されません。	
ファイルのアップロード通知	オフ	
新しいオブジェクトのストレージクラス	Amazon S3 Standard	これにより、頻繁にアクセスされるオブジェクトデータを、地理的に離れた複数のアベイラビリティーゾーン (AZ) に冗長的に保存できるようになります。Amazon S3 Standard ストレージクラスの詳細については、「Amazon Simple Storage Service ユーザーガイドの「アクセス頻度の高いオブジェクトのスト

設定	デフォルトの値	注意事項
		レージクラス」を参照してください。
暗号化	S3 マネージドキーを用いたサーバー側の暗号化 (SSE-S3)	S3 ファイルゲートウェイがアップロード、更新、または変更するすべての Amazon S3 オブジェクトは、Amazon S3 マネージドキーを使用したサーバー側の暗号化によってデフォルトで暗号化されます。
オブジェクトメタデータ	Guess MIME タイプ	これにより、Storage Gateway はアップロードされたオブジェクトのファイル拡張子に基づいて、多目的インターネットメール拡張 (MIME) アベイラビリティーゾーン (AZ)タイプを推測できます。 このオプションを使用するには、ファイル共有に関連付けられている Amazon S3 バケットのアクセスコントロールリスト (ACL) をオンにする必要があります。ACL がオフになっている場合、ファイル共有は Amazon S3 バケットにアクセスできず、無期限に使用不可の状態のままになります。

設定	デフォルトの値	注意事項
アクセスベースの列挙	アクティブ化されていません	ディレクトリ列挙中、ファイル共有上のファイルとフォルダはすべてのユーザーに表示されます。アクセスベースの列挙は、共有のアクセスコントロールリスト (ACL) に基づいて、SMB ファイル共有上のファイルとフォルダの列挙をフィルタリングするシステムです。
リクエスタ支払いを有効にする	オフ	詳細については、リクエスタ支払いバケットを参照してください。
日和見ロックのサポート	On	これにより、ファイル共有は日和見ロックを使用して、ファイルバッファリング戦略を最適化できます。ほとんどの場合、日和見ロックを有効化すると、特に Windows コンテキストメニューに関してパフォーマンスが向上します。
監査ログ	オフ	Amazon CloudWatch グループへのログ記録は、デフォルトでオフになっています。
大文字と小文字の区別を強制	オフ	これにより、クライアントは大文字と小文字の区別を制御できます。

設定	デフォルトの値	注意事項
S3 バケットへのアクセス	新しい IAM ロールを作成する	デフォルト オプションでは、ファイルゲートウェイがユーザーに代わって新しい IAM ロールとアクセス ポリシーを作成できます。

カスタム設定で SMB ファイル共有を作成する

カスタム設定でサーバーメッセージブロック (SMB) ファイル共有を作成するには、次の手順を使用します。デフォルト設定で SMB ファイル共有を作成するには、「デフォルト設定を使用して SMB ファイル共有を作成する」を参照してください。

> **Important**
>
> ファイルゲートウェイからデータをアップロードするときに S3 バージョニング、クロスリージョンレプリケーション、または Rsync ユーティリティを使用すると、コストに大きな影響が生じる可能性があります。詳細については、「ファイルゲートウェイからデータをアップロードする際の予期しないコストを回避する」を参照してください。

前提条件

ファイル共有を作成する前に、次の作業を行います。

- ファイルゲートウェイの SMB セキュリティ設定を構成します。手順については、「ゲートウェイのセキュリティレベルの設定」を参照してください。
- 認証用に Microsoft Active Directory またはゲストアクセスも設定します。手順については、「Active Directory を使用してユーザーを認証する」または「ファイル共有へのゲストアクセスを提供する」を参照してください。
- セキュリティグループで必要なポートが開放されていることを確認します。詳細については、「ポート要件」を参照してください。

カスタマイズされた設定で SMB ファイル共有を作成するには

1. https://console.aws.amazon.com/storagegateway/home/ で AWS Storage Gatewayコンソールを開き、左側のナビゲーションペインからファイル共有を選択します。
2. [ファイル共有の作成] を選択します。
3. [設定をカスタマイズ] を選択します。このページの他のフィールドは無視できます。以降のステップで、ゲートウェイ、プロトコル、ストレージの設定を行うように求められます。
4. [ゲートウェイ] では、ドロップダウンリストから Amazon S3 ファイルゲートウェイを選択します。
5. CloudWatch ロググループでは、ドロップダウンリストから次のいずれかを選択します。

   - [ログの無効化] をクリックして、ログ記録をオフにします。
   - このファイル共有の新しいロググループを自動的に作成するには、[Storage Gateway で作成] を選択します。
   - このファイル共有のヘルスとリソースの通知を既存のロググループに送信するには、リストから目的のグループを選択します。

   監査ログの詳細については、S3 ファイルゲートウェイ監査ログについて」を参照してください。
6. (オプション) [タグ - オプション] で [新しいタグの追加] を選択し、ファイル共有のキーと値を入力します。タグは、Storage Gateway リソースの分類に役立つ大文字と小文字を区別するキーと値のペアです。タグを追加すると、ファイル共有のフィルタリングと検索が容易になります。この手順を繰り返して、最大 50 個のタグを追加できます。

   完了したら、[次へ] を選択します。
7. S3 バケットの場合は、次のいずれかを実行して、ファイルの保存先と取得先を指定します。

   - ファイル共有を Amazon Web Services アカウントの既存の S3 バケットに直接接続するには、ドロップダウンリストからバケット名を選択します。
   - ファイル共有を作成するために使用しているもの以外の Amazon Web Services アカウントが所有する既存の S3 バケットにファイル共有を接続するには、ドロップダウンリストから別のアカウントのバケットを選択し、クロスアカウントバケット名を入力します。
   - ファイル共有を新しい S3 バケットに接続するには、新しい S3 バケットの作成を選択し、新しいバケットの Amazon S3 エンドポイントがあるリージョンを選択し、一意の S3 バケット名を入力します。完了したら、[S3 バケットの作成] を選択します。Amazon S3 バケットの

作成の詳細については、Amazon S3 ユーザーガイドの「バケットの作成」を参照してください。

- アクセスポイント名を使用してファイル共有を S3 バケットに接続するには、ドロップダウンリストから Amazon S3 Access Points 名を選択し、アクセスポイント名を入力します。新しいアクセスポイントを作成する必要がある場合は、「S3 アクセスポイントの作成」を選択できます。詳細な手順については、Amazon S3 ユーザーガイドの「アクセスポイントの作成」を参照してください。アクセスポイントの詳細については、Amazon S3 ユーザーガイドの「Amazon S3 Access Points を使用したデータアクセスの管理」および「アクセスポイントへのアクセスコントロールの委任」を参照してください。
- アクセスポイントエイリアスを使用してファイル共有を S3 バケットに接続するには、ドロップダウンリストから [Amazon S3 Access Points エイリアス] を選択し、アクセスポイントエイリアスを入力します。新しいアクセスポイントを作成する必要がある場合は、[S3 アクセスポイントの作成] を選択できます。詳細な手順については、Amazon S3 ユーザーガイドの「アクセスポイントの作成」を参照してください。アクセスポイントのエイリアスの詳細については、Amazon S3 ユーザーガイドの「アクセスポイントにバケット形式のエイリアスを使用する」を参照してください。

> **Note**
>
> 各ファイル共有は 1 つの S3 バケットにのみ接続できますが、複数のファイル共有は同じバケットに接続できます。複数のファイル共有を同じバケットに接続する場合は、読み書きの競合を防ぐために、各ファイル共有で一意かつ重複しない S3 バケットプレフィックスを設定する必要があります。
>
> S3 ファイルゲートウェイは、バケット名にピリオド (.) を使った Amazon S3 バケットをサポートしていません。
>
> バケット名が Amazon S3 のバケット命名ルールに準拠していることを確認します。詳細については、「Amazon Simple Storage Service ユーザーガイド」で「バケットの命名規則」を参照してください。

8. (オプション) S3 バケットプレフィックスには、Amazon S3 で作成するオブジェクトに適用するファイル共有のプレフィックスを入力します。プレフィックスは、従来のファイル構造のディレクトリと同様に、S3 でデータを整理する方法です。詳細については、「Amazon S3 ユーザーガイド」の「プレフィックスを使用してオブジェクトを整理する」を参照してください。

> **Note**
>
> - 同じバケットに複数のファイル共有を接続する場合、読み書きの競合を防ぐために、各ファイル共有で一意かつ重複しないプレフィックスを設定する必要があります。
> - このプレフィックスは、スラッシュ (/) で終わる必要があります。
> - ファイル共有の作成後に、プレフィックスを修正したり削除することはできません。

9. リージョンでは、ドロップダウンリストからバケットの S3 エンドポイント AWS リージョン がある を選択します。このフィールドは、S3 バケットの別のアカウントのアクセスポイントまたはバケットを指定する場合にのみ表示されます。
10. 新しいオブジェクトのストレージクラスで、ドロップダウンリストからストレージクラスを選択します。ストレージクラスの詳細については、「ファイルゲートウェイでのストレージクラスの使用」を参照してください。
11. IAM ロールの場合は、次のいずれかを実行して、ファイル共有の IAM ロールを設定します。

    - ファイル共有が正しく機能するために必要なアクセス許可を持つ新しい IAM ロールを自動的に作成するには、ドロップダウンリストから [Storage Gateway で作成] を選択します。
    - 既存の IAM ロールを使用するには、ドロップダウンリストからロール名を選択します。
    - 新しい IAM ロールを作成するには、[ロールの作成] を選択します。詳細については、「 AWS Identity and Access Management ユーザーガイド」の「 AWS サービスにアクセス許可を委任するロールの作成」を参照してください。

    IAM ロールがファイル共有と S3 バケット間のアクセスを制御する方法の詳細については、「Amazon S3 バケットへのアクセスの許可」を参照してください。
12. プライベートリンクの場合、Virtual Private Cloud (VPC) のプライベートエンドポイント AWS を使用して と通信するようにファイル共有を設定する必要がある場合にのみ、以下を実行します。それ以外の場合は、この手順をスキップしてください。詳細については、PrivateLink ガイド」の「PrivateLink とは AWS」を参照してください。 AWS PrivateLink

    a. VPC エンドポイントを選択します。

    b. [VPC エンドポイントを識別する方法] では、次のいずれかを実行します。

        - [VPC エンドポイント ID] を選択し、[VPC エンドポイント] のドロップダウンリストから使用するエンドポイントを選択します。

- DNS 名を選択し、使用するエンドポイントの DNS 名を入力します。

13. [暗号化] で、ファイルゲートウェイにより Amazon S3 に保存されるオブジェクトの暗号化に使用する暗号化キーのタイプを選択します。

    - Amazon S3 で管理されるサーバーサイド暗号化 (SSE-S3) を使用するには、[S3 マネージドキー (SSE-S3)]を選択します。

      詳細については、「Amazon Simple Storage Service ユーザーガイド」の「Amazon S3 マネージドキーによるサーバー側の暗号化の使用」を参照してください。

    - AWS Key Management Service (SSE-KMS) で管理されるサーバー側の暗号化を使用するには、KMS マネージドキー (SSE-KMS) を選択します。プライマリ KMS キーで、既存の AWS KMS キーを選択するか、新しい KMS キーの作成を選択して、Key Management Service (AWS KMS) コンソールで新しい KMS AWS キーを作成します。

      詳細については AWS KMS、「 AWS Key Management Service デベロッパーガイド」のAWS「 Key Management Service とは」を参照してください。

    - AWS Key Management Service (DSSE-KMS) で管理される二層式サーバー側の暗号化を使用するには、 AWS Key Management Service キーによる二層式サーバー側の暗号化 (DSSE-KMS) を選択します。プライマリ KMS キーで、既存の AWS KMS キーを選択するか、新しい KMS キーの作成を選択して、Key Management Service (AWS KMS) コンソールで新しい KMS AWS キーを作成します。

      DSSE-KMS の詳細については、「Amazon Simple Storage Service ユーザーガイド」の AWS KMS 「キーによる二層式サーバー側の暗号化の使用」を参照してください。

      > **Note**
      >
      > DSSE-KMS および AWS KMS キーの使用には追加料金がかかります。詳細については、「AWS KMS 料金表」を参照してください。
      > リストにないエイリアスで AWS KMS キーを指定するか、別の AWS アカウントの AWS KMS キーを使用するには、 を使用する必要があります AWS Command Line Interface。非対称 KMS キーはサポートされていません。詳細については、AWS Storage Gateway API リファレンスの「CreateSMBFileShare」を参照してください。

> **Important**
>
> ファイル共有が、データを保存する Amazon S3 バケットと同じ暗号化タイプを使用していることを確認してください。

14. Guess MIME typesでは、Guess media MIME typeを選択して、Storage Gateway がファイル拡張子に基づいてアップロードされたオブジェクトの多目的インターネットメール拡張 (MIME) タイプを推測できるようにします。
15. [ファイル共有名] で、ファイル共有の名前を入力します。

> **Note**
>
> 有効な SMB ファイル共有名には、[、]、#、;、<、>、:、"、\、/、|、?、*、+、または Aまたは ASCII 制御文字を含めることはできません1-31。

16. [アップロードイベント] で、Amazon S3 にファイルが正常にアップロードされたときにゲートウェイが CloudWatch ログイベントを記録する場合は、[ゲートウェイによってファイルが正常にアップロードされたときにイベントを記録する] を選択します。[通知の遅延] は、最新のクライアント書き込み操作から `ObjectUploaded` ログ通知の生成までの遅延を制御します。クライアントは短時間でファイルに多数の小さな書き込みを行うこともあるため、同じファイルに対して複数の通知が連続して生成されないように、このパラメータをできるだけ長く設定することをお勧めします。詳細については、「ファイルのアップロード通知の受け取り」を参照してください。

> **Note**
>
> この設定は、S3 へのオブジェクトのアップロードのタイミングには影響せず、通知のタイミングにのみ影響します。
> この設定は、通知が送信される正確な時刻を指定することを目的としたものではありません。場合によっては、ゲートウェイが通知を生成して送信するために、指定された遅延時間よりも長い時間がかかることがあります。

完了したら、[次へ] を選択します。

17. [ファイル共有プロトコル] で、SMB を選択します。

18. [認証方法] で、使用する認証方法をドロップダウンリストから選択します。

    - 企業の Microsoft Active Directory を使用するか、SMB ファイル共有へのユーザーアクセスを認証 AWS Managed Microsoft AD するには、Active Directory を選択します。この方法を使用するには、ゲートウェイがドメインに参加している必要があります。詳細については、「Active Directory を使用してユーザーを認証する」を参照してください。

      > **Note**
      >
      > 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、Amazon EC2 インスタンスに_workspaceMembersセキュリティグループを追加し、 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。

    Join ステータスがゲートウェイが既に Active Directory ドメインに参加していることを示している場合は、次のステップに進みます。それ以外の場合は以下の作業を行います。

    1. [設定] を選択します。
    2. Domain には、ゲートウェイを参加させる Active Directory ドメインの名前を入力します。
    3. Username と Password を入力します。これらは、ゲートウェイがドメインに参加する際に使用されます。
    4. (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。
    5. (オプション) ドメインコントローラーには、ゲートウェイが Active Directory に接続する DC の名前を入力します。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。
    6. [Active Directory に参加]を選択します。

> **Note**
>
> ドメインに参加すると、既定のコンテナ (組織単位ではない) に Active Directory アカウントが作成され、ゲートウェイの Gateway ID がアカウント名として使用されます (例：SGW-1234ADE)。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、ドメイン参加プロセスを容易にするためにアカウントを事前にステージングする必要がある場合は、このアカウントを事前に作成しておく必要があります。
>
> 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。

- 設定したゲストパスワードを提供するすべてのユーザーにパスワード保護されたアクセスを許可するには、[ゲストアクセス] を選択します。この方法を使用するには、お使いのファイルゲートウェイが Microsoft Active Directory ドメインの一部である必要はありません。[設定] を選択して [ゲストパスワード] を指定し、[保存] を選択します。

19. User accessでは、どの SMB クライアントがファイル共有にアクセスできるかを指定するために、次のいずれかを実行します。

    - Active Directory を通じて正常に認証されたすべてのユーザーにアクセス権を付与するには、All AD-authenticated usersを選択します。
    - 特定のユーザーまたはグループへのアクセスを許可または拒否するには、Specific AD-authenticated users or groupsを選択し、次の操作を行います。
        - [許可されたユーザーおよびグループ] で、[許可するユーザーの追加] または [許可するグループの追加] を選択し、ファイル共有のアクセスを許可する Active Directory ユーザーまたはグループを入力します。このプロセスを繰り返して、必要な数のユーザーとグループを許可します。
        - [拒否されたユーザーおよびグループ] で、[拒否するユーザーの追加] または[拒否するグループの追加] を選択し、ファイル共有のアクセスを拒否する Active Directory ユーザーまたはグループを入力します。このプロセスを繰り返して、必要な数のユーザーとグループを拒否します。

> **Note**
>
> User and group file share access セクションは、User authentication が Active Directory に設定されている場合にのみ表示されます。
> ユーザーまたはグループを指定するときは、ドメインを含めないでください。ドメイン名は、ゲートウェイが参加している特定の Active Directory のメンバーシップによって暗黙的に決定されます。

20. (オプション) [Admin user] に、Active Directory ユーザーおよびグループのカンマ区切りのリストを入力します。管理者ユーザーには、ファイル共有内のすべてのファイルおよびフォルダーのアクセスコントロールリスト (ACL) を更新する権限が付与されます。プレフィックスとしてグループ名に文字 @ を付ける必要があります。(例: `@group1`)
21. [アクセスタイプ] では、次のいずれかを選択します。
    - クライアントがファイル共有でファイルを読み書きできるようにするには、読み取り/書き込みを選択します。
    - クライアントがファイルを読み取ってもファイル共有に書き込めないようにするには、読み取り専用を選択します。

    > **Note**
    >
    > Microsoft Windows クライアントにマウントされたファイル共有で、[読み取り専用] を選択した場合は、予期しないエラーによってフォルダを作成できないことを示すメッセージが表示される場合があります。このメッセージは無視できます。

22. [ファイル/ディレクトリのアクセスコントロール] で、次のいずれかを選択します。
    - SMB ファイル共有内のファイルおよびフォルダにきめ細かいアクセス許可を設定するには、[Windows アクセスコントロールリスト] を選択します。詳細については、「Microsoft Windows ACL を使用して、SMB ファイル共有へのアクセスを制御する」を参照してください。
    - SMB ファイル共有を介して保存されるファイルやディレクトリへのアクセスを POSIX 権限で制御するには、[POSIX 権限] を選択します。
23. Access based enumerationの場合は、次のいずれかを実行します。

- 共有上のファイルとフォルダーを読み取りアクセス権を持つユーザーのみに表示するには、Hide files and directories where user doesn't have permissionを選択します。
- ディレクトリの列挙時に共有上のファイルとフォルダーをすべてのユーザーに表示するには、このチェックボックスをオフのままにします。

> **Note**
>
> アクセスベースの列挙は、共有のアクセスコントロールリスト (ACL) に基づいて、SMB ファイル共有上のファイルとフォルダの列挙をフィルタリングするシステムです。

24. File access options の場合は、以下のオプションのいずれかを選択します。

- オポチュニスティックロックを使用してファイル共有のファイルバッファリング戦略を最適化するには、日和見ロックを選択します。ほとんどの場合、日和見ロックを有効化すると、特に Windows コンテキストメニューに関してパフォーマンスが向上します。
- SMB クライアントではなくゲートウェイがファイル名の大文字と小文字の区別を制御するには、[大文字と小文字の区別を強制] を選択します。
- 両方の設定を無効にするには、[いずれも使用しない] を選択します。

> **Note**
>
> ファイルアクセスの競合を避けるため、これらの設定は相互に排他的であり、同時にアクティブ化することはできません。

25. (オプション)[S3 の自動キャッシュ更新] では、[キャッシュの更新間隔を設定] を選択し、ファイル共有のキャッシュを Time To Live (TTL) を使用して更新する時間を、[分] または [日] で指定します。TTL は、最後に実行された更新からの時間的長さです。TTL 間隔が経過すると、ディレクトリにアクセスしたときに、ゲートウェイは Amazon S3 バケットからそのディレクトリの内容を更新します。

> **Note**
>
> この値を 30 分より短く設定すると、多数の Amazon S3 オブジェクトが頻繁に作成または削除される状況では、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。

26. ファイルの所有権とアクセス許可については、S3 バケットを所有するアカウントがファイル共有によってバケットに書き込まれたすべてのオブジェクトを完全に制御できるようにする場合は、読み取り、書き込み、編集、削除のアクセス許可など、ゲートウェイによって作成されたファイルの所有権を S3 バケット所有者に付与する を選択します。 AWS

    完了したら、[次へ] を選択します。
27. ファイル共有設定を確認します。設定を変更するには、変更するセクションの [編集] を選択します。終了したら、[作成] を選択します。

SMB ファイル共有を作成したら、そのファイル共有の [詳細] タブの AWS Storage Gateway コンソールで設定を表示できます。ファイル共有をマウントする手順については、「SMB ファイル共有をクライアントにマウントする」を参照してください。

ファイル共有をコピーする

> **Note**
>
> ファイル共有のコピー機能は、Storage Gateway コンソールでのみ使用できます。この機能に対応する AWSCLI コマンドまたは API アクションはありません。

Storage Gateway コンソールを使用して、既存の NFS または SMB ファイル共有を別のゲートウェイにコピーできます。ファイル共有をコピーすると、元の共有の設定のほとんどを維持しながら、ソースファイル共有と同じ Amazon S3 バケットを指す新しいファイル共有が宛先ゲートウェイに作成されます。これは主にゲートウェイの移行を支援することを目的としており、設定を手動で再作成することなく、ファイル共有を代替ゲートウェイに移動できます。コピーしたファイル共有が新しいゲートウェイで正しく動作していることを確認したら、ソースゲートウェイから元のファイル共有を削除する必要があります。

考慮事項

ファイル共有をコピーする前に、次の点を考慮してください。

- 送信先ゲートウェイはアクティブ状態である必要があります。
- 送信元ゲートウェイと送信先ゲートウェイの両方が Amazon S3 File Gateway ゲートウェイである必要があります。異なるゲートウェイタイプ間でファイル共有をコピーすることはできません。

- コピーされたファイル共有は、ソースと同じ Amazon S3 バケットを指します。両方のファイル共有を長期間アクティブに維持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 Amazon S3 バケットに同時に書き込むと、データの不整合、キャッシュの競合、予期しない動作が発生する可能性があります。コピーしたファイル共有が正しく機能していることを確認したら、ソースファイル共有を削除します。
- コピーオペレーションでは、ファイル共有プロトコル (NFS または SMB) が保持されます。コピー中にプロトコルタイプを変更することはできません。
- ソースファイル共有が Amazon S3 バケットアクセスに IAM ロールを使用している場合は、コピーしたファイル共有に同じロールを使用するか、別の既存のロールを選択するか、コンソールで新しいロールを自動的に作成するかを選択できます。
- ソースファイル共有に CloudWatch ロググループモニタリングが設定されている場合、同じロググループを使用するか、別のロググループを選択するか、コンソールで新しいロググループを自動的に作成するかを選択できます。
- 異なる Active Directory ドメインに参加しているゲートウェイ間、または Active Directory 認証を使用するゲートウェイとゲストアクセスを使用するゲートウェイ間で SMB ファイル共有をコピーする場合は、コピーの完了後に SMB アクセス設定を確認して、アクセス許可が正しく設定されていることを確認します。
- レプリケート元ゲートウェイとレプリケート先ゲートウェイの VPC 設定が異なる場合 (たとえば、1 つのゲートウェイが VPC でアクティブ化され、もう 1 つのゲートウェイがアクティブ化されていない場合) 、コピーされたファイル共有はレプリケート先ゲートウェイのネットワーク設定を使用します。

> **Important**
>
> SMB ファイル共有をコピーする場合、ルートレベルのアクセスコントロールリスト (ACLs) は新しいファイル共有にコピーされません。コピーされたファイル共有は、デフォルトのルート ACLs で作成されます。ソースファイル共有でカスタムルート ACLs を設定している場合は、コピーの完了後にコピーされたファイル共有でカスタムルート ACL を手動で再設定する必要があります。

ファイル共有を別のゲートウェイにコピーする

Storage Gateway コンソールを使用してファイル共有をコピーするには

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、ファイル共有を選択します。
3. コピーするファイル共有を選択します。
4. アクションメニューから、ファイル共有を別のゲートウェイにコピーを選択します。
5. Gateway で、コピーを作成する送信先ゲートウェイを選択します。
6. IAM ロールの場合は、次のいずれかのオプションを選択します。

   - 同じ IAM ロールを使用する – ソースファイル共有と同じ IAM ロールを使用します。送信先ゲートウェイが同じアクセス許可を使用して Amazon S3 バケットにアクセスする必要がある場合は、このオプションを選択します。
   - 既存の IAM ロールを選択する – リストから別の IAM ロールを選択します。ロールが必要な Amazon S3 アクセス許可を付与していることを確認します。
   - 新しい IAM ロールの自動生成 – コンソールは、Amazon S3 バケットに必要なアクセス許可を持つ新しい IAM ロールを作成します。
7. ロググループで、次のいずれかのオプションを選択します。

   - 同じロググループを使用する – ソースファイル共有と同じ CloudWatch ロググループにヘルスログを送信します。
   - 既存のロググループを選択する – リストから別の CloudWatch ロググループを選択します。
   - 新しいロググループの自動生成 – コンソールは、コピーされたファイル共有用の新しい CloudWatch ロググループを作成します。
8. ファイル共有のコピーを選択します。

新しいファイル共有は、Creating というステータスのファイル共有リストに表示されます。共有が使用可能になったら、ソース共有と同じプロトコルを使用してクライアントにマウントできます。

コピー中に保持される設定

ファイル共有をコピーすると、次の設定がソースファイル共有から新しいコピーに引き継がれます。

- Amazon S3 バケット名とプレフィックス

- ストレージクラス
- オブジェクト暗号化設定 (SSE-S3、SSE-KMS、または DSSE-KMS)
- ファイル共有プロトコル (NFS または SMB)
- キャッシュの更新設定
- スカッシュ設定とクライアントアクセス (NFS ファイル共有)
- 認証方法、ファイル共有の可視性、アクセスベースの列挙 (SMB ファイル共有) などの SMB アクセス設定
- 許可および拒否されたユーザーとグループ (SMB ファイル共有)

以下の設定はコピーされず、送信先ゲートウェイの設定またはデフォルトを使用します。

- ゲートウェイネットワーク設定 (VPC エンドポイント、パブリックエンドポイント)
- Active Directory ドメインメンバーシップ (宛先ゲートウェイの AD 設定を使用)
- 帯域幅レート制限 (送信先ゲートウェイの制限を使用)
- ルートレベルの ACLs (SMB ファイル共有 – コピーされた共有はデフォルトのルート ACLs で作成されます)

ファイル共有のマウントと使用

このセクションのトピックでは、ファイル共有をクライアントにマウントする方法、ファイル共有を使用する方法、ファイルゲートウェイをテストする方法、およびテスト目的で作成する可能性のあるゲートウェイ、Amazon EC2 インスタンス、オンプレミス VM など、不要になったリソースをクリーンアップする方法について説明します。サポートされる Network File System (NFS) および Service Message Block (SMB) クライアントの詳細については、「ファイルゲートウェイでサポートされている NFS および SMB クライアント」を参照してください。

> **Note**
>
> には、ファイル共有のマウントに使用できるコマンドの例 AWS マネジメントコンソール も用意されています。

トピック

- NFS ファイル共有をクライアントにマウントする - クライアントのドライブに NFS ファイル共有をマウントし、Amazon S3 バケットにマッピングする方法を説明します。
- SMB ファイル共有をクライアントにマウントする - SMB ファイル共有をマウントし、クライアントがアクセス可能なドライブにマッピングする方法を説明します。
- 既存のオブジェクトがあるバケットでファイル共有を使用する - ファイルゲートウェイ以外で作成されたオブジェクトを含む Amazon S3 バケット上のファイル共有を、NFS または SMB を使用してエクスポートする方法を説明します。
- S3 ファイルゲートウェイをテストする - マッピングされたドライブにファイルとフォルダーをコピーし、それらが Amazon S3 バケットに自動的に表示されることを確認することで、ゲートウェイをテストする方法を説明します。

NFS ファイル共有をクライアントにマウントする

次の手順を使用して、クライアントのドライブに NFS ファイル共有をマウントし、Amazon S3 バケットにマッピングします。

ファイル共有をマウントして Amazon S3 バケットにマッピングするには

1. Microsoft Windows クライアントを使用している場合は、SMB ファイル共有を作成して、Windows クライアントにすでにインストールされている SMB クライアントを使用して、ファイル共有にアクセスすることをお勧めします。NFS を使用する場合は、Windows で NFS のサービスを有効にします。
2. NFS ファイル共有をマウントします。

   - Linux クライアントの場合は、コマンドプロンプトで以下のコマンドを入力します。

     sudo mount -t nfs -o nolock,hard *[GatewayVMIPAddress]*:/*[FileShareName]* *[ClientMountPath]*

   - Windows クライアントの場合は、コマンドプロンプト (cmd.exe) で次のコマンドを入力します。

     mount -o nolock -o mtype=hard *[GatewayVMIPAddress]*:/*[FileShareName]* *[WindowsDriveLetter]*

   たとえば、Windows クライアントで VM の IP アドレスが 123.123.1.2 で、ファイル共有名が `test-fileshare` であるとします。また、ドライブ T にマップするとします。この場合、コマンドは次のようになります。

   mount -o nolock -o mtype=hard 123.123.1.2:/test-fileshare T:

   > **Note**
   >
   > ファイル共有をマウントする際には、以下に注意してください。
   >
   > - デフォルトでは、Windows は NFS 共有のマウントにソフトマウントを使用します。接続の問題が発生した場合、ソフトマウントはタイムアウトしやすくなります。重要なワークロードにはハードマウントを使用することをお勧めします。ハードマウントの方が安全で、データの保持にも適しているためです。ハードマウントを使用するには、コマンドで `-o mtype=hard` スイッチを使用していることを確認してください。
   > - S3 ファイルゲートウェイは NFS ファイルロックをサポートしていません。NFS ファイル共有をマウントするときは、常に `-o nolock` オプションを使用してファイルロックをオフにします。
   > - フォルダとオブジェクトが 1 つのAmazon S3 バケット内にあり、同じ名前である場合があります。この場合、オブジェクト名に末尾のスラッシュが含まれていない場

合は、フォルダのみがファイルゲートウェイに表示されます。例えば、バケットに test または test/ という名前のオブジェクトと test/test1 という名前のフォルダが含まれる場合、test/ と test/test1 のみがファイルゲートウェイに表示されます。

- 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 クライアントを使用している場合は、mount コマンドをオプションなしで実行してマウントを行った後に、mount オプションを確認します。応答により、指定した最新のオプションを使用してファイル共有がマウントされたことを確認できます。また、これにより、キャッシュされた古いエントリを使用していないことを確認できます。クリアには、少なくとも 60 秒かかります。

次のステップ

S3 ファイルゲートウェイをテストする

SMB ファイル共有をクライアントにマウントする

ここでは、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。以下に、試すことができる追加オプションを示します。

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。

- コマンドプロンプト (cmdkey および net use) — コマンドプロンプトを使用してファイル共有をマウントします。認証情報を cmdkey で保存し、net use でドライブをマウントし、システムの再起動間で接続を維持したい場合は /persistent:yes および /savecred スイッチを含めます。使用する具体的なコマンドは、Microsoft Active Directory (AD) アクセス用かゲストユーザーアクセス用かによって異なります。例は以下に示します。
- File Explorer (ネットワーク ドライブのマッピング) - File Explorer を使用してファイル共有をマウントします。システム再起動後も接続を維持するかどうかを指定し、ネットワーク認証情報の入力を求める設定を行います。
- PowerShell スクリプト – ファイル共有をマウントするカスタム PowerShell スクリプトを作成します。スクリプトで指定したパラメータに応じて、システムの再起動間で接続が永続化され、マウント中にオペレーティングシステムで共有が表示または表示されない場合があります。

> **Note**
>
> Microsoft AD 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。
> ゲストユーザーの場合には、ファイル共有をマウントする前に、ゲストユーザーパスワードを保持していることを確認します。

承認された Microsoft AD ユーザー用に、コマンドプロンプトを使用して SMB ファイル共有をマウントするには：

1. ファイル共有をユーザーのシステムにマウントする前に、Microsoft AD ユーザーに SMB ファイル共有への必要なアクセス許可があることを確認してください。
2. ファイル共有をマウントするには、コマンドプロンプトで次のように入力します。

   ```
   net use WindowsDriveLetter: \\GatewayIPAddress\FileShareName /
   persistent:yes
   ```

特定のサインイン認証情報の組み合わせで SMB ファイル共有をマウントするには：

1. ファイル共有をシステムにマウントする前に、ユーザーに 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. Windows 認証情報マネージャーにユーザー認証情報を保存するには、コマンドプロンプトで次を入力します。

   ```
   cmdkey /add:GatewayIPAddress /user:DomainName\UserName /pass:Password
   ```
3. ファイル共有をマウントするには、コマンドプロンプトで次のように入力します。

   ```
   net use WindowsDriveLetter: \\GatewayIPAddress\FileShareName /
   persistent:yes /savecred
   ```

ゲストユーザー用に SMB ファイル共有をマウントするには、コマンドプロンプトを使用します。

1. ファイル共有をマウントする前に、ゲストユーザーパスワードを保持していることを確認します。
2. ゲスト認証情報を Windows 認証情報マネージャーに保存するには、コマンドプロンプトで次を入力します。

```
cmdkey /add:GatewayIPAddress /user:DomainName\smbguest /pass:Password
```

3. コマンドプロンプトで、以下を入力します。

```
net use WindowsDriveLetter: \\$GatewayIPAddress\$Path /user:$Gateway
ID\smbguest /persistent:yes /savecred
```

> **Note**
>
> ファイル共有をマウントする際には、以下に注意してください。
>
> - フォルダとオブジェクトが 1 つのAmazon S3 バケット内にあり、同じ名前である場合があります。この場合、オブジェクト名に末尾のスラッシュが含まれていない場合は、フォルダのみがファイルゲートウェイに表示されます。例えば、バケットに `test` または `test/` という名前のオブジェクトと `test/test1` という名前のフォルダが含まれる場合、`test/` と `test/test1` のみがファイルゲートウェイに表示されます。
> - ユーザー認証情報を保存し、システム再起動後も接続を維持するようにファイル共有接続を設定していない場合は、クライアントシステムを再起動するたびにファイル共有を再マウントする必要がある可能性があります。

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 Windows 検索 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] に「***[File Gateway IP]**[SMB File Share Name]***」と入力するか、または [Browse] 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) Microsoft AD ログオンまたはゲストアカウントのユーザーパスワードをユーザーに入力させる場合は、[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。

> **Note**
>
> ドット (.) 文字で始まるファイルまたはディレクトリは、Windows では非表示とマークされます。これらのファイルとディレクトリを表示するには、Windows File Explorer の [View]タブで [Hidden items] チェックボックスを選択する必要があります。

Storage Gateway マネジメントコンソールで、ファイル共有設定の編集、ユーザーやグループの許可および拒否の編集、およびゲストアクセスパスワードの変更ができます。また、ファイル共有のキャッシュデータをリフレッシュし、コンソールからファイル共有を削除することもできます。

SMB ファイル共有のプロパティを変更するには

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 [ファイル共有] を選択します。
3. [ファイル共有] ページで、変更する SMB ファイル共有のチェックボックスを選択します。
4. アクションで実行するアクションを選択します。
   - [ファイル共有の設定の編集] を選択して共有アクセスを変更してます。
   - [許可/拒否されたユーザーの編集] を選択して、ユーザーやグループを追加あるいは削除します。その後、許可されたユーザー、拒否されたユーザー、許可されたグループ、拒否されたグループに許可あるいは拒否するユーザーやグループを入力します。[エントリの追加] ボタンを使用して新規のアクセス権を作成し、[X] ボタンを使用してアクセスを削除します。

