aws

ユーザーガイド

AWSStorage Gateway

API バージョン 2021-03-31

AWSStorage Gateway: ユーザーガイド

Table of Contents

Amazon FSx ファイルゲートウェイとは何ですか?

Storage Gateway は、ファイルゲートウェイ、ボリュームゲートウェイ、テープゲートウェイのストレージソリューションを提供します。

Amazon FSx ファイルゲートウェイ (FSx ファイル) は、オンプレミス施設から Windows ファイルサーバーファイル共有用のクラウド内 FSx に低レイテンシーと効率的なアクセスを提供する新しいファイルゲートウェイタイプです。レイテンシーまたは帯域幅の要件のためにオンプレミスのファイルストレージを維持する場合は、FSx ファイルを使用して、フルマネージドで信頼性が高く、事実上無制限の Windows ファイル共有にシームレスにアクセスできます。AWSCloud by FSx for Windows File Server.

Amazon FSx ファイルゲートウェイを使用する利点

FSx ファイルには次の利点があります。

- オンプレミスのファイルサーバーを排除し、すべてのデータを統合するAWSクラウドストレージの規模と経済性を活用できます。
- クラウドデータへのオンプレミスのアクセスを必要とするものを含め、すべてのファイルワークロードに使用できるオプションを提供します。
- オンプレミスにとどまる必要があるアプリケーションでも、同じ低レイテンシーと高パフォーマンスを体験できるようになりました。AWSネットワークに負担をかけたり、最も要求の厳しいアプリケーションで発生するレイテンシーに影響を与えることなく、

Amazon FSx ファイルゲートウェイのしくみ

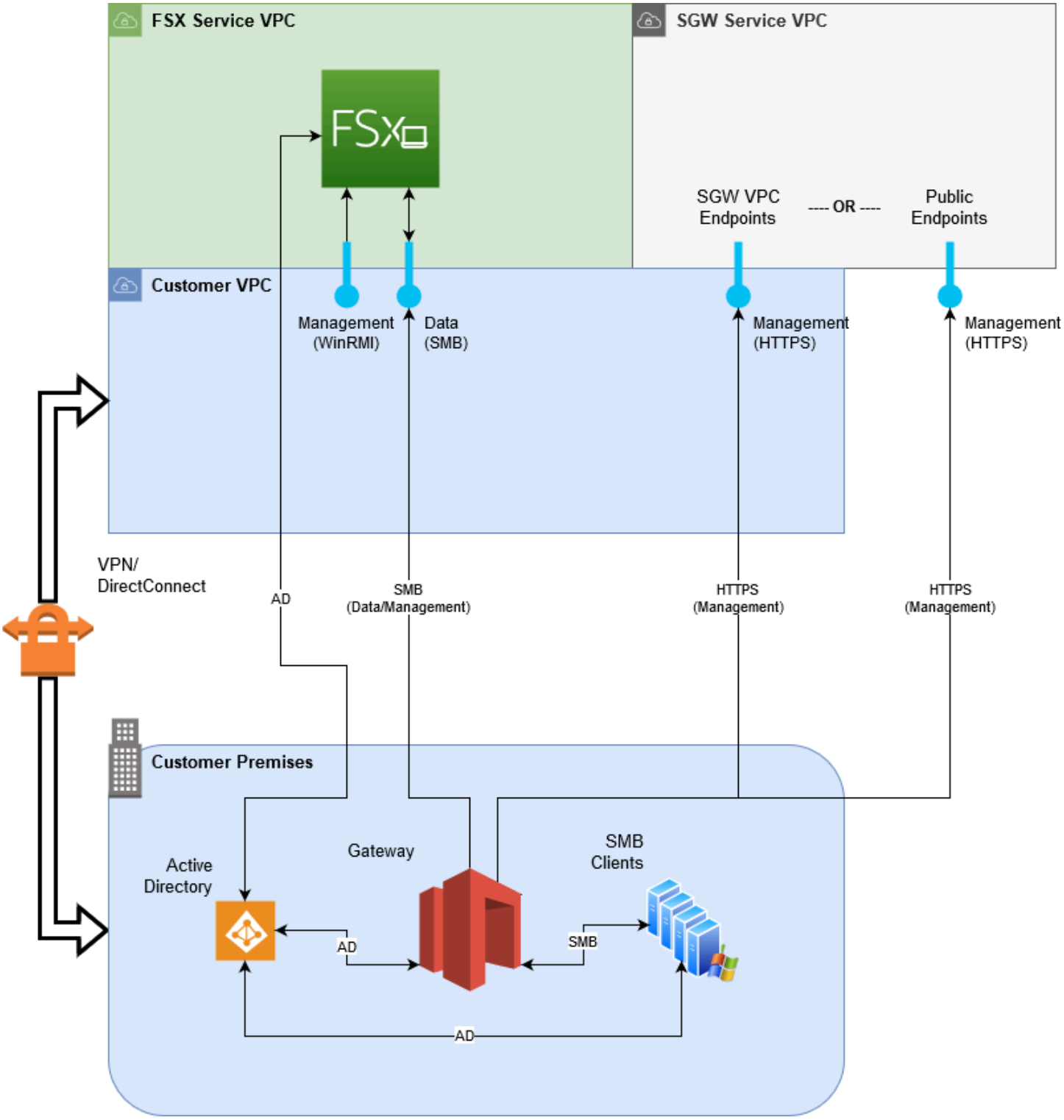
Amazon FSx ファイルゲートウェイ (FSx ファイル) を使用するには、少なくとも 1 つの Amazon FSx for Windows File Server ファイルシステムが必要です。また、VPN または Windows ファイルサーバーへの FSx へのオンプレミスアクセスも必要です。AWS Direct Connect接続. Amazon FSx ファイルシステムの使用方法の詳細については、「」を参照してください。Amazon FSx for Windows File Server とは何ですか?

FSx File VMware 仮想アプライアンスをダウンロードしてデプロイするか、AWSStorage Gateway ハードウェアアプライアンスをオンプレミス環境に導入します。アプライアンスをデプロイしたら、ストレージゲートウェイコンソールから、またはStorage Gateway API を使用して FSx ファイルをアクティブ化します。Amazon Elastic Compute Cloud (Amazon EC2) イメージを使用して FSx ファイルを作成することもできます。

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

ファイル共有が接続されると、FSx for Windows ファイルサーバーで利用可能なすべての機能を利用しながら、ファイルをローカルで読み書きできます。FSx ファイルは、ローカルファイル共有とその内容を、FSx for Windows ファイルサーバーでリモートに保存されたファイル共有にマップします。リモートファイルとローカルに表示されるファイルとその共有には 1:1 の対応があります。

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



図では、次の点に注意してください。

- AWS Direct Connectまたは VPNFSx ファイルが SMB を使用して Amazon FSx ファイル共有にアクセスできるようにし、FSx for Windows File Server オンプレミスの Active Directory ドメインに参加できるようにするために必要です。
- Amazon Virtual Private Cloud (Amazon VPC)は、プライベートエンドポイントを使用して FSx for Windows File Server サービス VPC およびStorage Gateway サービス VPC に接続するために必要です。FSx ファイルは、パブリックエンドポイントに接続することもできます。

Amazon FSx ファイルゲートウェイを全部使えるAWSFSx for Windows File Server が使用できるリージョン。

Amazon FSx ファイルゲートウェイのセットアップ

このセクションでは、Amazon FSx ファイルゲートウェイの使用を開始するための手順について説明します。開始するには、まず AWS にサインアップします。初めて使用する方には、リージョンそして要件セクション。

トピック

- Amazon Web Services にサインアップする
- IAM ユーザーを作成する
- ファイルゲートウェイのセットアップ要件
- AWS Storage Gateway へのアクセス
- AWS でサポートされているリージョン

Amazon Web Services にサインアップする

AWS アカウント をお持ちでない場合は、以下の手順を実行してアカウントを作成してください。

AWS アカウント にサインアップするには

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

   サインアップ手順の一環として、通話呼び出しを受け取り、電話のキーパッドを用いて確認コードを入力することが求められます。

IAM ユーザーを作成する

を作成した後AWSアカウントを作成するには、次の手順を使用します。AWS Identity and Access Management自分用の (IAM) ユーザー。次に、管理者権限を持つグループにユーザーを追加します。

自分用の管理者ユーザーを作成し、そのユーザーを管理者グループに追加するには (コンソール)

1. [IAM console] (ルートユーザー) を選択し、AWS アカウント の E メールアドレスを入力して、アカウント所有者として IAM コンソールにサインインします。次のページでパスワードを入力します。

> **Note**
>
> 次の IAM の **Administrator** ユーザーの使用に関するベストプラクティスに従って、ルートユーザーの認証情報は安全な場所に保管しておくことを強くお勧めします。ルートユーザーとしてのサインインは、いくつかのアカウントとサービスの管理タスクの実行にのみ使用してください。

2. ナビゲーションペインで、[Users] (ユーザー)、[Add user] (ユーザーを追加する) の順に選択します。
3. [User name] (ユーザー名) に「**Administrator**」と入力します。
4. [AWS Management Console access (アクセス)] の横にあるチェックボックスをオンにします。[Custom password] (カスタムパスワード) を選択し、その後テキストボックスに新しいパスワードを入力します。
5. (オプション) AWS では、デフォルトで、新しいユーザーは初回サインイン時に新しいパスワードを作成する必要があります。[User must create a new password at next sign-in] (ユーザーは次回のサインイン時に新しいパスワードを作成する必要がある) 隣にあるチェックボックスをクリアーにして、新しいユーザーがサインインしてからパスワードをリセットできるようにできます。
6. [Next: (次へ:)] を選択します アクセス許可.
7. [Set permissions] (アクセス許可の設定) で、[Add user to group] (ユーザーをグループに追加) を選びます。
8. [Create group] (グループの作成) を選びます。
9. [Create group] (グループの作成) ダイアログボックスで、[Group name] (グループ名) に「**Administrators**」と入力します。
10. [Filter policies] (フィルターポリシー) を選択し、次に [AWS managed - job function] (マネージド - ジョブの機能) を選択してテーブルのコンテンツをフィルタリングします。
11. ポリシーリストで、[AdministratorAccess] のチェックボックスを選択します。次に、[Create group] (グループの作成) を選びます。

> **Note**
>
> `AdministratorAccess` 許可を使用して、AWS Billing and Cost Management コンソールを使用する前に、IAM ユーザーおよびロールの請求へのアクセスをアクティブ

化する必要があります。これを行うには、請求コンソールへのアクセスの委任に関するチュートリアルのステップ 1 の手順に従ってください。

12. グループのリストに戻り、新しいグループのチェックボックスをオンにします。必要に応じて [Refresh] (更新) を選択し、リスト内のグループを表示します。
13. [Next: (次へ:)] を選択します タグ
14. (オプション) タグをキーバリューペアとしてアタッチして、メタデータをユーザーに追加します。IAM でのタグの使用の詳細については、IAM ユーザーガイドの「IAM リソースのタグ付け」を参照してください。
15. [Next: (次へ:)] を選択します 確認をクリックして、新しいユーザーに追加するグループメンバーシップのリストを表示します。続行する準備ができたら、[Create user] (ユーザーの作成) を選択します。

この同じプロセスにより、さらにグループとユーザーを作成し、そのユーザーに対し AWS アカウント のリソースへのアクセス権を付与できます。ポリシーを使用して特定の AWS リソースに対するユーザーの許可を制限する方法については、アクセス管理とポリシーの例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

以下の要件は、特記がない限り、のすべてのファイルゲートウェイタイプに共通です。AWS Storage Gateway。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

- 必要な前提条件
- ハードウェアとストレージの要件
- ネットワークとファイアウォールの要件
- サポートされているハイパーバイザーとホストの要件
- ファイルゲートウェイでサポートされる SMB クライアント
- 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

必要な前提条件

Amazon FSx ファイルゲートウェイ (FSx ファイルゲートウェイ) を使用する前に、次の要件を満たす必要があります。

- FSx for Windows File Server ファイルシステムを作成して設定します。手順については、以下を参照してください。ステップ 1: ファイルシステムの作成のAmazon FSx for Windows File Server ユーザーガイド。
- Microsoft Active Directory (AD) を設定します。
- ゲートウェイとゲートウェイ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。AWS。ゲートウェイを正常にダウンロード、アクティブ化、および更新するには、最低 100 Mbps が必要です。
- プライベートネットワーク、VPN、またはAWS Direct ConnectAmazon Virtual Private Cloud (Amazon VPC) と、FSx ファイルゲートウェイをデプロイするオンプレミス環境間で行われます。
- ゲートウェイが Active Directory ドメインコントローラの名前を解決できることを確認します。Active Directory ドメインで 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 [ネットワーク構成] メニューから DNS サーバーを手動で指定することができます。

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ハードウェアと設定、および必要なストレージに割り当てる最小ディスク容量に関する情報を示します。

オンプレミス VM のハードウェア要件

ゲートウェイをオンプレミスでデプロイする前に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低限のリソースを専有できることを確認してください。

- VM に割り当てられた仮想プロセッサ 4 個
- ファイルゲートウェイ用の 16 GiB の予約済み RAM
- ディスクの空き容量 80 GiB (VM イメージとシステムデータのインストール用)。

Amazon EC2 インスタンスタイプの要件

ゲートウェイを Amazon Elastic Compute Cloud (Amazon EC2) にデプロイする場合、インスタンスサイズは少なくとも必要です。**xlarge**ゲートウェイが機能するようにします。ただし、コンピューティング最適化インスタンスファミリーの場合は、少なくとも次のサイズが必要です**2xlarge**。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 — m4 または m5 インスタンスタイプ。

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

> **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する場合、ディスクは自動的に表示されます。Amazon EC2 インスタンスストレージの詳細については、「」を参照してください。インスタンスストレージのAmazon EC2 ユーザーガイド。

ストレージの要件

ゲートウェイには VM 用の 80 GiB に加えて、ゲートウェイ用のディスク領域が必要です。

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**
>
> キャッシュに 1 つ以上のローカルドライブを、最大容量まで構成できます。
> 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。ディスクがキャッシュとして割り当て済みである場合は、既存のディスクサイズを変更しないでください。

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。ゲートウェイを正常にダウンロード、アクティブ化、および更新するには、最低 100 Mbps が必要です。データ転送パターンによって、ワークロードをサポートするため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、Amazon EC2 で FSx ファイルゲートウェイをデプロイするか、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他のタイプのデプロイ (オンプレミスを含む) を使用する場合があります。AWSIP アドレスの範囲。このような場合、ゲートウェイがサービスの接続上の問題が発生すると、AWSIP 範囲の値が変更されます。-AWS使用する必要がある IP アドレス範囲の値は、の Amazon サービスのサブセットです。AWSでゲートウェイをアクティブ化するリージョン。現在の IP 範囲値については、を参照してください。AWSIP アドレスの範囲のAWS全般のリファレンス。

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の要件
- 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のセキュリティグループの設定

ポート要件

すべてのゲートウェイの種類に共通のポート

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

Protocol - 。	ポート	方向	出典	送信先	用途
転送制御プロトコル	443 (HTTPS)	アウトバウンド	Storage Gateway	AWS	Storage Gateway からへの通信

Protocol - 。	ポート	方向	出典	送信先	用途
					用AWSサービスエンドポイント。サービスエンドポイントの詳細については、「ファイアウォールとルーターを介した AWS Storage Gateway アクセスの許可」を参照してください。

Protocol - 。	ポート	方向	出典	送信先	用途
転送制御プロトコル	80 (HTTP)	インバウンド	に接続するホストAWS Management Console。	Storage Gateway	ローカルシステムでストレージゲートウェイのアクティベーションキーを取得するため。ポート 80 は、Storage Gateway アプライアンスのアクティベーションの間のみ使用されます。 Storage Gateway では、ポート 80 がパブリックにアクセス可能である必要はありません。ポート 80 へのアクセスに必要なレベルはネットワークの設定によって決まります。ゲートウェイコンソールからゲートウェイをアクティ

Protocol - 。	ポート	方向	出典	送信先	用途
					ブ化する場合、コンソールに接続するホストにゲートウェイのポート80へのアクセス権限が必要です。
UDP: UDP	53 (DNS)	アウトバウンド	Storage Gateway	DNS サーバー	Storage Gateway と DNS サーバー間の通信用。

Protocol - 。	ポート	方向	出典	送信先	用途
転送制御プロトコル	22 (サポートチャネル)	アウトバウンド	Storage Gateway	AWS Support	許可AWS Supportをクリックして、ゲートウェイの問題のトラブルシューティングを支援するためにゲートウェイにアクセスします。このポートは、ゲートウェイの通常のオペレーションでは開いておく必要はありませんが、トラブルシューティングでは必要です。
ユーザーデータグラムプロトコル	123 (NTP)	アウトバウンド	NTP クライアント	NTP サーバー	VM 時間をホスト時間に同期するためにローカルシステムで使用されます。

ファイルゲートウェイのポート

FSx ファイルゲートウェイの場合、ドメインユーザーがサーバーメッセージブロック (SMB) ファイル共有にアクセスできるようにするには、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 Microsoft Windows ドメイン (DNS が解決可能なもの) に参加させることができます。

また、 を使用することもできますAWS Directory Service作成するにはAWS Managed Microsoft ADAmazon Web Services スクラウド。ほとんどの場合AWS Managed Microsoft ADデプロイメントを行うには、VPC 用の動的ホスト構成プロトコル (DHCP) サービスを設定する必要があります。DHCP オプションを作成する方法については、「」を参照してください。DHCP オプションセットの作成のAWS Directory Service管理ガイド。