     > **Note**
     >
     > グループには @ 文字のプレフィックスを付ける必要があります。有効な形式は、`DOMAIN\User1`、`user1`、`@group1`、`@DOMAIN\group1` です。
5. 完了したら、[保存] を選択します。

   許可されたユーザーとグループを入力して、許可リストを作成します。許可リストが存在しない場合、すべての認証された Microsoft AD ユーザーが SMB ファイル共有にアクセスできます。拒否とマークされたすべてのユーザーとグループは拒否リストに追加され、SMB ファイル共有にアクセスできません。拒否リストと許可リストの両方にユーザーまたはグループがあるインスタンスでは、常に拒否リストが優先されます。

使用している SMB ファイル共有上でアクセスコントロールリスト (ACL) を有効にできます。ACL を有効にする方法については、「Windows ACL を使用して SMB ファイル共有へのアクセスを制限する」を参照してください。

次のステップ

S3 ファイルゲートウェイをテストする

既存のオブジェクトがあるバケットでファイル共有を使用する

NFS あるいは SMB のいずれかを使用して、ファイルゲートウェイ以外で作成されたオブジェクトがある Amazon S3 バケットでファイル共有をエクスポートできます。バケット内のオブジェクトがゲートウェイ外で作成されている場合、これらのオブジェクトにファイルシステムクライアントからアクセスすると、オブジェクトは NFS または SMB ファイルシステムにファイルとして表示されます。標準の Portable Operating System Interface (POSIX) アクセスおよびアクセス許可が、このファイル共有で使用されます。ファイルを Amazon S3 バケットに書き戻すと、ファイルは指定したプロパティとアクセス許可を継承します。

オブジェクトはいつでも S3 バケットにアップロードできます。ファイル共有でこれらの新しいオブジェクトをファイルとして表示するには、まず S3 バケットをリフレッシュする必要があります。詳細については、「the section called “Amazon S3 バケットのオブジェクトキャッシュの更新”」を参照してください。

> **Note**
>
> 1 つの Amazon S3 バケットに対して複数のライターを使用することはお勧めできません。使用する場合は、必ず事前に「Amazon S3 バケットに対して複数のライターを使用できますか?」セクション (Storage Gateway のよくある質問) をお読みください。

NFS を使用してアクセスするオブジェクトにメタデータのデフォルトを割り当てるには、「Amazon S3 ファイルゲートウェイの管理」でデフォルトのメタデータ値の編集に関する項目を参照してください。

SMB では、Microsoft AD あるいはゲストアクセスを使用して、既存のオブジェクトがある Amazon S3 バケット用に共有をエクスポートできます。SMB ファイル共有を介してエクスポートされたオブジェクトは、POSIX の所有権とアクセス許可を直属の親ディレクトリから継承します。ルートフォルダ下のオブジェクトについては、ルートのアクセスコントロールリスト (ACL) が継承されます。

ルート ACL の場合、所有者は `smbguest` であり、ファイルのアクセス許可は 666、ディレクトリは 777 です。これはすべての形式の認証されたアクセス (Microsoft AD およびゲスト) に適用されます。

S3 ファイルゲートウェイをテストする

マッピングされたドライブにファイルとフォルダをコピーし、Amazon S3 バケットに自動的に表示されることを確認することでゲートウェイをテストするには、次の手順に従います。

ファイルを Windows クライアントから Amazon S3 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 S3 バケットの名前が付いています。
2. ドライブにファイルまたはフォルダをコピーします。
3. Amazon S3 マネジメントコンソールで、マッピングしたバケットに移動します。指定した Amazon S3 バケットにコピーしたファイルおよびフォルダが表示されます。

   作成したファイル共有は、 AWS Storage Gateway マネジメントコンソールのファイル共有タブで確認できます。

NFS あるいは SMB クライアントは、ファイルの書き込み、読み取り、削除、名前変更、切り捨てができます。

> **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。

ファイルゲートウェイの S3 での動作について、次の点に注意してください。

- 読み込みはリードスルーキャッシュから提供されます。つまり、データが使用できない場合は、S3 から取得され、キャッシュに追加されます。
- 書き込みは、ライトバックキャッシュを使用して、最適化されたマルチパート型アップロードにより S3 に送信されます。
- 読み込みと書き込みは、リクエストされた部分または変更された部分だけがネットワーク上で転送されるように最適化されます。

- 削除は S3 からオブジェクトを削除します。
- ディレクトリは、Amazon S3 コンソールと同じ構文を使用して、S3 のフォルダオブジェクトとして管理されます。空のディレクトリの名前を変更することができます。
- 再帰的なファイルシステムのオペレーションパフォーマンス (たとえば `ls -l`) は、バケット内のオブジェクトの数によって異なります。

Amazon S3 ファイルゲートウェイの管理

このセクションのトピックでは、Amazon S3 ファイルゲートウェイリソースを管理する方法について説明します。ゲートウェイ管理には、ゲートウェイがファイル共有と Amazon S3 バケットにアクセスするためのアクセス許可の付与、ゲートウェイとファイル共有の情報と設定の編集、ファイル共有の削除、キャッシュされたオブジェクトの更新、ゲートウェイとファイル共有の運用ステータスインジケータの理解が含まれます。

トピック

- 基本的なゲートウェイ情報を編集する - 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 ロググループなどを含む、既存のゲートウェイの基本情報を編集する方法について説明します。
- アクセスとアクセス許可の付与 - IAM ロールを使用して、Amazon S3 バケットと Amazon VPC エンドポイントのアクセス許可をゲートウェイに提供し、特定のセキュリティ問題を防ぎ、 AWS アカウント間でファイル共有をバケットに接続する方法について説明します。
- ファイル共有の削除 - Storage Gateway コンソールを使用してファイル共有を削除する方法について説明します。
- ゲートウェイ SMB 設定の編集 - セキュリティ戦略、Active Directory 認証、ゲストアクセス、ローカルグループのアクセス許可、ゲートウェイ上の SMB ファイル共有向けのファイル共有の可視性を制御するゲートウェイレベルの SMB 設定を編集する方法について説明します。
- SMB ファイル共有設定の編集 - SMB ファイル共有の名前、ログ記録、キャッシュ更新、ストレージクラス、ファイルエクスポートなどを設定する設定を編集する方法について説明します。
- SMB ファイル共有アクセスを制限する - 許可または拒否されたユーザーまたはグループを追加して、SMB ファイル共有へのアクセスを制限する方法について説明します。
- NFS ファイル共有設定の編集 - NFS ファイル共有の名前、ログ記録、キャッシュ更新、ストレージクラス、ファイルエクスポートなどを設定する設定を編集する方法について説明します。
- NFS ファイル共有のデフォルトメタデータ値の編集 - NFS ファイル共有のファイルとフォルダに対する Unix アクセス許可を含むデフォルトのメタデータ値を編集する方法について説明します。
- NFS ファイル共有アクセスを制限する - NFS ファイル共有向けに特定の IP アドレスまたは IP 範囲からクライアントへのアクセスを制限する方法について説明します。
- Amazon S3 バケットのオブジェクトキャッシュの更新 - ファイル共有の S3 バケットオブジェクトキャッシュを更新し、キャッシュを自動的に更新するようにスケジュールを設定する方法について説明します。

- S3 Object Lock の使用 - Amazon S3 ファイルゲートウェイが S3 Object Lock特徴量とどのように連携するかについて説明します。
- ファイル共有ステータス - ファイル共有ステータスを表示および解釈する方法について説明します。
- ゲートウェイのステータス - ゲートウェイステータスを表示および解釈する方法について説明します。
- Amazon S3 ファイルゲートウェイの帯域幅の管理 - ゲートウェイから へのアップロードスループットを制限 AWS して、ゲートウェイが使用するネットワーク帯域幅の量を制御する方法について説明します。

S3 ファイルゲートウェイの基本情報を編集するには

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。

ファイル共有とバケットへのアクセスとアクセス許可の付与

S3 File Gateway がアクティブ化されて実行されたら、追加のファイル共有を追加し、ゲートウェイやファイル共有 AWS アカウント とは異なる のバケットを含む Amazon S3 バケットへのアクセスを許可できます。以下のセクションでは、IAM ロールを使用して、ゲートウェイに Amazon S3 バケットと VPC エンドポイントのアクセス許可を付与し、特定のセキュリティ問題を防ぎ、 AWS アカウント間でファイル共有をバケットに接続する方法について説明します。

ファイル共有を追加する方法については、「ファイル共有の作成」を参照してください。

このセクションでは、ファイル共有と Amazon S3 バケットへのアクセスとアクセス許可を付与する方法に関する追加情報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

- Amazon S3 バケットに対するアクセス権限の付与 - ファイルゲートウェイにアクセス権限を付与して Amazon S3 バケットにファイルをアップロードし、バケットへの接続に使用するアクセスポイントまたは Amazon Virtual Private Cloud (Amazon VPC) エンドポイントに対してアクションを実行する方法について説明します。
- サービス間の混乱した代理の防止 - 共通のセキュリティ問題は、アクションを実行する許可を持たないエンティティが、より特権のあるエンティティにアクションを実行するように強制できるセキュリティの問題です。
- クロスアカウントアクセスでのファイル共有の使用 - Amazon Web Services アカウントおよび、別の Amazon Web Services アカウントに属するリソースにアクセスするあカウントのユーザーにアクセス権限が付与されます。

Amazon S3 バケットに対するアクセス権限の付与

ファイル共有を作成する際、ファイルゲートウェイは Amazon S3 バケットへのファイルアップロード、およびバケット接続に使用するアクセスポイントや仮想プライベートクラウド（VPC）エンドポイントに対するアクションを実行するためにアクセス権限を必要とします。このアクセスを付与するために、ファイルゲートウェイは、このアクセスを付与する IAM ポリシーに関連付けられた AWS Identity and Access Management (IAM) ロールを引き受けます。

このロールには、この IAM ポリシーに加え、Security Token Service (STS) 信頼関係が設定されていることが必要です。このポリシーによって、ロールで実行できるアクションが決まります。さらに、S3 バケットおよび関連するアクセスポイントまたは VPC エンドポイントには、IAM ロールによるアクセスを許可するアクセスポリシーが必要です。

これらのロールとアクセスポリシーは自分自身で作成したり、ユーザーに代わってファイルゲートウェイに作成させたりできます。ファイルゲートウェイでポリシーを作成した場合、そのポリシーには S3 アクションのリストが含まれます。ロールとアクセス許可については、IAM ユーザーガイドの [AWS のサービスのサービスにアクセス許可を委任するロールの作成] を参照してください。

次に示すのは、ファイルゲートウェイが IAM ロールを引き受けられるようにする信頼ポリシーの例です。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "storagegateway.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

> **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

ファイルゲートウェイがユーザーに代わってポリシーを作成しないようにするには、独自のポリシーを作成してファイル共有にアタッチします。これを行う方法については、「ファイル共有の作成」を参照してください。

次のポリシーの例では、ポリシーに表示されたすべての Amazon S3 アクションを、ファイルゲートウェイが実行することを許可します。ステートメントの最初の部分では、リストされたすべてのアクションを `amzn-s3-demo-bucket` という S3 バケットで実行するよう許可します。次に、`amzn-s3-demo-bucket` のすべてのオブジェクトでリストされたアクションを許可します。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:GetAccelerateConfiguration",
                "s3:GetBucketLocation",
                "s3:GetBucketVersioning",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3:ListBucketMultipartUploads"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Effect": "Allow"
        },
```

```
        {
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectVersion",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Effect": "Allow"
        }
    ]
}
```

次のポリシー例は前述のポリシーと似ていますが、ファイルゲートウェイがアクセスポイントを介してバケットにアクセスするために必要なアクションを実行できるようにします。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectVersion",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:us-east-1:111122223333:accesspoint/
TestAccessPointName/*",
            "Effect": "Allow"
```

```
        }
    ]
}
```

> **Note**
>
> ファイル共有を VPC エンドポイント経由で S3 バケットに接続する必要がある場合は、『AWS PrivateLink ユーザーガイド』の「Amazon S3 のエンドポイントポリシー」を参照してください。

> **Note**
>
> 暗号化されたバケットの場合、ファイル共有は送信先 S3 バケットアカウントのキーを使用する必要があります。

> **Note**
>
> ファイルゲートウェイが暗号化に SSE-KMS または DSSE-KMS を使用している場合は、ファイル共有に関連付けられた IAM ロールに kms:Encrypt、kms:Decrypt、kms:ReEncrypt*、kms:GenerateDataKey、および kms:DescribeKey のアクセス許可が含まれていることを確認してください。詳細については、「Storage Gateway でアイデンティティベースのポリシー (IAM ポリシー) を使用する」を参照してください。

サービス間の混乱した代理の防止

混乱した代理問題は、アクションを実行する許可を持たないエンティティが、より特権のあるエンティティにアクションを実行するように強制できるセキュリティの問題です。では AWS、サービス間のなりすましにより、混乱した代理問題が発生する可能性があります。サービス間でのなりすましは、1 つのサービス (呼び出し元サービス) が、別のサービス (呼び出し対象サービス) を呼び出すときに発生する可能性があります。呼び出し元サービスは、本来ならアクセスすることが許可されるべきではない方法でその許可を使用して、別のお客様のリソースに対する処理を実行するように操作される場合があります。これを防ぐため、 AWS では、アカウントのリソースへのアクセス権が付与さ

れたサービスプリンシパルで、すべてのサービスのデータを保護するために役立つツールを提供しています。

リソースポリシーで aws:SourceArnおよび aws:SourceAccount グローバル条件コンテキストキーを使用して、 がリソースに別のサービス AWS Storage Gateway に付与するアクセス許可を制限することをお勧めします。両方のグローバル条件コンテキストキーを同じポリシーステートメントで使用する場合は、aws:SourceAccount 値と、aws:SourceArn 値に含まれるアカウントが、同じアカウント ID を示している必要があります。

aws:SourceArn 値は、ファイル共有が関連付けられている Storage Gateway の ARN である必要があります。

混乱した代理問題から保護するための最も効果的な方法は、リソースの完全な ARN を指定して aws:SourceArn グローバル条件コンテキストキーを使用することです。リソースの完全な ARN が不明な場合や、複数のリソースを指定する場合は、aws:SourceArn グローバルコンテキスト条件キーを使用して、ARN の未知部分をワイルドカード (*) で表します。例えば、arn:aws:*servicename*::*123456789012*:* です。

次の例では、Storage Gateway で aws:SourceArn および aws:SourceAccount グローバル条件コンテキストキーを使用して、混乱した代理問題を回避する方法を示します。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
       "Sid": "ConfusedDeputyPreventionExamplePolicy",
       "Effect": "Allow",
       "Principal": {
         "Service": "storagegateway.amazonaws.com"
       },
       "Action": "sts:AssumeRole",
       "Condition": {
         "StringEquals": {
           "aws:SourceAccount": "444455556666"
         },
         "ArnLike": {
          "aws:SourceArn": "arn:aws:storagegateway:us-
east-1:444455556666:gateway/sgw-123456DA"
        }
```

```
      }
    }
  ]
}
```

クロスアカウントアクセスでのファイル共有の使用

クロスアカウントアクセスでは、Amazon Web Services アカウントおよびそのアカウントのユーザーに、別の Amazon Web Services アカウントに属するリソースに対するアクセス権限が付与されます。ファイルゲートウェイを使用すると、1 つの Amazon Web Services アカウント内のファイル共有を使用して、別の Amazon Web Services アカウントに属する Amazon S3 バケットのオブジェクトにアクセスできます。

ある Amazon Web Services アカウントが所有するファイル共有を使用して、別の Amazon Web Services アカウントの S3 バケットにアクセスするには

1. アクセスする必要のある S3 バケットと、そのバケット内のオブジェクトへのアクセス権限が、S3 バケットの所有者から Amazon Web Services アカウントに付与されていることを確認します。このアクセス権を付与する方法については、Amazon Simple Storage Service ユーザーガイドの「例 2: バケット所有者がクロスアカウントのバケットのアクセス許可を付与する」を参照してください。必要なアクセス権限のリストについては、「Amazon S3 バケットに対するアクセス権限の付与」を参照してください。
2. ファイル共有が S3 バケットにアクセスするために使用する IAM ロールには、`s3:GetObjectAcl` や `s3:PutObjectAcl` などのオペレーションを行うアクセス権限が含まれていることを確認します。さらに、この IAM ロールにはアカウントがこの IAM ロールを引き受けることができる信頼ポリシーが含まれていることを確認します。このような信頼ポリシーの例については、「Amazon S3 バケットに対するアクセス権限の付与」を参照してください。

   ファイル共有が既存のロールを使用して S3 バケットにアクセスする場合は、`s3:GetObjectAcl` および `s3:PutObjectAcl` オペレーションに対するアクセス許可を含める必要があります。このロールには、アカウントがこのロールを引き受けることを許可する信頼ポリシーも必要です。このような信頼ポリシーの例については、「Amazon S3 バケットに対するアクセス権限の付与」を参照してください。
3. https://console.aws.amazon.com/storagegateway/home でファイル共有を作成またはファイル共有設定を編集するときに、S3 バケット所有者がアクセスできるゲートウェイファイルを選択します。

クロスアカウントアクセスのファイル共有を作成または更新して、ファイル共有をオンプレミスにマウントした場合は、セットアップをテストすることを強くお勧めします。これを行うには、ディレクトリの内容一覧を表示するか、テストファイルを書き込んで S3 バケットのオブジェクトとして表示されることを確認します。

> **Important**
>
> クロスアカウントにファイル共有に使用するアカウントへのアクセス権限が付与されるようにポリシーが正しくセットアップされていることを確認します。正しく設定されていない場合には、操作している Amazon S3 バケットに伝達していないオンプレミスアプリケーションからファイルを更新します。

リソース

アクセスポリシーおよびアクセスコントロールリストの詳細については、以下を参照してください。

Amazon Simple Storage Service ユーザーガイドのアクセスポリシーのオプションを使用するためのガイドライン

『Amazon Simple Storage Service ユーザーガイド』の「アクセスコントロールリスト (ACL) の概要」

ファイル共有の削除

ファイル共有が不要になった場合は、Storage Gateway コンソールから削除できます。ファイル共有を削除すると、ゲートウェイは、ファイル共有でマッピングされている Amazon S3 バケットからデタッチされます。ただし、S3 バケットとその内容は削除されません。

ファイル共有を削除する際にゲートウェイから S3 バケットにデータをアップロードしている場合は、すべてのデータがアップロードされるまで削除プロセスは完了しません。データが完全にアップロードされるまで、ファイル共有のステータスは「削除中 (DELETING)」になります。

データが完全にアップロードされるまで待ちたくない場合は、本トピックの後半の「ファイル共有を強制的に削除するには」の手順を参照してください。

ファイル共有を削除するには

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。

2. [ファイル共有] を選択し、削除するファイル共有を 1 つ以上選択します。
3. [アクション] で、[ファイル共有の削除] 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. 指定したテープを削除することを確認し、確認ボックスに 「delete」と入力して [Delete (削除)] を選択します。

場合によっては、ファイル共有を削除する前に、Network File System (NFS) ファイル共有のファイルに書き込まれるデータがすべてアップロードされるまで待機することがあります。例えば、書き込まれたもののまだアップロードされていないデータを意図的に破棄したい場合や、ファイル共有をバックアップしている Amazon S3 バケットが既に削除されている場合など、指定されたデータのアップロードができなくなっている可能性があります。

このような場合は、 AWS マネジメントコンソール または `DeleteFileShare` API オペレーションを使用して、ファイル共有を強制的に削除できます。このオペレーションでは、データのアップロードプロセスは中断されます。このオペレーションを実行すると、ファイル共有は、FORCE_DELETING ステータスに変わります。Storage Gateway コンソールからファイル共有を強制的に削除するには、次の手順を参照してください。

ファイル共有を強制的に削除するには

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. ファイル共有リストページで、上記の手順で削除フラグを付けたファイル共有を選択して詳細を表示します。数秒後、[詳細] タブに削除通知メッセージが表示されます。
3. [詳細] タブに表示されるメッセージで、強制的に削除するファイル共有の ID を確認し、確認のボックスを選択してから、[今すぐ強制削除] を選択します。

> **Note**
>
> 強制削除オペレーションを元に戻すことはできません。
> ファイル共有を強制的に削除すると、マルチパートアップロードから部分的に転送されたファイルが Amazon S3 に残り、ストレージ料金が発生する可能性があります。これらのファイルパーツを自動的に削除するように Amazon S3 バケットライフサイクルルールを設定することをお勧めします。詳細については、「ベストプラクティス: マルチパートアップロードの管理」を参照してください。

また、DeleteFileShare API オペレーションを使用して、ファイル共有を強制的に削除することもできます。API を使用してファイル共有を削除するには、`storagegateway:DeleteFileShare` IAM ポリシーのアクセス許可が必要です。

ゲートウェイの SMB 設定の編集

ゲートウェイレベルの SMB 設定では、ゲートウェイ上の SMB ファイル共有のセキュリティ戦略、Active Directory 認証、ゲストアクセス、ローカルグループのアクセス許可、ファイル共有の可視性を設定できます。

ゲートウェイレベルの SMB 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. [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、編集する設定を選択します。

このセクションでは、ゲートウェイの個々の SMB 設定の設定に関する追加情報と手順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

- ゲートウェイのセキュリティレベルを設定する - セキュリティレベルを設定してサーバーメッセージブロック (SMB) の署名や暗号化などの接続要件を指定する方法、および SMB バージョン 1 クライアントからの接続を許可するかどうかについて説明します。
- Active Directory 認証の設定 - SMB ファイル共有へのユーザー認証アクセス用に企業の Active Directory または AWS Managed Microsoft AD を設定する方法について説明します。
- ゲストアクセスの付与 - 正しいゲストアカウントのユーザー名とパスワードを提供するすべてのユーザーのゲストアクセスを許可するようにゲートウェイを設定する方法について説明します。
- ローカルグループの設定 - Active Directory ユーザーに特別なファイル共有アクセス許可を付与するためのローカルグループを設定する方法について説明します。
- ファイル共有の可視性を設定するには - ユーザーに共有を一覧表示するときにゲートウェイ上の共有を表示するかどうかを指定する方法について説明します。

ゲートウェイのセキュリティレベル設定

S3 ファイルゲートウェイを使用して、ゲートウェイのセキュリティレベルを指定することができます。このセキュリティレベルを指定することで、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 暗号化を義務付けるか、または SMB バージョン 1 を許可するかどうかを設定できます。

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が高いほど、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。

- AES256 暗号化を適用する – このオプションを選択した場合、S3 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 のすべての現在の 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した場合、S3 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 のすべての現在の 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、S3 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 のすべての現在の SMB クライアントで機能します。

- [Client negotiated (交渉したクライアント)] — このオプションを選択した場合、リクエストは、クライアントによって交渉された内容に応じて確立されます。このオプションは、環境内の異なるクライアント間で互換性を最大限に高める場合に推奨されます。

> **Note**
>
> 2019 年 6 月 20 日以前にアクティブ化されたゲートウェイの場合、デフォルトのセキュリティレベルは [Client negotiated (交渉したクライアント)] です。
> 2019 年 6 月 20 日以降にアクティブ化されたゲートウェイの場合、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. [Save (保存)] を選択します。

Active Directory を使用したユーザーの認証

企業の Active Directory を使用するか、ユーザーが SMB ファイル共有への認証アクセス AWS Managed Microsoft AD を行うには、Microsoft AD ドメイン認証情報を使用してゲートウェイの SMB 設定を編集します。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 ファイル共有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。

また、SMB ファイル共有でアクセスコントロールリスト (ACL) を有効にすることもできます。ACL をアクティブ化する方法については、「Windows ACL を使用して SMB ファイル共有へのアクセスを制限する」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. [Save changes (変更の保存)] をクリックします。

ファイル共有へのアクセスを特定の AD ユーザーおよびグループに制限するには

1. Storage Gateway コンソールで、アクセスを制限するファイル共有を選択します。
2. [Actions (アクション)] ドロップダウンメニューから、[ファイル共有アクセス設定の編集] を選択します。
3. (オプション) [User and group file share access (ユーザーとグループのファイル共有アクセス)] セクションで、設定を選択します。

   [Allowed users and groups (許可されたユーザーおよびグループ)] で、[Add allowed user (許可するユーザーの追加)] または [Add allowed group(許可するグループの追加)] を選択し、ファイル共有のアクセスを許可する AD ユーザーまたはグループを入力します。このプロセスを繰り返して、必要な数のユーザーとグループを許可します。

   [Denied users and groups] (拒否されたユーザーおよびグループ) で、[Add denied user] (拒否するユーザーの追加) または[Add denied group] (拒否するグループの追加) を選択し、ファイル共有のアクセスを拒否する AD ユーザーまたはグループを入力します。このプロセスを繰り返して、必要な数のユーザーとグループを拒否します。

   > **Note**
   >
   > [Active Directory] が選択されている場合のみ、[User and group file share access (ユーザーとグループのファイル共有アクセス)] セクションが表示されます。
   > グループには @ 文字のプレフィックスを付ける必要があります。有効な形式は、`DOMAIN\User1`、`user1`、`@group1`、`@DOMAIN\group1` です。
   > [Allowed and Denied Users and Groups (許可および拒否されたユーザーとグループ)] のリストを設定した場合、Windows ACL はそれらのリストを上書きするアクセスを許可しません。
   > [Allowed and Denied Users and Groups (許可および拒否されたユーザーとグループ)] のリストは ACL の前に評価され、ファイル共有をマウントまたはアクセスできるユーザーを制御します。ユーザーまたはグループが Allowed (許可された) リストに配置されている場合、リストはアクティブと見なされ、それらのユーザーのみがファイル共有をマウントできます。

ユーザーがファイル共有をマウントすると、ACL は、ユーザーがアクセスできる特定のファイルまたはフォルダを制御する、より詳細な保護を提供します。詳細については、「新しい SMB ファイル共有での Windows ACL」を参照してください。

4. エントリの追加が完了したら、[Save (保存)] を選択します。

ファイル共有のアクセス権限のゲストへの付与

正しいゲストアカウントのユーザー名とパスワードを提供できるすべてのユーザーにゲストアクセスを許可するように S3 ファイルゲートウェイを設定できます。ユーザーがファイルゲートウェイにアクセスできる唯一の方法にする場合は、ゲートウェイを Microsoft Active Directory ドメインに加える必要はありません。このゲストアクセス方法を使用して、Active Directory ドメインのメンバーである S3 ファイルゲートウェイにファイル共有を作成することもできます。

ゲストアクセス認証方法を使用するようにファイル共有を設定する場合、ゲストアクセスユーザー名は `smbguest` です。ゲストアクセスを使用するファイル共有を作成する前に、`smbguest` ユーザー向けにデフォルトのパスワードを変更する必要があります。

ゲストユーザー `smbguest` のパスワードを変更するには、次の手順を使用します。

ゲストアクセスパスワードを変更するには

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. 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 [Gateways (ゲートウェイ)] を選択し、ゲストアクセスを提供するゲートウェイの [Name (名前)] を選択します。
3. [Actions (アクション)] ドロップダウンメニューから、[Edit SMB settings (SMB 設定の編集)] を選択し、[ゲストアクセス設定] を選択します。
4. [Guest password (ゲストパスワード)] で、設定するゲストアクセスパスワードを入力し、[Save changes (変更の保存)] を選択します。

ゲートウェイのローカルグループを設定するには

ローカルグループ設定では、ゲートウェイ上の SMB ファイル共有に対する特別なアクセス許可を Active Directory ユーザーまたはグループに付与できます。

ローカルグループ設定を使用して、ゲートウェイ管理者のアクセス許可を割り当てることができます。Gateway 管理者は、共有フォルダ Microsoft マネジメントコンソールのスナップインを使用して、開いているファイルとロックされているファイルを強制的に閉じることができます。

> **Note**
>
> ゲートウェイを Active Directory ドメインに結合する前に、少なくとも 1 つの Gateway Admin ユーザーまたはグループを追加する必要があります。

Gateway 管理者を割り当てるには

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. [Actions (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、[Local Group settings (ローカルグループ設定)] を選択します。
4. [Local Group settings (ローカルグループ設定)] セクションで、設定を選択します。このセクションは、Active Directory を使用するファイル共有に対してのみ表示されます。

   [Gateway Admins (ゲートウェイ管理者)] には、ローカルゲートウェイ管理者のアクセス許可を付与する Active Directory ユーザーとグループを追加します。ドメイン名を含めて、行ごとに 1 つのユーザーまたはグループを追加します。例えば、**`corp\Domain Admins`**。追加の行を作成するには、[Add new Gateway Admin (新しいゲートウェイ管理者の追加)] を選択します。

   > **Note**
   >
   > [Gateway Admins (ゲートウェイ管理者)]を編集すると、すべての SMB ファイル共有が切断および再接続されます。

5. [Save changes (変更を保存)]を選択し、[Proceed (続行)] を選択して、表示される警告メッセージを確認します。

ファイル共有の可視性を設定するには

ファイル共有の可視性により、ユーザーに共有の一覧を表示する場合に、ゲートウェイ上の共有が表示されるかどうかを制御します。ゲートウェイ上のファイル共有が表示されている場合、クライア

ントはゲートウェイの IP アドレスまたは DNS 名を知っていれば、ファイルブラウザを使用して共有を簡単に検出できます。ファイル共有が表示されない場合、クライアントは共有を検出するためにゲートウェイ IP または DNS 名に加えてファイル共有名を知っている必要があります。

> **Note**
>
> この設定は、デプロイ内のファイル共有へのアクセスを保護する有効な方法ではありません。セキュリティのため、特定のユーザーとグループへのアクセスを制限するアクセス許可を設定することをお勧めします。手順については、「SMB ファイル共有のユーザーとグループのアクセスを制限する」を参照してください。

ファイル共有の可視性を設定するには

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. [Actions (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、[ファイル共有の可視性設定] を選択します。
4. [Visibility status (可視性のステータス)] でチェックボックスをオンにし、ユーザーに共有を一覧表示する際に、このゲートウェイ上の共有を表示させます。ユーザーに共有のリストを表示する際に、このゲートウェイ上の共有が表示されないようにするには、このチェックボックスをオフにします。

SMB ファイル共有の設定の編集

既存の SMB ファイル共有の次の設定を編集できます。

- File share name (ファイル共有名) - ファイル共有の名前を入力する
- Audit logs (監査ログ) - 監査ログをオンまたはオフにする
- Existing log group list (既存のロググループリスト) - 監査ログの既存のロググループを選択する
- Non-gateway file cache refresh time (ゲートウェイ以外のファイルキャッシュの更新時間) - ファイル共有のキャッシュを更新する間隔を指定する

> **Note**
>
> この値を 30 分より短く設定すると、多数の Amazon S3 オブジェクトが頻繁に作成または削除される状況では、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。

- Upload events settling time (アップロードイベントの確定時間) - クライアントがファイルへの書き込みを完了した最終時点から、`ObjectUploaded` 通知を生成するまでの待機時間を秒単位で指定する
- 新しいオブジェクトのストレージクラス - Amazon S3 バケットに作成された新しいオブジェクトで使用するストレージクラスを選択する
- Guess MIME type (MIME タイプの推測) - アップロードされたオブジェクトの MIME タイプを、ファイル拡張子に基づいて Storage Gateway に推測させるかどうかを選択する
- S3 バケット所有者がアクセスできるゲートウェイファイル - ファイル共有にリンクされている Amazon S3 バケットを所有する AWS アカウントがゲートウェイ上のファイルにアクセスできるようにするかどうかを選択します。
- リクエスタ支払いを有効にする - バケット所有者ではなく、ファイル共有からデータを読み取るアカウントまたはリクエストするアカウントに、アクセス料金の支払いを要求するかどうかを選択する
- Export as (次の形式でエクスポート) - ファイルが読み取り/書き込み状態または読み取り専用状態でエクスポートされるかどうかを選択する
- File and directory access controlled by (ファイルとディレクトリアクセスの制御元) - Windows ACL または POSIX アクセス許可を使用してファイルとディレクトリへのアクセスを制御するかどうかを選択する
- 日和見ロック(オプロック) - ファイル共有がオポチュニスティックロックを使用してファイルバッファリング戦略を最適化できるようにするかどうかを選択する
- Force case sensitivity (大文字と小文字の区別を強制) - クライアントまたはゲートウェイがファイル名とディレクトリ名の大文字と小文字の区別を制御するかどうかを選択する

> **Note**
>
> ファイル共有の大文字と小文字の区別が現在有効になっている場合、無効にすると、名前は同じですが、大文字と小文字が異なるファイル (file.txt、File.txt など) にアクセスできな

くなる可能性があります。大文字と小文字を区別しないクライアントは、1 つのバージョンにのみアクセスできます。

- Access based enumeration for files and directories (ファイルとディレクトリのアクセスベースの列挙) - ディレクトリの列挙中に共有上のファイルとフォルダをすべてのユーザーに表示するか、読み取りアクセス権を持つユーザーのみに表示するかを選択する

> **Note**
>
> 既存のファイル共有を編集して新しいバケットまたはアクセスポイントをポイントしたり、VPC エンドポイント設定を変更したりすることはできません。これらの設定は、新しいファイル共有を作成する場合にのみ設定できます。

ファイル共有の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. [File shares] を選択し、更新するファイル共有を選択します。
3. [Actions (アクション)] で、[Edit share settings (共有の設定の編集)] をクリックします。
4. 必要に応じて任意の設定を編集します。
5. [Save (保存)] を選択します。

SMB ファイル共有のユーザーおよびグループのアクセスを制限する

ファイル共有へのアクセスを制限するには、許可または拒否されたユーザーまたはグループを追加することをお勧めします。そうしないと、認証されたすべてのユーザーがファイル共有を利用できるようになってしまいます。

SMB のアクセス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. [File shares (ファイル共有)] を選択して、編集する SMB ファイル共有を選択します。

3. [Actions (アクション)] で、[Edit share access settings (共有のアクセス設定の編集)] を選択します。
4. (オプション) [User and group file share access (ユーザーとグループのファイル共有アクセス)] セクションで、設定を選択します。

   [Allowed users and groups (許可されたユーザーおよびグループ)] で、[Add allowed user (許可するユーザーの追加)] または [Add allowed group(許可するグループの追加)] を選択し、ファイル共有のアクセスを許可する AD ユーザーまたはグループを入力します。このプロセスを繰り返して、必要な数のユーザーとグループを許可します。[Allowed user and groups (許可されたユーザーとグループ)] のリストにないユーザーは、アクセスを拒否されます。

   [Denied users and groups (拒否されたユーザーおよびグループ)] で、[Add denied user (拒否するユーザーの追加)] または[Add denied group (拒否するグループの追加)] を選択し、ファイル共有のアクセスを拒否する AD ユーザーまたはグループを入力します。このプロセスを繰り返して、必要な数のユーザーとグループを拒否します。[Allowed user and groups (許可されたユーザーとグループ)] リストが空の場合、[Denied users and groups (拒否されたユーザーとグループ)] リストにあるユーザーを除くすべてのユーザーにアクセスが許可されます。

   > **Note**
   >
   > AD ユーザー名またはグループ名のみを入力します。ドメイン名は、ゲートウェイが結合されている特定の AD のゲートウェイのメンバーシップによって暗黙的に設定されます。
   > 許可された/拒否されたユーザーまたはグループを指定しない場合、認証されたすべての AD ユーザーがファイル共有をエクスポートできます。

既存のファイル共有のサーバー側の暗号化方法を変更する

次の手順では、Storage Gateway コンソールを使用して、既存の NFS または SMB ファイル共有のサーバー側の暗号化方法を変更する方法について説明します。Storage Gateway API を使用してこのアクションを実行するには、AWS Storage Gateway API リファレンスの「UpdateNFSFileShare」または「UpdateSMBFileShare」を参照してください。

> **Note**
>
> 暗号化方法を更新すると、更新後に Amazon S3 バケットに保存されている既存のオブジェクトに新しい方法が適用されます。

暗号化に SSE-KMS を使用するようにファイルゲートウェイを設定する場合は、ファイル共有に関連付けられた IAM ロールに `kms:Encrypt`、`kms:Decrypt`、`kms:ReEncrypt*`、`kms:GenerateDataKey`、`kms:DescribeKey` のアクセス許可を手動で追加する必要があります。詳細については、「Storage Gateway でアイデンティティベースのポリシー (IAM ポリシー) を使用する」を参照してください。

NFS または SMB ファイル共有のサーバー側の暗号化方法を変更するには

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. [File shares (ファイル共有)] を選択し、暗号化方法を変更するファイル共有を選択します。
3. [Actions (アクション)] で、[Edit file share encryption (ファイル共有暗号化の編集)] をクリックします。
4. [Encryption (暗号化)] では、Amazon S3 の保管中のファイルに使用する暗号化のタイプを選択します。

   - Amazon S3 で管理されるサーバーサイド暗号化 (SSE-S3) を使用するには、[S3 マネージドキー (SSE-S3)]を選択します。詳細については、「Amazon Simple Storage Service ユーザーガイド」の「Amazon S3 マネージドキーによるサーバー側の暗号化の使用」を参照してください。
   - AWS Key Management Service (SSE-KMS) で管理されるサーバー側の暗号化を使用するには、KMS マネージドキー (SSE-KMS) を選択します。プライマリ KMS キーで、既存の AWS KMS キーを選択するか、新しい KMS キーの作成を選択して、Key Management Service (AWS KMS) コンソールで新しい KMS AWS キーを作成します。

     詳細については AWS KMS、「 AWS Key Management Service デベロッパーガイド」のAWS「 Key Management Service とは」を参照してください。
   - AWS Key Management Service (DSSE-KMS) で管理される二層式サーバー側の暗号化を使用するには、 AWS Key Management Service キーによる二層式サーバー側の暗号化 (DSSE-KMS) を選択します。プライマリ KMS キーで、既存の AWS KMS キーを選択するか、新しい KMS キーの作成を選択して、Key Management Service (AWS KMS) コンソールで新しい KMS AWS キーを作成します。

     DSSE-KMS の詳細については、「Amazon Simple Storage Service ユーザーガイド」の AWS KMS「キーによる二層式サーバー側の暗号化の使用」を参照してください。

> **Note**
>
> DSSE-KMS および AWS KMS キーの使用には追加料金がかかります。詳細については、「AWS KMS 料金表」を参照してください。
> リストにないエイリアスで AWS KMS キーを指定するか、別の AWS アカウントの AWS KMS キーを使用するには、 を使用する必要があります AWS Command Line Interface。非対称 KMS キーはサポートされていません。詳細については、AWS Storage Gateway API リファレンスの「CreateSMBFileShare」を参照してください。

5. 完了したら、[変更を保存] を選択します。

NFS ファイル共有の設定の編集

作成後に既存の NFS ファイル共有の設定を編集するには、次の手順に従います。

> **Note**
>
> 既存のファイル共有を編集して新しいバケットまたはアクセスポイントをポイントしたり、VPC エンドポイント設定を変更したりすることはできません。これらの設定は、新しいファイル共有を作成する場合にのみ設定できます。

ファイル共有の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. [File shares] を選択し、更新するファイル共有を選択します。
3. [Actions (アクション)] で、[Edit share settings (共有の設定の編集)] をクリックします。
4. [File share name] (ファイル共有名) で、ファイル共有の名前を入力します。
5. [Audit logs (監査ログ)] で、以下のいずれかを選択します。

   - このファイル共有の新しいロググループを作成するには、[Create a new log group (新しいロググループを作成する)] を選択します。
   - このファイル共有のヘルスとリソースの通知を既存のロググループに送信するには、[Use and existing log group (既存のロググループを使用)] を選択します。
   - このファイル共有のログ記録を無効にするには、[ログの無効化] を選択します。

監査ログの詳細については、「S3 ファイルゲートウェイ監査ログについて」を参照してください。

6. [Non-gateway file cache refresh time (非ゲートウェイファイルキャッシュの更新時間)] については、[Set refresh interval (更新間隔の設定)] を選択し、TTL (Time To Live) を使用してファイル共有のキャッシュを更新する時間を分または日で設定します。TTL は、最後に実行された更新からの時間的長さです。TTL 間隔が経過すると、ディレクトリにアクセスしたときに、ゲートウェイは Amazon S3 バケットからそのディレクトリの内容を更新します。

   > **Note**
   >
   > この値を 30 分より短く設定すると、多数の Amazon S3 オブジェクトが頻繁に作成または削除される状況では、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。

7. [Upload events settling time (イベント確定時間のアップロード)] で、[Settling time (確定時間)] を選択し、確定時間を秒単位で入力します。[Settling time (確定時間)] は、最新のクライアント書き込み操作から `ObjectUploaded` ログ通知の生成までの遅延を制御します。クライアントは短時間でファイルに多数の小さな書き込みを行うこともあるため、同じファイルに対して複数の通知が連続して生成されないように、このパラメータをできるだけ長く設定することをお勧めします。詳細については、「ファイルのアップロード通知の受け取り」を参照してください。
8. [新しいオブジェクトのストレージクラス] で、ドロップダウンリストからストレージクラスを選択します。ストレージクラスの詳細については、「ファイルゲートウェイでのストレージクラスの使用」を参照してください。
9. [Object metadata (オブジェクトメタデータ)] で、以下の操作を行います。

   a. Storage Gateway がファイル拡張子に基づいてアップロードされたオブジェクトのメディアタイプを推測できるようにする場合は、[Guess MIME type (MIME タイプの推測)] を選択します。

   b. S3 バケットを所有するアカウントが、読み取り、書き込み、編集、削除のアクセス許可など、ゲートウェイによって作成されたファイルの完全な所有権を持つようにする場合は、S3 バケット所有者がアクセスできるゲートウェイファイルを選択します。 AWS S3
10. バケット所有者ではなくファイルリクエスタがデータリクエストのコストを支払い、S3 バケットからダウンロードする場合は、[リクエスタ支払いを有効にする] を選択します。
11.
12. [アクセスレベル] で、以下のいずれかを選択します。

- ルートスカッシュ (デフォルト): リモートスーパーユーザー (ルート) のアクセスは UID (65534) および GID (65534) にマッピングされます。
- All squash (すべてスカッシュ): すべてのユーザーアクセスはユーザー ID (UID) (65534) およびグループ ID (GID) (65534) にマッピングされます。
- No root squash (ルートスカッシュなし): リモートスーパーユーザー (ルート) はルートとしてのアクセスを受け取ります。

13. [次の形式でエクスポート] で、次のいずれかを選択します。

- クライアントがファイル共有でファイルを読み書きできるようにするには、読み取り/書き込みを選択します。
- クライアントがファイルを読み取ってもファイル共有に書き込めないようにするには、読み取り専用を選択します。

> **Note**
>
> Microsoft Windows クライアントにマウントされたファイル共有で、[読み取り専用] を選択した場合は、予期しないエラーによってフォルダを作成できないことを示すメッセージが表示される場合があります。このメッセージは無視できます。

14. 編集が終わったら、[変更を保存] を選択します。

NFS ファイル共有でのデフォルトのメタデータ値の編集

バケットのファイルまたはディレクトリのメタデータ値を設定しない場合、S3 ファイルゲートウェイによりデフォルトのメタデータ値が設定されます。これらの値にはファイルとフォルダの Unix アクセス許可が含まれています。メタデータのデフォルト値は、Storage Gateway コンソールで編集することが可能です。

S3 ファイルゲートウェイはファイルとフォルダを Amazon S3 に保存し、Unix ファイルのアクセス許可はオブジェクトメタデータに保存されます。S3 ファイルゲートウェイが、S3 ファイルゲートウェイによって保存されなかったオブジェクトを検出した場合、これらのオブジェクトには、Unix ファイルへのアクセス許可がデフォルトで割り当てられます。次の表では、デフォルトの Unix のアクセス許可を示しています。

メタデータ	説明
ディレクトリ権限	形式「nnnn」の Unix ディレクトリモード。たとえば、「0666」は、ファイル共有内のすべてのディレクトリのアクセスモードを表します。デフォルト値は 0777 です。
ファイル権限	形式「nnnn」の Unix ファイルモード。たとえば、「0666」はファイル共有内のファイルモードを表します。デフォルト値は 0666 です。
ユーザー ID	ファイル共有のファイルのデフォルトの所有者 ID。デフォルト値は 65534 です。
グループ ID	ファイル共有のデフォルトグループ ID。デフォルト値は 65534 です。

メタデータのデフォルト値を編集するには

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. [File shares] を選択し、更新するファイル共有を選択します。
3. [アクション] で、[メタデータのファイルのデフォルトの編集] を選択します。
4. [メタデータのファイルのデフォルトの編集] ダイアログボックスで、メタデータの情報を提供して、[保存] を選択します。

NFS ファイル共有のクライアントアクセスを制限する

NFS クライアントアクセス設定を に編集して、NFS ファイル共有への接続が許可されている NFS クライアントの特定のクライアント IP アドレスまたは CIDR ブロック範囲のリストを定義することをお勧めします。変更しない場合、ネットワークのすべてのクライアントがファイル共有にマウントできます。

NFS ファイル共有のクライアントアクセスを制限するには

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 [ファイル共有] を選択し、編集する NFS ファイル共有の [ファイル共有のファイル共有 ID] を選択します。
3. [Actions (アクション)] ドロップダウンメニューから、[ファイル共有アクセス設定の編集] を選択します。

   [Access object (アクセスオブジェクト)] セクションには、現在 NFS ファイル共有への接続が許可されている IP アドレスと CIDR ブロックのリストが表示されます。アクセスが現在制限されていない場合は、0.0.0.0/0 CIDR ブロックの [Allowed clients (許可されたクライアント)] の下にエントリが表示されます。これは、可能なすべての IPv4 アドレスの接続が許可されていることを示します。
4. [Allowed clients (許可されたクライアント)」で、0.0.0.0/0 CIDR ブロックの右側にある [Remove (削除)]を選択します。
5. [Add client (クライアントを追加)] を選択し、許可するクライアントの IP アドレスまたはアドレス範囲を CIDR 表記で指定します。
6. 必要に応じて IP アドレスまたは範囲を追加するには、前のステップを繰り返します。間違えたり、アクセスを取り消す必要がある場合は、リストから削除する IP アドレスまたは範囲の右側にある [Remove (削除)] を選択できます。
7. 完了したら、[変更を保存] を選択します。

Amazon S3 バケットのオブジェクトキャッシュの更新

NFS または SMB クライアントがファイルシステムオペレーションを実行すると、ゲートウェイはファイル共有に関連付けられた S3 オブジェクトキャッシュ内のインベントリを維持します。ゲートウェイは、このキャッシュされた在庫表を使用して、Amazon S3 リクエストのレイテンシーと頻度を減らします。このオペレーションでは、S3 ファイルゲートウェイのキャッシュストレージにファイルをインポートしません。キャッシュされたインベントリを更新するだけで、S3 オブジェクトキャッシュ内のオブジェクトのインベントリに変更が反映されます。

ファイル共有の S3 バケットオブジェクトキャッシュを更新するには、次のリストからユースケースに最適な方法を選択し、対応する以下の手順を実行します。

> **Note**
>
> 使用する方法に関係なく、ディレクトリを初めて一覧表示すると、ゲートウェイは Amazon S3 からディレクトリのメタデータコンテンツを一覧表示します。ディレクトリの初期化に必要な時間は、そのディレクトリのエントリ数に比例します。

トピック

Storage Gateway コンソールを使用して自動キャッシュ更新スケジュールを設定する

次の手順では、指定した有効期限 (TTL) 値に基づいて自動キャッシュ更新スケジュールを設定します。TTL ベースのキャッシュ更新スケジュールを設定する前に、次の点を考慮してください。

- TTL は、特定のディレクトリの最後のキャッシュ更新からの時間の長さとして測定されます。
- TTL ベースのキャッシュ更新は、指定された TTL 期間が終了した後に特定のディレクトリにアクセスした場合にのみ発生します。
- 更新は再帰的ではありません。アクセスされる特定のディレクトリでのみ発生します。
- 更新では、TTL の有効期限が切れてから同期されていないディレクトリに対してのみ Amazon S3 API コストが発生します。
  - ディレクトリは、NFS または SMB アクティビティによってアクセスされる場合にのみ同期されます。
  - 同期は、指定した TTL 周期よりも頻繁に発生することはありません。
- TTL ベースのキャッシュ更新の設定は、ゲートウェイと Amazon S3 バケット間のワークフローの外部で、Amazon S3 バケットのコンテンツを頻繁に直接更新する場合にのみ推奨されます。
- 有効期限が切れた TTLs を持つディレクトリにアクセスする NFS および SMB オペレーションは、ゲートウェイがディレクトリの内容を更新する間ブロックされます。

> **Note**
>
> キャッシュの更新によりディレクトリアクセスオペレーションがブロックされる可能性があるため、デプロイに実用的な最長の TTL 期間を設定することをお勧めします。

Storage Gateway コンソールを使用して自動キャッシュ更新スケジュールを設定するには

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. [File shares (ファイル共有)] を選択します。
3. 更新スケジュールを設定するファイル共有を選択します。
4. [Actions (アクション)] で、[Edit share settings (共有の設定の編集)] をクリックします。
5. [S3 からのキャッシュを自動化で更新する] のチェックボックスをオンにし、有効期限 (Time To Live = TTL) を使用してファイル共有のキャッシュ更新を実行する時間を日、時間、分で指定します。TTL は、ディレクトリにアクセスすると、ファイルゲートウェイが最初にそのディレクトリのコンテンツを Amazon S3 バケットから更新するようになる、最後の更新からの期間です。
6. [Save changes] (変更の保存) をクリックします。

Amazon CloudWatch ルール AWS Lambda で を使用して自動キャッシュ更新スケジュールを設定する

Amazon CloudWatch ルール AWS Lambda で を使用して自動キャッシュ更新スケジュールを設定するには

1. S3 ファイルゲートウェイで使用されている S3 バケットを特定します。
2. [Event (イベント)] セクションが空白であることを確認します。このセクションは、後で自動的に入力されます。
3. IAM ロールを作成し、Lambda 関数 `lambda.amazonaws.com` との信頼関係を許可します。
4. 以下のポリシーを使用します。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "StorageGatewayPermissions",
            "Effect": "Allow",
            "Action": "storagegateway:RefreshCache",
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchLogsPermissions",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:CreateLogGroup",
                "logs:PutLogEvents"
            ],
            "Resource": "*"
        }
    ]
}
```

5. Lambda コンソールから Lambda 関数を作成します。
6. Lambda タスクに次の関数を使用します。

```
import json
import boto3
client = boto3.client('storagegateway')
def lambda_handler(event, context):
    print(event)
    response = client.refresh_cache(
        FileShareARN='arn:aws:storagegateway:ap-southeast-2:672406474878:share/
share-E51FBS9C'
    )
    print(response)
    return 'Your FileShare cache has been refreshed'
```

7. [Execution role] (実行ロール) で、作成した IAM ロールを選択します。

8. オプションで、Amazon S3 のトリガーを追加し、イベント (ObjectCreated または ObjectRemoved) を選択します。

   > **Note**
   >
   > RefreshCache では、新しいプロセスを開始する前に、前のプロセスを完了する必要があります。バケット内で多数のオブジェクトを作成または削除すると、パフォーマンスが低下する可能性があります。このため、S3 トリガーは使用しないことをお勧めします。代わりに、以下で説明する Amazon CloudWatch ルールを使用します。

9. CloudWatch コンソールで CloudWatch ルールを作成し、スケジュールを追加します。通常は、30 分間の固定レートの設定が推奨されます。ただし、S3 バケットが大規模な場合は、これを 1~2 時間にすることも可能です。
10. CloudWatch イベントのための新しいトリガーを追加し、作成したルールを選択します。
11. Lambda 設定を保存します。[テスト] を選択します。
12. [S3 PUT] をクリックし、要件に合わせてテストのカスタマイズを行います。
13. テストが成功します。成功しない場合は、JSON で要件を変更して再テストします。
14. Amazon S3 コンソールを開き、作成したイベントと Lambda 関数の ARN が存在することを確認します。
15. Amazon S3 コンソールまたは AWS CLIを使用して、オブジェクトをソース S3 バケットにアップロードします。

    CloudWatch コンソールは、次のような CloudWatch 出力を生成します。

```
{
    u'Records': [
        {u'eventVersion': u'2.0', u'eventTime': u'2018-09-10T01:03:59.217Z',
 u'requestParameters': {u'sourceIPAddress': u'MY-IP-ADDRESS'},
        u's3': {u'configurationId': u'95a51e1c-999f-485a-b994-9f830f84769f',
 u'object': {u'sequencer': u'00549CC2BF34D47AED', u'key': u'new/filename.jpeg'},
        u'bucket': {u'arn': u'arn:aws:s3:::amzn-s3-demo-bucket', u'name':
 u'MY-GATEWAY-NAME', u'ownerIdentity': {u'principalId': u'A3OKNBZ72HVPP9'}},
 u's3SchemaVersion': u'1.0'},
        u'responseElements': {u'x-amz-id-2':
 u'76tiugjhvjfyriugiug87t890nefevbck0iA3rPU9I/s4NY9uXwtRL75tCyxasgsdgfsq+IhvAg5M=',
 u'x-amz-request-id': u'651C2D4101D31593'},
        u'awsRegion': u'MY-REGION', u'eventName': u'ObjectCreated:PUT',
 u'userIdentity': {u'principalId': u'AWS:AROAI5LQR5JHFHDFHDFHJ:MY-USERNAME'},
 u'eventSource': u'aws:s3'}
```

```
    ]
}
```

Lambda 呼び出では、次のように出力されます。

```
{
    u'FileShareARN': u'arn:aws:storagegateway:REGION:ACCOUNT-ID:share/MY-SHARE-
ID',
        'ResponseMetadata': {'RetryAttempts': 0, 'HTTPStatusCode': 200,
 'RequestId': '6663236a-b495-11e8-946a-bf44f413b71f',
            'HTTPHeaders': {'x-amzn-requestid': '6663236a-b495-11e8-946a-
bf44f413b71f', 'date': 'Mon, 10 Sep 2018 01:03:59 GMT',
                'content-length': '90', 'content-type': 'application/x-amz-
json-1.1'
        }
    }
}
```

この更新は、クライアントにマウントされた NFS 共有に反映されます。

> **Note**
>
> 何百万ものオブジェクトを含む大規模なバケットで、大きなオブジェクトの作成または削除を更新するキャッシュの場合、更新に数時間かかる場合があります。

16. Amazon S3 コンソールまたは AWS CLIを使用して、オブジェクトを手動で削除します。
17. クライアントにマウントされている NFS 共有を表示します。(キャッシュが更新されたことにより) オブジェクトが消去されていることを確認します。
18. CloudWatch Logs をチェックして、イベント `ObjectRemoved:Delete` での削除に関するログを確認します。

```
{
    u'account': u'MY-ACCOUNT-ID', u'region': u'MY-REGION', u'detail': {}, u'detail-
type': u'Scheduled Event', u'source': u'aws.events',
    u'version': u'0', u'time': u'2018-09-10T03:42:06Z', u'id':
 u'6468ef77-4db8-0200-82f0-04e16a8c2bdb',
    u'resources': [u'arn:aws:events:REGION:MY-ACCOUNT-ID:rule/FGw-RefreshCache-CW']
}
```

> **Note**
>
> Cron ジョブまたはスケジュールされたタスクの場合、CloudWatch ログのイベントは `u'detail-type': u'Scheduled Event'` になります。

Storage Gateway コンソールを使用して手動キャッシュ更新を実行する

Storage Gateway コンソールを使用して手動キャッシュ更新を実行するには

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. [File shares (ファイル共有)] を選択し、更新を実行するファイル共有を選択します。
3. [Actions (アクション)] では、[Refresh cache (キャッシュを更新)] を選択します。

   更新処理にかかる時間は、ゲートウェイにキャッシュされているオブジェクトの数、および S3 バケットに対して追加または削除されたオブジェクトの数によって異なります。

Storage Gateway API を使用して手動キャッシュ更新を実行する

次の手順で、Storage Gateway API を使用して手動キャッシュ更新を実行します。API ベースのキャッシュ更新を実行する前に、次の点を考慮してください。

- 再帰更新または非再帰的更新を指定できます。
- 再帰更新は、リソースを大量に消費し、コストが高くなります。
- 更新には、リクエストで引数として渡すディレクトリと、再帰的な更新を指定した場合のそれらのディレクトリの子孫に対してのみ Amazon S3 API コストが発生します。
- 更新は、ゲートウェイの使用中に他のオペレーションと同時に実行されます。
  - NFS および SMB オペレーションは、オペレーションによってアクセスされるディレクトリの更新がアクティブでない限り、通常、更新中にブロックされません。
  - ゲートウェイは、現在のキャッシュコンテンツが古くなっているかどうかを判断できず、鮮度に関係なく NFS および SMB オペレーションに現在のコンテンツを使用します。
  - キャッシュ更新はゲートウェイ仮想ハードウェアリソースを利用するため、更新の進行中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。

- API ベースのキャッシュ更新の実行は、ゲートウェイと Amazon S3 バケット間のワークフローの外部で、Amazon S3 バケットの内容を直接更新する場合にのみ推奨されます。

> **Note**
>
> ゲートウェイワークフローの外部で Amazon S3 コンテンツを更新する特定のディレクトリがわかっている場合は、これらのディレクトリを API ベースの更新リクエストで指定して、Amazon S3 API のコストとゲートウェイのパフォーマンスへの影響を軽減することをお勧めします。

Storage Gateway API を使用して手動キャッシュ更新を実行するには

- Storage Gateway API を使用して HTTP POST リクエストを送信し、目的のパラメータを使用して `RefreshCache`オペレーションを呼び出します。詳細については、AWS Storage Gateway API リファレンスの「RefreshCache」を参照してください。

> **Note**
>
> `RefreshCache` リクエストの送信は、キャッシュ更新操作を開始するだけです。キャッシュの更新が完了しても、必ずしもファイルの更新が完了したとは限りません。ゲートウェイのファイル共有で新しいファイルを確認する前にファイルの更新オペレーションが完了したかどうかを判断するには、`refresh-complete` 通知を使用します。これをするには、Amazon CloudWatch Events を介して通知を受け取ることができます。詳細については、「ファイルオペレーションについての通知を受信する」を参照してください。

S3 ファイルゲートウェイでの S3 Object Lock の使用

Amazon S3 ファイルゲートウェイは、Amazon S3 Object Lock が有効化された、S3 バケットへのアクセスをサポートしています。Amazon S3 Object Lock により、「Write-Once-Read-Many (WORM)」モデルを使用したオブジェクトの保存が可能になります。Amazon S3 Object Lock を使用すると、S3 バケット内のオブジェクトが削除または上書きされるのを防ぐことができます。Amazon S3 Object Lock では、オブジェクトのバージョニングと連携してデータを保護します。

Amazon S3 Object Lock を有効化した後も、そのオブジェクトの変更は可能です。例えば、S3 ファイルゲートウェイ上のファイル共有を経由すれば、オブジェクトの書き込み、削除、または名前変更

を行うことができます。このようにしてオブジェクトを変更すると、S3 ファイルゲートウェイは前のバージョン (つまりロックされたオブジェクト) に影響せずに、オブジェクトの新しいバージョンを配置します。

例えば、S3 ファイルゲートウェイの NFS または SMB インターフェイスを使用してファイルを削除する際に、対応する S3 オブジェクトがロックされていると、ゲートウェイはオブジェクトの新しいバージョンに S3 削除マーカーを付加し、元のバージョンのオブジェクトをそのまま保存します。同様に、S3 ファイルゲートウェイがロックされたオブジェクトのコンテンツまたはメタデータを変更した場合、そのオブジェクトの新しいバージョンはその変更と共にアップロードされますが、元のロックされたバージョンのオブジェクトは変更されません。

Amazon S3 Object Lock の詳細については、Amazon Simple Storage Service ユーザーガイドの「S3 オブジェクトロックの使用」を参照してください。

ファイル共有のステータスについて

ステータスを確認することで、ファイル共有の状態を一目で確認できます。ステータスがファイル共有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。

ファイル共有のステータスは、Storage Gateway コンソールの Status (ステータス) 列で表示できます。ファイル共有が正しく機能している場合は、AVAILABLE のステータスが表示されます。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	ファイル共有は適切に設定され、使用可能です。これは、正常に動作しているファイル共有の標準ステータスです。
[CREATING] (作成中)	ファイル共有は作成中でまだ使用できません。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。ファイル共有がこのステータスでスタックした場合、ゲートウェイ VM の接続が失われた可能性があります AWS。
[UPDATING] (更新中)	ファイル共有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。ファイル共有がこのステータスでスタ

ステータス	意味
	ックした場合、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	ファイル共有は削除中です。ファイル共有は、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	ファイル共有は強制的に削除されます。ファイル共有はすぐに削除され、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。
利用不可	ファイル共有が異常です。アクションは必要ありません。考えられる原因には、ロールポリシーエラーや、存在しない Amazon S3 バケットへのマッピングなどがあります。異常な状態を引き起こしていた問題が解決すると、ファイル共有は使用可能な状態に戻ります。

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。

Amazon S3 ファイルゲートウェイの帯域幅の管理

ゲートウェイから へのアップロードスループットを制限 AWS して、ゲートウェイが使用するネットワーク帯域幅の量を制御できます。デフォルトでは、アクティブ化されたゲートウェイのレート制限は設定されていません。

bandwidth-rate-limitスケジュールは、、 AWS Software Development Kit (SDK) AWS マネジメントコンソール、または AWS Storage Gateway API を使用して設定できます (AWS Storage Gateway API リファレンスのUpdateBandwidthRateLimitSchedule」を参照してください) 。帯域幅レート制限スケジュールを使用すると、制限が 1 日または 1 週間を通して自動的に変更されるように設定できます。詳細については、「Storage Gateway コンソールを使用して、ゲートウェイの帯域幅レート制限スケジュールを表示および編集します。」を参照してください。

Storage Gateway コンソールまたは Amazon CloudWatch の [Monitoring (モニタリング)] タブの CloudBytesUploaded メトリクスを通じて、Storage Gateway のアップロードスループットをモニタリングできます。

> **Note**
>
> 帯域幅のレート制限は、Storage Gateway ファイルのアップロードにのみ適用されます。他のゲートウェイオペレーションは影響を受けません。
> 帯域幅レート制限は、アップロードされるすべてのファイルのスループットを 1 秒あたりに平均して調整することで機能します。アップロードがマイクロ秒単位またはミリ秒単位で帯域幅レート制限を一時的に超えることもありますが、これによって長時間にわたって大きなスパイクが発生することは通常ありません。

帯域幅レート制限の設定とスケジュールは、Amazon FSx ファイルゲートウェイタイプでは現在サポートされていません。

トピック

- Storage Gateway コンソールを使用して、ゲートウェイの帯域幅レート制限スケジュールを表示および編集します。
- を使用したゲートウェイ帯域幅レート制限の更新 AWS SDK for Java
- を使用したゲートウェイ帯域幅レート制限の更新 AWS SDK for .NET
- を使用したゲートウェイ帯域幅レート制限の更新 AWS Tools for Windows PowerShell

Storage Gateway コンソールを使用して、ゲートウェイの帯域幅レート制限スケジュールを表示および編集します。

このセクションでは、ゲートウェイの帯域幅レート制限スケジュールを表示および編集する方法について説明します。

帯域幅レート制限スケジュールを表示および編集するには

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. 左側のナビゲーションペインで [ゲートウェイ] を選択してから、管理対象のゲートウェイを選択します。
3. [Actions (アクション)] で、[Edit bandwidth rate limit schedule (帯域幅レート制限スケジュールの編集)] を選択します。

   ゲートウェイの帯域幅レート制限スケジュールは、[帯域幅レート制限スケジュールの編集] ダイアログボックスに表示されます。デフォルトでは、新規のゲートウェイには、帯域幅レート制限が定義されていません。
4. (オプション) [新しい帯域幅レート制限を追加] を選択して、設定可能な新しい間隔をスケジュールに追加します。追加する間隔ごとに、次の情報を入力します。

   - アップロード速度 — アップロード速度の制限をメガビット/秒 (Mbps) 単位で入力します。最小値は 100 Mbps です。

- 曜日 — 間隔を適用する定期的な曜日を選択します。間隔は、平日 (月曜日から金曜日) 、週末 (土曜日と日曜日) 、毎日、または毎週特定の日に適用できます。帯域幅レート制限を毎日、常に均一に適用するには、No schedule (スケジュールなし) を選択します。
- [Start time (開始時間)] – HH:MM 形式とゲートウェイの UTC からのタイムゾーンオフセットを使用して、帯域幅期間の開始時間を入力します。

> **Note**
>
> 帯域幅レート制限期間は、ここで分単位で指定した 1 分間の最初から始まります。

- [End time (終了時間)] – HH:MM 形式とゲートウェイの GMT からのタイムゾーンオフセットを使用して、帯域幅期間の終了時間を入力します。

> **Important**
>
> 帯域幅レート制限期間は、ここで分単位で指定した 1 分間の最後に終了します。1 時間の終わりに終了する期間をスケジュールするには、「**59**」と入力します。
> 連続する期間を続けてスケジュールする際に、1 時間の開始時に移行し、期間の間に中断がないようにするには、最初の期間の終了時間を「**59**」分と入力します。後の期間の開始時間は、「**00**」分と入力します。

5. (オプション) 帯域幅レート制限スケジュールが完了するまで、必要に応じて前のステップを繰り返します。スケジュールから間隔を削除する必要がある場合は、[削除] を選択します。

> **Important**
>
> 帯域幅レート制限期間を重複させることはできません。期間の開始時間は、前の期間の終了時間より後、かつ、次の区間の開始時間より前である必要があります。

6. 完了したら、[変更を保存] を選択します。

を使用したゲートウェイ帯域幅レート制限の更新 AWS SDK for Java

帯域幅レート制限をプログラムで更新することで (例えば、スケジュールされたタスクを使用することで)、一定期間にわたって制限を自動的に調整できます。次の例は、 AWS SDK for Javaを使用して、ゲートウェイの帯域幅レート制限を更新する方法を示しています。サンプルコードを使用するに

は、Java コンソールアプリケーションの実行について理解している必要があります。詳細については、AWS SDK for Java デベロッパーガイドの「Getting Started」を参照してください。

Example: を使用したゲートウェイ帯域幅レート制限の更新 AWS SDK for Java

次の Java コードの例では、ゲートウェイの帯域幅レート制限を更新します。このサンプルコードを使用するには、サービスエンドポイント、ゲートウェイ Amazon リソースネーム (ARN)、およびアップロード制限を指定する必要があります。Storage Gateway で使用可能な AWS サービスエンドポイントの一覧については、「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」でご確認ください。

```
   import java.io.IOException;

   import com.amazonaws.AmazonClientException;
   import com.amazonaws.auth.PropertiesCredentials;
   import com.amazonaws.services.storagegateway.AWSStorageGatewayClient;
   import com.amazonaws.services.storagegateway.model.
UpdateBandwidthRateLimitScheduleRequest;
   import com.amazonaws.services.storagegateway.model.
UpdateBandwidthRateLimitScheduleReturn;

   import java.util.Arrays;
   import java.util.Collections;
   import java.util.List;

   public class UpdateBandwidthExample {

       public static AWSStorageGatewayClient sgClient;

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

       // The endpoint
       static String serviceURL = "https://storagegateway.us-east-1.amazonaws.com";

       // Rates
       static long uploadRate = 100 * 1024 * 1024;  // Bits per second, minimum 100
Megabits/second

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

           // Create a Storage Gateway client
           sgClient = new AWSStorageGatewayClient(new PropertiesCredentials(
```

```
UpdateBandwidthExample.class.getResourceAsStream("AwsCredentials.properties")));
           sgClient.setEndpoint(serviceURL);

           UpdateBandwidth(gatewayARN, uploadRate, null); // download rate not
supported by S3 File Gateways

       }

       private static void UpdateBandwidth(String gatewayArn, long uploadRate, long
downloadRate) {
           try
           {
               BandwidthRateLimit bandwidthRateLimit = new
BandwidthRateLimit(downloadRate, uploadRate);
               BandwidthRateLimitInterval noScheduleInterval = new
BandwidthRateLimitInterval()
                   .withBandwidthRateLimit(bandwidthRateLimit)
                   .withDaysOfWeek(Arrays.asList(1, 2, 3, 4, 5, 6, 0))
                   .withStartHourOfDay(0)
                   .withStartMinuteOfHour(0)
                   .withEndHourOfDay(23)
                   .withEndMinuteOfHour(59);
               UpdateBandwidthRateLimitScheduleRequest
updateBandwidthRateLimitScheduleRequest =
                   new UpdateBandwidthRateLimitScheduleRequest()
                   .withGatewayARN(gatewayArn)
                   .with
BandwidthRateLimitIntervals(Collections.singletonList(noScheduleInterval));

               UpdateBandwidthRateLimitScheduleReturn
updateBandwidthRateLimitScheuduleResponse =
sgClient.UpdateBandwidthRateLimitSchedule(updateBandwidthRateLimitScheduleRequest);

               String returnGatewayARN =
updateBandwidthRateLimitScheuduleResponse.getGatewayARN();
               System.out.println("Updated the bandwidth rate limits of " +
returnGatewayARN);
               System.out.println("Upload bandwidth limit = " + uploadRate + " bits
per second");
           }
           catch (AmazonClientException ex)
           {
```

```
                System.err.println("Error updating gateway bandwith.\n" +
ex.toString());
            }
        }
    }
```

を使用したゲートウェイ帯域幅レート制限の更新 AWS SDK for .NET

帯域幅レート制限をプログラムで更新することで (例えば、スケジュールされたタスクを使用することで)、一定期間にわたって制限を自動的に調整できます。次の例は、.NET 用 AWS Software Development Kit (SDK) を使用してゲートウェイの帯域幅レート制限を更新する方法を示しています。サンプルコードを使用するには、.NET コンソールアプリケーションの実行について理解している必要があります。詳細については、AWS SDK for .NET デベロッパーガイドの「Getting Started」を参照してください。