FSx ファイルゲートウェイには、以下のポートが必要です。

Protocol - 。	ポート	方向	出典	送信先	用途
ユーザーデータグラムプロトコル NetBIOS	137	インバウンドとアウトバウンド		Microsoft Active Directory	Microsoft Active Directory に接続する場合。
ユーザーデータグラムプロトコル NetBIOS	138	インバウンドとアウトバウンド			データグラムのサービス用
TCP LDAP	389	インバウンドとアウトバウンド			ディレクトリシステムエージェント (DSA) クライアント接続用
TCP v2/v3 データ	445	アウトバウンド			ファイルゲートウェイと FSx for Windows File Server 間のストレージデータ転送
TCP (HTTPS)	443	アウトバウンド		Storage Gateway	管理制御：Storage Gateway 仮

Protocol - 。	ポート	方向	出典	送信先	用途
				サービスエンドポイント	想マシンからAWSサービスエンドポイント
TCP HTTPS	443	アウトバウンド		Amazon CloudFront	ゲートウェイのアクティブ化
転送制御プロトコル	443	アウトバウンド		VPC エンドポイントの使用状況	管理制御：Storage Gateway 仮想マシンからAWSサービスエンドポイント。
転送制御プロトコル	1026	アウトバウンド			制御トラフィックに使用
転送制御プロトコル	1027	アウトバウンド			アクティベーション中にのみ使用され、その後閉じることができます
転送制御プロトコル	1028	アウトバウンド			制御トラフィックに使用

Protocol - 。	ポート	方向	出典	送信先	用途
転送制御プロトコル	1031年	アウトバウンド			ファイルゲートウェイのソフトウェアアップデートにのみ使用
転送制御プロトコル	2222	アウトバウンド			VPC エンドポイントを使用するときに、ゲートウェイへのサポートチャネルを開くために使用
TCP (HTTPS)	8080	インバウンド			ハードウェアアプライアンスのアクティベーションのために一時的に必要です。

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の要件

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

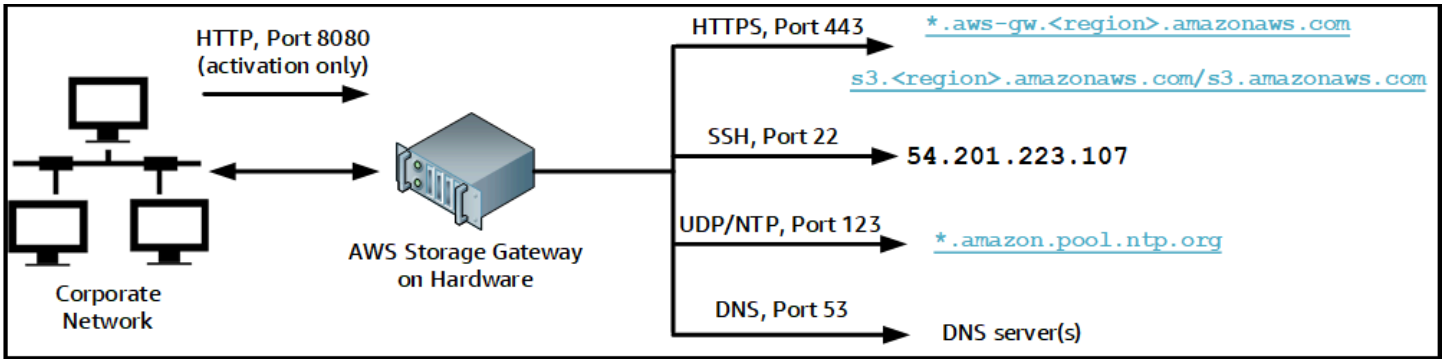
- インターネットアクセス— サーバー上の任意のネットワークインターフェイスを介した、インターネットへの常時接続のネットワーク接続。
- DNS サービス— DNS サーバー間の通信のための DNS サービス。
- 時刻同期— 自動的に設定された Amazon NTP タイムサービスにアクセス可能である必要があります。

- IP address— 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。

Protocol - 。	ポート	方向	出典	送信先	用途
SSH	22	アウトバウンド	ハードウェアアプライアンス	54.201.223.107	サポートチャネル
DNS	53	アウトバウンド	ハードウェアアプライアンス	DNS サーバー	名前解決

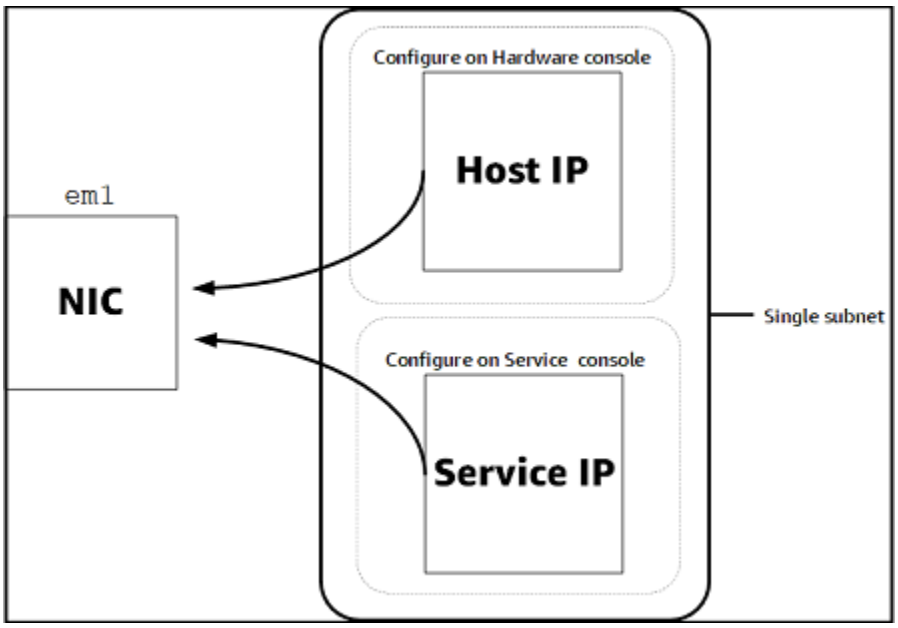
Protocol - 。	ポート	方向	出典	送信先	用途
UDP/NTP	123	アウトバウンド	ハードウェアアプライアンス	`*.amazon.pool.ntp.org`	時刻同期
HTTPS	443	アウトバウンド	ハードウェアアプライアンス	`*.amazonaws.com`	データ転送
HTTP	8080	インバウンド	AWS	ハードウェアアプライアンス	アクティベーション (短時間のみ)

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

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

> **Note**
>
> サーバーの背面とポートを示す図については、「」を参照してください。ハードウェアアプライアンスのラックマウントと電源への接続。

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、ゲートウェイ用でもホスト用でも、同じサブネットにある必要があります。次の図は、アドレス割り当てスキームを示しています。



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

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

ゲートウェイがと通信するために次のサービスエンドポイントにアクセスする必要があります。AWS。ファイアウォールまたはルーターを使用してネットワークトラフィックをフィルタリングまたは制限する場合は、これらのサービスエンドポイントで送信通信を許可するように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。AWS。

> **Important**
>
> ゲートウェイに応じてAWSリージョン、置換##サービスエンドポイントで正しいリージョン文字列を指定します。

次のサービスエンドポイントは、ヘッドバケット操作のすべてのゲートウェイに必要となります。

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

次のサービスエンドポイントは、すべてのゲートウェイで制御パス (anon-cp,client-cp,proxy-app) とデータパス (dp-1) オペレーション.

```
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
```

次の例は、米国西部 (オレゴン) リージョン () のゲートウェイサービスエンドポイントです。us-west-2).

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

次の Amazon CloudFront エンドポイントは、使用できるリストを取得するためにStorage Gateway に必要となります。AWS地域。

```
https://d4kdq0yaxexbo.cloudfront.net/
```