Example: を使用してゲートウェイ帯域幅レート制限を更新する AWS SDK for .NET

次の C# コードの例では、ゲートウェイの帯域幅レート制限を更新します。このサンプルコードを使用するには、サービスエンドポイント、ゲートウェイ Amazon リソースネーム (ARN)、およびアップロード制限を指定する必要があります。Storage Gateway で使用可能な AWS サービスエンドポイントの一覧については、「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」でご確認ください。

```
    using System;
    using System.Collections.Generic;
    using System.Linq;
    using System.Text;
    using Amazon.StorageGateway;
    using Amazon.StorageGateway.Model;

    namespace AWSStorageGateway
    {
        class UpdateBandwidthExample
        {
            static AmazonStorageGatewayClient sgClient;
            static AmazonStorageGatewayConfig sgConfig;

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

            // The endpoint
```

```
            static String serviceURL = "https://storagegateway.us-
east-1.amazonaws.com";

            // Rates
            static long uploadRate = 100 * 1024 * 1024;  // Bits per second, minimum
 100 Megabits/second

            public static void Main(string[] args)
            {
                // Create a Storage Gateway client
                sgConfig = new AmazonStorageGatewayConfig();
                sgConfig.ServiceURL = serviceURL;
                sgClient = new AmazonStorageGatewayClient(sgConfig);

                UpdateBandwidth(gatewayARN, uploadRate, null);

                Console.WriteLine("\nTo continue, press Enter.");
                Console.Read();
            }

            public static void UpdateBandwidth(string gatewayARN, long uploadRate, long
 downloadRate)
            {
                try
                {
                   BandwidthRateLimit bandwidthRateLimit = new
 BandwidthRateLimit(downloadRate, uploadRate);
                   BandwidthRateLimitInterval noScheduleInterval = new
 BandwidthRateLimitInterval()
                    .withBandwidthRateLimit(bandwidthRateLimit)
                    .withDaysOfWeek(Arrays.asList(1, 2, 3, 4, 5, 6, 0))
                    .withStartHourOfDay(0)
                    .withStartMinuteOfHour(0)
                    .withEndHourOfDay(23)
                    .withEndMinuteOfHour(59);
                  List <BandwidthRateLimitInterval> bandwidthRateLimitIntervals = new
 List<BandwidthRateLimitInterval>();
                  bandwidthRateLimitIntervals.Add(noScheduleInterval);
                  UpdateBandwidthRateLimitScheduleRequest
 updateBandwidthRateLimitScheduleRequest =
                    new UpdateBandwidthRateLimitScheduleRequest()
                       .withGatewayARN(gatewayARN)
                       .with BandwidthRateLimitIntervals(bandwidthRateLimitIntervals);
```

```
                    UpdateBandwidthRateLimitScheduleReturn
updateBandwidthRateLimitScheuduleResponse =
sgClient.UpdateBandwidthRateLimitSchedule(updateBandwidthRateLimitScheduleRequest);
                    String returnGatewayARN =
updateBandwidthRateLimitScheuduleResponse.GatewayARN;
                    Console.WriteLine("Updated the bandwidth rate limits of " +
returnGatewayARN);
                    Console.WriteLine("Upload bandwidth limit = " + uploadRate + " bits
per second");
                }
                catch (AmazonStorageGatewayException ex)
                {
                    Console.WriteLine("Error updating gateway bandwith.\n" +
ex.ToString());
                }
            }
        }
    }
```

を使用したゲートウェイ帯域幅レート制限の更新 AWS Tools for Windows PowerShell

帯域幅レート制限をプログラムで更新することで (例えば、スケジュールされたタスクを使用することで)、一定期間にわたって制限を自動的に調整できます。次の例は、 AWS Tools for Windows PowerShellを使用して、ゲートウェイの帯域幅レート制限を更新する方法を示しています。サンプルコードを使用するには、PowerShell スクリプトの実行について理解している必要があります。詳細については、AWS Tools for PowerShell ユーザーガイドの「使用開始」を参照してください。

Example: を使用してゲートウェイ帯域幅レート制限を更新する AWS Tools for Windows PowerShell

次の PowerShell スクリプトの例では、ゲートウェイの帯域幅レート制限を更新します。このサンプルスクリプトを使用するには、ゲートウェイ Amazon リソースネーム (ARN)、およびアップロード制限を指定する必要があります。

```
    <#
    .DESCRIPTION
        Update Gateway bandwidth limits schedule

    .NOTES
        PREREQUISITES:
        1) AWS Tools for PowerShell from https://aws.amazon.com/powershell/
```

```
        2) Credentials and region stored in session using Initialize-AWSDefault.
        For more info, see https://docs.aws.amazon.com/powershell/latest/userguide/
specifying-your-aws-credentials.html



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

    $UploadBandwidthRate = 100 * 1024 * 1024
    $gatewayARN = "*** provide gateway ARN ***"

    $bandwidthRateLimitInterval = New-Object
 Amazon.StorageGateway.Model.BandwidthRateLimitInterval
    $bandwidthRateLimitInterval.StartHourOfDay = 0
    $bandwidthRateLimitInterval.StartMinuteOfHour = 0
    $bandwidthRateLimitInterval.EndHourOfDay = 23
    $bandwidthRateLimitInterval.EndMinuteOfHour = 59
    $bandwidthRateLimitInterval.DaysOfWeek = 0,1,2,3,4,5,6
    $bandwidthRateLimitInterval.AverageUploadRateLimitInBitsPerSec =
 $UploadBandwidthRate

    #Update Bandwidth Rate Limits
    Update-SGBandwidthRateLimitSchedule -GatewayARN $gatewayARN `
                                        -BandwidthRateLimitInterval
 @($bandwidthRateLimitInterval)

    $schedule =  Get-SGBandwidthRateLimitSchedule -GatewayARN $gatewayARN

    Write-Output("`nGateway: " + $gatewayARN);
    Write-Output("`nNew bandwidth throttle schedule: " +
 $schedule.BandwidthRateLimitIntervals.AverageUploadRateLimitInBitsPerSec)
```

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。
- S3 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。S3 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「ファイル共有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
- ファイル共有が利用不可:`FileSharesUnavailable` >= 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 S3 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。

S3 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 S3 File GatewayFSx 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 S3 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
- ファイルオペレーションについての通知を受信する
- ゲートウェイメトリクスについて
- ファイル共有メトリクスについて
- S3 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 S3 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、S3 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、S3 ファイルゲートウェイがファイルを Amazon S3 バケット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 S3 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。

以下に示しているのは、S3 ファイルゲートウェイによってレポートされるエラーの例です。

```
{
    "severity": "ERROR",
    "bucket": "bucket-smb-share2",
    "roleArn": "arn:aws:iam::123456789012:role/amzn-s3-demo-bucket",
    "source": "share-E1A2B34C",
    "type": "InaccessibleStorageClass",
    "operation": "S3Upload",
    "key": "myFolder/myFile.text",
    "gateway": "sgw-B1D123D4",
    "timestamp": "1565740862516"
}
```

このエラーは、S3 ファイルゲートウェイがオブジェクト `myFolder/myFile.text` をAmazon S3 にアップロードできないことを意味します。これは、 オブジェクトがAmazon S3 Standardストレージクラスから移行し、S3 Glacier Flexible RetrievalまたはS3 Glacier Deep Archiveストレージクラスに移行したためです。

前述のゲートウェイヘルスログでは、以下の項目は特定の情報を示します。

- `source: share-E1A2B34C` は、このエラーが発生したファイル共有を示します。
- `"type": "InaccessibleStorageClass"` は、発生したエラーのタイプを示します。この場合、ゲートウェイが指定されたオブジェクトを Amazon S3 にアップロードしようとしたとき、または Amazon S3 から読み取ろうとしたときに、このエラーが発生しました。ただしこの場合、オブジェクトは Amazon Glacier に移行しています。`"type"` の値は、S3 ファイルゲートウェイで発生したいずれかのエラーであると考えられます。考えられるエラーのリストについては、「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。
- `"operation": "S3Upload"` は、ゲートウェイがこのオブジェクトを S3 にアップロードしようとしたときに、このエラーが発生したことを示します。
- `"key": "myFolder/myFile.text"` は、失敗の原因となったオブジェクトを示します。

- `gateway": "sgw-B1D123D4` は、このエラーが発生した S3 ファイルゲートウェイを示します。
- `"timestamp": "1565740862516"` は、エラーが発生した時間を示します。

S3 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。

S3 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、S3 File GatewayFSx 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。S3 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。 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

ファイルオペレーションについての通知を受信する

Storage Gateway は、ファイル操作が完了したときに次の CloudWatch イベントを開始できます：

- ゲートウェイによる、ファイル共有から Amazon S3 へのファイルの非同期アップロードが完了したときに、通知を受けることができます。`NotificationPolicy` パラメータを使用して、ファイルのアップロード通知をリクエストします。これにより、Amazon S3 へのファイルアップロードが完了するたびに通知が送信されます。詳細については、「ファイルのアップロード通知の受け取り」を参照してください。
- ゲートウェイによる、ファイル共有から Amazon S3 へのワーキングファイルセットの非同期アップロードが完了したときに、通知を受けることができます。NotifyWhenUploaded API オペレーションを使用して、ワーキングファイルセットのアップロード通知をリクエストできます。これにより、作業ファイルセット内のすべてのファイルが Amazon S3 にアップロードされたときに、通知が送信されます。詳細については、「ワーキングファイルセットのアップロード通知の受け取り」を参照してください。
- ゲートウェイによる S3 バケットのキャッシュの更新が完了したときに、通知を受けることができます。Storage Gateway コンソールまたは API を通じて RefreshCache 操作を実行する際は、操作完了時の通知を購読してください。詳細については、「キャッシュ更新通知の取得」を参照してください。

リクエストしたファイルオペレーションが完了すると、Storage Gateway は CloudWatch Events を介して通知を送信します。Amazon SNS、Amazon SQS、 AWS Lambda 関数などのイベントターゲットを介して通知を送信するように CloudWatch Events を設定できます。例えば、E メールやテキストメッセージなどの通知を Amazon SNS コンシューマーに送信するように Amazon SNS ターゲットを設定できます。CloudWatch Events の詳細については、「Amazon CloudWatch Events とは」を参照してください。

CloudWatch Events 通知をセットアップするには

1. Amazon SNS トピックや Lambda 関数などのターゲットを作成して、Storage Gateway でリクエストされたイベントが発生したときに呼び出されるようにします。
2. Storage Gateway のイベントに応じてターゲットを呼び出すルールを、CloudWatch Events コンソールで作成します。
3. ルールで、イベントタイプのイベントパターンを作成します。この通知は、イベントがこのルールパターンに一致したときに送信されます。
4. ターゲットを選択し、設定を指定します。

次の例は、指定されたゲートウェイと指定された AWS リージョンで指定されたイベントタイプを開始するルールを示しています。たとえば、イベントタイプとして `Storage Gateway File Upload Event` を指定できます。

```
{
   "source":[
      "aws.storagegateway"
   ],
   "resources":[
      "arn:aws:storagegateway:AWS Region:account-id
                  :gateway/gateway-id"
   ],
   "detail-type":[
      "Event type"
   ]
}
```

CloudWatch Events ルールの使用方法については、Amazon CloudWatch Events ユーザーガイドの「イベントでトリガーする CloudWatch Events のルールの作成」を参照してください。

ファイルのアップロード通知の受け取り

ファイルのアップロード通知を使用できるユースケースには、次の 2 つがあります。

- アップロードされるファイルのクラウド内処理を自動化するユースケースでは、`NotificationPolicy` パラメータを呼び出して通知 ID を返すことができます。ファイルがアップロードされたときに発生する通知には、API によって返されたものと同じ通知 ID が付けられます。アップロードしているファイルのリストを追跡するためにこの通知 ID をマッピングする

場合、同じ ID の付いたイベントが生成されるときに、 AWS にアップロードされるファイルの処理を開始できます。

- コンテンツ配信のユースケースでは、2 つの S3 ファイルゲートウェイを同じ Amazon S3 バケットにマッピングできます。Gateway1 のファイル共有クライアントは新しいファイルを Amazon S3 にアップロードする場合があります。ファイルは Gateway2 のファイル共有クライアントによって読み取られます。ファイルは Amazon S3 にアップロードされますが、Amazon S3 ではローカルにキャッシュされたファイルのバージョンが使用されるため、Gateway2 からはファイルが見えません。ファイルを Gateway2 で表示するには、`NotificationPolicy` パラメータを使用して Gateway1 に対してファイルのアップロード通知をリクエストし、ファイルアップロードの完了時に通知を受け取ることができます。次に、CloudWatch Events を使用して、Gateway2 のファイル共有に対して RefreshCache リクエストを自動的に発行できます。RefreshCache リクエストが完了すると、新しいファイルが Gateway2 に表示されます。

Example例 – ファイルのアップロード通知

以下の例では、作成したルールにイベントが一致する場合に CloudWatch を介して送信されるファイルのアップロード通知を示しています。この通知は JSON 形式です。この通知をテキストメッセージとしてターゲットに配信するように設定できます。`detail-type` は、`Storage Gateway Object Upload Event` です。

```
{
    "version": "0",
    "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
    "detail-type": "Storage Gateway Object Upload Event",
    "source": "aws.storagegateway",
    "account": "123456789012",
    "time": "2020-11-05T12:34:56Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:storagegateway:us-east-1:123456789011:share/share-F123D451",
        "arn:aws:storagegateway:us-east-1:123456789011:gateway/sgw-712345DA",
        "arn:aws:s3:::do-not-delete-bucket"
    ],
    "detail": {
        "object-size": 1024,
        "modification-time": "2020-01-05T12:30:00Z",
        "object-key": "my-file.txt",
        "event-type": "object-upload-complete",
        "prefix": "prefix/",
        "bucket-name": "amzn-s3-demo-bucket",
```

```
    }
}
```

フィールド名	説明
version (バージョン)	IAM ポリシーの現在のバージョン
id	IAM ポリシーを識別する ID。
detail-type	送信された通知を開始したイベントの説明。
ソース	リクエストと通知のソースである AWS サービス。
アカウント	リクエストと通知が生成された AWS アカウントの ID。
時間	Amazon S3 へのファイルのアップロードリクエストが行われた日時。
リージョン	リクエストと通知の送信元の AWS リージョン。
リソース	ポリシーが適用される Storage Gateway リソース。
object-size	オブジェクトのサイズ (バイト単位)。
modification-time	クライアントがファイルを修正した時刻。
object-key	ファイルへのパス。
event-type	通知を開始した CloudWatch Events。
prefix	S3 バケットのプレフィックス名。
bucket-name	S3 バケットの名前。

ワーキングファイルセットのアップロード通知の受け取り

ワーキングファイルセットのアップロード通知を使用できるユースケースには、次の 2 つがあります。

- アップロードされるファイルのクラウド内処理を自動化するユースケースでは、NotifyWhenUploaded API を呼び出して通知 ID を返すことができます。ファイルのワーキングセットがアップロードされたときに発生される通知には、API によって返されたものと同じ通知 ID が付けられます。この通知 ID をマッピングしてアップロードするファイルのリストを追跡する場合、同じ ID のイベントが生成され AWS たときにアップロードされるファイルのワーキングセットの処理を開始できます。
- コンテンツ配信のユースケースでは、2 つの S3 ファイルゲートウェイを同じ Amazon S3 バケットにマッピングできます。Gateway1 のファイル共有クライアントは新しいファイルを Amazon S3 にアップロードする場合があります。ファイルは Gateway2 のファイル共有クライアントによって読み取られます。ファイルは Amazon S3 にアップロードされますが、S3 ではローカルにキャッシュされたファイルのバージョンが使用されるため、Gateway2 からはファイルが見えません。ファイルを Gateway2 で表示するには、NotifyWhenUploaded API オペレーションを使用して Gateway1 に対してファイルのアップロード通知をリクエストし、ファイルのワーキングセットのアップロードが完了したときに通知を受け取ります。次に、CloudWatch Events を使用して、Gateway2 のファイル共有に対して RefreshCache リクエストを自動的に発行できます。RefreshCache リクエストが完了すると、新しいファイルが Gateway2 に表示されます。このオペレーションでは、ゲートウェイのキャッシュストレージにファイルをインポートしません。キャッシュされたインベントリを更新するだけで、S3 バケット内のオブジェクトのインベントリに変更が反映されます。

Example例 – ワーキングファイルセットのアップロード通知

以下の例では、作成したルールにイベントが一致する場合に CloudWatch を介して送信されるワーキングファイルセットのアップロード通知を示しています。この通知は JSON 形式です。この通知をテキストメッセージとしてターゲットに配信するように設定できます。detail-type は、Storage Gateway File Upload Event です。

```
{
    "version": "2012-10-17",
    "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
    "detail-type": "Storage Gateway File Upload Event",
    "source": "aws.storagegateway",
    "account": "123456789012",
```

```
    "time": "2017-11-06T21:34:42Z",
    "region": "us-east-2",
    "resources": [
        "arn:aws:storagegateway:us-east-2:123456789011:share/share-F123D451",
        "arn:aws:storagegateway:us-east-2:123456789011:gateway/sgw-712345DA"
    ],
    "detail": {
        "event-type": "upload-complete",
        "notification-id": "11b3106b-a18a-4890-9d47-a1a755ef5e47",
        "request-received": "2018-02-06T21:34:42Z",
        "completed": "2018-02-06T21:34:53Z"
    }
}
```

フィールド名	説明
version (バージョン)	IAM ポリシーの現在のバージョン
id	IAM ポリシーを識別する ID。
detail-type	送信された通知を開始したイベントの説明。
ソース	リクエストと通知のソースである AWS サービス。
アカウント	リクエストと通知が生成された AWS アカウントの ID。
時間	Amazon S3 へのファイルのアップロードリクエストが行われた日時。
リージョン	リクエストと通知の送信元の AWS リージョン。
リソース	ポリシーが適用される Storage Gateway リソース。
event-type	通知を開始した CloudWatch Events。
notification-id	送信された通知のランダムに生成された ID。この ID は UUID 形式です。これは、

フィールド名	説明
	NotifyWhenUploaded が呼び出されたときに返される通知 ID です。
request-received	ゲートウェイが NotifyWhenUploaded リクエストを受信した日時。
完了	ワーキングセット内のすべてのファイルが Amazon S3 にアップロードされた日時。

キャッシュ更新通知の取得

キャッシュ更新通知のユースケースでは、同じ Amazon S3 バケットにマッピングされた 2 つの S3 ファイルゲートウェイを用意し、Gateway1 の NFS クライアントが S3 バケットに新しいファイルをアップロードできます。ファイルは Amazon S3 にアップロードされますが、キャッシュを更新するまでは Gateway2 にファイルが表示されません。これは、Gateway2 が Amazon S3 内のファイルをローカルにキャッシュしたバージョンを使用しているためです。キャッシュの更新が完了したら Gateway2 内のファイルを使用して何らかの作業を行う予定があるとします。大きいファイルは Gateway2 に表示されるまでに時間がかかる場合があるため、キャッシュの更新の完了時に通知を受け取りたいことがあります。すべてのファイルが Gateway2 に表示されるようになったら通知を受け取るように、Gateway2 からキャッシュ更新の通知をリクエストできます。

Example例 – キャッシュの更新通知

以下の例では、作成したルールにイベントが一致する場合に CloudWatch を介して送信されるキャッシュの更新通知を示しています。この通知は JSON 形式です。この通知をテキストメッセージとしてターゲットに配信するように設定できます。detail-type は、Storage Gateway Refresh Cache Event です。

```
{
    "version": "2012-10-17",
    "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
    "detail-type": "Storage Gateway Refresh Cache Event",
    "source": "aws.storagegateway",
    "account": "209870788375",
    "time": "2017-11-06T21:34:42Z",
    "region": "us-east-2",
    "resources": [
        "arn:aws:storagegateway:us-east-2:123456789011:share/share-F123D451",
```

```
        "arn:aws:storagegateway:us-east-2:123456789011:gateway/sgw-712345DA"
    ],
    "detail": {
        "event-type": "refresh-complete",
        "notification-id": "1c14106b-a18a-4890-9d47-a1a755ef5e47",
        "started": "2018-02-06T21:34:42Z",
        "completed": "2018-02-06T21:34:53Z",
        "folderList": [
            "/"
        ]
    }
}
```

フィールド名	説明
version (バージョン)	IAM ポリシーの現在のバージョン
id	IAM ポリシーを識別する ID。
detail-type	送信された通知を開始したイベントの種類の説明。
ソース	リクエストと通知のソースである AWS サービス。
アカウント	リクエストと通知が生成された AWS アカウントの ID。
時間	作業セット内のファイルの更新リクエストが行われた日時。
リージョン	リクエストと通知の送信元の AWS リージョン。
リソース	ポリシーが適用される Storage Gateway リソース。
event-type	通知を開始した CloudWatch Events。
notification-id	送信された通知のランダムに生成された ID。この ID は UUID 形式です。これは、

フィールド名	説明
	RefreshCache が呼び出されたときに返される通知 ID です。
開始	ゲートウェイが RefreshCache リクエストを受信し、更新が開始された日時。
完了	作業セットの更新が完了した日時。
folderList	キャッシュ内で更新されたフォルダのパスのコンマ区切りリスト。デフォルトは ["/"] です。

ゲートウェイメトリクスについて

次の表は、S3 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、特定のファイル共有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、ファイル共有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、ファイル共有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、S3 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
AuditNotifications	このメトリクスは、出力された監査ログの数を報告します。

メトリクス	説明
	単位: カウント
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
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
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

メトリクス	説明
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。 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。 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。 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
FileSharesUnavailable	このメトリクスは、このゲートウェイ上で 利用不可 状態にあるファイル共有の数を提供します。 このメトリクスがファイル共有が使用できないと報告した場合、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

メトリクス	説明
FilesRenamed	このメトリクスは、報告期間中に名前が変更されたファイルの数を追跡します。 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
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

メトリクス	説明
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
NfsSessions	このメトリクスは、ゲートウェイでアクティブな NFS セッションの数を報告します。 単位: カウント
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
S3GetObjectRequestTime	このメトリクスは、ゲートウェイが S3 のオブジェクト取得 (GET) リクエストを完了するまでの時間を報告します。 単位: ミリ秒

メトリクス	説明
S3PutObjectRequestTime	このメトリクスは、ゲートウェイが S3 put オブジェクトリクエストを完了するまでの時間を報告します。 単位: ミリ秒
S3UploadPartRequestTime	このメトリクスは、ゲートウェイが S3 アップロードパートリクエストを完了するまでの時間を報告します。 単位: ミリ秒
SmbV1Sessions	このメトリクスは、ゲートウェイでアクティブな SMBv1 セッションの数を報告します。 単位: カウント
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。 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。 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

ファイル共有メトリクスについて

ファイル共有に関する Storage Gateway メトリクスについて、以下に説明します。各ファイル共有には、一連の関連付けられたメトリクスがあります。一部の共有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、ゲートウェイの代わりにファイル共有を対象としています。

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、ファイル共有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、ファイル共有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共有を識別する `File share 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。

メトリクス	説明
	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。 **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

メトリクス	説明
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
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

メトリクス	説明
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

S3 ファイルゲートウェイ監査ログについて

Amazon S3 ファイルゲートウェイ(S3 ファイルゲートウェイ)の監査ログは、ファイル共有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。これらを使用して、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。

オペレーション

次の表は、S3 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

次の表は、S3 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を示しています。

属性	定義
accessMode	オブジェクトのアクセス許可の設定。
accountDomain (SMB のみ)	クライアントのアカウントが属する Active Directory (AD) ドメイン。
accountName (SMB のみ)	クライアントのアクティブディレクトリユーザー名。
bucket	S3 バケット名
clientGid (NFS のみ)	オブジェクトにアクセスするユーザーのグループの識別子。
clientUid (NFS のみ)	オブジェクトにアクセスするユーザーの識別子。
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)。
groupId	オブジェクトのグループ所有者の識別子。
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)。
gateway	Storage Gateway 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)。
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。
objectName	オブジェクトへのフルパス。

属性	定義
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。
operation	オブジェクトのアクセスオペレーションの名前。
ownerId	オブジェクトの所有者の識別子。
securityDescriptor (SMB のみ)	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。
shareName	アクセスされている共有の名前。
source	監査対象のファイル共有の ID。
sourceAddress	ファイル共有クライアントマシンの IP アドレス。
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)。
timestamp	ゲートウェイの OS タイムスタンプに基づくオペレーションの発生時刻。
version	監査ログ形式のバージョン。

オペレーションごとにログに記録される属性

次の表は、S3 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 - SMBのみ)	属性の書き込み (chown)	属性の書き込み (chmod)	属性の書き込み (chgrp)
access			X	X					X	
accoun main (SMBのみ)	X	X	X	X	X	X	X	X	X	X
accoun me (SMBのみ)	X	X	X	X	X	X	X	X	X	X
bucket	X	X	X	X	X	X	X	X	X	X
client (NFSのみ)	X	X	X	X	X	X		X	X	X
client (NFSのみ)	X	X	X	X	X	X		X	X	X
ctime			X	X						
groupI			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 - SMBのみ)	属性の書き込み (chown)	属性の書き込み (chmod)	属性の書き込み (chgrp)
fileSinBytes				X						
gatewa	X	X	X	X	X	X	X	X	X	X
mtime			X	X						
newObjName					X					
objecte	X	X	X	X	X	X	X	X	X	X
objecte	X	X	X	X	X	X	X	X	X	X
operat	X	X	X	X	X	X	X	X	X	X
ownerI			X	X				X		
securiescrip (SMBのみ)							X	X		
shareN	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 - SMBのみ)	属性の書き込み (chown)	属性の書き込み (chmod)	属性の書き込み (chgrp)
source	X	X	X	X	X	X	X	X	X	X
sourceress	X	X	X	X	X	X	X	X	X	X
status	X	X	X	X	X	X	X	X	X	X
timest	X	X	X	X	X	X	X	X	X	X
versio	X	X	X	X	X	X	X	X	X	X

S3 ファイルゲートウェイのキャッシュレポートを作成する

S3 ファイルゲートウェイは、特定のファイル共有のローカルアップロードキャッシュ内にあるファイルのメタデータのレポートを生成できます。フィルターと追加の条件を適用して、レポートに表示されるキャッシュされたファイルの特定のタイプを決定できます。このレポートを使用すると、ゲートウェイの問題を特定し、解決するのに役立ちます。たとえば、ゲートウェイから Amazon S3 へのファイルのアップロードが失敗している場合、アップロードに失敗している特定のファイルとその失敗原因を一覧にしたレポートを作成できます。レポートは、指定したフィルターパラメータのセットと一致するファイルのリストを含む CSV ファイルです。出力ファイルは、レポートを設定する際に指定したバケットの場所に Amazon S3 オブジェクトとして保存されます。 AWS Storage Gateway API を使用してキャッシュレポートを作成するには、Storage Gateway API リファレンスの StartCacheReport を参照してください。Storage Gateway コンソールでキャッシュレポートを作成するには、次の手順を使用します。

前提条件

- ゲートウェイには、キャッシュレポートを保存する Amazon S3 バケットに対する `s3:PutObject` および `s3:AbortMultipartUpload` アクセス許可が必要です。
- ファイル共有に関する他のキャッシュレポートと同時には実行できません。
- ファイル共有の既存のキャッシュレポートは 10 個未満でなければなりません。
- ゲートウェイはオンラインであり、 に接続されている必要があります AWS。
- ゲートウェイルートディスクには、20 GB 以上の空き容量が必要です。

Storage Gateway コンソールを使用してキャッシュレポートを作成するには

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home/) を開きます。
2. ページの左側にあるナビゲーションペインで [ファイル共有] を選択し、キャッシュレポートを作成するファイル共有を選択します。
3. [アクション] ドロップダウンメニューから、[キャッシュレポートの作成] を選択します。
4. Amazon S3 ロケーション には、完了したキャッシュレポートの CSV ファイルオブジェクトを Amazon S3 に保存したい場所の、Amazon S3 バケットとプレフィックスを入力します。既存の Amazon S3 ストレージからバケットとプレフィックスを選択するには、[S3 を参照]を選択します。
5. IAM ロールの場合は、次のいずれかを実行して、キャッシュレポートを生成して保存するためのアクセス許可をファイルゲートウェイに付与する IAM ロールを指定します。
   - 既存の IAM ロールを指定するには、ドロップダウンリストからロールを選択します。
   - 新しい IAM ロールを手動で作成するには、[ロールの作成]を選択し、IAM コンソールを使用して新しいロールを作成します。

> **Note**
>
> 指定する IAM ロールには、レポートバケットの Amazon S3 ロケーションへのオブジェクトの書き込み、およびレポートバケットへのマルチパートアップロードを停止するための次のアクセス許可が必要です。
>
> - `s3:PutObject`
> - `s3:AbortMultipartUpload`

ロールは、`storagegateway.amazonaws.com`サービスが `sts:AssumeRole`アクションを使用してロールを引き受けることも許可する必要があります。

6. レポートフィルターでは、次のいずれかを実行して、キャッシュレポートに含めるファイルを決定します。

   - 現在 Amazon S3 へのアップロードに失敗したすべてのキャッシュ済みファイルを含めるには、アップロードに失敗したすべてのファイルを選択します。
   - 特定の理由で Amazon S3 へのアップロードに失敗したファイルのみを含めるには、特定のアップロード失敗の理由のみを選択します。次に、失敗理由で、以下の理由のいずれか一つ以上を選択します。
     - アクセスできないストレージクラス – ゲートウェイは、オブジェクトが保存されている Amazon S3 ストレージクラスにアクセスできません。詳細については、「エラー: InaccessibleStorageClass」を参照してください。
     - 無効なオブジェクトの状態 – ゲートウェイ上のファイルの状態が Amazon S3 での状態と一致しません。詳細については、「エラー: InvalidObjectState」を参照してください。
     - 見つからないオブジェクト – オブジェクトは Amazon S3 で削除または移動されました。詳細については、「エラー: ObjectMissing」を参照してください。
     - S3 アクセス拒否 – Amazon S3 バケットアクセス IAM ロールでは、ゲートウェイがアップロード操作を実行することを許可していません。詳細については、「エラー: S3AccessDenied」を参照してください。

   > **Note**
   >
   > ファイルのアップロード失敗フラグは、24 時間ごとに、およびゲートウェイの再起動時にリセットされます。リセット後、再びフラグが立てられる前にこのレポートでファイルがキャプチャされた場合、それらのファイルはファイルのアップロード失敗として報告されません。

7. [VPC エンドポイントを使用して S3 に接続する場合] には、次のいずれかを実行して、ゲートウェイが Amazon S3 バケットに接続する方法を指定します。

   - Amazon VPC を使用せずに直接接続するには、[バケットに直接接続]を選択します。

- 既存の Amazon VPC エンドポイントのリストを参照するには、[VPC エンドポイントの選択] を選択し、表示される [VPC エンドポイント] のドロップダウンリストからエンドポイントを指定します。
- DNS 名で既存の Amazon VPC エンドポイントを指定するには、VPC エンドポイント DNS 名の入力を選択し、表示される VPC エンドポイント DNS 名フィールドに DNS 名を入力します。

> **Note**
>
> ファイル共有で VPC エンドポイントを使用して通常のオペレーションで Amazon S3 に接続する場合は、キャッシュレポートを設定するときに同じ VPC を使用することをお勧めします。無効な VPC 設定など、何らかの理由でゲートウェイが Amazon S3 バケットに接続できない場合、キャッシュレポートの作成は失敗します。

8. (オプション) [タグ - オプション] で [新しいタグの追加] を選択し、キーとキャッシュレポートの値を入力します。

   タグは、Storage Gateway リソースの分類に役立つ大文字と小文字を区別するキーと値のペアです。タグを追加すると、キャッシュレポートのフィルタリングと検索が容易になります。この手順を繰り返して、最大 50 個のタグを追加できます。
9. 終了したら、[レポートを作成] を選択します。

   Storage Gateway がレポートの生成を開始します。ファイル共有の詳細ページの [キャッシュレポート] タブで進行状況を確認し、ステータスを表示できます。

S3 ファイルゲートウェイのキャッシュレポートの表示と管理

キャッシュレポートには、指定したフィルターや条件に従って、特定のファイル共有のローカルキャッシュ内にあるファイルが一覧表示されます。特定のファイル共有の既存のキャッシュレポートのリストを表示したり、レポートの進行状況とステータスを確認したり、 AWS Storage Gateway API または Storage Gateway コンソールを使用して不要になったレポートを削除したりできます。

API を使用してキャッシュレポートを管理するには、Storage Gateway API リファレンスの以下のセクションを参照してください:

- ListCacheReports
- DescribeCacheReport

- CancelCacheReport
- DeleteCacheReport

Storage Gateway コンソールでキャッシュレポートを管理するには、次の手順を使用します。

Storage Gateway コンソールを使用してキャッシュレポートを管理するには

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home/) を開きます。
2. ページの左側にあるナビゲーションペインで [ファイル共有] を選択し、キャッシュレポートを管理するファイル共有を選択します。
3. ファイル共有の詳細ページで、キャッシュレポートタブを選択します。このタブには、ファイル共有の既存のキャッシュレポートが一覧表示され、レポートファイルが Amazon S3 に保存されているステータス、進行状況、オブジェクトパスに関する情報が表示されます。
4. 次のいずれかを行います。
   - レポート ARN や関連するタグなど、特定のレポートの追加の詳細を表示するには、レポート ID 列からレポートを選択します。
   - 同時に管理する複数のレポートを指定するには、チェックボックス列を使用してレポートを選択します。
5. 1 つ以上のレポートを管理するには、アクション ドロップダウンメニューから次のいずれかを選択します。
   - キャッシュレポートの削除 — Storage Gateway データベースからキャッシュレポートのレコードを削除します。古いキャッシュレポートのレコードを削除して、新しいレポート用のスペースを確保します。各ファイル共有には、いつでも最大 10 個の既存のキャッシュレポートを含めることができます。

     > **Note**
     >
     > この手順を使用してキャッシュレポートレコードを削除しても、Amazon S3 からレポートファイルオブジェクトは削除されません。

   - レポートのキャンセル — これにより、現在進行中のレポートがキャンセルされます。レポートの設定ミスがあった場合や、レポートの完了に異常に時間がかかっている場合は、進行中のレポートをキャンセルします。プロンプトが表示されたら、キャンセルを確定します。

> **Note**
>
> 完了時間は、キャッシュ内のファイル数によって大きく異なる場合があります。通常、ほとんどのレポートは 5 分以内に完了します。

Storage Gateway コンソールには、キャンセルまたは削除アクションの結果を示すメッセージが表示されます。

S3 ファイルゲートウェイキャッシュレポートで提供される情報について

キャッシュレポートには、指定したフィルターや条件に従って、特定のファイル共有のローカルキャッシュ内にあるファイルが一覧表示されます。各キャッシュレポートには、以下の情報が含まれます。

- バケット — ファイル共有に関連付けられている Amazon S3 バケットまたはアクセスポイント。
- S3ObjectKey — このファイルのデータとメタデータを保存する Amazon S3 オブジェクト。このオブジェクトには、S3 にアップロードされた最新のデータがありますが、S3 へのアップロードに失敗したデータが欠落している可能性があります。
- FilePath — ゲートウェイキャッシュ内のファイルエントリのファイルパス。これは、ファイル共有をマウントして参照する際にファイルを見つけられる場所です。
- RenamedTo — 名前が変更されたファイルの新しいパス。ファイル共有上でファイルの名前を変更すると、ゲートウェイはそのファイルの古い場所と新しい場所の両方を追跡する必要があります。このフィールドには、ファイルが移動された場所が表示され、ファイルが複数回名前変更された場合でも、ファイルの名前変更オペレーションを追跡するのに役立ちます。この情報は、ファイル共有内のファイルが Amazon S3 バケット内のオブジェクトにどのように対応しているかを理解する必要がある場合に特に役立ちます。

  次の例は、ファイルが Amazon S3 で直接上書きされ、ファイルゲートウェイを介して名前が変更される複雑なシナリオのキャッシュレポートエントリを示しています。このシナリオでは、ゲートウェイはファイル `A.txt` を S3 にアップロードした後、ローカルキャッシュの空き容量を確保するためにファイルの内容を削除します。その後、関連付けられた S3 オブジェクトは、ゲートウェイを介さずに直接 S3 上で上書きされます。このため、S3 オブジェクトとゲートウェイが期

待する内容との不一致により、InvalidObjectState が発生します。同時に、ファイル A.txt はゲートウェイを通じてファイル B.txt に名前が変更されました。

バケット	S3Obje ey	FilePat	Renam	タイプ	IsDirt	IsDataI ty	IsDelet	IsFailin ToUplc	Upload or	SizeInE es	IsWholeFi leInCache
sample ket-iad	A.txt	/B.txt		ファイル	TRUE	FALSE	FALSE	TRUE	Invalid(jectSta	4	FALSE
sample ket-iad	A.txt	/A.txt	/B.txt	ファイル	TRUE	FALSE	TRUE	FALSE		4	FALSE