Storage Gateway 仮想マシンは、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
2.amazon.pool.ntp.org
3.amazon.pool.ntp.org
```

- ストレージゲートウェイ：サポート対象AWS地域とリストAWSStorage Gateway で使用できるサービスエンドポイントについては、を参照してください。AWS Storage Gatewayエンドポイントとクォータのの 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：サポート対象AWSハードウェアアプライアンスで使用できるリージョンについては、を参照してください。Storage Gateway ハードウェアアプライアンスのの AWS全般のリファレンス。

Amazon EC2 ゲートウェイインスタンスのセキュリティグループの設定

EclipseAWS Storage Gatewayでは、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。

  ゲートウェイのセキュリティグループに属さないインスタンスにゲートウェイへの接続を許可する必要がある場合、ポート 80 でのみ接続を許可することをお勧めします (アクティベーション用)。
- 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のために AWS Support を使用する場合にのみ、ポート 22 アクセスを許可します。詳細については、「君が欲しいAWS SupportEC2 ゲートウェイのトラブルシューティングに役立つ」を参照してください。

サポートされているハイパーバイザーとホストの要件

Storage Gateway は、オンプレミスで仮想マシン (VM) アプライアンスとして、物理ハードウェアアプライアンスとして、またはAWSAmazon EC2 インスタンスとして。

Storage Gateway は、次のハイパーバイザーのバージョンとホストをサポートしています。

- VMware ESXi Hypervisor (バージョン 6.0、6.5、6.7) — 無料版の VMware は、VMware Web サイト。このセットアップでは、ホストに接続するために VMware vSphere クライアントも必要です。
- Microsoft Hyper-V Hypervisor (バージョン 2012 R2 または 2016) Hyper-V の無料スタンドアロン版を Microsoft Download Center から入手できます。このセットアップでは、ホストに接続する Microsoft Windows クライアントコンピュータには Microsoft Hyper-V Manager が必要になります。
- Linux カーネルベースの仮想マシン (KVM) 無料のオープンソースの仮想化テクノロジー。KVM は Linux バージョン 2.6.20 以降のすべてのバージョンに含まれています。Storage Gateway は CentOS/RHEL 7.7、Ubuntu 16.04 LTS、および Ubuntu 18.04 LTS ディストリビューションでテストおよびサポートされています。他の最新の Linux ディストリビューションは動作しますが、機能やパフォーマンスは保証されません。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。
- Amazon EC2 インスタンス — Storage Gateway は、ゲートウェイ VM イメージを含む Amazon マシンイメージ (AMI) を提供します。Amazon EC2 にゲートウェイをデプロイする方法については、「」を参照してください。Amazon EC2 ホストへのファイルゲートウェイのデプロイ。

- ストレージゲートウェイハードウェアアプライアンス — Storage Gateway は、仮想マシンインフラストラクチャが制限されている場所でのオンプレミス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を提供します。

> **Note**
>
> Storage Gateway 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リカバリ」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る SMB クライアント

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

- Microsoft Windows Server 2008 以降
- Windows デスクトップバージョン: 10、8、7
- Windows Server 2008 以降で動作する Windows Terminal Server

> **Note**
>
> サーバーメッセージブロックの暗号化には、SMB v2.1 をサポートするクライアントが必要です。

ファイルゲートウェイでサポートされているファイルシステムオペレーション

SMB クライアントは、ファイルの書き込み、読み取り、削除、切り捨てができます。クライアントからStorage Gateway に送信された書き込みは、同期的にローカルキャッシュに書き込まれます。次に、最適化された転送を介して非同期的に Amazon FSx に書き込まれます。読み取りはまずローカ

ルキャッシュから行われます。データがない場合は、リードスルーキャッシュとして Amazon FSx 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。Amazon FSx から削除ファイルを削除します。

AWS Storage Gateway へのアクセス

♪AWS Storage Gatewayコンソールを使用して、ゲートウェイの各種設定および管理タスクを実行します。このガイドでは、「使用開始」をはじめ、さまざまなセクションで、コンソールからゲートウェイの機能を使う方法を説明しています。

また、AWS Storage Gateway API を使ってプログラム的にゲートウェイの設定や管理を行う方法もあります。 API の詳細については、「Storage Gateway の API リファレンス」を参照してください。

また、 を使用することもできますAWSSDK (Storage Gateway を操作するアプリケーションを開発する SDK)。-AWSSDK for Java、.NET、PHP は、プログラミング作業を簡素化するため、基盤となるStorage Gateway API をラップします。SDK ライブラリのダウンロードについては、「」を参照してください。AWSデベロッパーセンター。

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

AWS でサポートされているリージョン

Amazon FSx ファイルゲートウェイは、ファイルデータをAWSAmazon FSx ファイルシステムが配置されているリージョン。ゲートウェイのデプロイを開始する前に、Storage Gateway コンソールの右上隅にあるリージョンを選択してください。

- Amazon FSx ファイルゲートウェイ — サポート対象AWS地域とリストAWSAmazon FSx ファイルゲートウェイで使用できるサービスエンドポイントについては、「」を参照してください。Amazon FSx ファイルゲートウェイエンドポイントとクォータのAWS全般のリファレンス。
- Storage Gateway — サポート対象AWS地域とリストAWSStorage Gateway で使用できるサービスエンドポイントについては、を参照してください。AWS Storage Gatewayエンドポイントとクォータのリファレンス。
- 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されているリージョンについては、を参照してください。AWS Storage Gatewayハードウェアアプライアンスのリージョンのリファレンス。

Storage Gateway ハードウェアアプライアンスの使用

Storage Gateway ハードウェアアプライアンスは、Storage Gateway ソフトウェアがプリインストールされている物理ハードウェアアプライアンスです。からハードウェアアプライアンスを管理できます。ハードウェアのページでAWS Storage Gatewayconsole.

ハードウェアアプライアンスは、高性能な 1U サーバーであり、データセンター内にデプロイするか、自社のファイアウォール内にオンプレミスでデプロイできます。ハードウェアアプライアンスの購入とアクティベーションを行うと、アクティベーションプロセスによって、ハードウェアアプライアンスはAWSアカウント. アクティベーションの後、ハードウェアアプライアンスは、コンソールの Gateway として表示されます。ハードウェアページで. ハードウェアアプライアンスは、ファイルゲートウェイ、テープゲートウェイ、またはボリュームゲートウェイタイプとして設定できます。ハードウェアアプライアンスでこれらのゲートウェイタイプをデプロイしてアクティベートする手順は、仮想プラットフォームでの手順と同じです。

Storage Gateway ハードウェアアプライアンスは、AWS Storage Gatewayconsole.

ハードウェアアプライアンスを注文するには

1. でStorage Gateway コンソールを開きます。https://console.aws.amazon.com/storagegateway/homeを選択し、AWSアプライアンスを使用するリージョン。
2. 選択ハードウェアナビゲーションペインを使用する場合。
3. 選択アプライアンスの注文[] を選択してから、進む。にリダイレクトされます。AWSElemental Applianceおよびソフトウェア管理コンソールを使用して、販売見積りをリクエストします。
4. 必要な情報を入力し、[送信]。

情報が確認されると、販売見積書が生成され、注文プロセスを進めて発注書を提出するか、前払いの手配を行うことができます。

ハードウェアアプライアンスの販売見積または注文履歴を表示するには

1. でStorage Gateway コンソールを開きます。https://console.aws.amazon.com/storagegateway/home。
2. 選択ハードウェアナビゲーションペインを使用する場合。
3. 選択見積もりと注文[] を選択してから、進む。にリダイレクトされます。AWSElemental Applianceおよびソフトウェア管理コンソールを使用して、販売見積と注文履歴を確認します。

以下のセクションでは、Storage Gateway ハードウェアアプライアンスの設定、構成、アクティベーション、起動、使用の手順について説明します。

トピック

AWS でサポートされているリージョン

Storage Gateway ハードウェアアプライアンスは、法的に許可され、米国政府によって輸出が許可されている全世界に発送できます。サポートされているについてはAWSリージョン、「」を参照してくださいStorage Gateway ハードウェアアプライアンスのAWS全般のリファレンス。

ハードウェアアプライアンスの設定

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コンソールを使用して、ネットワークを設定し、への常時接続を提供できます。AWSアプライアンスをアクティベートします。アクティベーションは、アプライアンスとを関連付けます。AWSアクティベーションプロセスで使用されるアカウント。アプライアンスのアクティベーションが完了したら、Storage Gateway コンソールからファイル、ボリューム、またはテープゲートウェイを起動できます。

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ラックマウントと電源への接続」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) とStorage Gateway (サービス) の両方に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、「ネットワークパラメータの設定」を参照してください。
3. コンソールでハードウェアアプライアンスをアクティブ化するハードウェアのページでAWSお好みのリージョン。詳細については、「ハードウェアアプライアンスのアクティベーション」を参照してください。
4. Storage Gateway をハードウェアアプライアンス上にインストールします。詳細については、「ゲートウェイの設定」を参照してください。

   ハードウェアアプライアンスでゲートウェイは、VMware ESXi、Microsoft Hyper-V、Linux カーネルベースの仮想マシン (KVM)、または Amazon EC2 でゲートウェイをセットアップするのと同じ方法でにセットアップします。

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の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。これを行うとキャッシュが大きくなるため、内のデータにアクセスするときのレイテンシーが低くなります。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) を購入すると、使用可能なストレージを 12 TB に増やすことができます。これは、コンソールで購入可能です。ハードウェアページで. ハードウェアアプライアンスの注文と同じ注文プロセスに従って、Storage Gateway コンソールから販売見積りをリクエストすることで、追加のSSDを注文できます。

その後、それらをハードウェアアプライアンスに追加してアクティブ化できます。ハードウェアアプライアンスをすでにアクティベートしていて、アプライアンスの使用可能なストレージを 12 TB に増やす場合は、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。連絡先AWSこれを行う手順のSupport。
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銅線ネットワークカードまたは 10G DA/SFP+ ネットワークカードが付属します。

- 10G-ベースT NIC 構成:

  - 10GにはCAT6ケーブルを使用し、1GにはCAT5 (e) を使用します。
- 10G DA/SFP+ NIC 構成:
  - Twinax 銅直接接続ケーブルを最大 5 メートルまで使用可能
  - デル/インテル互換 SFP+ 光モジュール (SR または LR)
  - SFP/SFP+ 銅トランシーバ 1G ベース T または 10G ベース T

ハードウェアアプライアンスのラックマウントと電源への接続

Storage Gateway ハードウェアアプライアンスのボックスを解除したら、同梱されている指示に従ってサーバーをラックマウントします。アプライアンスは 1U フォームファクタで、標準の国際電気技術委員会 (IEC) に準拠した 19 インチラックに適合します。

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

- 電源ケーブル: 1 つは必須です。2 つを推奨します。
- サポートされているネットワークケーブル (ハードウェアアプライアンスに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 (インテル互換)、または SFP to Base-T銅トランシーバ。
- 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。

ハードウェアアプライアンスの寸法

ハードウェアアプライアンスを電源に接続するには

> **Note**
>
> 以下の手順を実行する前に、Storage Gateway ハードウェアアプライアンスのすべての要件を満たしていることを確認します。詳細は、「」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の要件。

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

   次のイメージでは、さまざまな接続を備えたハードウェアアプライアンスを示します。

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

> **Note**
>
> ハードウェアアプライアンスは 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しているスイッチポートを非 VLAN トランキングポートとして設定します。

3. キーボードとモニターを接続します。
4. 次のイメージに示すように、前面パネルの電源ボタンを押して、サーバーの電源をオンにします。

サーバーが起動されると、ハードウェアコンソールがモニターに表示されます。ハードウェアコンソールは、固有のユーザーインターフェイスです。AWSを使用して、初期ネットワークパラメーターを設定します。アプライアンスを接続するには、これらのパラメータを設定します。AWS次の方法でトラブルシューティングを行うサポートチャネルを開きます。AWSSupport 対象。

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

初めてパスワードを設定するには

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

この時点で、ハードウェアコンソールには、以下のように表示されます。

次のステップ

ネットワークパラメータの設定

ネットワークパラメータの設定

サーバーが起動したら、ハードウェアアプライアンスのラックマウントと電源への接続 に従って、ハードウェアコンソールで、最初のパスワードを入力します。

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

ネットワークアドレスを設定するには

1. [Configure Network] を選択して、Enter キーを押します。[Configure Network] 画面で、次のように表示されます。

2. [IP Address] に有効な IPv4 アドレスを入力します。以下のいずれかのソースを使用します。

   - 動的ホスト構成プロトコル (DHCP) サーバーによって物理ネットワークポートに割り当てられた IPv4 アドレスを使用します。

     この場合には、この IPv4 アドレスを記録し、それを後のアクティベーション手順を使用します。
   - 静的 IPv4 アドレスを割り当てます。これを行うには、[] を選択します。静的のem1セクションを開き、を押します。Enterをクリックすると、次に示すように、[静的 IP の設定] 画面が表示されます。

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

   有効な IPv4 アドレスを入力したら、Down arrow または Tab キーを押します。

   > **Note**
   >
   > 他のインターフェイスを設定する場合は、同じ Always-On 接続を提供する必要があります。AWS要件にリストされているエンドポイント。

3. [Subnet] で有効なサブネットマスクを入力し、Down arrow キーを押します。

4. [Gateway] で、ネットワークゲートウェイの IPv4 アドレスを入力し、Down arrow キーを押します。
5. [DNS1] で、ドメインネームサービス (DNS) サーバーの IPv4 アドレスを入力し、Down arrow を押します。
6. (オプション) [DNS2] で、2 番目の IPv4 アドレスを入力し、Down arrow を押します。2 番目の DNS サーバーの割り当ては、最初の DNS サーバーが使用不可となった場合に、追加の冗長性を提供します。
7. [Save] を選択して Enter を押し、アプライアンスの静的 IPv4 アドレス設定を保存します。

ハードウェアコンソールからログアウトするには

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

次のステップ

ハードウェアアプライアンスのアクティベーション

ハードウェアアプライアンスのアクティベーション

IP アドレスを設定した後、以下の手順に従って、コンソールの [ハードウェア] ページで、この IP アドレスを入力します。アクティベーションプロセスにより、ハードウェアアプライアンスが適切なセキュリティ認証情報を備えていることを検証して、アプライアンスをAWSアカウント.

ハードウェアアプライアンスは、サポートされているいずれかでアクティブ化することを選択できます。AWS地域。サポートされているリストについてはAWSリージョン、「」を参照してくださいStorage Gateway ハードウェアアプライアンスのAWS全般のリファレンス。

アプライアンスを初めてアクティベートするには、またはAWSゲートウェイがデプロイされていないリージョン

1. にサインインします。AWS Management Consoleで、Storage Gateway コンソールを開きます。AWS Storage Gatewayマネジメントコンソールハードウェアをアクティブ化するために使用するアカウント資格情報を使用します。

   これが最初のゲートウェイである場合AWSリージョン、スプラッシュ画面が表示されます。これでゲートウェイを作成した後AWSリージョンでは、画面が表示されなくなります。

> **Note**
>
> アクティベーションを行う場合のみは、次の条件が満たされている必要があります。
>
> - ブラウザは、ハードウェアアプライアンスと同じネットワーク上になければなりません。
> - ファイアウォールは、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. 選択開始方法[ゲートウェイの作成] ウィザードを表示し、ハードウェアアプライアンスでホストプラットフォームの選択ページで、次のようにします。
3. [次へ] を選択すると、次に示すように、[Connect to hardware] 画面が表示されます。
4. を使用する場合IP アドレスのハードウェアアプライアンスにConnectセクションで、アプライアンスの IPv4 アドレスを入力します。次に接続をクリックして、次に示すように、[Activate Hardware] 画面に移動します。
5. [Hardware name] に、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. を使用する場合ハードウェアタイムゾーン[] で、ローカル設定を入力します。

   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。現地時間の午前 2 時を更新の時間として設定します。

   > **Note**
   >
   > これにより、通常の業務時間外に標準の更新を行うことができるため、アプライアンスのタイムゾーンを設定することをお勧めします。

7. (オプション) [RAID Volume Manager] は [ZFS] の設定のままにします。

   ZFS は、ハードウェアアプライアンスの RAID ボリュームマネージャーとして使用され、パフォーマンスとデータ保護が向上します。ZFS は、ソフトウェアベースのオープンソースファイルシステムと、論理ボリュームマネージャーです。ハードウェアアプライアンスは、ZFS RAID 用に特別に調整されています。ZFS RAID の詳細については、「ZFS」の Wikipedia のページを参照してください。
8. [Next] を選択して、アクティベーションを終了します。

次のように、[ハードウェア] ページにコンソールバナーが表示され、ハードウェアアプライアンスが正常にアクティベート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。次に、アプライアンスでファイル、テープ、またはキャッシュ型ボリュームゲートウェイを起動します。

次のステップ

ゲートウェイの起動

ゲートウェイの起動

アプライアンス上で、ファイルゲートウェイ、ボリュームゲートウェイ (キャッシュ) 、またはテープゲートウェイの 3 つのストレージゲートウェイのいずれかを起動できます。

ハードウェアアプライアンスでゲートウェイを起動するには

1. にサインインします。AWS Management Consoleで、Storage Gateway コンソールを開きます。https://console.aws.amazon.com/storagegateway/home。
2. [ハードウェア] を選択します。
3. [アクション] で [ゲートウェイの起動] を選択します。
4. [ゲートウェイタイプ] で、[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 (キャッシュ型)] を選択します。
5. [ゲートウェイ名] に、ゲートウェイ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. [ゲートウェイの起動] を選択します。

選択したゲートウェイタイプ用のStorage Gateway ソフトウェアがアプライアンスにインストールされます。ゲートウェイがとして表示されるまで、最大 5 ~ 10 分かかることがあります。オンラインコンソールを使用する場合。

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

次のステップ

ゲートウェイの IP アドレスの設定

ゲートウェイの IP アドレスの設定

ハードウェアアプライアンスをアクティブ化する前に、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にしてStorage Gateway を起動したら、ハードウェアアプライアンスで実行される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ているゲートウェイに静的 IP アドレスを割り当てるには、そのゲートウェイのローカルコンソールから IP アドレスを設定します。アプリケーション (NFS や SMB クライアント、iSCSI イニシエータなど) は、この IP アドレスに接続します。ハードウェアアプライアンスのコンソールから、ゲートウェイのローカルコンソールにアクセスできます。

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

1. ハードウェアコンソールで、[Open Service Console] を選択し、ゲートウェイのローカルコンソールのログイン画面を開きます。
2. localhost のログインパスワードを入力し、`Enter` キーを押します。

   デフォルトのアカウントは `admin` で、デフォルトのパスワードは `password` です。
3. デフォルトパスワードを変更します。[Actions (アクション)]、[Set Local Password (ローカルパスワードの設定)] の順に選択し、[Set Local Password (ローカルパスワードの設定)] ダイアログボックスに、新しい認証情報を入力します。
4. (オプション) プロキシ設定の構成 手順については、「ハードウェアアプライアンスのラックマウントと電源への接続」を参照してください。
5. 次に示すように、ゲートウェイのローカルコンソールの [Network Settings] ページに移動します。

6. 2 と入力すると、次に示すように [Network Configuration] ページに移動します。

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

ゲートウェイのローカルコンソールを終了するには

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

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

次のステップ

ゲートウェイの設定

ゲートウェイの設定

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

ハードウェアアプライアンスからのゲートウェイの削除

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

ハードウェアアプライアンスからゲートウェイを削除するには

1. ゲートウェイのチェックボックスをオンにします。
2. [アクション] で [ゲートウェイの削除] を選択します。
3. [Remove gateway from hardware appliance] のダイアログボックスで、[Confirm] を選択します。

> **Note**
>
> ゲートウェイを削除すると、アクション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、「AWS Storage Gateway コンソールを使用したゲートウェイの削除と関連リソースの除去」を参照してください。

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

ハードウェアアプライアンスの削除

でハードウェアアプライアンスをアクティブ化した後AWSアカウントの場合は、別の方法で移動してアクティブ化する必要があるかもしれませんAWSアカウント. この場合、まず [] からアプライアンスを削除します。AWSアカウントを作成し、別のアカウントでアクティベートするAWSアカウント. アプライアンスは、から完全に削除することもできます。AWSもはや必要がなくなったので、アカウントを作成します。ハードウェアアプライアンスを削除するには、以下の手順に従います。

ハードウェアアプライアンスを削除するには

1. ハードウェアアプライアンスにゲートウェイをインストールした場合は、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、「」を参照してください。[ハードウェアアプライアンスからのゲートウェイの削除]。
2. [ハードウェア] ページで、削除する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。
4. [リソースの削除を確認] ダイアログボックスで、確認のチェックボックスをオンにして [Delete (削除)] を選択します。正常に削除されたことを示すメッセージが表示されます。

   ハードウェアアプライアンスを削除すると、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すべてのリソースも削除されますが、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。

AWS Storage Gatewayの開始方法

このセクションでは、でファイルゲートウェイを作成してアクティブ化する方法の手順を確認できます。AWS Storage Gateway。開始する前に、「」で説明されている必要な前提条件およびその他の要件を満たしていることを確認します。Amazon FSx ファイルゲートウェイのセットアップ。

トピック

- ステップ 1: Amazon FSx for Windows File Server ファイルシステムを作成する
- ステップ 2: (オプション) Amazon VPC エンドポイントを作成する
- ステップ 3: 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

ステップ 1: Amazon FSx for Windows File Server ファイルシステムを作成する

で Amazon FSx ファイルゲートウェイを作成するにはAWS Storage Gatewayで、最初のステップは Amazon FSx for Windows File Server ファイルシステムを作成することです。Amazon FSx ファイルシステムを作成済みの場合は、次のステップに進みます。ステップ 2: (オプション) Amazon VPC エンドポイントを作成する。

> **Note**
>
> FSX ファイルゲートウェイから Amazon FSX ファイルシステムに書き込む場合は、次の制限が適用されます。
>
> - Amazon FSx ファイルシステムとお使いの FSx ファイルゲートウェイは、同じファイルシステムで所有されている必要があります。AWSアカウントと同じ場所にあるAWSリージョン。
> - 各ゲートウェイは、5 つのアタッチされたファイルシステムをサポートできます。ファイル・システムを接続すると、選択したゲートウェイが容量にあるかどうかが Storage Gateway コンソールから通知されます。その場合、別のゲートウェイをアタッチする前に、別のゲートウェイを選択するか、ファイルシステムをデタッチする必要があります。
> - FSx File Gateway はソフトストレージクォータ (ユーザーがデータ制限を超えた場合に警告を発する) をサポートしますが、ハードクォータ (書き込みアクセスを拒否してデータ制限を強制する) はサポートしていません。ソフトクォータは、Amazon FSx 管理者ユーザーを除くすべてのユーザーでサポートされています。ストレージクォータのセットアッ

プの詳細については、「」を参照してください。ストレージクォータのAmazon FSx for Windows File Server ユーザーガイド。

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

1. を開くAWS Management Consoleでhttps://console.aws.amazon.com/fsx/home/をクリックし、ゲートウェイを作成するリージョンを選択します。
2. 「」の指示に従って、Amazon FSx の開始方法のAmazon FSx for Windows File Server ユーザーガイド。

ステップ 2: (オプション) Amazon VPC エンドポイントを作成する

で Amazon FSx ファイルゲートウェイを作成する場合は、この手順は必要ありません。AWS Storage Gateway。ただし、Storage Gateway にVirtual Private Cloud (VPC) エンドポイントを作成し、VPC でゲートウェイをアクティブ化することをお勧めします。これにより、VPC とStorage Gateway との間にプライベート接続が作成されます。

Storage Gateway の VPC エンドポイントがすでに作成されている場合は、FSX ファイルゲートウェイに使用できます。複数のゲートウェイをサポートできる単一の VPC エンドポイントにより、VPC にデプロイされたゲートウェイが Storage Gateway サービス VPC に接続できるようになります。Storage Gateway の VPC エンドポイントをすでに作成している場合は、次のステップに進みます。ステップ 3: 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。

Amazon VPC エンドポイントを作成するには

1. を開くAWS Management Consoleでhttps://console.aws.amazon.com/vpc/home/を選択し、AWSゲートウェイを作成するリージョン。
2. 左のナビゲーションペインで、[] を選択します。エンドポイント[] を選択してから、エンドポイントの作成。
3. リポジトリの []エンドポイントの作成ページで、[] を選択します。AWSサービスにとってサービスカテゴリ。
4. を使用する場合サービス名をクリックして、[] を検索します。`storagegateway`。リージョンは、デフォルトでサインインしているリージョンに設定されます。たとえば、`com.amazonaws.region.storagegateway`。したがって、米国東部 (オハイオ) にサインインしている場合は、`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. を使用する場合セキュリティグループで、VPC で使用する新しいセキュリティグループを作成します。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 1026
   - TCP 1027
   - TCP 1028
   - TCP 1031
   - TCP 2222

   > **Note**
   >
   > ゲートウェイは、これらのポートを使用して、Storage Gateway 管理サービスと通信します。VPC エンドポイントを使用している場合は、ゲートウェイの IP アドレスからのインバウンドアクセス用に次のポートが開いている必要があります。

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次のとおりです。Pending。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。

   > **Note**
   >
   > この VPC エンドポイントの名前を指定することをお勧めします。たとえば、**`StorageGatewayEndpoint`**。

9. エンドポイントが作成されたら、[] を選択します。エンドポイント[] を選択し、[] を選択します。VPC エンドポイント。
10. 左DNS 名セクションで、アベイラビリティーゾーンを指定していない最初のドメインネームシステム (DNS) 名を使用します。DNS 名は、次のようになります。

    ```
    vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
    east-1.vpce.amazonaws.com
    ```

> **Note**
>
> この DNS 名は、VPC に割り当てられている Storage Gateway エンドポイントプライベート IP アドレスに解決されます。

11. ファイアウォールで開く必要があるポートのリストを確認します。

これで VPC エンドポイントを作成したので、FSx File Gateway を作成できます。

次のステップ

the section called “ステップ 3: FSx ファイルゲートウェイを作成してアクティブ化する”

ステップ 3: Amazon FSx ファイルゲートウェイを作成してアクティブ化する

このセクションでは、でファイルゲートウェイを作成、デプロイ、およびアクティブ化する方法の手順を確認できます。AWS Storage Gateway。

トピック

Amazon FSx ファイルゲートウェイをセットアップする

新しい FSx ファイルゲートウェイをセットアップするには

1. を開くAWS Management Consoleでhttps://console.aws.amazon.com/storagegateway/home/を選択し、AWS リージョンゲートウェイを作成する場所。
2. 選択ゲートウェイの作成をクリックして、[] を開きます。ゲートウェイの設定ページで.
3. 左ゲートウェイ設定[] 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。ゲートウェイを作成したら、この名前を検索して、リストページでゲートウェイを検索できます。AWS Storage Gatewayconsole.

b. を使用する場合ゲートウェイのタイムゾーンで、ゲートウェイをデプロイする世界の地域のタイムゾーンを選択します。

4. 左ゲートウェイのオプションセクションに設定します。ゲートウェイタイプで、Amazon FSx ファイルゲートウェイ。

5. 左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. を使用する場合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 のコンソール・ページに表示されるプラットフォーム固有の指示に従って、ホスト・プラットフォームをセットアップします。以下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、および構成します。
- 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、および構成します。
- Linux KVM— 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、および設定します。
- Amazon EC2— Amazon EC2 インスタンスを設定して起動します。ゲートウェイをホストします。
- ハードウェアアプライアンス— 専用物理ハードウェアアプライアンスを注文するAWS[] を選択すると、ゲートウェイをホストできます。

b. を使用する場合ゲートウェイの設定を確認で、チェックボックスをオンにして、選択したホストプラットフォームのデプロイメント手順を実行したことを確認します。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。

6. ゲートウェイがセットアップされたら、ゲートウェイがどのように接続して通信するかを選択する必要があります。AWS。選択次をクリックして、[] に進みます。

Amazon FSx ファイルゲートウェイをConnect するAWS

新しい FSx ファイルゲートウェイをに接続するにはAWS

1. まだ実行していない場合は、「」で説明する手順を実行します。Amazon FSx ファイルゲートウェイをセットアップする。完了したら、[] を選択します。次をクリックして、[] を開きます。に接続します。AWSのページでAWS Storage Gatewayconsole.
2. 左エンドポイントオプションセクションに設定します。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。以下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— ゲートウェイがと通信するAWSパブリックインターネット経由で このオプションを選択した場合は、FIPS 対応エンドポイントチェックボックスをオンにして、接続が連邦情報処理標準 (FIPS) に準拠している必要があるかどうかを指定します。

     > **Note**
     >
     > アクセス時に FIPS 140-2 検証済みの暗号化モジュールが必要な場合はAWSコマンドラインインターフェイスまたは API を使用して、FIPS 準拠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 サービスエンドポイントは、一部でのみ使用できます。AWS地域。詳細については、AWS Storage Gateway 全般のリファレンスの「AWS エンドポイントとクォータ」を参照してください。

   - VPC がホストされている— ゲートウェイがと通信するAWSVirtual Private Cloud (VPC) とのプライベート接続を使用して、ネットワーク設定をコントロールできます。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。また、その VPC エンドポイントドメインネームシステム (DNS) 名または IP アドレスを指定することもできます。
3. 左ゲートウェイ接続オプションセクションに設定します。接続オプションで、ゲートウェイの識別方法を選択します。AWS。以下のオプションから選択できます。

   - IP address— 対応するフィールドにゲートウェイの IP アドレスを指定します。この IP アドレスは、パブリックであるか、現在のネットワーク内からアクセス可能である必要があります。また、Web ブラウザから IP アドレスに接続できる必要があります。

ゲートウェイ IP アドレスを取得するには、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します。

- アクティベーションキー— 対応するフィールドにゲートウェイのアクティベーションキーを指定します。ゲートウェイの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できます。ゲートウェイの IP アドレスが使用できない場合は、このオプションを選択します。

4. これで、ゲートウェイの接続方法を選択しました。AWSの場合は、ゲートウェイをアクティブ化する必要があります。選択次をクリックして、[] に進みます。

設定を確認し、Amazon FSx ファイルゲートウェイをアクティブ化する

新しい FSx ファイルゲートウェイをアクティブ化するには

1. まだ実行していない場合は、次のトピックで説明する手順を実行します。

   - Amazon FSx ファイルゲートウェイをセットアップする
   - Amazon FSx ファイルゲートウェイをConnect するAWS

   完了したら、[] を選択します。次をクリックして、[] を開きます。確認してアクティブ化します。のページでAWS Storage Gatewayconsole.

2. ページの各セクションの最初の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含まれている場合は、編集をクリックして、対応する設定ページに戻り、変更を加えます。

   > **Important**
   >
   > ゲートウェイがアクティブ化された後は、ゲートウェイオプションまたは接続設定を変更することはできません。

4. ゲートウェイをアクティブ化したので、ローカルストレージディスクを割り当ててログを構成するための最初の構成を実行する必要があります。選択次をクリックして、[] に進みます。

Amazon FSx ファイルゲートウェイを設定する

新しい FSx ファイルゲートウェイで初回設定を実行するには

1. まだ実行していない場合は、次のトピックで説明する手順を実行します。

   - Amazon FSx ファイルゲートウェイをセットアップする
   - Amazon FSx ファイルゲートウェイをConnect するAWS
   - 設定を確認し、Amazon FSx ファイルゲートウェイをアクティブ化する

   完了したら、[] を選択します。次をクリックして、[] を開きます。ゲートウェイの設定のページでAWS Storage Gatewayconsole.
2. 左キャッシュ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、150 ギガバイト (GiB) 以上の容量を持つ少なくとも 1 つのローカルディスクをCache。このセクションにリストされてい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した物理ストレージに対応しています。
3. 左CloudWatch ロググループセクションで、ゲートウェイの健全性を監視するための Amazon CloudWatch Logs の設定方法を選択します。以下のオプションから選択できます。

   - 新しいロググループの作成— ゲートウェイを監視する新しいロググループを設定します。
   - 既存のロググループを使用する— 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。
   - ロギングを無効化します。— Amazon CloudWatch Logs を使用してゲートウェイを監視しないでください。
4. 左CloudWatch アラームセクションで、ゲートウェイのメトリックスが定義された制限から逸脱したときに通知するように Amazon CloudWatch アラームを設定する方法を選択します。以下のオプションから選択できます。

   - アラームを無効化します。— CloudWatch アラームを使用してゲートウェイのメトリクスに関する通知を受け取らないでください。
   - CloudWatch アラームのカスタム— ゲートウェイのメトリクスについて通知されるように、新しい CloudWatch アラームを設定します。選択アラームの作成をクリックして、Amazon CloudWatch コンソールでメトリクスを定義してアラームアクションを指定します。手順については、以下を参照してください。Amazon CloudWatch アラームを使用するのAmazon CloudWatch ユーザーガイド。

5. （オプション）タグセクションで、[] を選択します。新しいタグを追加をクリックし、リストページでゲートウェイの検索やフィルタリングに便利な大文字と小文字の区別があるキーと値のペアを入力します。AWS Storage Gatewayconsole. 必要な数のタグを追加するには、この手順を繰り返します。
6. （オプション）VMware HA 設定の確認セクションで、VMware High Availability (HA) が有効になっているクラスターの一部として VMware ホストにゲートウェイがデプロイされている場合は、VMware HA の確認をクリックして、HA 設定が正常に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。
   > この手順は、ゲートウェイ設定プロセスを完了するために必要ありません。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. 選択設定[] をクリックすると、ゲートウェイの作成が完了します。

   新しいゲートウェイのステータスを確認するには、[ゲートウェイのページでAWS Storage Gatewayconsole.

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

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

Active Directory 設定の構成

このステップでは、Storage Gateway ゲートウェイで Amazon FSx ファイルゲートウェイアクセス設定を構成し、Microsoft Active Directory に参加します。

Active Directory 設定の構成

1. Storage Gateway コンソールで、FSx ファイルシステムの接続。
2. リポジトリの []ゲートウェイの確認ページのゲートウェイのリストで、使用する Amazon FSx ファイルゲートウェイを選択します。

   ゲートウェイがない場合は、作成する必要があります。ゲートウェイが Active Directory ドメインコントローラの名前を解決できることを確認します。詳細については、「必要な前提条件」を参照してください。
3. の値を入力します。Active Directory 設定:

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

   - を使用する場合ドメイン名で、使用するActive Directory のドメイン名を入力します。
   - を使用する場合ドメインユーザーで、Active Directory のユーザー名を入力します。
   - を使用する場合ドメインパスワードで、ドメインユーザーのパスワードを入力します。

     > **Note**
     >
     > アカウントによってサーバーをドメインに結合することができる必要があります。

   - を使用する場合組織単位-オプションでは、Active Directory が属する組織単位を指定できます。
   - の値を入力します。ドメインコントローラー-オプション。
4. 選択次をクリックして、[] を開きます。FSx ファイルシステムをアタッチするページで.

次のステップ

Amazon FSx for Windows File Server ファイルシステムをアタッチします。

Amazon FSx for Windows File Server ファイルシステムをアタッチします。

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

> **Note**
>
> Amazon FSX ファイルゲートウェイから Amazon FSx ファイルシステムに書き込みを行う場合は、以下の制限が適用されます。
>
> - Amazon FSx ファイルシステムとあなたの FSx ファイルは、同じファイルによって所有されている必要があります。AWS アカウント同じ場所にあるAWS リージョン。
> - 各ゲートウェイは 5 つまでのファイルシステムをサポートできます。ファイル· システムを接続すると、選択したゲートウェイが容量にあるかどうかが Storage Gateway コンソールから通知されます。その場合、別のゲートウェイをアタッチする前に、別のゲートウェイを選択するか、ファイルシステムをデタッチする必要があります。
> - FSx File はソフトストレージクォータ (ユーザーがデータ制限を超えた場合に警告する) をサポートしますが、ハードクォータ (書き込みアクセスを拒否してデータ制限を強制する) はサポートしていません。ソフトクォータは、Amazon FSx 管理者ユーザーを除くすべてのユーザーでサポートされています。ストレージクォータの設定の詳細については、「」を参照してください。ストレージクォータ「Amazon FSx ユーザーガイド」を参照してください。

Amazon FSx ファイルシステムをアタッチするには

1. Storage Gateway コンソールで、FSx ファイルシステム >FSx ファイルシステムの接続[] ページで、[] の次のフィールドに入力します。FSx ファイルシステム設定セクションに追加します。
   - を使用する場合FSx ファイルシステム名で、アタッチするファイルシステムを、ドロップダウンリストから選択します。
   - を使用する場合ローカルエンドポイント IP アドレスで、クライアントが FSx ファイルシステム上のファイル共有を参照するために使用するゲートウェイ IP アドレスを入力します。

> **Note**
>
> - ゲートウェイにファイルシステムを 1 つだけアタッチする場合は、このフィールドを空白のままにして、ゲートウェイのすべての IP アドレスでファイルシステム上の共有を使用できるようにします。複数のファイルシステムを接続する場合は、各ファイルシステムに IP アドレスを指定する必要があります。
> - IP アドレスなしでファイルシステムをアタッチし、後で別のファイルシステムをアタッチする必要がある場合は、最初のファイルシステムをデタッチし、IP アドレスで再接続する必要があります。
> - Amazon EC2 ゲートウェイの場合、EC2 インスタンスのプライベート IP アドレスを指定できます。ただし、別のファイルシステムによってすでに使用されている場合は、ゲートウェイに新しいプライベートアドレスを追加してから再起動する必要があります。詳細については、「」を参照してください。複数の IP アドレスのAmazon EC2 ユーザーガイド。
> - オンプレミスゲートウェイの場合、プライマリネットワークインターフェイス (静的または DHCP) の IP アドレスを指定できます。ただし、別のファイルシステムですでに使用されている場合は、仮想 IP として使用できるプライマリインターフェイスと同じサブネットから別の IP アドレスを指定する必要があります。プライマリ以外のネットワークインターフェイスに割り当てられた IP アドレスを使用しないでください。

2. 左サービスアカウント設定[] セクションで、Amazon FSx ファイルシステムに関連付けられているユーザー名とパスワードを入力します。

> **Note**
>
> このユーザーは、Amazon FSx ファイルシステムに関連付けられている Active Directory サービスのBackup オペレータグループのメンバーであるか、同等の権限を持っている必要があります。

> **Important**
>
> ファイル、フォルダ、およびファイルメタデータに対する十分なアクセス許可を確保するために、このユーザーをファイルシステム管理者グループのメンバーにすることをお勧めします。

使用している場合AWS Directory ServiceAmazon FSx for Windows File Server と Microsoft Active Directory の場合、ユーザーはAWSが委任した FSx 管理者グループ。Amazon FSx for Windows File Server で自己管理型 Active Directory を使用している場合、ユーザーは 2 つのグループ (ドメイン管理者またはファイルシステムを作成したときにファイルシステム管理用に指定したカスタム委任ファイルシステム管理者グループ) のいずれかのメンバーである必要があります。
詳細については、「」を参照してください。Amazon FSx サービスアカウントへの権限の委任のAmazon FSx for Windows File Server ユーザーガイド。

3. 左監査ログセクションで、[] を選択します。既存のログタイプをクリックし、Amazon FSx ファイルシステムへのアクセスを監視するために使用するログを選択します。新しいものを作成することもできます。システムを監視しない場合は、[] を選択します。[Disable logging (ログ記録の無効化)]。
4. を使用する場合自動キャッシュ更新設定で、キャッシュを自動的に更新する場合は、更新間隔の設定5分から 30 日の間隔を指定します。
5. (オプション)タグセクションで、[] を選択します。新しいタグを追加をクリックして、設定にタグを付けるためのキーと値を追加します。
6. 選択次[] を選択し、[] の設定を確認します。設定を変更するには、[] を選択します。編集各セクションで説明します。
7. 完了したら、[Finish] を選択します。

次のステップ

ファイル共有をマウントして使用します。

ファイル共有をマウントして使用します。

ファイル共有をクライアントにマウントする前に、Amazon FSx ファイルシステムのステータスが使用可能。ファイル共有がマウントされたら、Amazon FSx ファイルゲートウェイ (FSx ファイル) の使用を開始できます。

トピック

クライアントに SMB ファイル共有をマウントします。

この手順では、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。

- `-net use` command — [] を使用した場合を除いて、複数のシステム再起動をまたいでは保持されません。`/persistent:(yes:no)`スイッチ。
- `-CmdKey`コマンドラインユーティリティ — 再起動後にも保持される、マウントされた SMB ファイル共有への永続的な接続を作成します。
- ファイルエクスプローラーにマッピングされるネットワークドライブ — サインインで再接続するためにマウントされたファイル共有を設定して、ネットワーク認証情報の入力を必要とします。
- PowerShell スクリプト — 永続性があり、マウント中にオペレーティングシステムで表示または非表示できます。

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

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

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

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

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

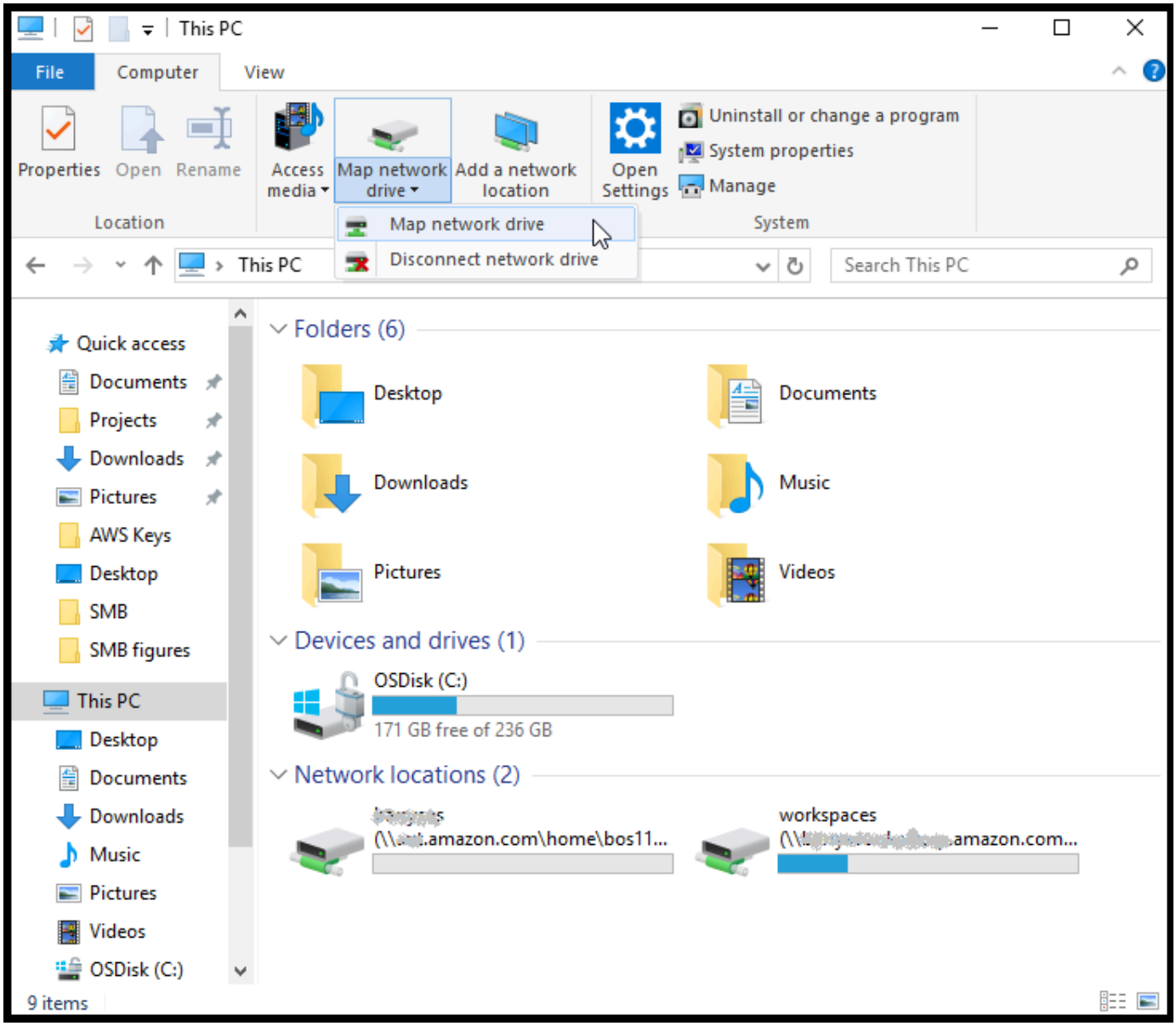
1. Windows キーを押し、「」と入力します。**cmd**[] の順にクリックし、コマンドプロンプトメニューアイテムを表示します。
2. [] のコンテキスト (右クリック) メニューを開きます。コマンドプロントを選択し、管理者として実行。
3. 次のコマンドを入力します。

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

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

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

1. Windows キーを押し、「」と入力します。**File Explorer**の検索ウィンドウボックス、または**Win+E**。
2. ナビゲーションペインで [] を選択します。このPC。
3. リポジトリの []Computer[] タブで、[]ネットワークドライブをマッピングします。[] を選択してから、ネットワークドライブをマッピングします。ここでも、次のスクリーンショットに示すように。



4. 左ネットワークドライブをマッピングします。] ダイアログボックスで、[] のドライブ文字を選択します。Drive。
5. を使用する場合フォルダ「」と入力します。***[File Gateway IP]**[SMB File Share Name]***、またはブラウズ[] ダイアログボックスから SMB ファイル共有を選択します。
6. (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、[Reconnect at sign-up (サインアップ時に再接続)] を選択します。
7. (オプション) Active Directory ログオンあるいはゲストアカウントユーザーパスワードをユーザーが入力するようにする場合には、[Connect using different credentials (異なる認証情報を使用して接続)] を選択します。
8. [完了] を選択して、マウントポイントを完了します。

FSx ファイルをテストする

ファイルとディレクトリは、マップ済みのドライブにコピーできます。ファイルは FSx for Windows File Server システムに自動的にアップロードされます。

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

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

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

Virtual Private Cloud でゲートウェイをアクティベートする

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。これで、ソフトウェアアプライアンスを使用して、にデータを転送することができます。AWSゲートウェイが通信していないストレージAWSパブリックインターネット経由でのストレージサービス。Amazon VPC サービスを使用して、起動できますAWSカスタム仮想ネットワーク内のリソース。Virtual Private Cloud (VPC) を使用して、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、「」を参照してください。Amazon VPC とは?のAmazon VPC User Guide。

VPC 内の Storage Gateway VPC エンドポイントでゲートウェイを使用するには、以下の操作を行います。

- 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、VPC エンドポイント ID を取得します。ゲートウェイを作成してアクティブ化するときに、この VPC エンドポイント ID を指定します。
- ファイルゲートウェイをアクティブ化する場合は、Amazon S3 用の VPC エンドポイントを作成します。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します。
- ファイルゲートウェイをアクティブ化する場合は、HTTP プロキシを設定し、それをファイルゲートウェイの VM ローカルコンソールで設定します。このプロキシは、ハイパーバイザーベースのオンプレミスのファイルゲートウェイに必要です。これには、VMware、Microsoft HyperV をベースとするものや Linux カーネルベースの仮想マシン (KVM) などがあります。このような場合、ゲートウェイが VPC の外部から Amazon S3 プライベートエンドポイントにアクセスできるようにするためには、プロキシが必要です。HTTP プロキシの設定方法については、「HTTP プロキシの設定」を参照してください。

> **Note**
>
> ゲートウェイは、VPC エンドポイントが作成されたリージョンと同じリージョンでアクティブ化する必要があります。
> ファイルゲートウェイの場合、ファイル共有用に構成された Amazon S3 ストレージは、Amazon S3 用の VPC エンドポイントを作成したリージョンと同じリージョンに存在している必要があります。

トピック

Storage Gateway 用の VPC エンドポイントの作成

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 用の VPC エンドポイントがすでに設定されている場合は、それを使用できます。

Storage Gateway 用の VPC エンドポイントを作成するには

1. AWS Management Console にサインインして、Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) 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. リポジトリの []エンドポイントの作成[] ページで [] を選択しますAWSサービスにとってサービスのカテゴリ。
4. [サービス名] には [com.amazonaws.*region*.storagegateway] を選択します。例えば、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 [pending (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. [DNS 名] セクションで、アベイラビリティーゾーンを指定していない最初の DNS 名を使用します。DNS 名は以下のように表示されます。`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できます。

> **Important**
>
> ファイルゲートウェイを作成する場合は、Amazon S3 のエンドポイントも作成する必要があります。上記の「Storage Gateway 用の VPC エンドポイントを作成するには」セクションに示されているステップに従います。ただし、`com.amazonaws.us-east-2.s3`代わりに [サービス名] の下にあります。次に、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、以下を参照してください。ゲートウェイエンドポイントの作成。

HTTP プロキシの設定と構成 (オンプレミスのファイルゲートウェイのみ)

ファイルゲートウェイをアクティブ化する場合は、HTTP プロキシを設定し、ファイルゲートウェイの VM ローカルコンソールを使用して構成する必要があります。このプロキシは、オンプレミスのファイルゲートウェイが VPC の外部から Amazon S3 プライベートエンドポイントにアクセスするために必要です。Amazon EC2 に既に HTTP プロキシがある場合は、それを使用できます。ただし、必ず次の 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する必要があります。

- TCP 443
- TCP 1026
- TCP 1027
- TCP 1028

- TCP 1031
- TCP 2222

Amazon EC2 プロキシがない場合は、次の手順に従って HTTP プロキシを設定および構成します。

プロキシサーバーをセットアップするには

1. Amazon EC2 Linux AMI を起動します。ネットワークに最適化されたインスタンスファミリー (例: c5n.large) を使用することをお勧めします。
2. 次のコマンドを使用して squid をインストールします。**sudo yum install squid**。 これにより、デフォルトの設定ファイルがに作成されます。/etc/squid/squid.conf。
3. この設定ファイルの内容を以下に置き換えます。