- タイプ — エントリが FILE か DIRECTORY のどちら用であるかを示します。
- IsDirty — Amazon S3 にまだアップロードされていないファイルの変更がある場合は、TRUE を報告します。これには、ファイルのデータが変更されていない場合でも、ファイル名や読み取り/書き込みアクセス許可などのメタデータへの変更が含まれます。
- IsDataDirty — ファイルのデータに変更があり、まだ Amazon S3 にアップロードされていない場合は、TRUE を報告します。
- IsDeleted — ファイルがゲートウェイ上で削除されている場合は、TRUE を報告します。ファイルが削除済みとしてマークされている場合、常にダーティとしてマークされます。
- IsFailingToUpload — ファイルの Amazon S3 へのアップロードに問題がある場合は、TRUE を報告します。このステータスは 24 時間ごとにリセットされ、ゲートウェイがアップロードを再試行し、問題が解決されたかどうかを確認できます。ゲートウェイは、アップロードに失敗したファイルの新しい書き込みオペレーションを拒否します。ゲートウェイがファイル全体をキャッシュに保持していない場合、読み取りオペレーションも拒否されます。
- UploadError — ファイルの Amazon S3 へのアップロードを妨げているエラー。これらのエラーを解決するための詳細と推奨される手順については、「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。
- SizeInBytes — ファイルの合計サイズ。
- IsWholeFileInCache — ファイルの全データが現在ゲートウェイキャッシュに格納されている場合は、TRUE を報告します。この値が Amazon S3 へのアップロードに失敗しているファイルで TRUE の場合、ゲートウェイはそのファイルの読み取りを許可します。

ゲートウェイの維持

Amazon S3 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 S3 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 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 – 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、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、ゲートウェイアプライアンスソフトウェアのリリースノート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から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から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して、ルーティングテーブルの保存、 への接続などのメンテナンスタスクを実行できます 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。
ip6tables	IPv6 パケットフィルタリングと NAT 用の管理ツール。
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。

コマンド	関数
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。
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
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。

メッセージ	説明
[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。
[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。
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。

コマンド	関数
iptables	IPv4 パケットフィルタリングおよび NAT の管理ツール。
ip6tables	IPv6 パケットフィルタリングと NAT 用の管理ツール。
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。
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 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

> **Note**
>
> Storage Gateway AL2 から AL2023 への移行を実行する場合は、開始する前に、Storage Gateway AL2 から AL2023 への移行キャンペーンの移行前チェックリストのすべての項目を完了していることを確認してください。

既存の S3 File GatewayFSx 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。

既存の S3 ファイルゲートウェイを置き換えるには、2 つの方法があります。次の表に、各メソッドの利点と欠点を示します。この情報を使用して、ゲートウェイ環境に最適な方法を選択し、以下の対応するセクションの手順ステップを参照してください。

> **Note**
>
> いずれかの方法を完了するために新しい Storage Gateway ローカルコンソールにサインインする必要がある場合、最初のユーザー名は admin、一時パスワードは password です。

> **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。

	メソッド 1: キャッシュディスクとゲートウェイ ID を代替インスタンスに移行する*	メソッド 2: 空のキャッシュディスクと新しいゲートウェイ ID を持つ代替インスタンス
キャッシュディスクデータ	キャッシュディスク上のデータは保持されます。この方法は、ゲートウェイに大きなキャッシュディスクがある場合や、アプリケーションがキャッシュ外読み取り操作による遅延に影響を受けやすい場合に有効です。	キャッシュ内のデータは AWS クラウドからダウンロードされます。この方法は、書き込み負荷が高いワークロードに最適であり、アプリケーションがキャッシュ外読み取りによる遅延を許容できる場合に適しています。
ダウンタイム	移行プロセス中、ゲートウェイは 1〜2 時間オフラインになります。	ファイル共有は常に利用できますが、クライアントは新しいインスタンスへの移行中にあるファイル共有から別のファイル共有に切り替えると、カットオーバーのダウンタイムが短くなります。 **Note** 2 つのファイル共有から 1 つの Amazon S3 バケットへの同時書き込みはサポートされていないため、すべてのクライアントは徐々にではなく、1 つの共有から別の共有に同時に再マッピングする必要があります。

	メソッド 1: キャッシュディスクとゲートウェイ ID を代替インスタンスに移行する*	メソッド 2: 空のキャッシュディスクと新しいゲートウェイ ID を持つ代替インスタンス
ゲートウェイ ID	新しいゲートウェイは、置き換えるゲートウェイからゲートウェイ ID を継承します。	既存のゲートウェイと置き換え用ゲートウェイは、それぞれ異なる一意のゲートウェイ ID を持っています。
コストの含意	キャッシュされたデータを保存すると、再ダウンロードが不要になり、S3 の追加コストは発生しません。	この方法では、特に S3 からデータを取得する必要がある場合、追加料金が発生することがあります。このアプローチでは、S3 バケットによってバックアップされたファイル共有が S3 Intelligent-Tiering、S3 Standard-IA、S3 One Zone-IA、または S3 ライフサイクルポリシーを介して GLACIER に移行されたオブジェクトなどのストレージクラスを使用している場合、S3 データの取得にかなりのコストが発生する可能性があります。 SMB ファイル共有の場合、ルート ACL がファイル共有に設定されている場合は、移行されたゲートウェイに再適用する必要があります。このアクションは、ファイル共有内のすべてのオブジェクトに再帰的に設定を適用し、コストへの影響をもたらします。

> **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。

メソッド 1: キャッシュディスクとゲートウェイ ID を代替インスタンスに移行する

S3 ファイルゲートウェイのキャッシュディスクとゲートウェイ ID を代替インスタンスに移行するには:

1. 既存の S3 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。
2. ゲートウェイを最新バージョンに更新するには、次の手順を使用します。
   a. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
   b. ナビゲーションペインで、ゲートウェイを選択し、移行する古い S3 ファイルゲートウェイを選択します。
   c. 利用可能な場合は、今すぐ更新を選択します。そうでない場合、ゲートウェイは既に最新バージョンです。
3. 既存の S3 ファイルゲートウェイの [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。
4. ハイパーバイザーコントロールを使用してホスト仮想マシン (VM) をオフにして、既存の S3 ファイルゲートウェイをシャットダウンします。

   Amazon EC2 インスタンスのシャットダウンの詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスの停止と起動」を参照してください。

   KVM、VMware、または Hyper-V VM のシャットダウンの詳細については、ハイパーバイザからのドキュメントを参照してください。
5. 古いゲートウェイ VM から、ルートディスクおよびキャッシュディスクを含むすべてのディスクを取り外します。

> **Note**
>
> ルートディスクのボリューム ID と、そのルートディスクに関連付けられているゲートウェイ ID を書き留めます。このディスクは、後のステップで新しい Storage Gateway ハイパーバイザーからデタッチする必要があります。

S3 ファイルゲートウェイの VM として Amazon EC2 インスタンスを使用している場合は、Amazon EC2 ユーザーガイドのWindows インスタンスから Amazon EBS ボリュームをデタッチするまたはLinux インスタンスから Amazon EBS ボリュームをデタッチするを参照してください。

KVM、VMware、または Hyper-V VM からのディスクのデタッチについては、ハイパーバイザーからのドキュメントを参照してください。

6. 新しい S3 File Gateway ハイパーバイザー VM インスタンスを作成しますが、ゲートウェイとしてアクティブ化しないでください。後のステップで、この新しい VM は、古いゲートウェイの ID を引き継ぎます。

   新しい Storage Gateway ハイパーバイザー VM の作成に関する詳細については、「ホストプラットフォームの選択と VM のダウンロード」を参照してください。

   > **Important**
   >
   > 新しい VM に S3 File Gateway イメージを使用します。別のゲートウェイタイプ (ボリュームゲートウェイやテープゲートウェイなど) のイメージでは、移行されたゲートウェイの起動が失敗します。

   > **Note**
   >
   > 新しい VM には、キャッシュ用のディスクを追加しないでください。この VM は、旧 VM で使用していたキャッシュディスクをそのまま使用します。

> **Note**
>
> VM をダウンロードしたら、コンソールウィザードを閉じます。この時点ではアクティベーションを続行しないでください。

7. 古い VM と同じネットワーク設定を使用するように新しい Storage Gateway VM を設定します。

   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。

   ゲートウェイ VM の静的 IP アドレスを手動で設定する必要がある場合は、「ネットワークパラメータの設定」を参照してください。

   ゲートウェイ VM が Socket Secure version 5 (SOCKS5) プロキシを使用してインターネットに接続する必要がある場合は、「HTTP プロキシを介して EC2 にデプロイされたゲートウェイをルーティングする」を参照してください。

   > **Note**
   >
   > NFS または SMB クライアントを再設定しないように、古いゲートウェイ VM から同じ静的 IP アドレスまたはホスト名を再利用できます。

8. 新しい Storage Gateway VM を起動します。
9. 古いゲートウェイ VM からデタッチしたすべてのディスクを新しいゲートウェイ VM にアタッチします。これには、古いゲートウェイのルートディスクとキャッシュディスク (複数可) が含まれます。新しいゲートウェイ VM の独自のルートディスクをデタッチしないでください。

   > **Note**
   >
   > 正常に移行するには、すべてのディスクを変更しないでください。ディスクサイズやその他の値を変更すると、メタデータに不整合が発生し、移行が成功しなくなります。

10. ゲートウェイ移行プロセスを開始するには、新しいゲートウェイ VM のローカルコンソールに接続するか、新しいゲートウェイ VM の IP アドレス (以下で説明) にウェブリクエストを行います。

a. ローカルコンソールを使用するには、Migrate Gateway の オプションを選択し、プロンプトが表示されたら既存のゲートウェイ ID を指定します。古いゲートウェイで以前に適用された設定を新しいゲートウェイにコピーするプロンプトが表示されます。適用するか、後で手動で設定するかを選択できます。「ゲートウェイローカルコンソールへのアクセス」を参照してください。

b. または、次の形式を使用する URL を使用して新しい VM に接続することで、ゲートウェイ移行プロセスを開始することもできます。

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

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

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

ブラウザから、またはコマンドラインから `curl` を使用して、この URL で移行プロセスを開始します。

ゲートウェイの移行プロセスが正常に完了すると、移行が正常に完了したことを確認するメッセージが表示されます。

11. ゲートウェイのステータスが AWS Storage Gateway コンソールで実行中と表示されるまで待ちます。使用可能な帯域幅によっては、最大 10 分かかる場合があります。
12. 新しい Storage Gateway VM を停止します。
13. 以前に書き留めたボリューム ID を持つ古いゲートウェイのルートディスクを新しいゲートウェイからデタッチします。
14. 新しい Storage Gateway VM を起動します。
15. ゲートウェイが Active Directory ドメインに参加している場合は、ドメインに再度参加します。手順については、Active Directory を使用してユーザーを認証するを参照してください。

> **Note**
>
> S3 ファイルゲートウェイのステータスが [参加] と表示されている場合でも、このステップを完了する必要があります。

16. ゲートウェイが SMB ゲストアクセス認証方法を使用している場合は、パスワードを再入力する必要があります。手順については、「ファイル共有へのゲストアクセスを提供する」を参照してください。
17. 共有が新しいゲートウェイ VM の IP アドレスで使用可能であることを確認し、古いゲートウェイ VM を削除します。

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

EC2 インスタンスの削除の詳細については、Amazon EC2 ユーザーガイドのインスタンスの終了を参照してください。KVM、VMware、または Hyper-V VM を削除する方法の詳細については、使用しているハイパーバイザーのドキュメントを参照してください。

メソッド 2: 空のキャッシュディスクと新しいゲートウェイ ID を持つ代替インスタンス

空のキャッシュディスクと新しいゲートウェイ ID を持つ代替 S3 ファイルゲートウェイインスタンスを設定するには:

1. 既存の S3 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共有を設定する前に、[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ます。
2. AWS Command Line Interface (AWS CLI) を使用して、既存の S3 File GatewayFSxとファイル共有に関する設定情報を収集して保存します。

   a. S3 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. S3 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、ドメイン名、Microsoft Active Directory のステータス、ゲストパスワードが設定されているかどうか、セキュリティ戦略のタイプなど、SMB ファイル共有に関するメタデータを含む JSON ブロックを出力します。

c. S3 ファイルゲートウェイの各 SMB およびネットワークファイルシステム (NFS) ファイル共有のファイル共有情報を保存します。

- SMB ファイル共有には、次のコマンドを使用します。

```
aws storagegateway describe-smb-file-shares --file-share-arn-list
 "arn:aws:storagegateway:us-east-2:123456789012:share/share-987A654B"
```

このコマンドは、名前、ストレージクラス、ステータス、IAM ロール Amazon リソースネーム (ARN)、S3 ファイルゲートウェイ 、SMB ファイル共有に関するメタデータを含む JSON ブロックを出力します。

- NFS ファイル共有には、次のコマンドを使用します。

```
aws storagegateway  describe-nfs-file-shares --file-share-arn-list
 "arn:aws:storagegateway:us-east-2:123456789012:share/share-321A978B"
```

このコマンドは、名前、ストレージクラス、ステータス、IAM ロール ARN、S3 ファイルゲートウェイ へのアクセスが許可されているクライアントのリスト、NFS クライアントがマウントポイントを識別するために使用するパスなど、NFS ファイル共有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 S3 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共有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共有を作成します。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。

> **Note**
>
> ゲートウェイ間でファイル共有設定をコピーできるようになりました。詳細については、「ファイル共有のコピー」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、古いファイル共有から新しいファイル共有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**
>
> S3 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、ファイル共有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。ファイル共有に関連付けられた Amazon S3 バケット内のデータが不要な場合は、Amazon S3 バケットを削除することもできます。手順については、「バケットの削除」を参照してください。

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

S3 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、S3 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。
> Amazon EC2 インスタンスでは、S3 バケット内のオブジェクトが 500 万個を超え、汎用 SSD ボリュームを使用している場合、起動中のゲートウェイで許容できるパフォーマンスを得るには、最小 350 GiB のルート EBS ボリュームが必要です。ボリュームサイズを引き上げる方法については、「Elastic Volumes を使用して EBS ボリュームを変更する (コンソール)」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共有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共有からの読み取りです。キャッシュミス読み取りオペレーションは、Amazon S3 から提供されるファイル共有からの読み取りです。

次の表は、S3 ファイルゲートウェイの構成の例を示しています。

Linux クライアントでの S3 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: 512 GiB キャッシュ、io1、1,500 個のプロビジョンド IOPS 最小ネットワークパフォーマンス: 10 Gbps CPU: 16 vCPU | RAM: 32 GB Linux には NFS プロトコルを推奨	NFSv3 - 1 スレッド	110 MiB/秒 (0.92 Gbps)	590 MiB/秒 (4.9 Gbps)	310 MiB/秒 (2.6 Gbps)
	NFSv3 - 8 スレッド	160 MiB/秒 (1.3 Gbps)	590 MiB/秒 (4.9 Gbps)	335 MiB/秒 (2.8 Gbps)
	NFSv4 - 1 スレッド	130 MiB/秒 (1.1 Gbps)	590 MiB/秒 (4.9 Gbps)	295 MiB/秒 (2.5 Gbps)
	NFSv4 - 8 スレッド	160 MiB/秒 (1.3 Gbps)	590 MiB/秒 (4.9 Gbps)	335 MiB/秒 (2.8 Gbps)
	SMBv3 - 1 スレッド	115 MiB/秒 (1.0 Gbps)	325 MiB/秒 (2.7 Gbps)	255 MiB/秒 (2.1 Gbps)
	SMBv3 - 8 スレッド	190 MiB/秒 (1.6 Gbps)	590 MiB/秒 (4.9 Gbps)	335 MiB/秒 (2.8 Gbps)
Storage Gateway ハードウェアアプライアンス	NFSv3 - 1 スレッド	265 MiB/秒 (2.2 Gbps)	590 MiB/秒 (4.9 Gbps)	310 MiB/秒 (2.6 Gbps)

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
最小ネットワークパフォーマンス: 10 Gbps	NFSv3 - 8 スレッド	385 MiB/秒 (3.1 Gbps)	590 MiB/秒 (4.9 Gbps)	335 MiB/秒 (2.8 Gbps)
	NFSv4 - 1 スレッド	310 MiB/秒 (2.6 Gbps)	590 MiB/秒 (4.9 Gbps)	295 MiB/秒 (2.5 Gbps)
	NFSv4 - 8 スレッド	385 MiB/秒 (3.1 Gbps)	590 MiB/秒 (4.9 Gbps)	335 MiB/秒 (2.8 Gbps)
	SMBv3 - 1 スレッド	275 MiB/秒 (2.4 Gbps)	325 MiB/秒 (2.7 Gbps)	255 MiB/秒 (2.1 Gbps)
	SMBv3 - 8 スレッド	455 MiB/秒 (3.8 Gbps)	590 MiB/秒 (4.9 Gbps)	335 MiB/秒 (2.8 Gbps)
ルートディスク: 80 GB、io1 SSD、4,000 IOPS キャッシュディスク: 4 x 2 TB NVME キャッシュディスク 最小ネットワークパフォーマンス: 10 Gbps CPU: 32 vCPU | RAM: 244 GB Linux には NFS プロトコルを推奨	NFSv3 - 1 スレッド	300 MiB/秒 (2.5 Gbps)	590 MiB/秒 (4.9 Gbps)	325 MiB/秒 (2.7 Gbps)
	NFSv3 - 8 スレッド	585 MiB/秒 (4.9 Gbps)	590 MiB/秒 (4.9 Gbps)	580 MiB/秒 (4.8 Gbps)
	NFSv4 - 1 スレッド	355 MiB/秒 (3.0 Gbps)	590 MiB/秒 (4.9 Gbps)	340 MiB/秒 (2.9 Gbps)
	NFSv4 - 8 スレッド	575 MiB/秒 (4.8 Gbps)	590 MiB/秒 (4.9 Gbps)	575 MiB/秒 (4.8 Gbps)
	SMBv3 - 1 スレッド	230 MiB/秒 (1.9 Gbps)	325 MiB/秒 (2.7 Gbps)	245 MiB/秒 (2.0 Gbps)
	SMBv3 - 8 スレッド	585 MiB/秒 (4.9 Gbps)	590 MiB/秒 (4.9 Gbps)	580 MiB/秒 (4.8 Gbps)

Windows クライアントでの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: 512 GiB キャッシュ、io1、1,500 個のプロビジョンド IOPS 最小ネットワークパフォーマンス: 10 Gbps CPU: 16 vCPU | RAM: 32 GB Windows には SMB プロトコルを推奨	SMBv3 - 1 スレッド	150 MiB/秒 (1.3 Gbps)	180 MiB/秒 (1.5 Gbps)	20 MiB/秒 (0.2 Gbps)
	SMBv3 - 8 スレッド	190 MiB/秒 (1.6 Gbps)	335 MiB/秒 (2.8 Gbps)	195 MiB/秒 (1.6 Gbps)
	NFSv3 - 1 スレッド	95 MiB/秒 (0.8 Gbps)	130 MiB/秒 (1.1 Gbps)	20 MiB/秒 (0.2 Gbps)
	NFSv3 - 8 スレッド	190 MiB/秒 (1.6 Gbps)	330 MiB/秒 (2.8 Gbps)	190 MiB/秒 (1.6 Gbps)
Storage Gateway ハードウェアアプライアンス 最小ネットワークパフォーマンス: 10 Gbps	SMBv3 - 1 スレッド	230 MiB/秒 (1.9 Gbps)	255 MiB/秒 (2.1 Gbps)	20 MiB/秒 (0.2 Gbps)
	SMBv3 - 8 スレッド	835 MiB/秒 (7.0 Gbps)	475 MiB/秒 (4.0 Gbps)	195 MiB/秒 (1.6 Gbps)
	NFSv3 - 1 スレッド	135 MiB/秒 (1.1 Gbps)	185 MiB/秒 (1.6 Gbps)	20 MiB/秒 (0.2 Gbps)
	NFSv3 - 8 スレッド	545 MiB/秒 (4.6 Gbps)	470 MiB/秒 (4.0 Gbps)	190 MiB/秒 (1.6 Gbps)

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: 4 x 2 TB NVME キャッシュディスク 最小ネットワークパフォーマンス: 10 Gbps CPU: 32 vCPU | RAM: 244 GB Windows には SMB プロトコルを推奨	SMBv3 - 1 スレッド	230 MiB/秒 (1.9 Gbps)	265 MiB/秒 (2.2 Gbps)	30 MiB/秒 (0.3 Gbps)
	SMBv3 - 8 スレッド	835 MiB/秒 (7.0 Gbps)	780 MiB/秒 (6.5 Gbps)	250 MiB/秒 (2.1 Gbps)
	NFSv3 - 1 スレッド	135 MiB/秒 (1.1 Gbps)	220 MiB/秒 (1.8 Gbps)	30 MiB/秒 (0.3 Gbps)
	NFSv3 - 8 スレッド	545 MiB/秒 (4.6 Gbps)	570 MiB/秒 (4.8 Gbps)	240 MiB/秒 (2.0 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。

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

Amazon S3 ファイルゲートウェイでは、1 つの Storage Gateway アプライアンスに最大 50 個のファイル共有をアタッチできます。ゲートウェイごとに複数のファイル共有を追加することで、管

理するゲートウェイと仮想ハードウェアリソースを減らしても、ユーザーとワークロードの増大に対応できます。他の要因に加え、ゲートウェイで管理するファイル共有数が、ゲートウェイのパフォーマンスに影響を及ぼすことがあります。このセクションでは、アタッチされたファイル共有数に応じた、予想できるゲートウェイのパフォーマンスの変化について説明します。また、複数の共有を管理するゲートウェイのパフォーマンスを最適化するために推奨される仮想ハードウェアの構成を示します。

一般的に、単一の Storage Gateway が管理するファイル共有数を増やすと、次の結果が生じることがあります。

- ゲートウェイの再起動により多くの時間がかかる。
- vCPU や RAM などの仮想ハードウェアリソースの使用率が増える。
- 仮想ハードウェアリソースが飽和状態になると、データおよびメタデータオペレーションのパフォーマンスが低下する。

次の表に、複数のファイル共有を管理するゲートウェイに推奨される仮想ハードウェア設定を示します。

ゲートウェイあたりのファイル共有数	推奨されるゲートウェイ容量の設定	推奨される vCPU コア	推奨 RAM	推奨ルートディスクサイズ			
1 ~ 10	小	4 (EC2 インスタンスタイプ m4.xlarge 以上)	16 GiB	80 GiB			
10 ~ 20	中	8 (EC2 インスタンスタイプ m4.2xlarge 以上)	32 GiB	160 GiB			

ゲートウェイあたりのファイル共有数	推奨されるゲートウェイ容量の設定	推奨される vCPU コア	推奨 RAM	推奨ルートディスクサイズ			
20 以上	大	16 (EC2 インスタンスタイプ m4.4xlarge 以上)	64 GiB	240 GiB			

上記の推奨される仮想ハードウェア構成に加えて、複数のファイル共有を管理する Storage Gateway アプライアンスを設定および保守するための以下のベストプラクティスを推奨します。

- ファイル共有数とゲートウェイの仮想ハードウェアにかかる負荷との関係は必ずしも直線的ではないことに注意してください。一部のファイル共有は、他のファイル共有よりもスループットが高くなり、そのため他よりもハードウェアの負荷が高くなる可能性もあります。前の表の推奨事項は、最大ハードウェア容量とさまざまなファイル共有スループットレベルに基づいています。
- 1 つのゲートウェイに複数のファイル共有を追加するとパフォーマンスが低下する場合は、最もアクティブなファイル共有を他のゲートウェイに移動することを検討してください。特に、非常に高いスループットを必要とするアプリケーションでファイル共有を使用する場合は、そのファイル共有専用に別のゲートウェイを作成することを検討してください。
- 複数の高スループットアプリケーション用に 1 つのゲートウェイを設定したり、複数の低スループットアプリケーションを別のゲートウェイに設定する構成は推奨されません。別の方法として、ハードウェアの過負荷を防ぐため、高スループットと低スループットのファイル共有を複数のゲートウェイに均等に分散させることを検討してください。ファイル共有のスループットを測定するには、`ReadBytes` および `WriteBytes` メトリクスを使用します。詳細については、「計測スループットについて」を参照してください。

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 お客様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。
- クラウド内のセキュリティ – 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、「Data Privacy FAQChina」を参照してください。 欧州におけるデータ保護に関する情報については、General Data Protection Regulation (GDPR) Center 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、その中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 を操作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

Storage Gateway は、SSL/TLS (Secure Socket Layers/Transport Layer Security) を使用して、ゲートウェイアプライアンスと AWS ストレージ間で転送されるデータを暗号化します。デフォルトでは、Storage Gateway は Amazon S3 で管理される暗号化キー (SSE-S3) を使用して、Amazon S3 に格納されているすべてのデータをサーバー側で暗号化します。Storage Gateway API を使用して、AWS Key Management Service (SSE-KMS) キーを使用したサーバー側の暗号化で、クラウド内に保存されたデータを暗号化するようにゲートウェイを設定することもできます。

ファイル共有の暗号化

SSE-KMS または DSSE-KMS を使用して、保存されたオブジェクトを AWS KMSマネージドキーで暗号化するように S3 ファイルゲートウェイ上のファイル共有を設定できます。サポートされているファイル共有暗号化方法の詳細については、「Amazon S3 のファイルゲートウェイによって保存されているオブジェクトの暗号化」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 S3 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
- Windows ACL を使用して SMB ファイル共有へのアクセスを制限する

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

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。、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、まず、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 root 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 にアクセスすることを人間 AWS のユーザーに要求する」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たときに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最大数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

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 AWS 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AWS Storage Gatewayで定義されるアクション」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制御 (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制御 (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スイッチロールの使用時に自動的に作成されます。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 AWS 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 – 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

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"
            }
         }
      }
   ]
}
```

Windows ACL を使用して SMB ファイル共有へのアクセスを制限する

Amazon S3 ファイルゲートウェイは、SMB ファイル共有を介して保存されるファイルとディレクトリへのアクセスを制御するために、POSIX アクセス許可または Windows ACL という 2 つの異なる方法をサポートしています。

このセクションでは、認証に Microsoft Active Directory (AD) を使用する SMB ファイル共有におけるMicrosoft Windows アクセスコントロールリスト (ACL) の使用方法について説明します。Windows ACL を使用することで、SMB ファイル共有内のファイルとフォルダにおける詳細なアクセス権限を設定することができます。

SMB ファイル共有における Windows ACL の主要な特徴を以下に示します。

- Windows ACL は、ファイルゲートウェイが Active Directory ドメインに参加している場合、SMB ファイル共有に対してデフォルトで選択されます。
- ACL が有効である場合、ACL の情報は Amazon S3 のオブジェクトメタデータに保持されます。
- ゲートウェイは、ファイルまたはフォルダごとに最大で 10 個までの ACL を保持します。
- ゲートウェイの外部で作成された S3 オブジェクトにアクセスする際、 ACL が有効化された SMB ファイル共有を使用すると、これらオブジェクトは親フォルダからの ACL 情報を継承します。

> **Note**
>
> SMB ファイル共有のデフォルトのルート ACLはすべてのユーザーにフルアクセスを提供しますが、ルート ACL でこのアクセス権限を変更することもできます。ファイル共有のアクセスを制御するには、ルート ACL を使用します。ファイル共有をマウント (ドライブのマッピング) できるユーザーを設定し、ファイル共有で再帰的にファイルとフォルダに対してユーザーが取得する権限の内容を設定できます。ただし、ACL が維持されるように、このアクセス許可を S3 バケットの上位レベルフォルダに設定することをお勧めします。

CreateSMBFileShare API オペレーションを使用して新規の SMB ファイル共有を作成するときに、Windows ACL を有効にできます。または、UpdateSMBFileShare API オペレーションを使用して、既存の SMB ファイル共有で Windows ACL を有効にします。

新規の SMB ファイル共有で Windows ACL を有効にする

新規の SMB ファイル共有で Windows ACL を有効化にするには、次の手順を実行してください。

新規の SMB ファイル共有を作成時に、Windows ACL を有効化するには

1. ファイルゲートウェイを作成します (まだ作成していない場合)。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。
2. ゲートウェイがドメインに結合していない場合は、これをドメインに追加します。詳細については、「Active Directory を使用してユーザーを認証する」を参照してください。
3. SMB ファイル共有を作成します。詳細については、以下を参照してください。
4. Storage Gateway コンソールからファイル共有で Windows ACL を有効化します。

   Storage Gateway コンソールを使用するには、次の操作を行います。

   a. ファイル共有を選択し、ファイル共有の編集 を選択します。
   b. ファイル/ディレクトリのアクセスコントロール オプションで、[Windows アクセスコントロールリスト] を選択します。
5. (オプション) 管理者ユーザーにファイル共有内のすべてのファイルで ACL を更新する権限があるようにするには、管理者ユーザーを AdminUsersList に追加します。

   > **Note**
   >
   > SMB ファイル共有の設定で [許可および拒否されたユーザーとグループ] のリストを設定した場合、ACL はこれらのリストを上書きしてアクセスを許可することはありません。
   > [Allowed and Denied Users and Groups (許可および拒否されたユーザーとグループ)] のリストは ACL の前に評価され、ファイル共有をマウントまたはアクセスできるユーザーを制御します。ユーザーまたはグループが Allowed (許可された) リストに配置されている場合、リストはアクティブと見なされ、それらのユーザーのみがファイル共有をマウントできます。
   > ユーザーがファイル共有をマウントすると、ACL は、ユーザーがアクセスできる特定のファイルまたはフォルダを制御する、より詳細な保護を提供します。
6. ルートフォルダの親フォルダで ACL を更新します。これを行うには、Windows ファイルエクスプローラーを使用して、SMB ファイル共有内のフォルダの ACL を設定します。

   > **Note**
   >
   > ルートの親フォルダではなく、ルートで ACL を設定した場合、ACL のアクセス許可は Amazon S3 では保持されません。

ファイル共有のルートで ACL を直接設定するのではなく、ファイル共有のルートの最上位フォルダで ACL を設定することが推奨されます。このアプローチによって、Amazon S3 で情報がオブジェクトメタデータとして保持されます。

7. 必要に応じて継承を有効にします。

> **Note**
>
> 2019 年 5 月 8 日以降に作成されたファイル共有で継承を有効にできます。

継承を有効にしてアクセス許可を再帰的に更新すると、Storage Gateway では S3 バケット内のすべてのオブジェクトが更新されます。バケット内のオブジェクトの数によっては、更新の完了に時間がかかる場合があります。

既存の SMB ファイル共有で Windows ACL を有効にする

POSIX アクセス権限が設定されている既存の SMB ファイル共有で Windows ACL を有効にするには、次の手順を実行してください。

Storage Gateway コンソールを使用して既存の SMB ファイル共有で Windows ACL を有効化するには

1. ファイル共有を選択し、ファイル共有の編集 を選択します。
2. ファイル/ディレクトリのアクセスコントロール オプションで、[Windows アクセスコントロールリスト] を選択します。
3. 必要に応じて継承を有効にします。

> **Note**
>
> ルートレベルで ACL を設定してゲートウェイを削除すると、ACL を再度リセットする必要があるため、これは推奨されません。

継承を有効にしてアクセス許可を再帰的に更新すると、Storage Gateway では S3 バケット内のすべてのオブジェクトが更新されます。バケット内のオブジェクトの数によっては、更新の完了に時間がかかる場合があります。

Windows ACL を使用する場合の制限事項

Windows ACL を使用して SMB ファイル共有へのアクセスを制限するときに、次の制限に留意してください。

- Windows ACL は、Windows SMB クライアントを使用してファイル共有にアクセスする場合に、認証に Active Directory を使用しているファイル共有でのみサポートされています。
- ファイルゲートウェイでは、ファイルとディレクトリごとに最大で 10 個の ACL エントリがサポートされています。
- ファイルゲートウェイは、システムアクセスコントロールリスト (SACL) エントリである `Audit` および `Alarm` エントリをサポートしていません。 ファイルゲートウェイは、任意アクセスコントロールリスト (DACL) エントリである `Allow` および `Deny` エントリをサポートしています。
- ファイルゲートウェイは、アドバンストアクセスコントロールエントリ (ACE) アクセス許可をサポートしていません。
- SMB ファイル共有のルート ACL 設定はゲートウェイのみであり、この設定はケートウェイの更新と再起動後にも維持されます。

> **Note**
>
> ルートの親フォルダではなくルートで ACL を設定した場合、ACL のアクセス許可は Amazon S3 では保持されません。

以上の条件を踏まえて、次を必ず実行します。

- 同じ Amazon S3 バケットにアクセスする複数のゲートウェイを設定する場合は、各ゲートウェイ上でそのルート ACL を設定して、アクセス許可の整合性を維持します。
- ファイル共有を削除して、同じ Amazon S3 バケット上で再作成する場合、一連の同じルート ACL を使用するようにしてください。

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 AWS Storage Gateway コンソール。

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 アカウント内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ログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集されたイベントデータを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、ファイル共有、高可用性、データ復旧、セキュリティ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: ファイル共有に関する問題 - ファイル共有で想定外の問題が発生した場合に行うアクションについて説明します。
- 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。

トラブルシューティング: セキュリティスキャンで NFS ポートの開放が検出される

特定の NFS ポートは、SMB ファイル共有でのみ使用するゲートウェイでも、デフォルトで有効になっています。Qualys などのサードパーティのセキュリティソフトウェアを使用してファイルゲートウェイがデプロイされているネットワークをスキャンする場合、スキャン結果はこれらの NFS ポートの開放を潜在的なセキュリティ脆弱性として報告することがあります。SMB ファイル共有でのみゲートウェイを使用し、セキュリティ上の理由から未使用の NFS ポートを無効にする場合は、次の手順を行います。

ファイルゲートウェイで NFS ポートを無効にするには:

1. ローカルコンソールでの Storage Gateway コマンドの実行 で説明されている手順を使用して、ゲートウェイローカルコンソールのコマンドプロンプトにアクセスします。
2. NFS トラフィックを無効にするには、次のコマンドを入力します。

   IPv4

   ```
   iptables -I INPUT -p udp -m udp --dport 111 -j DROP
   iptables -I INPUT -p udp -m udp --dport 2049 -j DROP
   iptables -I INPUT -p udp -m udp --dport 20048 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 111 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 2049 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 20048 -j DROP
   ```

IPv6