```
#
# Recommended minimum configuration:
#

# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
acl localnet src 10.0.0.0/8              # RFC1918 possible internal network
acl localnet src 172.16.0.0/12       # RFC1918 possible internal network
acl localnet src 192.168.0.0/16    # RFC1918 possible internal network
acl localnet src fc00::/7       # RFC 4193 local private network range
acl localnet src fe80::/10      # RFC 4291 link-local (directly plugged) machines

acl SSL_ports port 443
acl SSL_ports port 1026
acl SSL_ports port 1027
acl SSL_ports port 1028
acl SSL_ports port 1031
acl SSL_ports port 2222
acl CONNECT method CONNECT

#
# Recommended minimum Access Permission configuration:
#
# Deny requests to certain unsafe ports
http_access deny !SSL_ports

# Deny CONNECT to other than secure SSL ports
```

```
http_access deny CONNECT !SSL_ports

# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localnet
http_access allow localhost

# And finally deny all other access to this proxy
http_access deny all

# Squid normally listens to port 3128
http_port 3128

# Leave coredumps in the first cache dir
coredump_dir /var/spool/squid

#
# Add any of your own refresh_pattern entries above these.
#
refresh_pattern ^ftp:                    1440       20%        10080
refresh_pattern ^gopher:            1440       0%          1440
refresh_pattern -i (/cgi-bin/|\?) 0             0%          0
refresh_pattern .                              0              20%        4320
```

4. プロキシサーバーをロックダウンする必要がなく、変更が不要な場合は、次のコマンドを使用してプロキシサーバーを有効にし、起動します。これらのコマンドを実行すると、起動時にサーバーが起動します。

```
sudo chkconfig squid on
sudo service squid start
```

これで、Storage Gateway の HTTP プロキシを使用するように設定されました。プロキシを使用するようにゲートウェイを設定する場合は、デフォルトの squid ポート 3128 を使用します。生成された squid conf ファイルは、必要とされる以下の TCP ポートにデフォルトで対応しています。

- TCP 443

- TCP 1026
- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

VM ローカルコンソールを使用して HTTP プロキシを設定するには

1. ゲートウェイの VM ローカルコンソールにログインします。ログイン方法については、ファイルゲートウェイのローカルコンソールにログインする を参照してください。
2. メインメニューで、[HTTP プロキシの設定] を選択します。
3. [設定] メニューで、[HTTP プロキシの設定] を選択します。
4. プロキシサーバーのホスト名とポートを入力します。

HTTP プロキシの設定方法に関する詳細については、HTTP プロキシの設定 を参照してください。

HTTP プロキシで必要なポートへのトラフィックを許可する

HTTPプロキシを使用する場合は、Storage Gateway から次の宛先およびポートへのトラフィックを許可するようにしてください。

パブリックエンドポイント経由で通信している場合、は、次のStorage Gateway サービスと通信を行います。