```
ip6tables -I INPUT -p udp -m udp --dport 111 -j DROP
ip6tables -I INPUT -p udp -m udp --dport 2049 -j DROP
ip6tables -I INPUT -p udp -m udp --dport 20048 -j DROP
ip6tables -I INPUT -p tcp -m tcp --dport 111 -j DROP
ip6tables -I INPUT -p tcp -m tcp --dport 2049 -j DROP
ip6tables -I INPUT -p tcp -m tcp --dport 20048 -j DROP
```

3. 次のコマンドを入力して、ブロックされた NFS ポートが IP テーブルに表示されることを確認します。

   IPv4

   ```
   iptables -n -L -v --line-numbers
   ```

   IPv6

   ```
   ip6tables -n -L -v --line-numbers
   ```

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。」	このエラーは、次の原因で発生することがあります。 • 解凍され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	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
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)」	
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。

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。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。
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。

問題	実行するアクション
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。
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、「S3 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。

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。

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

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 ゲートウェイのトラブルシューティングを支援 サポート 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連絡して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: 1344 (0x00000540)

Amazon S3 へのファイルの移行中に、10 を超えたアクセスコントロールエントリ (ACEs) を持つファイルを Amazon S3 にコピーしようとすると、ERROR 1344 (0x00000540) が発生することがあります。アクセスコントロールエントリは、アクセスコントロールリスト (ACL) に記載されています。

Amazon S3 ファイルゲートウェイは、特定のファイルまたはフォルダごとに 10 個の ACE エントリのみを保持できます。

エラー 1344 を解決するには: NTFS セキュリティを送信先ディレクトリにコピーします。

10 を超えるエントリのあるファイルまたはフォルダの Windows アクセス許可のエントリの数を減らします。一般的な方法は、エントリの完全なリストを備えたグループを作成し、エントリのリストをその単一のグループに置き換えることです。エントリ数が 10 未満になったら、ファイルまたはフォルダのゲートウェイへのコピーを再試行できます。

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: InaccessibleStorageClass

オブジェクトを Amazon S3 Standardのストレージクラスから出した場合、`InaccessibleStorageClass` エラーが発生する場合があります。

通常、このエラーは、ファイルゲートウェイが 指定されたオブジェクトを Amazon S3 バケットにアップロードしようとした場合か、またはそこからオブジェクトを読み取ろうとした場合に発生します。このエラーでは、通常、オブジェクトは Amazon Glacier に移動され、S3 Glacier Flexible Retrieval あるいは S3 Glacier Deep Archive ストレージクラスのいずれかにあります。

S3 ファイルゲートウェイは、このエラーが原因で現在 Amazon S3 へのアップロードに失敗しているゲートウェイキャッシュ内のすべてのファイルを一覧表示するキャッシュレポートを生成できます。このレポートの情報は、 サポート を使用してゲートウェイ、Amazon S3、または IAM 設定の問題を解決するのに役立ちます。詳細については、「キャッシュレポートの作成」を参照してください。

InaccessibleStorageClass エラーを解決するには

- S3 Glacier Flexible Retrieval あるいは S3 Glacier Deep Archive ストレージクラスから、オブジェクトを S3 の元のストレージクラスに復元します。

  アップロードエラーを修正するためにオブジェクトを S3 バケットに復元すると、ファイルは最終的にアップロードされます。読み取りエラーを修正するためにオブジェクトを復元すると、ファイルゲートウェイの SMB クライアントまたは NFS クライアントがファイルを読み取れるようになります。

エラー: InvalidObjectState

指定されたファイルゲートウェイ以外のライターが、指定された Amazon S3 バケット内の指定されたファイルを変更すると、`InvalidObjectState` 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 S3 のファイルの状態と一致しなくなります。以降、Amazon S3 へのファイルのアップロードまたは Amazon S3 からのファイルの取得は失敗します。

S3 ファイルゲートウェイは、このエラーが原因で現在 Amazon S3 へのアップロードに失敗しているゲートウェイキャッシュ内のすべてのファイルを一覧表示するキャッシュレポートを生成できます。このレポートの情報は、 サポート を使用してゲートウェイ、Amazon S3、または IAM 設定の問題を解決するのに役立ちます。詳細については、「キャッシュレポートの作成」を参照してください。

InvalidObjectState エラーを解決するには

ファイルを変更するオペレーションが `S3Upload` または `S3GetObject` の場合は、次の手順を実行します。

1. ファイルの最新のコピーを SMB または NFS 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 S3 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。これは、 AWS マネジメントコンソール または を使用して実行できます AWS CLI。
2. AWS マネジメントコンソール または を使用して Amazon S3 内のファイルを削除します AWS CLI。
3. SMB または NFS 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。
4. SMB または NFS 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 Amazon S3 にコピーします。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: ObjectMissing

指定されたファイルゲートウェイ以外のライターが、指定されたファイルを S3 バケットから削除すると、`ObjectMissing` エラーが発生する場合があります。以降、Amazon S3 へのオブジェクトのアップロード、または Amazon S3 からのオブジェクトの取得は失敗します。

S3 ファイルゲートウェイは、このエラーが原因で現在 Amazon S3 へのアップロードに失敗しているゲートウェイキャッシュ内のすべてのファイルを一覧表示するキャッシュレポートを生成できます。このレポートの情報は、 サポート を使用してゲートウェイ、Amazon S3、または IAM 設定の問題を解決するのに役立ちます。詳細については、「キャッシュレポートの作成」を参照してください。

ObjectMissing エラーを解決するには

ファイルを変更するオペレーションが S3Upload または S3GetObject の場合は、次の手順を実行します。

1. ファイルの最新のコピーを SMB または NFS 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 または NFS 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 または NFS 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: RoleTrustRelationshipInvalid

このエラーは、ファイル共有の IAM ロールで IAM の信頼関係が正しく設定されていない (つまり IAM ロールで storagegateway.amazonaws.com という名前の Storage Gateway プリンシパルが信頼されていない) 場合に発生します。その結果、ファイルゲートウェイでは、ファイル共有をバックアップする S3 バケットでオペレーションを実行するための認証情報を取得できなくなります。

RoleTrustRelationshipInvalid エラーを解決するには

- ファイル共有の IAMrole によって信頼されるプリンシパルとして storagegateway.amazonaws.com を含めるには、IAM コンソールまたは IAM API を使用します。IAM ロールの詳細については、「チュートリアル: IAM ロールを使用して AWS アカウント間でアクセスを委任する」を参照してください。

エラー: S3AccessDenied

ファイル共有の Amazon S3 バケットアクセス AWS Identity and Access Management (IAM) ロールにS3AccessDeniedエラーが発生することがあります。この場合、エラー内の roleArn により指定された S3 バケットにアクセスする IAM ロールでは、関連するオペレーションは許可されません。オペレーションが許可されないのは、Amazon S3 プレフィックスで指定されたディレクトリ内のオブジェクトに対するアクセス許可のためです。

S3 ファイルゲートウェイは、このエラーが原因で現在 Amazon S3 へのアップロードに失敗しているゲートウェイキャッシュ内のすべてのファイルを一覧表示するキャッシュレポートを生成できます。このレポートの情報は、 サポート を使用してゲートウェイ、Amazon S3、または IAM 設定の問題を解決するのに役立ちます。詳細については、「キャッシュレポートの作成」を参照してください。

S3AccessDenied エラーを解決するには

- ファイルゲートウェイのヘルスログで `roleArn` にアタッチされている Amazon S3 のアクセスポリシーを変更して、Amazon S3 オペレーションに対するアクセス許可を付与します。アクセスポリシーで、エラーの原因となったオペレーションに対するアクセス許可を付与されていることを確認します。また、`prefix` のログで指定されたディレクトリに対するアクセス許可も許可します。Amazon S3 のアクセス許可についての詳細は、「Amazon Simple Storage Service ユーザーガイドの「ポリシーでのアクセス許可の指定」を参照してください。

  これらのオペレーションにより、`S3AccessDenied` エラーが発生する可能性があります。

  - `S3HeadObject`
  - `S3GetObject`
  - `S3ListObjects`
  - `S3DeleteObject`
  - `S3PutObject`

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: セキュリティスキャンで NFS ポートの開放が検出される

特定の NFS ポートは、SMB ファイル共有でのみ使用するゲートウェイでも、デフォルトで有効になっています。Qualys などのサードパーティのセキュリティソフトウェアを使用してファイルゲートウェイがデプロイされているネットワークをスキャンする場合、スキャン結果はこれらの NFS ポートの開放を潜在的なセキュリティ脆弱性として報告することがあります。SMB ファイル共有でのみゲートウェイを使用し、セキュリティ上の理由から未使用の NFS ポートを無効にする場合は、次の手順を行います。

ファイルゲートウェイで NFS ポートを無効にするには:

1. ローカルコンソールでの Storage Gateway コマンドの実行 で説明されている手順を使用して、ゲートウェイローカルコンソールのコマンドプロンプトにアクセスします。
2. NFS トラフィックを無効にするには、次のコマンドを入力します。

   IPv4

   ```
   iptables -I INPUT -p udp -m udp --dport 111 -j DROP
   iptables -I INPUT -p udp -m udp --dport 2049 -j DROP
   iptables -I INPUT -p udp -m udp --dport 20048 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 111 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 2049 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 20048 -j DROP
   ```

   IPv6

   ```
   ip6tables -I INPUT -p udp -m udp --dport 111 -j DROP
   ip6tables -I INPUT -p udp -m udp --dport 2049 -j DROP
   ip6tables -I INPUT -p udp -m udp --dport 20048 -j DROP
   ip6tables -I INPUT -p tcp -m tcp --dport 111 -j DROP
   ip6tables -I INPUT -p tcp -m tcp --dport 2049 -j DROP
   ip6tables -I INPUT -p tcp -m tcp --dport 20048 -j DROP
   ```

3. 次のコマンドを入力して、ブロックされた NFS ポートが IP テーブルに表示されることを確認します。

   IPv4

   ```
   iptables -n -L -v --line-numbers
   ```

   IPv6

   ```
   ip6tables -n -L -v --line-numbers
   ```

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

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、Amazon S3 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 S3 バケット 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。

ゲートウェイを介した Amazon S3 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 S3 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 S3 にアップロードされる速度よりも速いペースで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す、1 つ以上のキャッシュディスクを追加する、またはクライアントの書き込み速度を遅く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。
- S3PutObjectRequestTime、S3UploadPartRequestTime、または S3GetObjectRequestTime が高い場合、ネットワークにボトルネックが発生している可能性があります。ネットワークを分析して、ゲートウェイに想定どおりの帯域幅が確保されていることを確認してください。

ゲートウェイが想定よりも多くの Amazon S3 オペレーションを実行している

ファイルゲートウェイが想定よりも多くの Amazon S3 オペレーションを実行している場合は、FilesRenamed メトリクスを確認します。名前変更オペレーションはAmazon S3で実行すると

コストがかかります。ワークフローを最適化して、名前変更オペレーションの数を最小限に抑えます。

Amazon S3 バケット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 S3 バケット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。

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 Amazon S3 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、Amazon S3 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。

  NFS の場合は、クライアントがソフトマウントではなくハードマウントを使用してマウントされていることを確認してください。

トラブルシューティング: ファイル共有に関する問題

このセクションでは、ファイル共有で想定外の問題が発生した場合に行うアクションについて説明します。

トピック

ファイル共有が CREATING、UPDATING、または DELETING 状態でスタックする

ファイル共有ステータスは、ファイル共有の状態をまとめたものです。S3 File Gateway ファイル共有が `CREATING`、、`UPDATING`または `DELETING`状態でスタックしている場合は、次のトラブルシューティングステップを使用して問題を特定して解決します。

IAM ロールのアクセス許可と信頼関係を確認する

ファイル共有に関連付けられた AWS Identity and Access Management (IAM) ロールには、Amazon S3 バケットにアクセスするための十分なアクセス許可が必要です。さらに、ロールの信頼ポリシーは、ロールを引き受けるアクセス許可を Storage Gateway サービスに付与する必要があります。

IAM ロールのアクセス許可を確認するには:

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで Roles (ロール) を選択してください。
3. ファイル共有に関連付けられている IAM ロールを選択します。

4. [信頼関係] タブを選択します。
5. Storage Gateway が信頼されたエンティティとしてリストされていることを確認します。Storage Gateway が信頼されたエンティティでない場合は、信頼関係の編集を選択し、次のポリシーを追加します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "storagegateway.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

6. IAM ロールに正しいアクセス許可があり、Amazon S3 バケットが IAM ポリシーにリソースとしてリストされていることを確認します。詳細については、「Amazon S3 バケットに対するアクセス権限の付与」を参照してください。

> **Note**
>
> サービス間の混乱した代理防止の問題を回避するには、条件コンテキストキーを含む信頼関係ポリシーを使用します。詳細については、「the section called “サービス間の混乱した代理の防止”」を参照してください。

リージョンで AWS STS がアクティブ化されていることを確認します。

AWS リージョンで AWS Security Token Service (AWS STS) が非アクティブ化されている場合、ファイル共有は `CREATING`または `UPDATING`状態でスタックする可能性があります。

AWS STS ステータスを確認するには:

1. https://console.aws.amazon.com/iam/ で AWS Identity and Access Management コンソールを開きます。

2. ナビゲーションペインで [アカウント設定] を選択します。
3. Security Token Service (STS) セクションで、ファイル共有を作成する AWS リージョンのステータスがアクティブであることを確認します。
4. ステータスが非アクティブの場合は、アクティブ化を選択してそのリージョン AWS STS で を有効にします。

S3 バケットが存在し、命名規則に従っていることを確認する

ファイル共有には、Amazon S3 の命名規則に従った有効な Amazon S3 バケットが必要です。

S3 バケットを確認するには:

1. Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. ファイル共有にマッピングされた Amazon S3 バケットが存在することを確認します。バケットが存在しない場合は、バケットを作成します。バケットを作成すると、ファイル共有ステータスは に変わりますAVAILABLE。詳細については、Amazon Simple Storage Service ユーザーガイドの「バケットの作成」を参照してください。
3. バケット名が Amazon Simple Storage Service ユーザーガイドのバケット命名規則に準拠していることを確認します。

> **Note**
>
> S3 File Gateway は、バケット名にピリオド (.) を含む Amazon S3 バケットをサポートしていません。

ファイル共有を DELETING 状態で強制的に削除する

ファイル共有を削除すると、ゲートウェイは関連付けられた Amazon S3 バケットから共有を削除します。ただし、現在アップロード中のデータは、削除が完了する前に引き続きアップロードされます。このプロセス中に、ファイル共有のステータスが表示されますDELETING。

> **Important**
>
> ゲートウェイCachePercentDirtyの Amazon CloudWatch メトリクスをチェックして、アップロード保留中のデータの量を確認します。Storage Gateway メトリクスの詳細につ

いては、「」を参照してくださいthe section called “S3 ファイルゲートウェイのモニタリング”。

進行中のすべてのアップロードが完了するまで待機しない場合は、ファイル共有を強制的に削除できます。

ファイル共有を強制的に削除するには:

1. https://console.aws.amazon.com/storagegateway/ 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、ファイル共有を選択します。
3. 削除するファイル共有を選択します。
4. 詳細タブを選択し、このファイル共有が削除されているメッセージを確認します。
5. メッセージ内のファイル共有の ID を確認し、確認ボックスを選択します。

> **Note**
>
> 強制削除オペレーションを元に戻すことはできません。

6. 今すぐ強制削除を選択します。

または、 AWS CLI delete-file-share コマンドを使用して、 `--force-delete`パラメータを に設定することもできます`true`。

> **Important**
>
> ファイル共有を強制的に削除する前に、ゲートウェイが `OFFLINE`状態になっていないことを確認してください。ゲートウェイがオフラインの場合は、まずオフラインの問題を解決します。詳細については、「the section called “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”」を参照してください。

ゲートウェイ仮想マシン (VM) がすでに削除されている場合は、Storage Gateway コンソールからゲートウェイを削除して、 `DELETING`状態でスタックしているファイル共有を含む、関連するすべてのファイル共有を削除する必要があります。詳細については、「the section called “ゲートウェイおよびリソースの削除”」を参照してください。

ネットワーク接続に関する問題のトラブルシューティングを行う

ネットワークの問題により、ファイル共有が CREATING、、UPDATINGまたは DELETING状態から移行できなくなる可能性があります。一般的なネットワークの問題は次のとおりです。

- ゲートウェイがオフラインであるか、ゲートウェイ VM が削除されます。
- Storage Gateway と Amazon S3 サービスエンドポイント間のネットワークアクセスはブロックされます。
- ゲートウェイが Amazon S3 との通信に使用する Amazon S3 Amazon VPC エンドポイントが削除されました。
- 必要なネットワークポートが開いていないか、ネットワークルーティングが正しく設定されていません。

ゲートウェイローカルコンソールから S3 接続をテストする

S3 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。詳細については、「the section called “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”」を参照してください。
2. Storage Gateway - 設定のメインメニューに、テスト S3 接続に対応する番号を入力します。
3. Amazon S3 エンドポイントタイプを選択します。
   - インターネットゲートウェイ、NAT ゲートウェイ、トランジットゲートウェイ、または Amazon S3 ゲートウェイの Amazon VPC エンドポイントを通過する Amazon S3 トラフィックの場合は、「パブリック」を選択します。
   - Amazon S3 インターフェイス Amazon VPC エンドポイントを通過する Amazon S3 トラフィックの場合は、VPC (PrivateLink) を選択します。
   - FIPS エンドポイントの場合は、FIPS オプションを選択します。
4. Amazon S3 バケットリージョンを入力します。
5. Amazon VPC エンドポイントを使用する場合は、Amazon S3 Amazon VPC エンドポイントの DNS 名 (例:) を入力しますvpce-0329c2790456f2d01-0at85l34。

ゲートウェイは、ネットワーク接続と SSL 接続の両方を検証する接続テストを自動的に実行します。テストが失敗した場合:

- ネットワークテストの失敗 - 通常、ファイアウォールルール、セキュリティグループ設定、または不適切なネットワークルーティングが原因で発生します。必要なポートが開いていて、ネットワークルーティングが正しく設定されていることを確認します。
- SSL テストの失敗 - ゲートウェイ VM と Amazon S3 サービスエンドポイントの間で SSL 検査またはディープパケット検査が発生していることを示します。Storage Gateway トラフィックの SSL およびディープパケットインスペクションを無効にします。

プロキシ設定の確認

ゲートウェイがプロキシサーバーを使用している場合は、プロキシがネットワーク通信をブロックしていないことを確認します。

プロキシ設定を確認するには:

1. Storage Gateway - Configuration メインメニューで、HTTP/SOCKS Proxy Configuration に対応する番号を入力します。
2. 現在のネットワークプロキシ設定を表示するオプションを選択します。
3. プロキシが設定されている場合は、Amazon S3 トラフィックが Storage Gateway からポート 3128 (または設定されたリスナーポート) 経由でプロキシサーバーに流れ、ポート 443 経由で Amazon S3 エンドポイントに流れることを確認します。
4. プロキシまたはファイアウォールが、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していることを確認します。詳細については、必要なネットワークポートを参照してください。

問題が解決しない場合は、プロキシ設定を一時的に削除して、プロキシが問題の原因となっているかどうかを判断できます。

セキュリティグループとネットワークルーティングを検証する

- Amazon EC2 上のゲートウェイの場合 - セキュリティグループで Amazon S3 エンドポイントに対してポート 443 が開いていることを確認します。Amazon EC2 サブネットのルートテーブルが Amazon S3 トラフィックを Amazon S3 エンドポイントに適切にルーティングしていることを確認します。詳細については、必要なネットワークポートを参照してください。
- オンプレミスゲートウェイの場合 - ファイアウォールルールが必要なポートを許可し、ローカルルートテーブルが Amazon S3 トラフィックを Amazon S3 エンドポイントに適切にルーティングすることを確認します。詳細については、必要なネットワークポートを参照してください。

- VPC エンドポイント - ゲートウェイで使用される Amazon S3 Amazon VPC エンドポイントが削除されていないことを確認します。Amazon VPC エンドポイントが削除され、ゲートウェイにパブリック IP アドレスがない場合、ゲートウェイは Amazon S3 と通信できません。

ファイル共有を作成できない

1. ファイル共有が CREATING ステータスのまま止まっているためにファイル共有を作成できない場合には、ファイル共有をマッピングした S3 バケットが存在することを確認します。これを行う方法については、「ファイル共有が CREATING、UPDATING、または DELETING 状態でスタックする」を参照してください。
2. S3 バケットが存在する場合は、ファイル共有を作成するリージョンで AWS Security Token Service がアクティブ化されていることを確認します。セキュリティトークンが有効になっていない場合は、有効にする必要があります。を使用してトークンをアクティブ化する方法については AWS Security Token Service、IAM ユーザーガイドの「 AWS リージョンでの AWS STS のアクティブ化と非アクティブ化」を参照してください。

SMB ファイル共有で複数の異なるアクセス方法が使えない

SMB ファイル共有には、以下の制約があります。

1. 同じクライアントが Active Directory とゲストアクセスの SMB ファイル共有の両方をマウントしようとすると、次のエラーメッセージが表示されます。`Multiple connections to a server or shared resource by the same user, using more than one user name, are not allowed. Disconnect all previous connections to the server or shared resource and try again.`
2. Windows ユーザーは、2 つのゲストアクセスの SMB ファイル共有に接続することはできません。新しいゲストアクセス接続が確立されると切断される場合があります。
3. Windows クライアントは、同じゲートウェイによってエクスポートされた、ゲストアクセスと Active Directory の SMB ファイル共有の両方をマウントすることはできません。

マッピングされた S3 バケットに複数のファイル共有を書き込めない

1 つの S3 バケットに複数のファイル共有を書き込むことを許可するよう S3 バケットを設定することは推奨されません。このやり方では、想定外の結果を引き起こす場合があります。

代わりに、各 S3 バケットに 1 つのファイル共有のみ書き込めるようにすることが推奨されます。ファイル共有に関連付けられた 1 つのロールのみがバケットに書き込めるようにするバケットポリシーを作成します。詳細については、「ファイルゲートウェイのベストプラクティス」を参照してください。

監査ログを使用する場合の削除済みロググループの通知

ロググループが存在しない場合、ユーザーはそのメッセージの下にあるロググループリンクを選択して、新しいロググループを作成するか、または既存のロググループを使用して、監査ログの対象として利用できます。

S3 バケットにファイルをアップロードできない

S3 バケットにファイルをアップロードできない場合には、以下を行います。

1. S3 バケットにファイルをアップロードする Amazon S3 ファイルゲートウェイに必要なアクセス権限があることを確認します。詳細については、「Amazon S3 バケットに対するアクセス権限の付与」を参照してください。
2. バケットを作成したロールに S3 バケットに書き込みを行う許可があることを確認します。詳細については、「ファイルゲートウェイのベストプラクティス」を参照してください。
3. ファイルゲートウェイが暗号化に SSE-KMS または DSSE-KMS を使用している場合は、ファイル共有に関連付けられた IAM ロールに kms:Encrypt、kms:Decrypt、kms:ReEncrypt*、kms:GenerateDataKey、および kms:DescribeKey のアクセス許可が含まれていることを確認してください。詳細については、「Storage Gateway でアイデンティティベースのポリシー (IAM ポリシー) を使用する」を参照してください。

SSE-KMS を使用して、S3 バケットに保存されたオブジェクトを暗号化するように、デフォルトの暗号化を変更できない

デフォルトの暗号化を変更して SSE-KMS (AWS KMS– マネージドキーを使用したサーバー側の暗号化) を S3 バケットのデフォルトにすると、Amazon S3 ファイルゲートウェイがバケットに保存するオブジェクトは SSE-KMS で暗号化されません。デフォルトでは、S3 ファイルゲートウェイで S3 バケットにデータを書き込む際、Amazon S3 で管理されるサーバー側の暗号化 (SSE-S3) が使用されます。デフォルトを変更しても、暗号化は自動的に変更されません。

独自の AWS KMS キーで SSE-KMS を使用するように暗号化を変更するには、SSE-KMS 暗号化を有効にする必要があります。これを行うには、ファイル共有を作成するときに KMS キーの Amazon

リソースネーム (ARN) を指定します。ファイル共有の KMS 設定は、UpdateNFSFileShare または UpdateSMBFileShare API オペレーションを使用して更新することもできます。この更新は、更新後に S3 バケットに保存されているオブジェクトに適用されます。詳細については、「を使用したデータ暗号化 AWS KMS」を参照してください。

オブジェクトのバージョニングが有効になっている S3 バケットで直接行われた変更は、ファイル共有で表示される内容に影響することがあります。

S3 バケットのオブジェクトが別のクライアントから書き込まれている場合、S3 バケットオブジェクトのバージョニングの結果として S3 バケットのビューが最新でなくなる可能性があります。目的のファイルを調べる前に必ずキャッシュを更新してください。

オブジェクトのバージョニングは、同じ名前のオブジェクトの複数のコピーを保存することによりデータを保護するためのオプションの S3 バケット機能です。各コピーには、個別の ID 値があります (file1.jpg: ID="xxx" および file1.jpg: ID="yyy" など)。同じ名前のオブジェクトの数とその存続期間は、Amazon S3 ライフサイクルポリシーによって制御されます。これらの Amazon S3 の概念の詳細については、「Amazon S3 開発者ガイド」の「バージョニングの使用」と「オブジェクトのライフサイクルの管理」を参照してください。

バージョニングされたオブジェクトを削除すると、そのオブジェクトには削除マーカーのフラグが付けられますが保持されます。バージョニングがオンになっているオブジェクトは、S3 バケット所有者のみが完全に削除することができます。

S3 ファイルゲートウェイでは、表示されるファイルは、オブジェクトが取得されたかキャッシュが更新された時点の S3 バケットにおけるオブジェクトの最新バージョンです。S3 ファイルゲートウェイは、古いバージョン、または削除対象としてマークされたすべてのオブジェクトを無視します。ファイルを読み込むとき、最新バージョンからデータを読み取ります。ファイル共有にファイルを書き込むと、S3 ファイルゲートウェイにより、指定オブジェクトの新しいバージョンが変更を適用して作成され、そのバージョンが最新バージョンになります。

S3 ファイルゲートウェイは、以前のバージョンから読み取りを続けます。アプリケーション外で S3 バケットに新しいバージョンが追加された場合、ゲートウェイによる更新は以前のバージョンに基づいて行われます。オブジェクトの最新バージョンを読み取るには、「Amazon S3 バケットのオブジェクトキャッシュの更新」で説明されているように、RefreshCache API アクションを使用するか、コンソールから更新します。

> **Important**
>
> ファイル共有以外の経路から、S3 ファイルゲートウェイの S3 バケットにオブジェクトまたはファイルを書き込むことは推奨されません。

オブジェクトのバージョニングを有効にして S3 バケットに書き込む場合、Amazon S3 ファイルゲートウェイは S3 オブジェクトの複数のバージョンを作成することがあります。

オブジェクトのバージョニングを有効にすると、NFS または SMB クライアントからファイルを更新するたびに、Amazon S3 でオブジェクトの複数のバージョンが作成されることがあります。S3 バケットにオブジェクトの複数のバージョンが作成される可能性があるシナリオを次に示します。

- Amazon S3 にアップロードされたファイルが、NFS または SMB クライアントによってAmazon S3 ファイルゲートウェイ内で変更されると、S3 ファイルゲートウェイはファイル全体をアップロードするのではなく、新しいデータまたは変更されたデータのみをアップロードします。ファイルを変更すると、Amazon S3 オブジェクトの新しいバージョンが作成されます。
- NFS または SMB クライアントによってファイルゲートウェイにファイルが書き込まれると、S3 ファイルゲートウェイによりファイルデータが Amazon S3 にアップロードされます。その後、メタデータ (所有権、タイムスタンプなど) がアップロードされます。ファイルデータをアップロードすると Amazon S3 オブジェクトが作成され、ファイルのメタデータをアップロードすると、Amazon S3 オブジェクトのメタデータが更新されます。このプロセスにより、別のバージョンのオブジェクトが作成され、オブジェクトのバーションが 2 つになります。
- S3 ファイルゲートウェイが大きなファイルをアップロードする場合、クライアントがファイルゲートウェイへの書き込みを完了する前に、ファイルを小さく分けてアップロードする必要がある場合があります。その理由には、キャッシュ領域の解放や、ファイルへの書き込み率が高いことなどが挙げられます。この処理では、S3 バケットで複数バージョンのオブジェクトが作成されることがあります。

オブジェクトを異なるストレージクラスに移動するライフサイクルポリシーを設定する前に、S3 バケットをモニタリングして、オブジェクトのバージョン数を確認する必要があります。S3 バケット内のオブジェクトのバージョン数を最小限に抑えるには、過去のバージョンのライフサイクルに有効期限を設定する必要があります。S3 バケット間で、同一リージョンでのレプリケーション (SRR) またはクロスリージョンでのレプリケーション (CRR) を使用すると、使用されるストレージが増加します。レプリケーションの詳細については、「レプリケーション」を参照してください。

> **Important**
>
> オブジェクトのバージョニングが有効になっているときに使用されているストレージの量を把握するまで、S3 バケット間のレプリケーションを設定しないでください。

バージョニングされた S3 バケットを使用すると、ファイルを変更するたびに S3 オブジェクトの新しいバージョンが作成されるため、Amazon S3 内のストレージの量が大幅に増加します。この動作を上書きし、保持されるバージョンの数を制限するポリシーを別に作成しない限り、デフォルトでは、Amazon S3 はこれらのすべてのバージョンを保存し続けます。オブジェクトのバージョニングを有効にして、ストレージ使用量が異常に大きいことに気づいた場合、ストレージポリシーが適切に設定されていることを確認してください。ブラウザリクエストに対する `HTTP 503-slow down` 応答の数が増えても、オブジェクトのバージョニングの問題が発生する可能性があります。

S3 ファイルゲートウェイのインストール後にオブジェクトのバージョニングを有効にした場合、すべての一意のオブジェクトが保持され (`ID="NULL"`)、ファイルシステムにそれらすべてが表示されます。新しいバージョンのオブジェクトには固有の ID が割り当てられます (古いバージョンは保持されます)。オブジェクトのタイムスタンプに基づいて、最新のバージョニングされたオブジェクトのみが NFS ファイルシステムに表示されます。

オブジェクトのバージョニングを有効にすると、S3 バケットをバージョニングが設定されていない状態に戻すことはできません。ただし、バージョニングを停止することは可能です。バージョニングを停止した場合、新しいオブジェクトに ID が割り当てられます。`ID="NULL"` 値を持つ同じ名前のオブジェクトが存在する場合は、以前のバージョンが上書きされます。ただし、`NULL` 以外の ID が格納されているバージョンは保持されます。タイムスタンプは、新しいオブジェクトを最新のオブジェクトとして識別します。そのオブジェクトが NFS ファイルシステムに表示されます。

S3 バケットに対する変更が Storage Gateway に反映されない

Storage Gateway は、ファイル共有を使用してローカルでキャッシュにファイルが書き込まれると、ファイル共有キャッシュを自動的に更新します。ただし、ファイルを Amazon S3 に直接アップロードしても、Storage Gateway はキャッシュを自動的に更新しません。これを行う際には、`RefreshCache` オペレーションを実行して、ファイル共有の変更を確認します。複数のファイル共有がある場合は、各ファイル共有に対して `RefreshCache` オペレーションを実行する必要があります。

次のように、Storage Gateway コンソールと AWS Command Line Interface (AWS CLI) を使用してキャッシュを更新できます。

- Storage Gateway コンソールを使用してキャッシュを更新するには、「Amazon S3 バケット内のオブジェクトの更新」を参照してください。
- AWS CLIを使用してキャッシュを更新するには次の手順を実行します。
  1. コマンド `aws storagegateway list-file-shares` を実行します
  2. 更新するキャッシュとのファイル共有の Amazon リソースナンバー (ARN) をコピーします。
  3. ARN を `--file-share-arn` の値として `refresh-cache` コマンドを次のように実行します。

     ```
     aws storagegateway refresh-cache --file-share-arn
     arn:aws:storagegateway:eu-west-1:12345678910:share/share-FFDEE12
     ```

`RefreshCache` オペレーションを自動化するには、「Storage Gateway で RefreshCache 操作を自動化する方法」を参照してください。

ACL のアクセス許可が予期する動作を行わない

アクセスコントロールリスト (ACL) 権限が SMB ファイル共有で所定の動作を行わない場合は、テストを実行できます。

これを行うには、まず、Microsoft Windows ファイルサーバーあるいはローカル Windows ファイル共有でアクセス権限をテストします。次に、ゲートウェイのファイル共有と動作を比較します。

再帰的なオペレーションを実行すると、ゲートウェイのパフォーマンスが低下した

一部のケースでは、ディレクトリの名前変更や ACL での継承を有効にするなどの再帰的なオペレーションを実行し、その変更をツリー全体に強制的に適用することがあります。これを行った場合、S3 ファイルゲートウェイはこのオペレーションを再帰的にファイル共有のすべてのオブジェクトに適用します。

例えば、S3 バケット内の既存のオブジェクトに継承を適用するとします。S3 ファイルゲートウェイは、バケット内のすべてのオブジェクトに継承を再帰的に適用します。このようなオペレーションは、ゲートウェイの実行が拒否される要因となることがあります。

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
- メトリクス

ヘルス通知

VMware vSphere HA でゲートウェイを実行すると、すべてのゲートウェイで、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
- 通知: HardReboot
- 通知: HealthCheckFailure
- 通知: AvailabilityMonitorTest

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 Amazon S3 バケット に、新しい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、「S3 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を作成します。詳細については、「ファイル共有の作成」「」を参照してください。

3. ファイル共有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 S3 バケット 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。

ベストプラクティス: マルチパートアップロードの管理

大きなファイルを転送する場合、S3 ファイルゲートウェイは Amazon S3 マルチパートアップロード特徴量を使用してファイルを小さな部分に分割し、効率を向上させるために並行して転送します。詳細については、「Amazon Simple Storage Service ユーザーガイド」の「マルチパートアップロードを使用したオブジェクトのアップロード」を参照してください。

マルチパートアップロードが何らかの理由で正常に完了しなかった場合、ゲートウェイは通常転送を停止し、Amazon S3 から部分的に転送されたファイルをすべて削除して、転送を再試行します。まれに、ハードウェアまたはネットワーク障害により、マルチパートアップロードが失敗した後にゲートウェイがクリーンアップできない場合、部分的に転送されたファイルの一部が Amazon S3 に残り、ストレージ料金が発生する可能性があります。

不完全なマルチパートアップロードによる Amazon S3 ストレージコストを最小限に抑えるためのベストプラクティスとして、`AbortIncompleteMultipartUpload`API アクションを使用して失敗した転送を自動的に停止し、指定された日数後に関連するファイル部分を削除する Amazon S3 バケットライフサイクルルールの設定を推奨します。手順については、「Amazon Simple Storage Service ユーザーガイド」の「不完全なマルチパートアップロードを削除するためのバケットライフサイクル設定の設定」を参照してください。

ベストプラクティス: ゲートウェイにコピーする前に、圧縮ファイルをローカルで解凍する

ゲートウェイに保存されている間に数千のファイルを含む圧縮アーカイブを解凍しようとすると、パフォーマンス関連の大幅な遅延が発生する可能性があります。任意のタイプのネットワークファイル共有に多数のファイルを含むアーカイブを解凍するプロセスには、本質的に大量の入出力オペレーション、メタデータキャッシュ操作、ネットワークオーバーヘッド、レイテンシーが含まれます。さらに、Storage Gateway はアーカイブの各ファイルがいつ解凍が完了したかを判断できず、プロセスが完了する前にファイルのアップロードを開始できるため、パフォーマンスにさらに影響します。これらの問題は、アーカイブ内のファイルが多数あるが、サイズが小さい場合に複合されます。

ベストプラクティスとして、圧縮アーカイブを解凍する前に、まずゲートウェイからローカルマシンに転送することを推奨します。その後、必要に応じて、robocopy や rsync などのツールを使用して、解凍したファイルをゲートウェイに転送できます。

Windows Server からデータをコピーするときにファイル属性を保持する

Microsoft Windows の基本的な copy コマンドを使用してファイルゲートウェイにファイルをコピーすることはできますが、このコマンドはデフォルトでファイルデータのみをコピーします。セキュリティ記述子などの特定のファイル属性は省略されます。対応するセキュリティ制限と随意アクセスコントロールリスト (DACL) 情報なしでファイルがゲートウェイにコピーされると、権限のないユーザーによってアクセスされる可能性があります。

Microsoft Windows サーバ でゲートウェイにファイルをコピーするときに、すべてのファイル属性とセキュリティ情報を保存するためのベストプラクティスとして、robocopy あるいは xcopy コマンドと、/copy:DS または /o フラグをそれぞれ使用することを推奨します。詳細については、Microsoft Windows Server コマンドリファレンスドキュメントの「robocopy」と「xcopy」を参照してください。

ベストプラクティス: キャッシュディスクの適切なサイズ設定

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に合わせる必要があります。読み取り負荷の高いワークロードや読み書きが混在するワークロードにおいては、読み取りに対するキャッシュヒットの割合が高いことが望まれます。これは、S3 ファイルゲートウェイの CacheHitPercent メトリクスを使用してモニタリングできます。

書き込みが多いワークロード (バックアップやアーカイブなど) の場合、S3 ファイルゲートウェイは、このデータを Amazon S3 に非同期でコピーする前に、ディスクキャッシュで受信書き込みをバッファします。書き込まれたデータをバッファするのに十分なキャッシュ容量があることを確認する必要があります。CachePercentDirty メトリクスは、まだ保持されていないディスクキャッシュの割合を示します AWS。

CachePercentDirty の低い値をお勧めします。値が一貫して 100% に近い場合は、S3 ファイルゲートウェイが受信書き込みトラフィックの速度に対応できないことを示します。これを回避するには、プロビジョニングされたディスクキャッシュ容量を増やすか、S3 ファイルゲートウェイから Amazon S3 に利用できる専用ネットワーク帯域幅を増やすか、またはその両方を行います。

キャッシュディスクのサイズ設定の詳細については、Amazon Web Services の公式 YouTube チャンネルの「Amazon S3 ファイルゲートウェイのキャッシュサイズ設定のベストプラクティス」を参照してください。

複数のファイル共有と Amazon S3 バケットの使用

複数のゲートウェイまたはファイル共有に書き込みを許可するように単一の Amazon S3 バケットを設定すると、結果が予測不能になる可能性があります。予期しない結果を避けるために、バケットは 2 つの方法のいずれかで設定できます。以下のオプションから、ユースケースに最適な設定方法を選択します。

- 各バケットに書き込むことができるファイル共有が 1 つだけになるように S3 バケットを設定します。異なるファイル共有を使用して、各バケットに書き込みます。

  これを実現するには、特定のファイル共有で使用されているロール以外のすべてのロールによるバケット内のオブジェクトの追加および削除を拒否する S3 バケットポリシーを作成します。同様のポリシーを各バケットにアタッチし、各バケットに書き込む別のファイル共有を指定します。

  次のポリシーの例では、S3 バケットに書き込むバケットを作成するロールを除くすべてのロールを拒否しています。`s3:DeleteObject` および `s3:PutObject` アクションは、`"TestUser"` を除くすべてのロールに対して拒否されます。このポリシーは、`"arn:aws:s3:::amzn-s3-demo-bucket/*"` バケット内のすべてのオブジェクトに適用されます。

  JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyMultiWrite",
         "Effect":"Deny",
         "Principal":"*",
         "Action":[
            "s3:DeleteObject",
            "s3:PutObject"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*",
         "Condition":{
            "StringNotLike":{
               "aws:userid":"TestUser:*"
            }
```

```
            }
        }
    ]
}
```