```
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
storagegateway.region.amazonaws.com:443 (Required for making API calls)
s3.region.amazonaws.com (Required only for File Gateway)
```

> **Important**
>
> ゲートウェイに応じてAWSリージョン、置換##は、対応するリージョン文字列でエンドポイントに表示されます。たとえば、米国西部 (オレゴン) リージョンにゲート

ウェイを作成する場合、エンドポイントはのようになります。`storagegateway.us-west-2.amazonaws.com:443`。

Storage Gateway が VPC エンドポイント経由で通信している場合、は VPC エンドポイントと通信します。AWSStorage Gateway VPC エンドポイント上の複数のポートと、Amazon S3 プライベートエンドポイント上のポート 443 を介してサービス。

- Storage Gateway の VPC エンドポイントの TCP ポート。
  - 443、1026、1027、1028、1031、2222
- S3 プライベートエンドポイントの TCP ポート
  - 443

Amazon FSx ファイルゲートウェイのリソースを管理する

以下のセクションでは、Amazon FSx ファイルゲートウェイ (FSx ファイル) リソースを管理する方法について説明します。これには、Amazon FSx ファイルシステムのアタッチとデタッチ、Microsoft Active Directory の設定が含まれます。

トピック

Amazon FSx ファイルシステムの接続

FSx for Windows File Server ファイルシステムを FSx ファイルに接続するには、FSx for Windows ファイルサーバーファイルシステムが必要です。ファイルシステムがない場合は、作成する必要があります。手順については、以下を参照してください。ステップ 1: ファイルシステムの作成のAmazon FSx for Windows File Server ユーザーガイド。

次のステップは、FSx ファイルをアクティブ化し、Active Directory ドメインに参加するようにゲートウェイを構成することです。手順については、「Active Directory 設定の構成」を参照してください。

> **Note**
>
> ゲートウェイがドメインに参加したら、ドメインに再度参加するように構成する必要はありません。

各ゲートウェイは、最大 5 個のファイルシステムをサポートできます。ファイルシステムの接続方法については、「」を参照してください。Amazon FSx for Windows File Server ファイルシステムをアタッチします。。

FSx ファイルのアクティブディレクトリの設定

FSx ファイルを使用するには、Active Directory ドメインに参加するようにゲートウェイを構成する必要があります。手順については、「Active Directory 設定の構成」を参照してください。

Active Directory 設定の構成

Active Directory ドメインに参加するようにゲートウェイを構成したら、Active Directory の設定を編集できます。

Active Directory 設定の編集

1. [Storage Gateway] コンソールを開きます。https://console.aws.amazon.com/storagegateway/home。
2. ナビゲーションペインで、[] を選択します。ゲートウェイ[] を選択してから、Active Directory 設定の編集対象ゲートウェイを選択します。
3. を使用する場合アクションで、SMB 設定の編集[] を選択してから、Active Directory 設定。
4. [Active Directory 設定] セクションで要求された情報を提供して、[] を選択します。変更の保存。

FSx ファイル設定の編集

ゲートウェイをアクティブ化した後で、ゲートウェイ設定を編集できます。

ゲートウェイ設定を編集するには

1. [Storage Gateway] コンソールを開きます。https://console.aws.amazon.com/storagegateway/home。
2. ナビゲーションペインで、[] を選択します。ゲートウェイ[] を選択してから、設定を編集するゲートウェイを選択します。
3. を使用する場合アクションで、ゲートウェイ情報を編集する。
4. を使用する場合ゲートウェイ名で、選択したゲートウェイの名前を編集します。
5. を使用する場合ゲートウェイのタイムゾーン[] で、タイムゾーンを選択します。
6. を使用する場合ゲートウェイヘルスロググループで、Amazon 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するオプションの 1 つを選択します。

を選択すると既存のロググループを使用する[] で、[] からロググループを選択します。既存のロググループリスト[] を選択してから、変更の保存。

Amazon FSx for Windows File Server ファイルシステム設定の編集

Amazon FSx for Windows File Server ファイルシステムを作成したら、ファイルシステムの設定を編集できます。

Amazon FSx ファイルシステム設定を編集するには

1. [Storage Gateway] コンソールを開きます。https://console.aws.amazon.com/storagegateway/home。
2. ナビゲーションペインで、[] を選択します。ファイルシステム[] を選択し、設定を編集するファイルシステムを選択します。
3. を使用する場合アクションで、ファイルシステム設定の編集。
4. [ファイルシステム設定] セクションで、ゲートウェイ、Amazon FSx の場所、および IP アドレスの情報を確認します。

   > **Note**
   >
   > ファイルシステムの IP アドレスは、ゲートウェイに接続された後で編集できません。IP アドレスを変更するには、ファイルシステムをデタッチして再接続する必要があります。

5. 左監査ログセクションで、CloudWatch ロググループを使用して Amazon FSx ファイルシステムへのアクセスを監視するオプションを選択します。既存のロググループを使用できます。
6. を使用する場合自動キャッシュ更新設定[] で、オプションを選択します。を選択すると更新間隔の設定で、Time To Live (TTL) を使用してファイルシステムのキャッシュを更新する時間を日、時、分で設定します。

   TTL は、最後の更新からの時間の長さです。その時間が経過した後にディレクトリにアクセスすると、ファイルゲートウェイは Amazon FSx ファイルシステムからそのディレクトリの内容を更新します。

> **Note**
>
> 有効な更新間隔の値は 5 分から 30 日の間です。

7. 左サービスアカウント設定-オプション[] セクションで、ユーザー名とパスワード。これらの認証情報は、Amazon FSx ファイルシステムに関連付けられた Active Directory サービスのBackup管理者ロールを持つユーザー用です。
8. [Save changes] (変更を保存) をクリックします。

Amazon FSx ファイルシステムのデタッチ

ファイルシステムをデタッチしても、FSx for Windows File Server 内のデータは削除されません。ファイルシステムを削除する前にこれらのファイルシステム上のファイル共有に書き込まれたデータは、FSx for Windows File Server アップロードされます。

Amazon FSx ファイルシステムをデタッチするには

1. [Storage Gateway] コンソールを開きます。https://console.aws.amazon.com/storagegateway/home。
2. 左のナビゲーションペインで、[] を選択します。ファイルシステム[] を選択してから、デタッチするファイルシステムを選択します。複数のファイルシステムを削除できます。
3. を使用する場合アクションで、ファイルシステムのデタッチ。
4. Enter**`detach`**確認するボックスで、Detach。

ファイルゲートウェイのモニタリング

で、ファイルゲートウェイと関連リソースを監視できます。AWS Storage GatewayAmazon CloudWatch メトリクスとファイル共有監査ログを使用して。また、CloudWatch イベントを使用して、ファイルオペレーションの完了時に通知を受け取ることができます。ファイルゲートウェイタイプのメトリクスの詳細については、「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。

トピック

- CloudWatch ロググループを使用したファイルゲートウェイのヘルスログの取得
- Amazon CloudWatch メトリクスを使用する
- ゲートウェイメトリクスについて
- ファイルシステムのメトリクスを理解する
- 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ファイルゲートウェイのヘルスログの取得

Amazon CloudWatch Logs を使用して、ファイルゲートウェイと関連リソースのヘルスに関する情報を取得できます。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、「」を参照してください。サブスクリプションを使用したログデータのリアルタイム処理のAmazon CloudWatch ユーザーガイド。

たとえば、ゲートウェイをモニタリングし、ファイルゲートウェイから Amazon FSx ファイルシステムへのファイルのアップロードに失敗したときに通知を受け取るように CloudWatch ロググループを設定できます。このグループの設定は、ゲートウェイをアクティブ化するときか、ゲートウェイをアクティブ化して実行した後に可能です。ゲートウェイ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、「」を参照してください。Amazon FSx ファイルゲートウェイを設定する。CloudWatch ロググループの一般情報については、「」を参照してください。ロググループとログストリームを操作するのAmazon CloudWatch ユーザーガイド。

以下に、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を示します。

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 S3 Glacier に移行されています。"type" の値は、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、「ファイルゲートウェイ問題のトラブルシューティング」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。

これらのタイプのエラーをトラブルシューティングおよび修正する方法については、「ファイルゲートウェイ問題のトラブルシューティング」を参照してください。

ゲートウェイのアクティブ化後に CloudWatch ロググループを設定する

以下の手順では、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。

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. にサインインします。AWS Management Consoleで、Storage Gateway コンソールを開きます。https://console.aws.amazon.com/storagegateway/home。
2. ナビゲーションペインで [] を選択します。ゲートウェイの順に選択し、CloudWatch ロググループを設定するゲートウェイを選択します。
3. を使用する場合アクションで、ゲートウェイ情報の編集。または、の詳細タブ、Health スロログそして[有効] なしで、ロググループを構成するをクリックして、[] を開きます。編集CustomerGatewayName[] ダイアログボックス。
4. を使用する場合ゲートウェイヘルスロググループで、次のいずれかを選択します。

   - [Disable logging (ログ記録の無効化)]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。
   - 新しいロググループの作成をクリックして、新しい CloudWatch ロググループを作成します。
   - 既存のロググループの使用をクリックして、すでに存在している CloudWatch ロググループを使用します。

[] から [] ロググループを選択します。既存のロググループリスト。

5. [Save changes] (変更を保存) 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 [] を選択します。ゲートウェイを選択し、CloudWatch ロググループを設定したゲートウェイを選択します。
   2. [の詳細タブ、およびHealth スログで、[CloudWatch Logs]。-ロググループの詳細CloudWatch コンソールでページが開きます。

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. にサインインします。AWS Management Consoleで、Storage Gateway コンソールを開きます。https://console.aws.amazon.com/storagegateway/home。
2. 選択ゲートウェイの順に選択し、CloudWatch ロググループを設定するゲートウェイを選択します。
3. を使用する場合アクションで、ゲートウェイ情報の編集。または、の詳細タブ、の横にあるログ記録、の下で[有効] なしで、ロググループを構成するをクリックして、[] を開きます。ゲートウェイ情報の編集[] ダイアログボックス。
4. を使用する場合ゲートウェイロググループで、既存のロググループの使用をクリックし、使用するロググループを選択します。

   ロググループがない場合は、[Create a new log group] を選択してロググループを作成します。ロググループを作成できる CloudWatch Logs コンソールが表示されます。新しいロググループを作成した場合は、更新ボタンを選択すると、ドロップダウンリストに新しいロググループが表示されます。
5. 完了したら、[Save] を選択します。
6. ゲートウェイのログを表示するには、ゲートウェイを選択してから、の詳細タブ。

エラーのトラブルシューティング方法については、「ファイルゲートウェイ問題のトラブルシューティング」を参照してください。

Amazon CloudWatch メトリクスを使用する

を使用して、ファイルゲートウェイのモニタリングデータを取得できます。AWS Management Consoleまたは CloudWatch API を使用します。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、AWSSDKまたはAmazon CloudWatch APIツール。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次のとおりです。GatewayIdそしてGatewayName。CloudWatch コンソールでは、Gateway Metrics表示して、ゲートウェイ固有のディメンションを選択します。ディメンションの詳細については、「」を参照してください。ディメンションのAmazon CloudWatch ユーザーガイド。
- メトリクス名 (ReadBytes など)。

次の表は、使用できるStorage Gateway の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。GatewayId ディメンションと GatewayName ディメンションの両方を指定することで、使用するファイルゲートウェイを特定できます。 ゲートウェイのスループットおよびレイテンシーデータは、ゲートウェイのすべての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。

- 利用可能なメトリクスの表示
- メトリクスの統計の取得

- CloudWatch アラームの作成d\

ゲートウェイメトリクスについて

次の表に、FSx ファイルゲートウェイを対象とするメトリクスを示します。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、ファイルシステム固有のメトリクスと同じ名前が付けられています。これらのメトリクスは、同じ種類の測定を表していますが、ファイルシステムではなくゲートウェイがスコープとなっています。

特定のメトリクスを使用するときに、対象がゲートウェイであるかファイルシステムであるかを常に指定します。具体的には、ゲートウェイメトリクスを操作する場合は、Gateway Nameメトリクスデータを表示するゲートウェイの場合。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。

次の表は、の情報を入手するために使用できるメトリクスを示しています。FSx ファイルゲートウェイ。

メトリクス	説明
AvailabilityNotifications	このメトリクスは、レポートの期間中に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を報告します。 単位：カウント
CacheDirectorySize	このメトリクスは、ゲートウェイキャッシュ内のフォルダーのサイズを追跡します。フォルダサイズは、最初のレベルのファイルとサブフォルダの数によって決定され、サブフォルダに再帰的にカウントされません。 このメトリックは、Averageゲートウェイキャッシュ内のフォルダの平均サイズを測定するための統計情報。このメトリックは、Maxゲートウェイキャッシュ内のフォルダーの最大サイズを測定するための統計情報。 単位：カウント

メトリクス	説明
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のサイズを追跡します。 このメトリックは、Average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するための統計情報。このメトリックは、Max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するための統計情報。 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込みオペレーションの割合。サンプリングは、レポート期間の最後に行われます。 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：割合 (%)
CachePercentDirty	に保管されていないゲートウェイキャッシュの全体的な割合AWS。サンプリングは、レポート期間の最後に行われます。 単位：割合 (%)
CachePercentUsed	使用されているゲートウェイキャッシュストレージの全体的な割合。サンプリングは、レポート期間の最後に行われます。 単位：割合 (%)

メトリクス	説明
CacheUsed	このメトリクスは、ゲートウェイキャッシュ内の使用バイト数を報告します。 単位：バイト
CloudBytesDownloaded	ゲートウェイがアップロードされた合計バイト数AWS報告期間中。 このメトリクスを Sum 統計と共に使用してスループットを測定し、Samples 統計と共に使用して、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
CloudBytesUploaded	ゲートウェイのダウンロード元の総バイト数AWS報告期間中。 このメトリクスを Sum 統計と共に使用してスループットを測定し、Samples 統計と共に使用して IOPS を測定します。 単位：バイト
FilesFailingUpload	このメトリクスは、へのアップロードに失敗したファイルの数をトラッキングします。AWS。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。 このメトリックは、Sum統計情報で、現在アップロードに失敗しているファイルの数を示します。AWS。 単位：カウント

メトリクス	説明
FileShares	このメトリクスは、ゲートウェイのファイル共有の数を報告します。 単位：カウント
FileSystem-ERROR	このメトリックは、このゲートウェイ上の エラー状態にあるファイルシステムの関連付けの数を示します。 このメトリックでは、ファイルシステムの関連付けが ERROR 状態にあると報告された場合、ゲートウェイに問題があり、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報告したときにアラームを作成することをお勧めします。 単位：カウント
HealthNotifications	このメトリックは、レポート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
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機している時間の割合。 単位：割合 (%)
MemTotalBytes	このメトリックは、ゲートウェイ上のメモリの総量を報告します。 単位：バイト
MemUsedBytes	このメトリックは、ゲートウェイの使用済みメモリの量を報告します。 単位：バイト

メトリクス	説明
RootDiskFreeBytes	このメトリクスは、ゲートウェイのルートディスクで利用可能なバイト数を報告します。 このメトリックが20GB未満の空き容量を報告する場合は、ルート・ディスクのサイズを大きくする必要があります。 単位：バイト
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、キャッシュの総キャッシュのサイズを報告します。 単位：バイト
UserCpuPercent	このメトリックは、ゲートウェイの処理に費やされた時間の割合を報告します。 単位：割合 (%)

ファイルシステムのメトリクスを理解する

ファイル共有に関するStorage Gateway のメトリクスについて以下に説明します。各ファイル共有には、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、同じ種類の測定結果を示しますが、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、対象がゲートウェイメトリクスであるかファイル共有メトリクスであるかを常に指定します。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。

次の表は、ファイル共有に関する情報を入手するために使用できるStorage Gatewayメトリクスを示しています。

メトリクス	説明
`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込みオペレーションの割合。サンプリングは、レポート期間の最後に行われます。 ファイル共有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：割合 (%)
`CachePercentDirty`	に保管されていないゲートウェイのキャッシュの割合全体に対するファイル共有の割合。AWS。サンプリングは、レポート期間の最後に行われます。 を使用する`CachePercentDirty` に保管されていないゲートウェイのキャッシュの割合全体を表示するゲートウェイのメトリクス。AWS。 単位：割合 (%)
`CachePercentUsed`	ゲートウェイのキャッシュストレージの総使用率に対する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
	ゲートウェイの CachePercentUsed メトリクスを使用して、ゲートウェイのキャッシュストレージの総使用率を表示します。 単位：割合 (%)
CloudBytesUploaded	ゲートウェイがアップロードされた合計バイト数AWS報告期間中。 このメトリクスを Sum 統計と共に使用してスループットを測定し、Samples 統計と共に使用して IOPS を測定します。 単位：バイト
CloudBytesDownloaded	ゲートウェイのダウンロード元の総バイト数AWS報告期間中。 このメトリクスを Sum 統計と共に使用してスループットを測定し、Samples 統計と共に使用して、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
ReadBytes	ファイル共有のレポート期間中にオンプレミスのアプリケーションから読み取られた総バイト数。 このメトリクスを Sum 統計と共に使用してスループットを測定し、Samples 統計と共に使用して IOPS を測定します。 単位：バイト

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 統計と共に使用してスループットを測定し、Samples 統計と共に使用して IOPS を測定します。 単位：バイト

ファイルゲートウェイ監査ログについて

Amazon FSx ファイルゲートウェイ (FSx ファイルゲートウェイ) の監査ログは、ファイルシステムの関連付けに含まれるファイルとフォルダへのユーザーアクセスに関する詳細を提供します。監査ログを使用して、ユーザーのアクティビティをモニタリングし、不適切なアクティビティパターンが検出された場合に対処できます。ログは、Windows セキュリティイベントの既存のログ処理ツールとの互換性をサポートするために、Windows Server セキュリティログイベントと同様のフォーマットになっています。

オペレーション

次の表では、ファイルゲートウェイの監査ログファイルのアクセスオペレーションについて説明します。

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。
名前の変更	既存のファイルまたはフォルダの名前を変更します。
削除	ファイルまたはフォルダを削除します。

オペレーション名	定義
属性の書き込み	ファイルまたはフォルダのメタデータ (ACL、所有者、グループ、アクセス許可) を更新します。

属性

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

属性	定義
`securityDescriptor`	オブジェクトに設定された随意アクセス制御リスト (DACL) を SDDL 形式で示します。
`sourceAddress`	ファイル共有クライアントマシンの IP アドレス。
`SubjectDomainName`	クライアントのアカウントが属する Active Directory (AD) ドメイン。
`SubjectUserName`	クライアントのアクティブディレクトリユーザー名。
`source`	Storage Gateway の ID。`FileSystemAssociation` それは監査中です。
`mtime`	オブジェクトのコンテンツが変更された時刻 (クライアントが設定します)。
`version`	監査ログ形式のバージョン。
`ObjectType`	オブジェクトがファイルまたはフォルダであるかどうかを定義します。
`locationDnsName`	FSx ファイルゲートウェイシステムの DNS 名。
`objectName`	オブジェクトへのフルパス。

属性	定義
ctime	オブジェクトの内容またはメタデータが変更された時刻 (クライアントが設定します)。
shareName	アクセスされている共有の名前。
operation	オブジェクトのアクセスオペレーションの名前。
newObjectName	名前を変更した後の新しいオブジェクトへのフルパス。
gateway	Storage Gateway ID。
status	オペレーションのステータス。成功のみがログに記録されます (失敗は、アクセス許可の拒否に伴う失敗を除き、ログに記録されます)。
fileSizeInBytes	ファイルの作成時にクライアントによって設定されたファイルのサイズ (バイト単位)。

オペレーションごとにログに記録される属性

次の表に、各ファイルアクセスオペレーションで記録されるFSx ファイルゲートウェイの監査ログ属性を示します。

	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/フォルダの名前を変更する	ファイル/フォルダの削除	属性の書き込み (ACLの変更)	属性の書き込み (chown)	属性の書き込み (chmod)	属性の書き込み (chgrp)
securiescrip							X			
sourceress	X	X	X	X	X	X	X	X	X	X
SubjecmainNa	X	X	X	X	X	X	X	X	X	X
SubjecerName	X	X	X	X	X	X	X	X	X	X
source	X	X	X	X	X	X	X	X	X	X
mtime			X	X						
versic	X	X	X	X	X	X	X	X	X	X
objecte	X	X	X	X	X	X	X	X	X	X
locatinsName	X	X	X	X	X	X	X	X	X	X
objecte	X	X	X	X	X	X	X	X	X	X
ctime			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/フォルダの名前を変更する	ファイル/フォルダの削除	属性の書き込み (ACLの変更)	属性の書き込み (chown)	属性の書き込み (chmod)	属性の書き込み (chgrp)
shareN	X	X	X	X	X	X	X	X	X	X
operat	X	X	X	X	X	X	X	X	X	X
newObj Name					X					
gatewa	X	X	X	X	X	X	X	X	X	X
status	X	X	X	X	X	X	X	X	X	X
fileSi nBytes				X						

ゲートウェイのメンテナンス

ゲートウェイの維持には、キャッシュストレージとアップロードバッファ領域の設定などのタスク、およびゲートウェイのパフォーマンスの一般的なメンテナンスが含まれます。これらのタスクは、すべてのゲートウェイの種類に共通です。

トピック

ゲートウェイ VM のシャットダウン

- ゲートウェイ VM ローカルコンソール：「」を参照してください。ローカルコンソールでのメンテナンスタスクの実行。
- Storage Gateway API：を参照してください。ShutdownGateway

Storage Gateway のローカルディスクの管理

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

トピック

ローカルディスクストレージの量を決定する

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。ゲートウェイには、次のストレージが必要です。

ファイルゲートウェイには、キャッシュとして使用するディスクが 1 つ以上必要です。次の表は、デプロイされるゲートウェイのローカルディスクストレージの推奨サイズを示しています。ゲートウェイをセットアップした後で、ワークロードの需要増に応じてローカルストレージを追加できます。

ローカルストレージ	説明	ゲートウェイタイプ
キャッシュストレージ	キャッシュストレージは、オンプレミスで耐久性の高い保存場所として、Amazon S3 またはファイルシステムへのアップロードを保留中のデータを保存する働きをします。	• ファイルゲートウェイ

> **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。ローカルディスクをプロビジョニングする場合は (キャッシュストレージとして使用する場合など)、仮想ディスクを VM と同じデータストアか、別のデータストアに保存するかを指定できます。
>
> 複数のデータストアがある場合は、キャッシュストレージ用に 1 つのデータストアを選択することを強くお勧めします。基になる物理ディスクが 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のバックアップに使用すると、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。

ゲートウェイの初期設定とデプロイ後、キャッシュストレージ用のディスクを追加することによってローカルストレージを調整できます。

割り当てるキャッシュストレージのサイズを決定する

キャッシュストレージ用のディスクをプロビジョニングするには、最初に、この概算値を使うことができます。その後、Amazon CloudWatch 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。また、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」を参照してください。

キャッシュストレージの追加

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容量を増やすことができます。既存のゲートウェイ機能を中断せずに、ゲートウェイにキャッシュ容量を追加できます。ストレージ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うことができます。

> **Important**
>
> 既存のゲートウェイにキャッシュを追加する場合、ホスト (ハイパーバイザーまたは Amazon EC2 インスタンス) に新しいディスクを作成することが重要です。ディスクがキャッシュとして割り当て済みである場合は、既存のディスクサイズを変更しないでください。キャッシュストレージとして割り当てられたキャッシュディスクを削除しないでください。

次の手順は、ゲートウェイのストレージを設定またはキャッシュする方法を示しています。