- 複数のファイル共有を同じ Amazon S3 バケットに書き込む場合は、ファイル共有が同じオブジェクトに同時に書き込もうとしないようにする必要があります。

  これを行うには、ファイル共有ごとに個別の一意のオブジェクトプレフィックスを設定します。つまり、各ファイル共有は対応するプレフィックスを持つオブジェクトにのみ書き込み、デプロイ内の他のファイル共有に関連付けられているオブジェクトには書き込みません。新しいファイル共有を作成するときに、S3 プレフィックス名フィールドでオブジェクトプレフィックスを設定します。

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。
- ファイル属性のサポート - ゲートウェイが DOS および Windows ファイル属性を処理する方法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 によって作成された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。
- ストレージクラスを使用する - ファイルゲートウェイがサポートする Amazon S3 ストレージクラスと、ストレージクラスを選択するときに考慮すべき点について説明します。
- Kubernetes CSI ドライバーの使用 - コンテナストレージインターフェイス (CSI) ドライバをインストールして設定し、Kubernetes インスタンスがストレージにファイルゲートウェイを使用できるようにする方法について説明します。

- Terraform モジュール - Terraform を使用して ファイルゲートウェイを仮想マシンとしてデプロイする方法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

- S3 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
- S3 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

S3 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Amazon S3 ファイルゲートウェイと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、「Amazon EC2 インスタンスをデプロイして Amazon S3 ファイルゲートウェイをホストする」および「」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 AWS Storage Gateway コンソールで 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
111	TCP、UDP	NFSv3
139	TCP、UDP	SMB
445	TCP	SMB
2049	TCP、UDP	NFS
20048	TCP、UDP	NFSv3

- 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

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				
終了時に削除	はい	はい				
暗号化された	いいえ	いいえ				
スループット	125	125				

S3 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Amazon S3 ファイルゲートウェイと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。
> S3 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_S3-1.25.0`

Amazon S3 ファイルゲートウェイをホストする Amazon EC2 インスタンスをデプロイするには

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 S3 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、「Amazon EC2 の Quicklaunch 設定仕様」および「」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。Amazon S3 ファイルゲートウェイおよび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 S3 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。
> NFS ファイル共有を作成する場合は、NFS アクセスには TCP/UDP ポート 2049、NFSv3 アクセスには TCP/UDP ポート 111、NFSv3 アクセスには TCP/UDP ポート 20048 を開く必要があります。
> SMB ファイル共有を作成する場合は、SMB アクセス用に TCP ポート 445 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 S3 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 S3 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_S3/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_S3/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": 4,
        "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/
FILE_S3/latest",
        "Name": "/aws/service/storagegateway/ami/FILE_S3/latest",
        "Value": "ami-123c45dd67d891000"
    }
}
```

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。

> **Note**
>
> Storage Gateway コンソールでファイル共有の情報ページに表示されるマウントコマンドの例には、そのファイル共有に関連付けられたゲートウェイに最後に追加されたネットワークアダプタの IP アドレスが常に含まれます。

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。

> **Note**
>
> Storage Gateway コンソールでファイル共有の情報ページに表示されるマウントコマンドの例には、そのファイル共有に関連付けられたゲートウェイに最後に追加されたネットワークアダプタの IP アドレスが常に含まれます。

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 S3 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、「Amazon S3 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」および「」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 S3 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:

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、次のいずれかのコマンドを使用します。

標準エンドポイント

標準 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"
```

デュアルスタックのエンドポイント

デュアルスタ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 :

IPv4

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=DUALSTACK&ipVersion=ipv4&no_redirect"
```

IPv6

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=DUALSTACK&ipVersion=ipv6&no_redirect"
```

FIPS エンドポイント

FIPS 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:

IPv4

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=FIPS_DUALSTACK&ipVersion=ipv4&no_redirect"
```

IPv6

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=FIPS_DUALSTACK&ipVersion=ipv6&no_redirect"
```

VPC エンドポイント

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。

Amazon Linux 2 (AL2) ベースのゲートウェイ

AL2 に基づくゲートウェイの標準エンドポイントまたは FIPS エンドポイントを選択できます。

> **Note**
>
> FIPS エンドポイントは、すべての で利用できるわけではありません AWS リージョン。詳細については、「サービス別の FIPS エンドポイント」を参照してください。

ローカルコンソールからAL2ベースの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. [AWS アプライアンスのアクティベーション - 設定] メインメニューから、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. 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、パブリックの場合は「1」、VPC の場合は「2」と入力します。
6. エンドポイントタイプとして、「Standard」には 1、または「Federal Information Processing Standard (FIPS)」には 2 を入力します。

Amazon Linux 2023 (AL2023) ベースのゲートウェイ

AL2023 に基づくゲートウェイでは、次のエンドポイントを使用できます。

- 標準エンドポイント (IPv4 のみをサポート)
- FIPS エンドポイント (IPv4 のみをサポート)
- デュアルスタックエンドポイント (IPv4 と IPv6 の両方をサポート)
- IPv4 と IPv6 の両方をサポートするデュアルスタックの FIPS エンドポイント

詳細については、「エンドポイントタイプ」を参照してください。

ローカルコンソールから AL2023 ベースのゲートウェイのアクティベーションキーを取得するには

1. ローカルコンソールにログインします。Windows コンピュータから Amazon EC2 インスタンスに接続する場合は、admin としてログインします。
2. [AWS アプライアンスのアクティベーション - 設定] メインメニューから、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. 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、パブリックの場合は「1」、VPC エンドポイントの場合は「2」と入力します。
6. [エンドポイントタイプの選択] の [FIPS を有効化しますか?] では、FIPS を有効にするには Yを、非 FIPS エンドポイントを使用するには N を入力します。
7. エンドポイントタイプの場合は、標準エンドポイントの場合は 1、デュアルスタックエンドポイントの場合は 2 と入力します。

- デュアルスタックエンドポイントの場合は、[IP バージョンを選択または終了:] のプロンプトで、IPv4 の場合は 1 を、IPv6 の場合は 2 を入力します。

Amazon S3 ファイルゲートウェイでのファイル属性のサポート

Amazon S3 ファイルゲートウェイは、デフォルトで DOS または Windows ファイル属性をサポートしています。S3 ファイルゲートウェイを使用すると、Amazon S3 に配置されたときに項目をアーカイブ済みとしてマークするなど、ファイルデータとメタデータを保持し、設定を更新できます。DOS および Windows ファイル属性の詳細については、Windows アプリ開発ドキュメントウェブサイトの「File Attribute Constants (ファイル属性定数)」の記事を参照してください。

S3 ファイルゲートウェイは、次の属性をサポートします。

- ReadOnly – S3 ファイルゲートウェイは、ReadOnly 属性が設定されたファイルへの変更を防ぎます。
- Archive – ファイルがゲートウェイに最初に追加されると、S3 ファイルゲートウェイはこの属性を設定します。

> **Note**
>
> バックアップアプリケーションは通常、Archive ビットが設定されたファイルをバックアップし、バックアップが成功するとそのビットをクリアします。

- 非表示 – サーバーメッセージブロック (SMB) クライアントは、このビットが設定されているファイルを非表示にします。
- System – この属性は、設定後も保持されます。

属性が設定されているファイルを S3 ファイルゲートウェイにコピーすると、ファイルの DOS または Windows 属性は S3 ファイルゲートウェイと Amazon S3 に保持されます。これらの属性は、ゲートウェイ上のファイルに対して更新でき、その更新は Amazon S3 のオブジェクトにも適用されます。ファイルがゲートウェイから削除された場合は、リクエスト時に、ゲートウェイが Amazon S3 からそのファイル、メタデータ、および永続属性を取得します。

> **Note**
>
> DOS 属性は、SMB 共有でのみサポートされており、アクセスが Windows アクセスコントロールリストによって制御されている場合に限られます。

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、 ロケーションと同じ 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、「 とは」を参照してください Direct Connect。 Direct Connect「 ユーザーガイド」の「」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 のファイル共有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。

IPv6 サポート

IPv6 サポートは、ゲートウェイアプライアンスバージョン 2.x 以降でのみ使用できます。ゲートウェイアプライアンスバージョン 1.x をバージョン 2.x に更新することはできません。IPv6 サポートを受けるには、ゲートウェイアプライアンスバージョン 1.x を移行または置き換える必要があります。

IPv6 には、次のデュアルスタックエンドポイントが必要です。

```
storagegateway.region.api.aws:443
activation-storagegateway.region.api.aws:443
controlplane-storagegateway.region.api.aws:443
proxy-storagegateway.region.api.aws:443
dataplane-storagegateway.region.api.aws:443
s3.dualstack.region.amazonaws.com
```

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 IDs を使用する場合、Amazon EC2 はリソース IDsで想定します。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。例えば、Storage Gateway では、ゲートウェイの ID は ですsgw-12A3456B。EC2 API でこの ID を使用する場合は、 に変更する必要がありますsgw-12a3456b。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。

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 S3 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 S3 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 S3 ファイルゲートウェイ(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。

S3 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 S3 ファイルゲートウェイの場合: sgw-file-s3-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、サードパーティのライセンスを参照してください。

Amazon S3 ファイルゲートウェイおよびの制限とクォータ

ファイル共有のクォータ

次の表は、ファイル共有のクォータの一覧です。

説明	制限
ゲートウェイごとのファイル共有の最大数 **Note** 各ファイル共有は 1 つの S3 バケットにのみ接続できますが、複数のファイル共有は同じバケットに接続できます。複数のファイル共有を同じバケットに接続する場合は、読み取り/書き込	50

説明	制限
みの競合を防ぐために、重複しない一意のプレフィックス名を各ファイル共有に設定する必要があります。 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。	
ゲートウェイがメタデータを同時にキャッシュできるファイルの最大数 Note S3 ファイルゲートウェイは Amazon S3 によってバックアップされているため、ゲートウェイを使用して保存またはアクセスできるフォルダーサイズやファイル数の最大値に制限はありません。 各ゲートウェイには、メタデータを同時にキャッシュできるファイルの数を決定する設定可能な制限があります。UpdateGatewayInformation API アクションを使用して、GatewayCapacity を `Small`、`Medium`、または `Large` に設定できます。この設定は、ゲートウェイのパフォーマンスとハードウェアの推奨構成に影響します。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。	ゲートウェイ容量: 小 — 500万ファイル 中 — 1000万ファイル 大 — 2000万ファイル

説明	制限
各ファイルの最大サイズ **Note** サイズ制限を超えるファイルを 1 つずつ書き込もうとすると、最初の 5 TiB だけがアップロードされます。サイズ制限を超えるファイルを一度に書き込もうとすると、Windows クライアントではファイルが作成されず、Linux クライアントではサイズ 0 のファイルが作成されます。	5 TiB
パスの最大長 **Note** クライアントは、この長さを超えるパスを作成できません。作成すると、エラーが発生します。この制限は、ファイルゲートウェイ、NFS、および SMB でサポートされているプロトコルに適用されます。 バイト単位のパス長は、UTF-8 エンコーディングの文字ビット値から計算されます。	1024 バイト

説明	制限
ファイル名の最大長 **Note** ファイルゲートウェイは、この長さを超えるファイル名をサポートしていません。 バイト単位のファイル名の長さは、UTF-8 エンコーディングの文字ビット値から計算されます。	255 バイト

ゲートウェイのローカルディスクの推奨サイズ

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

ゲートウェイタイプ	キャッシュ (最小)	キャッシュ (最大)
S3 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。

ストレージクラスを使用する

Amazon S3 ファイルゲートウェイは、Amazon S3 Standard、Amazon S3 Standard-Infrequent Access、Amazon S3 One Zone-Infrequent Access、Amazon S3 Intelligent-Tiering、Amazon Glacier ストレージクラスをサポートしています。ストレージクラスの詳細については、「Amazon Simple Storage Service ユーザーガイド」の「Amazon S3 ストレージクラス」を参照してください。

> **Note**
>
> S3 ファイルゲートウェイは現在、Amazon S3 Glacier Instant Retrieval ストレージクラスをサポートしていません。

トピック

ファイルゲートウェイでストレージクラスを使用する

ファイル共有を作成または更新する場合は、オブジェクトのストレージクラスを選択することができます。Amazon S3 標準ストレージクラス、または S3 標準 – IA、S3 1 ゾーン – IA、S3 Intelligent-Tiering ストレージクラスのいずれかを選択できます。これらのストレージクラスのいずれかに保存されたオブジェクトは、ライフサイクルポリシーを使用して GLACIER に移行させることができます。

Amazon S3 ストレージクラス	考慮事項
標準	アクセスが頻繁なファイルを、地理的に分散した複数のアベイラビリティーゾーン (AZ) に冗長的に保存するには、[標準] を選択します。これは、デフォルトのストレージクラスです。詳細については、「Amazon S3 の料金」を参照してください。
S3 Intelligent-Tiering	Intelligent-Tiering を選択すると、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

Amazon S3 ストレージクラス	考慮事項
	データを移動して、ストレージコストを最適化できます。 128 KB 未満のオブジェクトは、Intelligent-Tiering ストレージクラスの自動階層化の対象ではありません。これらのオブジェクトには頻繁アクセス階層の料金が課金されますが、自動階層化オブジェクトに対して課金されるモニタリング料金は発生しません。 S3 Intelligent-Tiering では現在、Archive Access 階層と Deep Archive Access 階層がサポートされています。S3 Intelligent-Tiering は、90 日間アクセスされなかったオブジェクトを自動的に Archive Access 階層へ移動し、その後さらに 180 日間アクセスされなかったオブジェクトを Deep Archive Access 階層へ自動的に移動します。アーカイブアクセス階層のいずれかにあるオブジェクトが復元されると、そのオブジェクトは数時間以内に Frequent Access 階層に移動され、取得できる状態になります。このため、オブジェクトが 2 つのアーカイブ階層のいずれかにしか存在しない場合、ファイル共有を介してファイルにアクセスしようとすると、ユーザーやアプリケーションでタイムアウトエラーが発生することがあります。ファイルゲートウェイが提供するファイル共有を介してアプリケーションがファイルにアクセスしている場合は、S3 Intelligent-Tiering のアーカイブ階層を使用しないでください。 所有者、タイムスタンプ、アクセス許可、ACL などのメタデータを更新するファイルオペレーションがファイルゲートウェイによって管理されるファイルに対して実行されると、既存のオブジェクトが削除され、この Amazon S3 スト

Amazon S3 ストレージクラス	考慮事項
	レージクラスにオブジェクトの新しいバージョンが作成されます。このストレージクラスを本番環境で使用する前に、ファイルオペレーションがオブジェクトの作成にどのように影響するかを検証してください。詳細については、「Amazon S3 の料金」を参照してください。

Amazon S3 ストレージクラス	考慮事項
S3 Standard – IA	アクセスが頻繁ではないオブジェクトデータを、地理的に分散した複数のアベイラビリティーゾーン (AZ) に冗長的に保存するには、[標準 – IA] を選択します。 標準 – IA ストレージクラスに保存されているオブジェクトには、30 日以内に上書き、削除、リクエスト、取得、またはストレージクラス間の移行を行うと、追加料金が発生する可能性があります。最小保存期間は 30 日です。30 日より前に削除されたオブジェクトには、残りの日数のストレージ料金に相当する日割り課金が発生します。これらのオブジェクトを変更する頻度、これらのオブジェクトを保持する期間、およびオブジェクトへの必要なアクセス頻度を検討します。128 KB 未満のオブジェクトには 128 KB 分の料金が課金され、早期削除料金が適用されます。 所有者、タイムスタンプ、アクセス許可、ACL などのメタデータを更新するファイルオペレーションがファイルゲートウェイによって管理されるファイルに対して実行されると、既存のオブジェクトが削除され、この Amazon S3 ストレージクラスにオブジェクトの新しいバージョンが作成されます。早期削除料金が適用されるため、このストレージクラスを本番環境で使用する前に、ファイルオペレーションがオブジェクトの作成にどのように影響するかを検証する必要があります。詳細については、「Amazon S3 の料金」を参照してください。

Amazon S3 ストレージクラス	考慮事項
S3 1 ゾーン - IA	アクセスが頻繁ではないファイルを 1 つのアベイラビリティーゾーン (AZ)に保存するには、1 ゾーン - IA を選択します。 1 ゾーン - IAストレージクラスに保存されているオブジェクトには、30 日以内に上書き、削除、リクエスト、取得、またはストレージクラス間の移行を行うと、追加料金が発生する可能性があります。最小ストレージ期間は 30 日です。30 日より前にオブジェクトを削除した場合、残りの日数分のストレージ料金に相当する日割り料金が発生します。これらのオブジェクトを変更する頻度、これらのオブジェクトを保持する期間、およびオブジェクトへの必要なアクセス頻度を検討します。128 KB 未満のオブジェクトには 128 KB 分の料金が課金され、早期削除料金が適用されます。 所有者、タイムスタンプ、アクセス許可、ACL などのメタデータを更新するファイルオペレーションがファイルゲートウェイによって管理されるファイルに対して実行されると、既存のオブジェクトが削除され、この Amazon S3 ストレージクラスにオブジェクトの新しいバージョンが作成されます。早期削除料金が適用されるため、このストレージクラスを本番環境で使用する前に、ファイルオペレーションがオブジェクトの作成にどのように影響するかを検証する必要があります。詳細については、「Amazon S3 の料金」を参照してください。

オブジェクトをファイル共有から S3 標準 -IA、S3 1 ゾーン - IA、または S3 Intelligent-Tiering ストレージクラスに直接書き込むこともできますが、特にアーカイブ後 30 日以内にオブジェクトを更新または削除する可能性がある場合は、ファイル共有から直接書き込むのではなく、ライフサイクルポ

リシーを使用してオブジェクトを移行することをお勧めします。ライフサイクルポリシーの詳細については、「オブジェクトのライフサイクル管理」を参照してください。

ファイルゲートウェイで GLACIER ストレージクラスを使用する

Amazon S3 のライフサイクルポリシーによってファイルを Amazon Glacier に移行する場合で、ファイルがファイル共有クライアントにキャッシュを介して参照可能である場合、ファイルを更新するときに I/O エラーが発生します。これらの I/O エラーが発生したときに通知を受け取れるように CloudWatch Events を設定し、その通知を使ってアクションを実行することをお勧めします。たとえば、アーカイブされたオブジェクトを Amazon S3 に復元するアクションを実行することができます。オブジェクトが S3 に復元された後、ファイル共有クライアントはファイル共有を介してオブジェクトに正常にアクセスして更新することができます。

アーカイブされたオブジェクトの復元の詳細については、「Amazon Simple Storage Service ユーザーガイド」の「アーカイブされたオブジェクトの復元」を参照してください。

> **Important**
>
> S3 ファイルゲートウェイは、S3 Glacier Instant Retrieval ストレージクラスを公式にサポートしていません。ライフサイクルポリシーまたは直接 PUT のリクエストを使用して、S3 Glacier Instant Retrieval のファイル共有バケット内のオブジェクトを指定できますが、S3 ファイルゲートウェイはそのストレージクラスにあるファイルを認識できず、他のオブジェクトと同様にファイルオペレーションを実行します。S3 Glacier Instant Retrieval は他の Amazon S3 ストレージクラスよりもアクセスコストが高いため、ウイルススキャン、`rsync`、名前変更などの一括ファイル操作では、慎重に管理しないと Amazon S3 の請求書が大きくなる可能性があります。このため、S3 ファイルゲートウェイで S3 Glacier Instant Retrieval を使用することはお勧めしません。

Kubernetes コンテナストレージインターフェイスドライバーの使用

Kubernetes は、コンテナ化されたアプリケーションのデプロイ、スケーリング、および管理を自動化するためのオープンソースシステムです。Kubernetes 環境では、コンテナは VM に似ていますが、アプリケーション間でオペレーティングシステム (OS) を共有できるよう、コンテナの分離レベルは緩くなっています。したがって、コンテナは VM よりも軽量であると見なされます。VM と同様に、コンテナには独自のファイルシステムがあり、CPU、メモリ、プロセススペースなどのリソー

スが割り当てられています。これらは基盤となるインフラストラクチャから切り離されるため、クラウドや OS ディストリビューション間で移植可能です。Kubernetes クラスターがある場合は、クラスター内のインスタンス全体に Kubernetes Container Storage Interface (CSI) ドライバーをインストールして設定し、既存の Amazon S3 ファイルゲートウェイをストレージとして使用できるようにします。

使用するファイル共有タイプの CSI ドライバーをインストールしたら、1 つ以上のストレージオブジェクトを作成する必要があります。ポッドがストレージをリクエストするときに Kubernetes で使用するプロビジョニングのタイプに応じて、単一の Kubernetes `StorageClass` オブジェクトを作成するか、Kubernetes コンピューティングポッドをファイル共有に接続するための `PersistentVolume` オブジェクトおよび `PersistentVolumeClaim` オブジェクトの両方を作成する必要があります。詳細については、https://kubernetes.io/docs/concepts/storage/ で Kubernetes オンラインドキュメントを参照してください。

トピック

SMB CSI ドライバーの使用

このセクションの手順に従って、Kubernetes クラスターのストレージに Amazon S3 ファイルゲートウェイで SMB ファイル共有を使用するために必要な CSI ドライバーをインストール、設定、または削除します。詳細については、https://github.com/kubernetes-csi/csi-driver-smb/blob/master/docs/install-csi-driver-master.md で、GitHub 上のオープンソース SMB CSI ドライバーのドキュメントを参照してください。

> **Note**
>
> `PersistentVolume` オブジェクトまたは `StorageClass` オブジェクトを作成するときに、`ReclaimPolicy` パラメータを指定して、オブジェクトが削除されたときに外部ストレージがどうなるかを決定できます。SMB CSI ドライバーは `Retain` および `Recycle` オプションをサポートしていますが、現在 `Delete` オプションをサポートしていません。

ドライバーのインストール

Kubernetes SMB CSI ドライバーをインストールするには:

1. Kubernetes クラスターの `kubectl` にアクセスできるコマンドラインターミナルから、次のコマンドを実行します。

   curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-smb/master/deploy/install-driver.sh | bash -s master --

2. 前のコマンドが終了するのを待ってから、次のコマンドを使用して CSI ドライバーポッドが実行されていることを確認します。

   kubectl -n kube-system get pod -o wide --watch -l app=csi-smb-controller

   kubectl -n kube-system get pod -o wide --watch -l app=csi-smb-node

   出力は次の例に類似したものになります:

```
NAME                                 READY   STATUS    RESTARTS   AGE     IP
            NODE
csi-smb-controller-56bfddd689-dh5tk  4/4     Running   0          35s
 10.240.0.19    k8s-agentpool-22533604-0
csi-smb-controller-56bfddd689-8pgr4  4/4     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
csi-smb-node-cvgbs                   3/3     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
csi-smb-node-dr4s4                   3/3     Running   0          35s
 10.240.0.4     k8s-agentpool-22533604-0
```

SMB StorageClass オブジェクトを作成する

Kubernetes クラスターの新しい SMB StorageClass オブジェクトを作成するには:

1. `storageclass.yaml` という名の設定ファイルを作成し、次の例と同様の内容を記述します。表示されている *`ExampleValues`* を、デプロイ固有の情報に置き換えます。

```
---
apiVersion: storage.k8s.io/v1
```

```
kind: StorageClass
metadata:
    name: ExampleStorageClassName
provisioner: smb.csi.k8s.io
parameters:
    source: "//gateway-dns-name-or-ip-address/example-share-name"
    # if csi.storage.k8s.io/provisioner-secret is provided, will create a sub
 directory
    # with PV name under source
    csi.storage.k8s.io/provisioner-secret-name: "examplesmbcreds"
    csi.storage.k8s.io/provisioner-secret-namespace: "examplenamespace"
    csi.storage.k8s.io/node-stage-secret-name: "examplesmbcreds"
    csi.storage.k8s.io/node-stage-secret-namespace: "examplenamespace"
volumeBindingMode: Immediate
reclaimPolicy: Retain
mountOptions:
    - dir_mode=0777
    - file_mode=0777
    - uid=1001
    - gid=1001
```

2. kubectl および storageclass.yaml にアクセスできるコマンドラインターミナルから、次のコマンドを実行します。

   kubectl apply -f storageclass.yaml

   > **Note**
   >
   > 前の手順の .yaml 設定テキストをほとんどのサードパーティ製 Kubernetes 管理およびコンテナ化プラットフォームに提供することで、StorageClass を作成することもできます。

3. 作成した新しい StorageClass を使用するように Kubernetes クラスターのポッドを設定します。詳細については、https://kubernetes.io/docs/concepts/storage/ で Kubernetes オンラインドキュメントを参照してください。

SMB PersistentVolume オブジェクトと PersistentVolumeClaim オブジェクトを作成する

新しい SMB PersistentVolume オブジェクトと PersistentVolumeClaim オブジェクトを作成するには:

1. 2つの設定ファイルを作成します。1 つは `persistentvolume.yaml`、もう 1 つは `persistentvolumeclaim.yaml` という名前にします。
2. `persistentvolume.yaml` には、次の例のようなコンテンツを追加します。表示されている *`ExampleValues`* を、デプロイ固有の情報に置き換えます。

```
---
apiVersion: v1
kind: PersistentVolume
metadata:
    name: pv-smb-example-name
    namespace: smb-example-namespace # PersistentVolume and PersistentVolumeClaim
 must use the same namespace parameter
spec:
    capacity:
        storage: 100Gi
    accessModes:
        - ReadWriteMany
    persistentVolumeReclaimPolicy: Retain
    mountOptions:
        - dir_mode=0777
        - file_mode=0777
        - vers=3.0
    csi:
        driver: smb.csi.k8s.io
        readOnly: false
        volumeHandle: examplehandle  # make sure it's a unique id in the cluster
        volumeAttributes:
            source: "//gateway-dns-name-or-ip-address/example-share-name"
        nodeStageSecretRef:
            name: example-smbcreds
            namespace: smb-example-namespace
```

3. `persistentvolumeclaim.yaml` には、次の例のようなコンテンツを追加します。表示されている *`ExampleValues`* を、デプロイ固有の情報に置き換えます。

```
---
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
    name: examplename-pvc-smb-static
    namespace: smb-example-namespace # PersistentVolume and PersistentVolumeClaim
 must use the same namespace parameter
spec:
    accessModes:
        - ReadWriteMany
    resources:
        requests:
            storage: 10Gi
        volumeName: pv-smb-example-name # make sure specfied volumeName matches the
 name of the PersistentVolume you created
        storageClassName: ""
```

4. kubectl および作成した2つの .yaml ファイルにアクセスできるコマンドラインターミナルから、次のコマンドを実行します。

   kubectl apply -f persistentvolume.yaml

   kubectl apply -f persistentvolumeclaim.yaml

   > **Note**
   >
   > 前の手順の .yaml 設定テキストを、ほとんどのサードパーティ製 Kubernetes 管理およびコンテナ化プラットフォームに提供することで、PersistentVolume オブジェクトと PersistentVolumeClaim オブジェクトを作成することもできます。

5. 作成した新しい PersistentVolumeClaim を使用するように Kubernetes クラスターのポッドを設定します。詳細については、https://kubernetes.io/docs/concepts/storage/ で Kubernetes オンラインドキュメントを参照してください。

ドライバーのアンインストール

Kubernetes SMB CSI ドライバーをアンインストールするには:

- Kubernetes クラスターの `kubectl` にアクセスできるコマンドラインターミナルから、次のコマンドを実行します。

  curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-smb/master/deploy/uninstall-driver.sh | bash -s --

NFS CSI ドライバーの使用

このセクションの手順に従って、Kubernetes クラスターのストレージに Amazon S3 ファイルゲートウェイで NFS ファイル共有を使用するために必要な CSI ドライバーをインストール、設定、または削除します。詳細については、https://github.com/kubernetes-csi/csi-driver-nfs/blob/master/docs/install-csi-driver-master.md の GitHub にあるオープンソースの NFS CSI ドライバードキュメントを参照してください。

ドライバーのインストール

Kubernetes NFS CSI ドライバーをインストールするには:

1. Kubernetes クラスターの `kubectl` にアクセスできるコマンドラインターミナルから、次のコマンドを実行します。

   curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-nfs/master/deploy/install-driver.sh | bash -s master --

2. 前のコマンドが終了するのを待ってから、次のコマンドを使用して CSI ドライバーポッドが実行されていることを確認します。

   kubectl -n kube-system get pod -o wide -l app=csi-nfs-controller

   kubectl -n kube-system get pod -o wide -l app=csi-nfs-node

   出力は次の例に類似したものになります:

```
NAME                                  READY   STATUS    RESTARTS   AGE     IP
            NODE
```

```
csi-nfs-controller-56bfddd689-dh5tk        4/4     Running   0          35s
 10.240.0.19    k8s-agentpool-22533604-0
csi-nfs-controller-56bfddd689-8pgr4        4/4     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
csi-nfs-node-cvgbs                         3/3     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
csi-nfs-node-dr4s4                         3/3     Running   0          35s
 10.240.0.4     k8s-agentpool-22533604-0
```

NFS StorageClass オブジェクトを作成する

Kubernetes クラスターの NFS StorageClass オブジェクトを作成するには:

1. storageclass.yaml という名前の設定ファイルを作成し、次の例と同様の内容を記述します。表示されている *ExampleValues* を、デプロイ固有の情報に置き換えます。

```
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
    name: example-nfs-classname
    namespace: example-namespace
provisioner: nfs.csi.k8s.io
parameters:
    server: gateway-dns-name-or-ip-address
    share: /example-share-name
reclaimPolicy: Retain
volumeBindingMode: Immediate
mountOptions:
    - hard
    - nfsvers=4.1
```

2. kubectl および storageclass.yaml にアクセスできるコマンドラインターミナルから、次のコマンドを実行します。

   kubectl apply -f storageclass.yaml

> **Note**
>
> 前の手順の `.yaml` 設定テキストをほとんどのサードパーティ製 Kubernetes 管理およびコンテナ化プラットフォームに提供することで、StorageClass を作成することもできます。

3. 作成した新しい StorageClass オブジェクトを使用するように、Kubernetes クラスターのポッドを設定します。詳細については、https://kubernetes.io/docs/concepts/storage/ で Kubernetes オンラインドキュメントを参照してください。

NFS PersistentVolume オブジェクトと PersistentVolumeClaim オブジェクトを作成する

新しい NFS PersistentVolume オブジェクトと PersistentVolumeClaim オブジェクトを作成するには:

1. `persistentvolume.yaml` と `persistentvolumeclaim.yaml` という名前の 2 つの設定ファイルを作成します。
2. `persistentvolume.yaml` には、次の例のようなコンテンツを追加します。表示されている *`ExampleValues`* を、デプロイ固有の情報に置き換えます。

```
---
apiVersion: v1
kind: PersistentVolume
metadata:
    name: pv-nfs-examplename
spec:
    capacity:
        storage: 10Gi
    accessModes:
        - ReadWriteMany
    persistentVolumeReclaimPolicy: Retain
    mountOptions:
        - hard
        - nolock
        - nfsvers=4.1
    csi:
        driver: nfs.csi.k8s.io
        readOnly: false
```

```
        volumeHandle: unique-volumeid-example # make sure it's a unique id in the
 cluster
        volumeAttributes:
            server: gateway-dns-name-or-ip-address
            share: /example-share-name
```

3. persistentvolumeclaim.yaml には、次の例のようなコンテンツを追加します。表示されている *ExampleValues* を、デプロイ固有の情報に置き換えます。

```
---
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
    name: examplename-pvc-nfs-static
spec:
    accessModes:
        - ReadWriteMany
    resources:
        requests:
            storage: 10Gi
    volumeName: pv-nfs-examplename # make sure specfied volumeName matches the name
 of the PersistentVolume you created
    storageClassName: ""
```

4. kubectl および 2 つの .yaml ファイルにアクセスできるコマンドラインターミナルから、次のコマンドを実行します。

   kubectl apply -f persistentvolume.yaml

   kubectl apply -f persistentvolumeclaim.yaml

> **Note**
>
> 前の手順の .yaml 設定テキストを、ほとんどのサードパーティ製 Kubernetes 管理およびコンテナ化プラットフォームに提供することで、PersistentVolume オブジェクトと PersistentVolumeClaim オブジェクトを作成することもできます。

5. 作成した新しい PersistentVolumeClaim オブジェクトを使用するように Kubernetes クラスターのポッドを設定します。詳細については、https://kubernetes.io/docs/concepts/storage/ で Kubernetes オンラインドキュメントを参照してください。

ドライバーのアンインストール

Kubernetes NFS CSI ドライバーをアンインストールするには:

- Kubernetes クラスターの `kubectl`にアクセスできるコマンドラインターミナルから、次のコマンドを実行します。

  curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-nfs/master/deploy/uninstall-driver.sh | bash -s master --

AWS Storage Gateway Terraform モジュール

HashiCorpTerraform は、HashiCorp Configuration Language (HCL)を使用して開発されたオープンソースの Infrastructure as Code (IaC) エンジンです。Terraform は、一貫したコマンドラインインターフェイス (CLI) ワークフローを提供します。このワークフローにより、バックエンドインフラストラクチャとして Amazon S3 ファイルゲートウェイを組み合わせて、数百に及ぶクラウドサービスを管理し、クラウド API を宣言型の構成ファイルとしてコード化できます。

Terraform を使用して、Amazon S3 ファイルゲートウェイをオンプレミスの仮想インフラストラクチャに仮想マシン (VM) として安全にデプロイできます。Terraform は、オンプレミスの仮想インフラストラクチャの自動化します。オンプレミスの VMware 仮想環境で Terraform を使用して Amazon S3 ファイルゲートウェイを迅速にデプロイする方法については、「Automate Amazon S3 ファイルゲートウェイdeployments in VMware with Terraform by HashiCorp」を参照してください。

> **Note**
>
> 希望するハイパーバイザープラットフォームの AWS Storage Gateway マシンイメージの最新バージョンを取得するように Terraform を設定する必要がある場合があります。Storage Gateway マシンイメージでは、次の命名規則を使用します。画像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_S3-1.25.0`

この自動化では、VM 環境にゲートウェイとファイル共有を完全にデプロイするために必要なすべてのリソースと依存関係を含む Amazon S3 ファイルゲートウェイをプロビジョニングする、カスタマイズ可能な Terraform モジュールが提供されます。Terraform モジュールは、ゲートウェイ VM をプロビジョニングし、ゲートウェイをアクティブ化し、キャッシュディスクを設定し、ゲートウェイをドメインに参加させ、Amazon S3 バケットを作成し、ファイル共有を作成してそれらをバケッ

トにマッピングします。オンプレミスで Amazon S3 ファイルゲートウェイを実行するために必要なリソースを作成する Terraform コードを含むリポジトリの完全なサンプルについては、GitHub の Terraform Storage Gateway モジュールのソースコードを参照してください。

> **Note**
>
> Terraform 用の Amazon S3 ファイルゲートウェイモジュールは、コミュニティによってサポートされている取り組みです。これは AWS サービスの一部ではありません。ベストエフォートサポートは AWS Storage コミュニティによって提供されます。

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 S3 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
IPv6 サポート	IPv6 サポートは、ゲートウェイアプライアンスバージョン 2.x 以降で使用できます。	2025 年 9 月 10 日
スループットと最適化のガイダンスを追加	パフォーマンスと最適化の章には、S3 ファイルゲートウェイのスループットを最大化し、SQL Server データベースバックアップのユースケースのデプロイを最適化するための推奨事項とベストプラクティスが含まれています。詳細については、「S3 ファイルゲートウェイスループットの最大化」および「S3 ファイルゲートウェイfor SQL Server データベースバックアップの最適化」を参照してください。	2025 年 6 月 13 日
キャッシュレポート機能を追加	S3 ファイルゲートウェイは、特定のファイル共有のローカルアップロードキャッシュに現在含まれているファイルについて、メタデータのレポートを生成できるようになりました。詳細については、「S3 ファイルゲートウェイ	2025 年 3 月 31 日

	のキャッシュレポートの作成」、「S3 ファイルゲートウェイのキャッシュレポートの表示と管理」、および「S3 ファイルゲートウェイキャッシュレポートで提供される情報について」を参照してください。	
AWS KMS キーによる二層式サーバー側の暗号化のサポートを追加 (DSSE-KMS)	AWS KMS キーによる二層式サーバー側の暗号化を使用して、S3 File Gateway が Amazon S3 にアップロードするファイルを暗号化できるようになりました。DSSE-KMS の詳細については、「Amazon S3 のファイルゲートウェイに保存されたオブジェクトを暗号化する」を参照してください。	2024 年 9 月 13 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 AWS Storage Gateway コンソール。	2024 年 6 月 6 日

新しい SMB セキュリティレベルを追加	S3 ファイルゲートウェイでは、SMB クライアント接続の 256 ビット AES 暗号化に使用できる、追加のセキュリティレベルをサポートするようになりました。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。	2024 年 5 月 23 日
S3 ファイルゲートウェイのゲートウェイアプライアンスソフトウェアバージョンレポートとリリースノート	Amazon S3 ファイルゲートウェイアプライアンスの各バージョンに含まれる新機能と更新された機能、改善点、修正点について説明するリリースノートを追加しました。Storage Gateway コンソールまたは AWS CLIを使用して、ゲートウェイのソフトウェアバージョン番号を確認できます。詳細については、「リリースノート — ゲートウェイアプライアンスソフトウェア」を参照してください。	2023 年 10 月 5 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
ゲートウェイあたりの最大ファイル共有数の増加	S3 ファイルゲートウェイは、ゲートウェイあたり最大 50 のファイル共有をサポートするようになりました。これは、以前の制限である 10 から増加しています。これにより、1 つのゲートウェイで作成できるファイル共有を増やし、管理する必要があるゲートウェイの数を減らすことができます。詳細については、「ファイル共有のクォータ」を参照してください。	2023 年 1 月 18 日

DOS 属性のサポートを追加	S3 ファイルゲートウェイは、Amazon S3 に保存されているファイルの DOS 属性をサポートするようになりました。これにより、ユーザーは、ファイルが Amazon S3 にアップロードされたときに、読み取り専用、非表示、システム、アーカイブなどの Windows ファイル属性を保持できます。詳細については、「Amazon S3 ファイルゲートウェイでのファイル属性のサポート」を参照してください。	2023 年 1 月 18 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

スケジュールベースのネットワーク帯域幅のスロットリングの追加	S3 ファイルゲートウェイは、Amazon S3 へのデータアップロードのスケジュールベースのネットワーク帯域幅スロットリングをサポートするようになりました。この機能を使用すると、ゲートウェイが特定の期間に使用するネットワーク帯域幅の量を制限できるため、ピーク時のネットワーク使用量を管理できます。詳細については、「S3 ファイルゲートウェイの帯域幅の管理」を参照してください。	2022 年 1 月 18 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

SMB ファイル共有でのファイルの強制終了のサポート	ローカルグループ設定を使用して、ゲートウェイ管理者のアクセス許可を割り当てられるようになりました。ゲートウェイ管理者は、共有フォルダ Microsoft マネジメントコンソールスナップインを使用して、SMB ファイル共有で開いてロックされているファイルを強制的に閉じることができます。詳細については、「ゲートウェイのローカルグループを設定する」を参照してください。	2021 年 10 月 12 日
NFS ファイル共有の監査ログのサポート	NFS ファイル共有を設定して、ファイル共有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する監査ログを生成できるようになりました。これらのログを使用して、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。詳細については、「ファイルゲートウェイの監査ログについて」を参照してください。	2021 年 10 月 12 日

アクセスポイントエイリアスのサポート	ファイルゲートウェイのファイル共有は、バケットスタイルのアクセスポイントエイリアスを使用して Amazon S3 ストレージに接続できるようになりました。詳細については、「ファイル共有の作成」を参照してください。	2021 年 10 月 12 日
VPC エンドポイントとアクセスポイントのサポート	ファイルゲートウェイのファイル共有は、 AWS PrivateLinkを使用する VPC 内のアクセスポイントまたはインターフェイスエンドポイントを介して S3 バケットに接続できるようになりました。詳細については、「ファイル共有の作成」を参照してください。	2021 年 7 月 7 日
日和見ロックのサポート	ファイルゲートウェイのファイル共有では、ファイル共有で日和見ロックを使用してファイルバッファリングにおける戦略を最適化できるようになりました。これにより、ほとんどの場合、特に Windows のコンテキストメニューに関するパフォーマンスが向上します。詳細については、「SMB ファイル共有の作成」を参照してください。	2021 年 7 月 7 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でのファイルのアップロード通知	ファイルゲートウェイで、ファイルのアップロード通知が利用できるようになりました。これにより、ファイルゲートウェイによりファイルが完全に Amazon S3 にアップロードされたときに通知が送信されます。詳細については、「ファイルのアップロード通知の受け取り」を参照してください。	2020 年 11 月 9 日
ファイルゲートウェイでのアクセスベースの列挙	ファイルゲートウェイで、アクセスベースの列挙が利用できるようになりました。これにより、共有の ACL に基づいて SMB ファイル共有上のファイルとフォルダの列挙をフィルタリングできます。詳細については、「SMB ファイル共有の作成」を参照してください。	2020 年 11 月 9 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

単一の Amazon S3 バケットにアタッチされた複数のファイル共有のサポート	ファイルゲートウェイで、単一の S3 バケットに対して複数のファイル共有を作成し、ディレクトリアクセスの頻度に基づいてファイルゲートウェイのローカルキャッシュをバケットと同期できるようになりました。必要なバケットの数を制限して、ファイルゲートウェイで作成するファイル共有を管理できます。S3 バケット用に複数の S3 プレフィックスを定義して、単一の S3 プレフィックスを単一のゲートウェイのファイル共有にマッピングできます。また、オンプレミスのファイル共有の命名規則に適合するように、ゲートウェイのファイル共有名をバケット名から独立したものとして定義することもできます。詳細については、「NFS ファイル共有の作成」または「SMB ファイル共有の作成」を参照してください。	2020 年 7 月 7 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

SMB ファイル共有の Microsoft Windows ACL SMB サポート	ファイルゲートウェイの場合、Microsoft Windows アクセスコントロールリスト (ACL) を使用して、サーバーメッセージブロック (SMB) ファイル共有へのアクセスを制御できるようになりました。詳細については、「Microsoft Windows ACL を使用して、SMB ファイル共有へのアクセスを制御する」を参照してください。	2019 年 5 月 8 日
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
サーバーメッセージブロック (SMB) プロトコルのサポート	ファイルゲートウェイで、ファイル共有にサーバーメッセージブロック (SMB) プロトコルを使用できるようになりました。詳細については、「ファイル共有の作成」を参照してください。	2018 年 6 月 20 日

以前の更新

以下の表に、2018 年 5 月より前の「AWS Storage Gateway ユーザーガイド」の各リリースにおける重要な変更点を示します。

変更	説明	変更日
S3 1 ゾーン IA ストレージクラスのサポート	ファイルゲートウェイで、S3 1 ゾーン IA をファイル共有のデフォルトのストレージクラスとして選択できるようになりました。このストレージクラスを使用すると、Amazon S3 の単一のアベイラビリティーゾー	2018 年 4 月 4 日

変更	説明	変更日
	ン (AZ) にオブジェクトデータを保存できます。詳細については、「ファイル共有の作成」を参照してください。	
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
キャッシュの更新通知、リクエスタ支払いおよび Amazon S3 バケットの固定 ACL のサポート。	ファイルゲートウェイで、ゲートウェイによる Amazon S3 バケットのキャッシュの更新が完了したときに、通知を受けることができるようになりました。詳細については、Storage Gateway API リファレンスの「RefreshCache.html」を参照してください。 ファイルゲートウェイでは、バケット所有者ではなくリクエスタまたはリーダーがアクセス料金を支払うように指定できるようになりました。 ファイルゲートウェイでは、NFS ファイル共有にマップされる S3 バケットの所有者に、書き込まれたファイルの完全な制御権を与えることができるようになりました。 詳細については、「ファイル共有の作成」を参照してください。	2018 年 3 月 1 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

変更	説明	変更日
ファイルアップロード通知と多目的インターネットメール拡張 (MIME) タイプの推測のサポート	ファイルゲートウェイで、NFS ファイル共有に書き込まれたすべてのファイルが Amazon S3 にアップロードされたときに通知を送信できるようになりました。詳細については、Storage Gateway API リファレンスの「NotifyWhenUploaded」を参照してください。 ファイルゲートウェイを使用して、アップロードされたオブジェクトの MIME タイプをファイルの拡張子に基づいて推測できるようになりました。詳細については、「ファイル共有の作成」を参照してください。	2017 年 11 月 21 日
VMware ESXi Hypervisor バージョン 6.5 のサポート	AWS Storage Gateway で VMware ESXi Hypervisor バージョン 6.5 がサポートされるようになりました。これは、バージョン 4.1、5.0、5.1、5.5、および 6.0 に加えてサポートされます。詳細については、「サポートされているハイパーバイザーとホストの要件」を参照してください。	2017 年 9 月 13 日
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

変更	説明	変更日
ファイル共有の設定を更新 ファイル共有のためのキャッシュ更新のサポート	ファイルゲートウェイで、ファイル共有の設定にマウントオプションが追加されました。ファイル共有に squash と読み取り専用オプションを設定できるようになりました。詳細については、「ファイル共有の作成」を参照してください。 ファイルゲートウェイで、最後にバケットのコンテンツのリストが取得され、その結果がキャッシュに保存された時点以降に Amazon S3 バケットに追加または削除されたオブジェクトを、検出できるようになりました。詳細については、API リファレンスの「RefreshCache」を参照してください。	2017 年 3 月 28 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 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。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、「S3 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

Storage Gateway AL2 から AL2023 への移行キャンペーン

AWSは、Storage Gateway アプライアンスオペレーティングシステム (OS) を Amazon Linux 2 から AL2023 に移行して、新しいハイブリッドクラウドストレージ機能を有効にし、最適なパフォーマンスとセキュリティ標準を維持します。この移行は、すべての AL2-based Storage Gateway アプライアンスバージョン S3 ファイルゲートウェイバージョン 1.x、テープゲートウェイバージョン 2.x、ボリュームゲートウェイバージョン 2.x に影響します。2026 年 6 月 30 日までに移行を完了する必要があります。その後、 AWSはこれらのシステムのサポートを終了します。

複数の方法でゲートウェイを移行する必要があるかどうかを特定できます。AWSコンソールは、影響を受けるゲートウェイのゲートウェイの詳細タブに非推奨メッセージを表示します。さらに、`DescribeGatewayInformation` API は、非推奨の日付フィールドをチェックするためのプログラムによるアクセスを提供します。AWSHealth Dashboard は、影響を受けるリソースタブの影響を受けるゲートウェイを一覧表示します。ただし、ゲートウェイが移行された直後にリストは更新されません。移行プロセス自体は、データの安全性を優先して設計されており、AWS移行を開始する前にオンプレミスゲートウェイ VM データのコピーを に保存し、必要に応じて簡単に復旧できるようにします。

AWSは、各ゲートウェイタイプに固有の包括的な移行ガイドを提供します。移行が完了したら、AWSコンソールのゲートウェイの詳細タブに非推奨の警告が表示されなくなったことを確認するか、 `DescribeGatewayInformation` API を使用して非推奨の日付フィールドがないことを確認することで、成功を検証する必要があります。AL20AL23 に正常に移行した後は、AL2 ゲートウェイに戻さないでください。元に戻すと運用上の問題が発生する可能性があります。 AL2023

移行期間中、 AWSは毎月リマインダー通知を E メールで送信し、AWSヘルスダッシュボードのスケジュールされた変更タブは移行の計画と完了に役立ちます。移行中に問題が発生した場合は、AWSサポートに連絡してサポートとトラブルシューティングのガイダンスを依頼してください。

クイックリンクとリソース

ゲートウェイバージョン移行リファレンス

移行が必要なゲートウェイは、ゲートウェイソフトウェアのバージョン番号に基づいて簡単に理解できます。Amazon Linux 2 OS に基づく最近アクティブ化されたゲートウェイでも、2026 年 6 月 30 日までに移行する必要があることに注意してください。

ゲートウェイタイプ	AL2 バージョン (移行が必要)	AL2023 バージョン (ターゲット)
S3 ファイルゲートウェイ	バージョン 1.x	バージョン 2.x
テープゲートウェイ	バージョン 2.x	バージョン 3.x
ボリュームゲートウェイ	バージョン 2.x	バージョン 3.x

移行タイムライン

移行タイムラインには、いくつかの重要なマイルストーンが含まれています。

- 2025 年 10 月 28 日: Storage Gateway コンソールから開始されたすべての新しいゲートウェイデプロイは、デフォルトで AL2023 イメージになります。
- 2026 年 1 月 5 日:AWS は新しい AL2 ゲートウェイのアクティベーションの制限を開始します。
- 2026 年 6 月 30 日: AL2-basedゲートウェイはソフトウェア更新の受信を停止し、AWSサポートは終了します。この日以降は、AL2-basedアプライアンスを引き続き使用できますが、新しいソフトウェア更新、セキュリティパッチ、またはバグ修正は行われず、これらのシステムを維持することはお客様の責任となります。

移行前チェックリスト

> **Important**
>
> 移行プロセスを開始する前に、次の要件を確認して、移行が成功していることを確認します。

- 最新のゲートウェイイメージを使用します。新しい Storage Gateway VM を作成する場合:
  - Amazon EC2 ゲートウェイの場合は、パブリック SSM パラメータから最新の AMI を使用するか、Storage Gateway コンソールを使用します。
  - オンプレミスゲートウェイの場合は、Storage Gateway コンソールから最新の VM イメージをダウンロードします。

- ハードウェア設定を一致させます。新しいゲートウェイ VM が既存のゲートウェイと同じ CPU、メモリ、ネットワークスループットを使用していることを確認します。EC2 ゲートウェイの場合は、同じインスタンスタイプを使用します。
- ルートディスクのサイズを確認します。新しいゲートウェイ VM のルートディスクは、既存のゲートウェイのルートディスクと少なくとも同じサイズである必要があります。既存のルートディスクの使用可能な容量が 20 GB 未満の場合は、新しいルートディスクのサイズを (既存のルートディスクサイズ) + (20 GB から既存のルートディスクの使用可能な容量を引いた値) に設定します。
- 保留中のソフトウェア更新を適用します。移行を開始する前に、保留中のソフトウェア更新を既存のゲートウェイに適用します。Storage Gateway コンソールを開き、ゲートウェイを選択し、利用可能な場合は今すぐ更新を選択します。
- 新しいゲートウェイからのネットワーク接続を確認します。移行を開始する前に、新しいゲートウェイ VM が以下に到達できることを確認します。
  - Storage Gateway サービスエンドポイント (または VPC エンドポイント) 。
  - Amazon S3 エンドポイント。
  - Active Directory/DNS サーバー (ゲートウェイがドメインに参加している場合) 。
  - ゲートウェイローカルコンソールのネットワーク接続テストを使用して、すべてのエンドポイントが合格したことを検証します。
- ファイルのアップロードの失敗を解決します。移行を開始する前に、ゲートウェイの `FilesFailingUpload` CloudWatch メトリクスがゼロであることを確認します。失敗状態のファイルは、最初に対処する必要がある未解決のエラーを示します。影響を受けるファイルを特定するには、キャッシュレポートを作成し、次に進む前に根本的な問題を解決します。
- キャッシュが同期するのを待ちます。 ゲートウェイの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ます。これにより、キャッシュされたすべてのデータが S3 にアップロードされたことが確認されます。

移行ガイド

- S3 ファイルゲートウェイ移行ガイド
- テープゲートウェイ移行ガイド
- ボリュームゲートウェイ移行ガイド

サポートとモニタリング

- Storage Gateway コンソール
- AWSPersonal Health ダッシュボード
- AWSサポートへのお問い合わせ

よくある質問

移行中にデータはどうなりますか?

データは移行プロセスAWS全体を通して に永続的に保存されます。移行手順には、必要に応じて簡単に復旧AWSできるように、オンプレミスゲートウェイ VM データのコピーを に保存することが含まれます。

移行中にダウンタイムはありますか?

移行のタイミングとサービスの中断の可能性は、ゲートウェイのタイプと設定によって異なります。詳細については、デプロイのゲートウェイ固有の移行ガイドを参照してください。

2026 年 6 月 30 日までに移行しなかった場合はどうなりますか?

ゲートウェイは通常どおり動作し、データは に安全に保存されますがAWS、更新とサポートを受け続けるには、影響を受けるゲートウェイを 2026 年 6 月 30 日までに移行する必要があります。

移行後も AL2 ベースのゲートウェイを引き続き使用できますか?

いいえ。正常に移行した後は、新しい AL2023 ゲートウェイと一緒に AL2 ゲートウェイを使用しないでください。今後は、新しい AL2023-basedゲートウェイのみを使用してください。AL2 ゲートウェイと AL2023 ゲートウェイの両方を同時に使用すると、運用上の問題が発生する可能性があります。

移行中に問題が発生しています。どうすればよいですか?

サポートが必要な場合は、 AWSサポートにお問い合わせください。サポートチームは、移行に関する問題のトラブルシューティングを支援し、プロセスを案内します。

ゲートウェイアプライアンスソフトウェアのリリースノート

これらのリリースノートでは、Amazon S3 ファイルゲートウェイアプライアンスの各バージョンに含まれる新機能と更新された機能、改善点、修正点について説明します。各ソフトウェアバージョンは、リリース日と一意のバージョン番号によって識別されます。

Storage Gateway コンソールで詳細ページを確認するか、次のような AWS CLI コマンドを使用して DescribeGatewayInformation API アクションを呼び出すことで、ゲートウェイのソフトウェアバージョン番号を確認できます。

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

バージョン番号は API レスポンスの `SoftwareVersion` フィールドで返されます。

> **Note**
>
> 次の状況では、ゲートウェイはソフトウェアバージョン情報を報告しません。
>
> - ゲートウェイはオフラインです。
> - ゲートウェイは、バージョンレポートをサポートしていない古いソフトウェアを実行しています。
> - ゲートウェイタイプは S3 ファイルゲートウェイではありません。

ゲートウェイのデフォルトの自動メンテナンスと更新スケジュールを変更する方法など、S3 ファイルゲートウェイの更新の詳細については、「ストレージゲートウェイコンソールを使用したゲートウェイ更新の管理 AWS Storage Gateway」を参照してください。

Amazon Linux 2 から AL2023 への S3 ファイルゲートウェイの移行の詳細については、「」を参照してくださいAL2 から AL2023 への移行。

Amazon Linux 2023 (AL2023) ベースのゲートウェイ

次の表に、AL2023 に基づくゲートウェイのリリースノートを示します。

> **Note**
>
> ゲートウェイバージョン 1.x.x を 2.x.x に更新することはできません。

リリース日	ソフトウェアのバージョン	リリースノート
2026-07-20	2.1.10	• セキュリティとパフォーマンスを向上させるために、オペレーティングシステムのコンポーネントとソフトウェアパッケージを更新します。 • キャッシュの実行が非常に低い場合に発生するゲートウェイの安定性の問題を修正しました。
2026-07-15	2.1.9	• セキュリティとパフォーマンスを向上させるために、オペレーティングシステムのコンポーネントとソフトウェアパッケージを更新します。
2026-06-16	2.1.8	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2026-05-21	2.1.7	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステム

リリース日	ソフトウェアのバージョン	リリースノート
		とソフトウェア要素を更新しました。
2026-05-14	2.1.6	メンテナンスアップデート： • 1.x から 2.x (AL2 から AL2023) への移行が改善されました。 • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2026-04-16	2.1.5	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。

リリース日	ソフトウェアのバージョン	リリースノート
2026-03-26	2.1.4	メンテナンスアップデート： **Note** このリリースでは、AD ドメインコントローラーの DCE/RPC Endpoint Mapper サービス (TCP ポート 135) へのより厳しい依存関係が導入されました。環境がこのポートのアウトバウンドトラフィックをブロックする場合は、接続の問題を回避するためにブロックを解除します。詳細については、「ファイルゲートウェイポートの要件」を参照してください。 • Active Directory ドメインコントローラーとゲートウェイ間のやり取りのために NTLM の非推奨を継続します。 • ネットワークの中断時の SMB スタックの耐障害性が向上しました。

リリース日	ソフトウェアのバージョン	リリースノート
2026-03-16	2.1.3	メンテナンスアップデート： • SMB トラフィックによる DNS の回復性が向上しました。 • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2026-03-02	2.0.7	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。

リリース日	ソフトウェアのバージョン	リリースノート
2026-02-12	2.1.2	メンテナンスアップデート： **Note** ロールアウトが一時停止されました。このリリースは、限定されたゲートウェイのセットにロールアウトされました。 • SMB 共有で Windows Explorer を使用する場合のセキュリティタブとクォータタブの欠落に関する問題を修正しました。 • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。

リリース日	ソフトウェアのバージョン	リリースノート
2026-02-02	2.1.1	メンテナンスアップデート： **Note** ロールアウトが一時停止されました。このリリースは、限定されたゲートウェイのセットにロールアウトされました。 • 大文字と小文字を区別しないファイルアクセスに関する SMB の問題を修正しました。 • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2026-01-21	2.0.6	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。

リリース日	ソフトウェアのバージョン	リリースノート
2026-01-16	2.1.0	メンテナンスアップデート： **Note** ロールアウトが一時停止されました。このリリースは、限定されたゲートウェイのセットにロールアウトされました。 • SMB スタックを更新しました。 • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2025-12-15	2.0.5	メンテナンスアップデート： • ルートディスクサイズメトリクスの問題を修正しました。 • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。

リリース日	ソフトウェアのバージョン	リリースノート
2025-11-12	2.0.4	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2025-11-12	2.0.4	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2025-10-15	2.0.3	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。

リリース日	ソフトウェアのバージョン	リリースノート
2025-09-15	2.0.2	メンテナンスアップデート： • ゲートウェイ容量の変更を妨げる問題を修正しました。 • UpdateSMBLocalGroups API の問題を修正しました。 • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2025-08-29	2.0.1	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。 • オンプレミスゲートウェイの初回リリース。
2025-08-21	2.0.0	特徴: • 新しいオペレーティングシステムの初回リリース。 • IPv6 のサポートの追加

Amazon Linux 2 (AL2) ベースのゲートウェイ

次の表に、AL2 に基づくゲートウェイのリリースノートを示します。

リリース日	ソフトウェアのバージョン	リリースノート
2026-07-20	1.28.10	Note このリリースは、限定されたゲートウェイのセットにロールアウトされました。 • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムのコンポーネントとソフトウェアパッケージを更新します。 • キャッシュの実行が非常に低い場合に発生するゲートウェイの安定性の問題を修正しました。
2026-07-15	1.28.9	Note このリリースは、限定されたゲートウェイのセットにロールアウトされました。 • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムのコンポーネントとソフトウェアパッケージを更新します。
2026-06-16	1.28.8	メンテナンスアップデート：

リリース日	ソフトウェアのバージョン	リリースノート
		• セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2026-05-26	1.28.7	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2026-05-18	1.28.6	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2026-04-16	1.28.5	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。

リリース日	ソフトウェアのバージョン	リリースノート
2026-03-26	1.28.4	メンテナンスアップデート： **Note** このリリースは、すでに 1.28 にあるゲートウェイでのみ使用できます。* **Note** このリリースでは、AD ドメインコントローラーの DCE/RPC Endpoint Mapper サービス (TCP ポート 135) へのより厳しい依存関係が導入されました。環境がこのポートのアウトバウンドトラフィックをブロックする場合は、接続の問題を回避するためにブロックを解除します。詳細については、「ファイルゲートウェイポートの要件」を参照してください。 • Active Directory ドメインコントローラーとゲートウェイ間のやり取りのために

リリース日	ソフトウェアのバージョン	リリースノート
		NTLM の非推奨を継続します。 • ネットワークの中断時の SMB スタックの耐障害性が向上しました。
2026-03-16	1.27.21	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2026-03-16	1.28.3	メンテナンスアップデート： **Note** このリリースは、すでに 1.28 にあるゲートウェイでのみ使用できます。* • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。

リリース日	ソフトウェアのバージョン	リリースノート
2026-02-27	1.27.20	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2026-02-11	1.28.2	メンテナンスアップデート： **Note** ロールアウトが一時停止されました。このリリースは、限定されたゲートウェイのセットにロールアウトされました。 • SMB 共有で Windows Explorer を使用する場合のセキュリティタブとクォータタブの欠落に関する問題を修正しました。 • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。

リリース日	ソフトウェアのバージョン	リリースノート
2026-02-02	1.28.1	メンテナンスアップデート： **Note** ロールアウトが一時停止されました。このリリースは、限定されたゲートウェイのセットにロールアウトされました。 • 大文字と小文字を区別しないファイルアクセスに関する SMB の問題を修正しました。 • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2026-01-21	1.27.19	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。

リリース日	ソフトウェアのバージョン	リリースノート
2026-01-16	1.28.0	メンテナンスアップデート： **Note** ロールアウトが一時停止されました。このリリースは、限定されたゲートウェイのセットにロールアウトされました。 • SMB スタックを更新しました。 • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2025-12-15	1.27.18	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2025-11-17	1.27.17	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。

リリース日	ソフトウェアのバージョン	リリースノート
2025-10-15	1.27.16	メンテナンスアップデート： • Upload Rename Order ログの問題を修正しました。 • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2025-09-22	1.27.15	メンテナンスアップデート： • Upload Rename Order ログの問題を修正しました。
2025-09-15	1.27.14	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2025-08-21	1.27.13	メンテナンスアップデート： • ゲートウェイのパフォーマンスに関するより深いインサイトを提供するために、システム統計とメトリクスを追加しました。

リリース日	ソフトウェアのバージョン	リリースノート
2025-08-18	1.27.12	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2025-08-11	1.27.11	メンテナンスアップデート： • 一部のゲートウェイの特定のファイルオペレーションでS3メタデータの更新に影響する問題を修正しました。
2025-07-15	1.27.10	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。 • ゲートウェイのUpload Rename Order口グに関連する問題を解決しました。

リリース日	ソフトウェアのバージョン	リリースノート
2025-06-23	1.27.9	メンテナンスアップデート： • ゲートウェイのUpload Rename Orderログに関連する問題を解決しました。 • 新しいゲートウェイの Upload Rename Order ログのアップロードを有効にしました。 • 正常にアップロードされなかったファイルの削除オペレーションをゲートウェイが正しく処理するように問題を修正しました。
2025-06-16	1.27.8	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。

リリース日	ソフトウェアのバージョン	リリースノート
2025-05-26	1.27.7	メンテナンスアップデート： • Rename Orderingに関する問題を解決しました。 Note この問題は一部のゲートウェイにのみ影響します。ゲートウェイを更新する必要がある場合は通知されます。 • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2025-05-15	1.27.6	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。

リリース日	ソフトウェアのバージョン	リリースノート
2025-04-28	1.27.5	メンテナンスアップデート： • アップロードのUpload Rename Order ログに関連する問題を修正しました。 • アップロードの問題の原因を特定するのに役立つデバッグツールを追加しました。 • ゲートウェイのパフォーマンスをより深く把握するためのシステム統計とメトリクスを追加しました。 • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2025-04-14	1.27.4	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2025-04-01	1.27.3	メンテナンスアップデート： • ゲートウェイログ設定の更新。お客様の操作は必要ありません。

リリース日	ソフトウェアのバージョン	リリースノート
2025-03-17	1.27.2	メンテナンスアップデート： • ゲートウェイから Amazon S3 へのアップロードに失敗したファイルのキャッシュされたファイル共有データとメタデータを削除する API アクションを追加しました。この関数を使用するには、 を許可リストに登録 AWS アカウント する必要があります。ゲートウェイでアップロードに失敗したファイルに問題がある場合は、 関数を AWS サポートロック解除して、その使用に関するガイダンスを提供します。 • 新しいゲートウェイがオブジェクトの名前変更アップロードオペレーションの順序を口グに記録する機能を追加しました。これにより、名前変更操作が繰り返しまたは重複した後にファイルが Amazon S3 にアップロードされないようになります。 • SMB が意図せずにポートを開くことに関連する問題を修正しました。 • セキュリティとパフォーマンスを向上させるために、オペレーティングシステム

リリース日	ソフトウェアのバージョン	リリースノート
		とソフトウェア要素を更新しました。
2025-02-17	1.27.1	メンテナンスアップデート： • Java 11 を削除しました。 • サポート 使用するキャッシュ関数を追加しました。 • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。

リリース日	ソフトウェアのバージョン	リリースノート
2025-01-17	1.27.0	特徴: • キャッシュレポート (近日公開) - S3 ファイルゲートウェイによって現在キャッシュされているファイルメタデータのレポートを生成するように設計された今後の機能の起動をサポートするようにゲートウェイソフトウェアを更新しました。ゲートウェイから Amazon S3 へのファイルのアップロードに失敗した場合、これらのレポートを使用して問題のトラブルシューティングを行うことができます。 メンテナンスアップデート: • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2025-01-09	1.26.9	メンテナンスアップデート: • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。

リリース日	ソフトウェアのバージョン	リリースノート
2024-12-18	1.26.8	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2024-11-18	1.26.7	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2024-10-17	1.26.6	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2024-09-30	1.26.5	メンテナンスアップデート： • サポートチャネルを許可しないオンプレミスゲートウェイの問題を修正しました • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。

リリース日	ソフトウェアのバージョン	リリースノート
2024-09-16	1.26.3	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2024-08-21	1.26.1	メンテナンスアップデート： • ログ記録に関連する問題を修正しました。
2024-08-19	1.26.0	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2024-07-16	1.25.2	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。

リリース日	ソフトウェアのバージョン	リリースノート
2024-06-17	1.25.1	メンテナンスアップデート： • プロキシ使用時に、DNS が無効になっている場合のアップグレードの問題を修正しました。 • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。

リリース日	ソフトウェアのバージョン	リリースノート
2024-05-15	1.25.0	特徴: • AES-128 または AES-256 暗号化の最小値を設定する機能を追加しました。これはゲートウェイの変更のみであり、今後のリリースで Storage Gateway コンソールで利用可能になります。 • ディスク容量が少ない場合のシステムログのローテーションが増加しました。以前は、ルートディスクを埋めたログ書き込みによりゲートウェイが停止していました。これで、スペースが減ると、ゲートウェイは古いログを削除して、新しいログのスペースを増やします。 • ファイルアップロードエラーのヘルス通知に S3 パスを追加しました。以前は、ヘルス通知にはゲートウェイ上の ファイルへのパスのみが表示されていました。通知に、ユーザーが S3 でファイルを見つけるのに役立つパスが表示されるようになりました。 • 強制的なファイル共有の削除中に、サービスはバックエンドブロッカーを無視するようになりました。以前

リリース日	ソフトウェアのバージョン	リリースノート
		は、ブロッカーに遭遇すると、強制削除は説明なしで停止します。これらのシナリオでは、強制削除が中断されないようになりました。 メンテナンスアップデート： • NFS スタックを更新します。 • Java 17 JRE をアップグレードしました。 • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2024-04-15	1.24.5	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2024-04-01	1.24.4	メンテナンスアップデート： • Network Time Protocol (NTP) コンポーネントの欠落に対処

リリース日	ソフトウェアのバージョン	リリースノート
2024-03-18	1.24.3	メンテナンスアップデート： • 大文字と小文字を区別するルックアップパフォーマンスに関連する問題を修正しました。 • プロセスがクラッシュする問題を修正しました。 • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。
2024-01-12	1.24.2	メンテナンスアップデート： • SMB ログ記録の問題に対処しました。
2023-12-27	1.24.1	メンテナンスアップデート： • SMB の安定性の問題に対処しました。

リリース日	ソフトウェアのバージョン	リリースノート

2023-12-01	1.24.0	特徴:
		• SMB スタックを更新しました。
		  • AES-256 暗号化のサポートに加えて、AES-128 暗号化と署名をリクエストする SMB 3.1.1 クライアントを使用する場合のより安全なバリアントが追加されました。
		  • SMBv1 (LANMAN/CIFS) サーバー側のコピーとサーバー側のワイルドカード拡張機能は削除されました。(SMBv2 と SMBv3 は影響を受けません)。これは、特定の SMBv1 ワークロードのパフォーマンスに悪影響を及ぼす可能性があります。SMBv1 を使用する場合は、SMBv2 または SMBv3 に移行することをお勧めします。
		
		メンテナンスアップデート:
		• セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。

リリース日	ソフトウェアのバージョン	リリースノート
2023-10-24	1.23.2	メンテナンスアップデート： • サポートチャネルが特定のユーザーに対して正しく接続されないことに関連する問題を修正しました。
2023-08-14	1.23.1	メンテナンスアップデート： • 新しいゲートウェイに同期サーバーを使用するようにNTP サーバーを更新しました。
2023-06-12	1.23.0	特徴: • 一部の AWS アカウントのアップロードスレッドが増加しました。 メンテナンスアップデート： • 大きなコピーでのアクセス違反の問題を修正しました。 • NFS の問題を修正。 • Java 8 を削除しました。 • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。

リリース日	ソフトウェアのバージョン	リリースノート
2023-04-19	1.22.1	メンテナンスアップデート： • フォルダとファイルの名前変更に関連する問題を修正しました。
2023-01-18	1.22.0	機能 • DOS 属性のサポートを追加。 • ゲートウェイあたりのサポートされているファイル共有の数を 10 から 50 に増やしました。 • ゲートウェイとサービスがいつ同期していないかを判断するクロックスキュー検出メカニズムを実装しました。 メンテナンスアップデート： • SMB スタックを更新しました。
2022-07-06	1.21.2	メンテナンスアップデート： • セキュリティとパフォーマンスを向上させるために、オペレーティングシステムとソフトウェア要素を更新しました。

リリース日	ソフトウェアのバージョン	リリースノート
2022-02-16	1.21.1	特徴: • キャッシュでの名前変更と削除の新しいメトリクスを追加しました。 メンテナンスアップデート： • その他の問題を修正。
2022-01-18	1.21.0	特徴: • 新しい CloudWatch メトリクスを追加しました。 • データアップロードの帯域幅スロットリングを追加しました。
2021-12-12	1.20.0	#####: • Log4j の脆弱性に対処しました。

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