ストレージを追加して設定またはキャッシュするには

1. 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プロビジョンします。ハイパーバイザーでディスクをプロビジョンする方法については、ハイパーバイザーのユーザーマニュアルを参照してください。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] コンソールを開きます。https://console.aws.amazon.com/storagegateway/home。
3. ナビゲーションペインで、[Gateways] を選択します。
4. [Actions] メニューで、[Edit local disks] を選択します。
5. [ローカルディスクの編集] ダイアログボックスで、プロビジョニング済みのディスクを識別し、どのディスクをキャッシュストレージに使用するかを決定します。

   ディスクが表示されない場合は、[Refresh] ボタンを選択します。
6. [Save] を選択して設定を保存します。

FSx ファイルゲートウェイはエフェメラルストレージをサポートしていません。

AWS Storage Gateway コンソールでのゲートウェイアップデートの管理

Storage Gateway は、ゲートウェイ用の重要なソフトウェア更新プログラムを定期的にリリースしています。Storage Gateway マネジメントコンソールで手動で更新プログラムを適用できます。または、設定された設定されたメンテナンススケジュール中に自動的に更新プログラムが適用されるのを待つこともできます。Storage Gateway は更新プログラムを毎分確認しますが、更新プログラムがある場合のみ、メンテナンスと再起動を行います。

Gateway ソフトウェアリリースには、によって検証されたオペレーティングシステムの更新とセキュリティパッチが定期的に含まれています。AWS。これらの更新は、通常 6 か月ごとにリリースされ、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。

> **Note**
>
> Storage Gateway アプライアンスは、管理対象組み込みデバイスとして扱い、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。通常のゲートウェイ更新メカニズム（SSM やハイパーバイザーツールなど）以外の方法で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。

ゲートウェイにアップデートが適用される前に、AWSは、Storage Gateway コンソールおよびAWS Health Dashboard。詳細については、「AWS Health Dashboard」を参照してください。VM は再起動されませんが、更新および再起動中はゲートウェイがしばらくの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、デフォルトの週単位のメンテナンススケジュールが設定されます。メンテナンススケジュールはいつでも変更できます。更新プログラムが利用可能な場合は、[Details] タブにメンテナンスメッセージが表示されます。また、[Details] タブには、最後に更新プログラムが正常にゲートウェイに適用された日時が表示されます。

メンテナンススケジュールを変更するには

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

2. ナビゲーションペインで、[Gateways] を選択し、続いて更新スケジュールを変更するゲートウェイを選択します。
3. [Actions (アクション)] で、[Edit maintenance window (メンテナンス時間の編集)] を選択し、メンテナンス時間の編集ダイアログボックスを開きます。
4. [Schedule (スケジュール)] で、[Weekly (毎週)] または [Monthly (毎月)] を選択して更新をスケジュールします。
5. [Weekly (毎週)] を選択した場合は、[Day of the week (曜日)] と [Time (時刻)] の値を変更します。

   [Monthly (毎月)] を選択した場合は、[Day of the month (日)] と [Time (時刻)] の値を変更します。このオプションを選択してエラーが発生した場合は、ゲートウェイが古いバージョンであり、まだ新しいバージョンにアップグレードされていないことを意味します。

   > **Note**
   >
   > その月の日に設定できる最大値は 28 です。28 を選択した場合、メンテナンスの開始時間は毎月の 28 日になります。

   メンテナンス開始時刻がの詳細次回開いたときのゲートウェイのタブの詳細タブ。

ローカルコンソールでのメンテナンスタスクの実行

ホストのローカルコンソールを使用して次のメンテナンスタスクを実行できます。ローカルコンソールタスクは VM ホストまたは Amazon EC2 インスタンスで実行できます。多くのタスクはさまざまなホストに共通していますが、異なる点もいくつかあります。

トピック

- VM ローカルコンソール (ファイルゲートウェイ) でのタスクの実行
- Amazon EC2 ローカルコンソール (ファイルゲートウェイ) でタスクを実行する
- ゲートウェイローカルコンソールへのアクセス
- ゲートウェイのネットワークアダプタの設定

VM ローカルコンソール (ファイルゲートウェイ) でのタスクの実行

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 カーネルベースの仮想マシン (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のローカルコンソールにログインする

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。初めてローカルコンソールにログインする場合は、デフォルトのユーザー名とパスワードを使用してログインします。これらのデフォルトのログイン認証情報を使用することで、ゲートウェイ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。AWS Storage Gatewayを使用すると、ローカルコンソールからパスワードを変更しなくても、Storage Gateway コンソールからパスワードを設定できます。新しいパスワードを設定するためにデフォルトパスワードを知っている必要はありません。詳細については、「ファイルゲートウェイのローカルコンソールにログインする」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

- ローカルコンソールに初めてログインする場合は、デフォルトの認証情報を使用して VM にログインします。デフォルトのユーザー名は `admin`、パスワードは `password` です。初めてではない場合は、認証情報を使用してログインします。

> **Note**
>
> デフォルトのパスワードを変更することをお勧めします。これを行うには、ローカルコンソールメニューから passwd を実行します (メインメニューの項目 6)。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ストレージゲートウェイコマンドを実行する」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、「ファイルゲートウェイのローカルコンソールにログインする」を参照してください。

Storage Gateway コンソールからローカルコンソールパスワードを設定する

ローカルコンソールに初めてログインするとき、デフォルトの認証情報を使用して VM にログインします。すべてのタイプのゲートウェイに、デフォルトの認証情報を使用します。ユーザー名は admin でパスワードは password です。

新しいゲートウェイを作成した直後に必ず新しいパスワードを設定することをお勧めします。このパスワードは、必要に応じてローカルコンソールではなく AWS Storage Gateway コンソールから設定できます。新しいパスワードを設定するためにデフォルトパスワードを知っている必要はありません。

Storage Gateway コンソールでローカルコンソールパスワードを設定するには

1. [Storage Gateway] コンソールを開きます。https://console.aws.amazon.com/storagegateway/home。
2. ナビゲーションペインで、[Gateways] を選択し、新しいパスワードを設定するゲートウェイを選択します。
3. [Actions] で、[Set Local Console Password] を選択します。
4. [Set Local Console Password] ダイアログボックスで、新しいパスワードを入力し、確認のためにパスワードを再入力してから、[Save] を選択します。

   デフォルトのパスワードは、新しいパスワードに置き換えられます。Storage Gateway はパスワードを保存するのではなく、VM に安全に送信します。

> **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 はすべてをルーティングします。AWSプロキシサーバーを介したエンドポイントトラフィック。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. リポジトリの []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の入力**1**をクリックして HTTP プロキシの設定を開始します。

3. [HTTP Proxy Configuration menu (HTTP プロキシ設定メニュー)] に「**1**」と入力し、HTTP プロキシサーバーのホスト名を指定します。

   以下に示すように、このメニューから他の HTTP 設定を設定できます。

To	操作
HTTP プロキシの設定	**1** と入力します。 設定を完了するには、ホスト名とポートを指定する必要があります。
HTTP プロキシの現在の設定を表示する	**2** と入力します。 HTTP プロキシが設定されていない場合は、" HTTP Proxy not configured " というメッセージが表示されます。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。
HTTP プロキシの設定を削除する	**3** と入力します。 "HTTP Proxy Configuration Removed " というメッセージが表示されます。

4. VM を再起動して HTTP 設定を適用します。

ゲートウェイネットワーク設定の構成

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. リポジトリの []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の入力**2**をクリックして、ネットワークの構成を開始します。

3. [Network Configuration (ネットワーク設定)] メニューで次のいずれかのオプションを選択します。

To	操作
ネットワークアダプタに関する情報を取得する	**1** と入力します。 アダプタ名のリストが表示され、たとえば**eth0**のように、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

To	操作
	ゲートウェイのデフォルトルートアダプタを設定する (オプション 5) 場合と同じアダプタ名を使用して、静的 IP アドレスを設定する (オプション 3) ことができます。
DHCP を設定する	**2** と入力します。 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。

To	操作
ゲートウェイの静的 IP アドレスを設定する	**3** と入力します。 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** ゲートウェイがすでにアクティブ化されている場合、設定を有効にするには、ストレージゲートウェイ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。 ゲートウェイで複数のネットワークインターフェイスを使用している場合は、有効になっ

To	操作
	ているインターフェイスのすべてを使用して、DHCP または静的 IP アドレスのどちらかを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、インターフェイスを有効にするには、静的 IP に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。
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	**4** と入力します。 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化されている場合、設定を有効にするには、Storage Gateway コンソールから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。

To	操作
ゲートウェイのデフォルトルートアダプタを設定する	**5** と入力します。 ゲートウェイで使用可能なアダプタが表示され、いずれかのアダプタなど、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。**eth0**。
ゲートウェイの DNS 設定を編集する	**6** と入力します。 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。
ゲートウェイの DNS 設定を表示する	**7** と入力します。 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	**8** と入力します。 ゲートウェイのデフォルトルートが表示されます。

ゲートウェイエンドポイントへの FSx ファイルゲートウェイゲートウェイ接続のテスト

ゲートウェイのローカルコンソールを使用してインターネット接続をテストできます。このテストは、ゲートウェイのネットワーク問題をトラブルシューティングするときに役立ちます。

ゲートウェイシステムリソースステータスの表示

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. 左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の入力**4**システムリソースチェックの結果を表示します。

   コンソールで各リソースに対して [OK]、[WARNING]、または [FAIL] というメッセージが表示されます。その説明は、次のとおりです。

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できます。Storage Gateway は、リソースチェックの

メッセージ	説明
	結果について説明するメッセージを表示します。
[FAIL]	リソースは最小要件を満たしていません。ゲートウェイは適切に機能していない可能性があります。Storage Gateway は、リソースチェックの結果について説明するメッセージを表示します。

また、コンソールには、エラーと警告の数がリソースチェックメニューオプションの横に表示されます。

ゲートウェイのネットワークタイムプロトコル (NTP) サーバーの構成

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. 左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の入力**5**システムの時間を管理してください。

3. [System Time Management (システム時刻管理)] メニューで、次のいずれかのオプションを選択します。

To	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。	**1** と入力します。 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。 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 の時刻とホストの時刻の同期」を参照してください。 Microsoft Hyper-V にデプロイされたゲートウェイの場合は、定期的に VM の時刻を確認する必要があります。詳細については、「ゲートウェイ VM の時刻の同期」を参照してください。 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

To	操作
	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	**2** と入力します。 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	**3** と入力します。 NTP サーバー設定が表示されます。

ローカルコンソールでストレージゲートウェイコマンドを実行する

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のコマンドを使用して、ルーティングテーブルの保存や Amazon Web Services Support への接続などのメンテナンスタスクを実行できます。

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. リポジトリの []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の入力**6**にとってコマンドプロント。

3. リポジトリの []AWSアプライアンスのアクティベーション-コマンドプロンプトコンソール、次のように入力します。**h**を押してからを押します。戻り値key。

次のスクリーンショットに示すように、コンソールには、[AVAILABLE COMMANDS (使用可能なコマンド)] メニューとコマンドの目的が表示されます。

4. コマンドプロンプトで、使用するコマンドを入力して手順に従います。

コマンドの機能を調べるには、コマンドプロンプトでコマンド名を入力してください。

ゲートウェイのネットワークアダプタの設定

デフォルトでは、Storage Gateway は E1000 ネットワークアダプタタイプを使用するように設定されていますが、VMXNET3 (10 GbE) ネットワークアダプタを使用するようにゲートウェイを再設定できます。複数の IP アドレスからStorage Gateway にアクセスできるように設定することもできます。これを行うには、複数のネットワークアダプタを使用するようにゲートウェイを設定します。

トピック

- VMXNET3 ネットワークアダプタを使用するようにゲートウェイを設定する

VMXNET3 ネットワークアダプタを使用するようにゲートウェイを設定する

Storage Gateway は、VMware ESXi ホストと Microsoft Hyper-V Hypervisor ホストの両方で E1000 ネットワークアダプタタイプを使用することをサポートしています。ただし、VMXNET3 (10 GbE) ネットワークアダプタタイプは VMware ESXi ハイパーバイザーでのみサポートされています。ゲートウェイが VMware ESXi ハイパーバイザーでホストされている場合は、VMXNET3 (10 GbE) アダプタタイプを使用するようにゲートウェイを再設定できます。このアダプタの詳細については、VMware ウェブサイトを参照してください。

KVM ハイパーバイザーホストの場合、Storage Gateway はvirtioネットワークデバイスドライバ。KVM ホスト用の E1000 ネットワークアダプタタイプの使用はサポートされていません。

> **Important**
>
> VMXNET3 を選択するには、ゲストオペレーティングシステムの種類が [Other Linux64] でなければなりません。

VMXNET3 アダプタを使用するようにゲートウェイを設定する手順を以下に示します。

1. デフォルトの E1000 アダプタを削除します。
2. VMXNET3 アダプタを追加します。
3. ゲートウェイを再起動します。
4. ネットワークに対してアダプタを設定します。

各ステップの実行方法について説明します。

デフォルト E1000 アダプタを削除し、VMXNET3 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. VMware で、ゲートウェイのコンテキスト (右クリック) メニューを開き、[Edit Settings] を選択します。
2. [Virtual Machine Properties] ウィンドウで [Hardware] タブを選択します。
3. [Hardware] で [Network adapter] を選択します。[Adapter Type (アダプタの種類)] セクションで現在のアダプタが E1000 であることを確認します。このアダプタを VMXNET3 アダプタに変更します。

4. E1000 ネットワークアダプタを選択し、[Remove] を選択します。この例では、E1000 ネットワークアダプタは Network adapter 1 です。

   > **Note**
   >
   > ゲートウェイで E1000 ネットワークアダプタと VMXNET3 ネットワークアダプタを同時に実行することはできますが、ネットワークで問題が発生する可能性があるため、お勧めしません。

5. [Add] を選択して Add Hardware ウィザードを開きます。
6. [Ethernet Adapter] を選択し、[Next] を選択します。
7. ネットワーク入力ウィザードで、**VMXNET3**にとってアダプタ入力を選択してから、[] を選択します。次。
8. Virtual Machine Properties (仮想マシンのプロパティ) ウィザードの [Adapter Type (アダプタの種類)] セクションで [Current Adapter (現在のアダプタ)] が [VMXNET3] に設定されていることを確認し、[OK] を選択します。
9. VMware VSphere クライアントで、ゲートウェイをシャットダウンします。
10. VMware vSphere クライアントでゲートウェイを再起動します。

ゲートウェイが再起動したら、インターネットへのネットワーク接続が確立されるように、追加したアダプタを再設定します。

ネットワークに対してアダプタを設定するには

1. vSphere クライアントで [Console] タブを選択してローカルコンソールを起動します。この設定タスクでは、デフォルトのログイン認証情報を使用して、ゲートウェイのローカルコンソールにログインします。デフォルトの認証情報を使用してログインする方法については、「ファイルゲートウェイのローカルコンソールにログインする」を参照してください。

2. プロンプトで「**2**」と入力して [Network Configuration (ネットワーク設定)] を選択し、**Enter** キーを押してネットワーク設定メニューを開きます。
3. プロンプトで「**4**」と入力して [Reset all to DHCP (すべて DHCP にリセット)] を選択し、プロンプトで「**y**」 (yes) と入力して、すべてのアダプタが Dynamic Host Configuration Protocol (DHCP) を使用するように設定します。使用可能なすべてのアダプタが DHCP を使用するように設定されます。

   ゲートウェイがすでにアクティブ化されている場合、Storage Gateway をシャットダウンして再起動する必要があります。ゲートウェイが再起動したら、インターネットへのネットワーク接続をテストする必要があります。ネットワーク接続をテストする方法については、「ゲートウェイエンドポイントへの FSx ファイルゲートウェイゲートウェイ接続のテスト」を参照してください。

Amazon EC2 ローカルコンソール (ファイルゲートウェイ) でタスクを実行する

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にログインする
- 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
- ゲートウェイネットワーク設定の構成

- ゲートウェイのネットワーク接続をテストする
- ゲートウェイシステムリソースステータスの表示
- ローカルコンソールで Storage Gateway コマンドを実行する

Amazon EC2 ゲートウェイのローカルコンソールにログインする

Secure Shell (SSH) クライアントを使用して Amazon EC2 インスタンスに接続できます。詳細については、「」を参照してください。インスタンスへの接続のAmazon EC2 ユーザーガイド。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 のキーペアの詳細については、「」を参照してください。Amazon EC2 のキーペアのAmazon EC2 ユーザーガイド。

ゲートウェイのローカルコンソールにログインするには

1. ローカルコンソールにログインします。Windows コンピュータから EC2 インスタンスに接続する場合は、admin としてログインします。
2. ログインした後、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 (次のスクリーンショットを参照)。

詳細については、	このトピックを参照してください
ゲートウェイの HTTP プロキシを設定する	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	ゲートウェイのネットワーク接続をテストする
ネットワークの接続をテストする	ゲートウェイのネットワーク接続をテストする
システムリソースチェックを表示する	Amazon EC2 ゲートウェイのローカルコンソールにログインする.
Storage Gateway コンソールコマンドの実行	ローカルコンソールで 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**」と入力してメニューを終了します。

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 は、Amazon EC2 にデプロイされたゲートウェイ間の Socket Secure バージョン 5 (SOCKS5) プロキシの設定をサポートします。AWS。

ゲートウェイがプロキシサーバーを使用してインターネットと通信する必要がある場合は、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 はすべてをルーティングします。AWSプロキシサーバーを介したエンドポイントトラフィック。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にログインする」を参照してください。
2. リポジトリの []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の入力**1**をクリックして HTTP プロキシの設定を開始します。
3. で次のいずれかのオプションを選択します。AWSアプライアンスのアクティベーション-設定HTTP プロキシ設定メニュー。

To	操作
HTTP プロキシの設定	**1** と入力します。 設定を完了するには、ホスト名とポートを指定する必要があります。
HTTP プロキシの現在の設定を表示する	**2** と入力します。

To	操作
	HTTP プロキシが設定されていない場合は、`HTTP Proxy not configured` というメッセージが表示されます。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。
HTTP プロキシの設定を削除する	**3** と入力します。 `"HTTP Proxy Configuration Removed "` というメッセージが表示されます。

ゲートウェイネットワーク設定の構成

ローカルコンソールを使用し、ドメイン名サーバー (DNS) 設定を表示して設定できます。

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。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にログインする」を参照してください。
2. リポジトリの []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の入力**2**をクリックして DNS サーバーの設定を開始します。

3. [Network Configuration (ネットワーク設定)] メニューで次のいずれかのオプションを選択します。

To	操作
ゲートウェイの DNS 設定を編集する	**1** と入力します。

To	操作
	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。
ゲートウェイの DNS 設定を表示する	**2** と入力します。 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。

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にログインする」を参照してください。
2. から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、対応する数字を入力して選択しますネットワーク接続テスト。

   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されます。まだアクティブ化されていないゲートウェイの場合は、エンドポイントタイプを指定する必要があります。AWS リージョン次の手順で説明されているように設定します。
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、対応する数字を入力して、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AWS リージョンテストしたいということ。サポート対象AWS リージョンのリストAWSStorage Gateway で使用できるサービスエンドポイントについては、を参照してください。AWS Storage Gatewayエンドポイントとクォータのの全般のリファレンス。

テストが進むにつれて、各エンドポイントに次のいずれかが表示されます。[成功]または[失敗]の接続ステータスを次のように示します。

メッセージ	説明
[成功]	Storage Gateway にはネットワーク接続があります。
[失敗]	Storage Gateway にはネットワーク接続がありません。

ゲートウェイシステムリソースステータスの表示

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。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にログインする」を参照してください。
2. 左Storage Gateway の設定メインメニューの入力**4**システムリソースチェックの結果を表示します。

   コンソールで各リソースに対して [OK]、[WARNING]、または [FAIL] というメッセージが表示されます。その説明は、次のとおりです。

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できます。Storage Gateway は、リソースチェックの結果について説明するメッセージを表示します。

メッセージ	説明
[FAIL]	リソースは最小要件を満たしていません。ゲートウェイは適切に機能していない可能性があります。Storage Gateway は、リソースチェックの結果について説明するメッセージを表示します。

また、コンソールには、エラーと警告の数がリソースチェックメニューオプションの横に表示されます。

ローカルコンソールで Storage Gateway コマンドを実行する

AWS Storage Gateway コンソールは、ゲートウェイの設定と問題の診断のための安全な環境を提供します。コンソールのコマンドを使用して、ルーティングテーブルの保存やAmazon Web Services Support への接続などのメンテナンスタスクを実行できます。

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にログインする」を参照してください。
2. 左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の入力**5**にとってゲートウェイコンソール。
3. コマンドプロンプトで、「**h**」と入力し、Return キーを押します。

   使用できるコマンドを示す [AVAILABLE COMMANDS (使用可能なコマンド)] メニューがコンソールに表示されます。次のスクリーンショットに示すように、メニューの後にゲートウェイコンソールプロンプトが表示されます。
4. コマンドプロンプトで、使用するコマンドを入力して手順に従います。

コマンドの機能を調べるには、コマンドプロンプトでコマンド名を入力してください。

ゲートウェイローカルコンソールへのアクセス

VM のローカルコンソールにアクセスする方法は、ゲートウェイ VM をデプロイしたハイパーバイザーの種類によって異なります。このセクションでは、Linux カーネルベースの仮想マシン (KVM)、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

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
   ```

   使用可能な仮想マシンは、Id で選択できます。

2. ローカルコンソールにアクセスするには、次のコマンドを使用します。

   ```
   # virsh console VM_Id
   ```

3. ローカルコンソールにログインするためのデフォルトの認証情報を取得するには、「ファイルゲートウェイのローカルコンソールにログインする」を参照してください。
4. ログイン後、ゲートウェイをアクティブ化して構成できます。

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. ゲートウェイの電源が入っていることを確認します。

> **Note**
>
> ゲートウェイ VM の電源が入っている場合は、次のスクリーンショットに示すように、VM アイコンと共に緑の矢印アイコンが表示されます。ゲートウェイ VM がオンになっていない場合は、緑色で選択してオンにすることができます。電源オンアイコンツールバーメニュー。

3. [Console] タブを選択します。

   しばらくすると、VM にログインできる状態になります。

> **Note**
>
> コンソールウィンドウからカーソルを解放するには、Ctrl + Alt キーを押します。

4. デフォルトの認証情報を使用してログインするには、「ファイルゲートウェイのローカルコンソールにログインする」の手順に進みます。

Microsoft Hyper-V でゲートウェイのローカルコンソールにアクセスする

ゲートウェイのローカルコンソールにアクセスするには (Microsoft Hyper-V)

1. Microsoft Hyper-V Manager の [Virtual Machines] リストで、ゲートウェイ VM を選択します。
2. ゲートウェイの電源が入っていることを確認します。

> **Note**
>
> ゲートウェイ VM の電源が入っている場合は、Runningと表示される。状態仮想マシンの (次のスクリーンショットを参照)。ゲートウェイ VM がオンになっていない場合は、を選択してオンにすることができます。を起動のアクションペイン。

3. [Actions] ペインの [Connect] を選択します。

   [Virtual Machine Connection] ウィンドウが表示されます。認証ウィンドウが表示されたら、ハイパーバイザー管理者から提供されたユーザー名とパスワードを入力します。

   しばらくすると、VM にログインできる状態になります。

4. デフォルトの認証情報を使用してログインするには、「ファイルゲートウェイのローカルコンソールにログインする」の手順に進みます。

ゲートウェイのネットワークアダプタの設定

このセクションでは、ゲートウェイに複数のネットワークアダプタを設定する方法について説明します。

トピック

- VMware ESXi ホストの複数の 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、2 番目のアダプタを設定しようとしています。以下の手順は、クラスターの VMware ESXi 用のアダプタを追加する方法を示しています。

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、[Edit Settings] を選択します。
4. リポジトリの []ハードウェアタブ仮想マシンのプロパティ] ダイアログボックスで、[] を選択します。を追加します。をクリックして、デバイスを追加します。
5. [Add Hardware] ウィザードに従って、ネットワークアダプタを追加します。

   a. [Device Type] ペインで [Ethernet Adapter] を選択してアダプタを追加し、[Next] を選択します。

   b. 左ネットワークネットワークタイプペインで、電源投入時にConnectが選択されています。タイプを選択してから、[] を選択します。次。

      Storage Gateway には E1000 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、[Finish] を選択します。
6. [概要VM のタブをクリックし、すべて表示の横にあるIP アドレスボックスに移動するとそのように表示されます。[Virtual Machine IP Addresses] ウィンドウに、ゲートウェイへのアクセスに使用できるすべての IP アドレスが表示されます。2 番目の IP アドレスがゲートウェイに対して表示されることを確認します。

> **Note**
>
> アダプタの変更が有効になり、VM のサマリ情報が更新されるまでに、しばらく時間がかかる場合があります。

次の画像は、あくまでも参考用です。実際には、IP アドレスの 1 つはゲートウェイが AWS と通信するためのアドレスであり、それ以外は別のサブネット内のアドレスです。

7. Storage Gateway コンソールでゲートウェイをオンにします。
8. 左NavigationStorage Gateway コンソールのペインで、ゲートウェイを選択し、アダプタを追加したゲートウェイを選択します。2 番目の IP アドレスが [詳細] タブに表示されることを確認します。

VMware、Hyper-V、KVM ホストに共通するローカルコンソールタスクについては、「VM ローカルコンソール (ファイルゲートウェイ) でのタスクの実行」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 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 でゲートウェイの VM を選択します。
3. VM がオフになっていない場合は、ゲートウェイのコンテキスト (右クリック) メニューを開き、[Turn Off] を選択します。
4. クライアントでゲートウェイ VM のコンテキストメニューを開き、[Settings] を選択します。
5. 左設定仮想マシンのダイアログボックス、ハードウェアで、ハードウェアの追加。
6. [Add Hardware] ペインで [Network Adapter] を選択し、[Add] を選択してデバイスを追加します。

7. ネットワークアダプタを設定し、[Apply] を選択して設定を適用します。

   以下の例では、新しいアダプタとして [Virtual Network 2] が選択されています。

8. [Settings] ダイアログボックスの [Hardware] で 2 つ目のアダプタが追加されたことを確認し、[OK] を選択します。
9. Storage Gateway コンソールでゲートウェイをオンにします。
10. [ナビゲーション] ペインで、[ゲートウェイ] を選択し、アダプタを追加したゲートウェイを選択します。2 番目の IP アドレスが [詳細] タブに表示されることを確認します。

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、「VM ローカルコンソール (ファイルゲートウェイ) でのタスクの実行」を参照してください。

AWS Storage Gateway コンソールを使用したゲートウェイの削除と関連リソースの除去

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、AWS Storage Gateway マネジメントコンソールに表示されなくなり、そのイニシエータへの iSCSI 接続が切断されます。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ゲートウェイを削除できます。ここでは、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、「」を参照してください。AWS Storage GatewayAPI リファレンス。

トピック

- Storage Gateway コンソールを使用したゲートウェイの削除
- オンプレミスでデプロイされているゲートウェイからのリソースの除去
- Amazon EC2 インスタンスにデプロイされているゲートウェイからのリソースの除去

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 カーネルベースの仮想マシン (KVM) クライアントを使用してホストに接続し、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] コンソールを開きます。https://console.aws.amazon.com/storagegateway/home。
2. ナビゲーションペインで [Gateways] を選択してから、削除するゲートウェイを選択します。
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。
4. > **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。
   > また、ゲートウェイを削除すると、復元できなくなります。

   表示される確認ダイアログボックスで、削除を確認するチェックボックスを選択します。リストされているゲートウェイ ID が削除するゲートウェイを指定していることを確認し、[削除] を選択します。

> **Important**
>
> ゲートウェイを削除すると、ソフトウェア料金は課金されなくなりますが、仮想テープ、Amazon Elastic Block Store (Amazon EBS) スナップショット、Amazon EC2 インスタンスなどのリソースは保持されます。これらのリソースに対する課金は継続されます。Amazon EC2 サブスクリプションをキャンセルすることにより、Amazon EC2 インスタンスと Amazon EBS スナップショットは、除去できます。Amazon EC2 サブスクリプションをキャンセルしたくない場合は、Amazon EC2 コンソールを使用して Amazon EBS スナップショットを削除できます。

オンプレミスでデプロイされているゲートウェイからのリソースの除去

このセクションでは、オンプレミスでデプロイされているゲートウェイからリソースを除去する手順について説明します。

VM にデプロイされているボリュームゲートウェイからのリソースの除去

削除するゲートウェイが仮想マシン (VM) にデプロイされている場合は、以下のアクションを実行してリソースをクリーンアップすることをお勧めします。

- ゲートウェイを削除します。

Amazon EC2 インスタンスにデプロイされているゲートウェイからのリソースの除去

Amazon EC2 インスタンスにデプロイしたゲートウェイを削除する場合は、AWSゲートウェイで使用されていたリソース。これにより、意図しない使用に対する課金を回避できるためです。

Amazon EC2 にデプロイされているキャッシュ型ボリュームからのリソースの除去

EC2 にキャッシュ型ボリュームのゲートウェイをデプロイした場合は、以下のアクションを実行して、ゲートウェイを削除し、そのリソースをクリーンアップすることをお勧めします。

1. 「」で示されているように、Storage Gateway コンソールでゲートウェイを削除します。Storage Gateway コンソールを使用したゲートウェイの削除。

2. Amazon EC2 コンソールで、インスタンスを再度使用する予定がある場合は、EC2 インスタンスを停止します。使用しない場合は、そのインスタンスを終了します。ボリュームを削除する予定である場合は、インスタンスを削除する前に、インスタンスにアタッチされているブロックデバイスとその ID を書き留めます。これらは、削除するボリュームを識別するために必要です。
3. Amazon EC2 コンソールで、インスタンスにアタッチされているすべての Amazon EBS ボリュームを再度使用する予定がない場合は、すべて削除します。詳細については、「」を参照してください。インスタンスとボリュームのクリーンアップのLinux インスタンス用 Amazon EC2 ユーザーガイド。

パフォーマンス

このセクションでは、Storage Gateway のパフォーマンスに関する情報を示します。

トピック

ゲートウェイのパフォーマンスの最適化

このセクションでは、ゲートウェイのパフォーマンスを最適化する方法について説明します。ガイダンスは、ゲートウェイへのリソースの追加およびアプリケーションサーバーへのリソースの追加に基づいています。

ゲートウェイへのリソースの追加

以下の 1 つ以上の方法でゲートウェイにリソースを追加することで、ゲートウェイのパフォーマンスを最適化できます。

より高性能なディスクの使用

ゲートウェイのパフォーマンスを最適化するには、Solid State Drive (SSD) や NVMe コントローラーなどの高性能のディスクを追加できます。また、Microsoft Hyper-V NTFS ではなく、ストレージエリアネットワーク (SAN) から直接 VM に仮想ディスクをアタッチできます。通常、ディスクパフォーマンスが向上すると、スループットおよび 1 秒あたりの入力/出力操作数 (IOPS) が改善します。ディスクの追加については、「」を参照してください。キャッシュストレージの追加。

スループットを測定するには、`ReadBytes`そして`WriteBytes`のメトリクス`Samples`Amazon CloudWatch 統計情報。たとえば、5 分間のサンプル期間の `ReadBytes` メトリックスの `Samples` 統計を 300 秒で割ると、IOPS がわかります。一般的なルールとして、ゲートウェイのこれらのメトリクスを確認する場合は、ディスク関連のボトルネックを示す低いスループットおよび低い IOPS トレンドを探します。

> **Note**
>
> CloudWatch メトリックスは、すべてのゲートウェイで使用できるわけではありません。ゲートウェイメトリクスについては、「ファイルゲートウェイのモニタリング」を参照してください。

ゲートウェイホストへの CPU リソースの追加

ゲートウェイホストサーバーの最小要件は、4 つの仮想プロセッサです。ゲートウェイのパフォーマンスを最適化するには、ゲートウェイ VM に割り当てられている 4 つの仮想プロセッサが 4 つのコアによってサポートされることを確認します。さらに、ホストサーバーの CPU をオーバーサブスクライブしていないことを確認します。

ゲートウェイホストサーバーに CPU を追加すると、ゲートウェイの処理能力が向上します。これにより、ゲートウェイは、アプリケーションからローカルストレージへのデータの保存とへのこのデータのアップロードの両方を並行して処理できます。また、CPU を追加すると、ホストが他の VM と共有される場合に、ゲートウェイで十分な CPU リソースを利用できます。十分な CPU リソースを提供することには、スループットを向上させる一般的な効果があります。

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

- 24 個の CPU。
- ファイルゲートウェイの 16 GiB の予約済み RAM
  - 16 TiB までのキャッシュサイズを持つゲートウェイ用の 16 GiB のリザーブド RAM
  - キャッシュサイズが 16 TiB ~ 32 TiB のゲートウェイ用の 32 GiB のリザーブド RAM
  - キャッシュサイズが 32 TiB ~ 64 TiB のゲートウェイ用の 48 GiB のリザーブド RAM
- 準仮想化コントローラー 1 にアタッチされているディスク 1 (ゲートウェイのキャッシュとして次のように使用する) :
  - NVMe コントローラーを使用する SSD。
- 準仮想化コントローラー 1 にアタッチされているディスク 2 (ゲートウェイアップロードバッファとして次のように使用する) :
  - NVMe コントローラーを使用する SSD。
- 準仮想化コントローラー 2 にアタッチされているディスク 3 (ゲートウェイアップロードバッファとして次のように使用する) :

    - NVMe コントローラーを使用する SSD。
- VM ネットワーク 1 に設定されたネットワークアダプタ 1:
    - VM ネットワーク 1 を使用し、取り込みに使用する VMXnet3 (10 Gbps) を追加する。
- VM ネットワーク 2 に設定されたネットワークアダプタ 2:
    - VM ネットワーク 2 を使用し、AWS への接続に使用する VMXnet3 (10 Gbps) を追加する。

別の物理ディスクを使用したゲートウェイ仮想ディスクのバックアップ

ゲートウェイのディスクをプロビジョニングする際、関連する物理ストレージディスクが同じであるローカルストレージ用にローカルディスクをプロビジョニングしないことを強くお勧めします。たとえば、VMware ESXi の場合、基盤となる物理ストレージリソースはデータストアとして表されます。ゲートウェイ VM をデプロイする場合は、VM ファイルを保存するデータストアを選択します。仮想ディスクをプロビジョニングする場合は (アップロードバッファとして使用する場合など)、仮想ディスクを VM と同じデータストアか、別のデータストアに保存できます。

複数のデータストアがある場合は、作成するローカルストレージのタイプごとに 1 つのデータストアを選択することを強くお勧めします。基になる物理ディスク 1 つのみによってサポートされるデータストアでは、パフォーマンスが低下することがあります。たとえば、そのようなディスクを使用して、ゲートウェイ設定のキャッシュストレージとアップロードバッファの両方がサポートされる場合です。同様に、RAID 1 のようなパフォーマンスの低い RAID 構成によってサポートされるデータストアでは、パフォーマンスが低下することがあります。

アプリケーション環境へのリソースの追加

アプリケーションサーバーとゲートウェイの間の帯域幅を増やす

ゲートウェイのパフォーマンスを最適化するには、アプリケーションとゲートウェイ間のネットワーク帯域幅が、アプリケーションのニーズを満たすようにしてください。♪ReadBytesそしてWriteBytes総データスループットを測定するためのゲートウェイのメトリック。

アプリケーションでは、必要なスループットと測定されたスループットを比較します。測定されたスループットが必要なスループットを下回る場合、アプリケーションとゲートウェイの間の帯域幅を増やすと、ネットワークがボトルネックであれば、パフォーマンスを向上させることができます。同様に、VM とローカルディスクの間の帯域幅を増やすことができます (直接接続されていない場合)。

アプリケーション環境への CPU リソースの追加

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

Storage Gateway での VMware vSphere ハイアベイラビリティの使用

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 VMware Cloud on AWS 上にデプロイされたゲートウェイは、ほとんどのサービス中断から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。

Storage Gateway で VMware HA を使用するには、次の手順を実行します。

トピック

- vSphere の VMware HA クラスターの設定
- ゲートウェイタイプ用の .ova イメージのダウンロード
- ゲートウェイのデプロイ
- (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
- ゲートウェイのアクティブ化
- VMware High Availability 設定のテスト

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 [Edit Cluster Settings] 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、以下の順序でオプションを設定します。

   - ホスト障害応答: VM を再起動します。
   - ホスト分離の応答: VM をシャットダウンして再起動する
   - PDL を使用したデータストア: Disabled
   - APD を使用したデータストア: Disabled
   - VM モニタリング: VM およびアプリケーションの監視

   例については、以下のスクリーンショットを参照してください。

2. 次の値を調整して、クラスターの感度を微調整します。

   - 障害間隔— この間隔の後、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待機します。
   - VM ごとの最大リセット— クラスターは、最大リセット時間枠内で最大数の VM を再起動します。
   - [Maximum resets Time— VM ごとの最大リセット数をカウントする時間枠。

   設定する値がわからない場合は、次の設定例を使用します。

   - [Failure interval]: **30** 秒
   - [Minimum uptime]: **120** 秒
   - [Maximum per-VM resets]: **3**
   - [Maximum resets time window]: **1** 時間

クラスターで他の 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用の .ova イメージのダウンロード

.ova イメージをダウンロードするには、次の手順を実行します。

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 —

ゲートウェイのデプロイ

設定したクラスターで、.ova イメージをクラスターのホストの 1 つにデプロイします。

ゲートウェイの .ova イメージをデプロイするには

1. .ova イメージをクラスター内のホストの 1 つにデプロイします。
2. ルートディスクとキャッシュ用に選択したデータストアが、クラスター内のすべてのホストで使用可能であることを確認します。

(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。

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。

   オーバーライドオプションについては、次のスクリーンショットを参照してください。

ゲートウェイのアクティブ化

ゲートウェイの .ova がデプロイされたら、ゲートウェイをアクティブ化します。ゲートウェイの種類ごとの違いについて説明します。

ゲートウェイをアクティブ化するには

- ゲートウェイの種類に基づいてアクティベーションの手順を選択します。
  - ファイルゲートウェイ —

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. で Storage Gateway コンソールを開きます。https://console.aws.amazon.com/storagegateway/home。
2. ナビゲーションペインで [Gateways] 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. [Actions] で、[Verify VMware HA (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。

Amazon CloudWatch ロググループで VMware HA イベントに関する情報があります。詳細については、CloudWatch ロググループを使用したファイルゲートウェイのヘルスログの取得を参照してください。

でのセキュリティAWSStorage Gateway

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

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

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

このドキュメントは、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。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するためにStorage Gateway を設定する方法について説明します。また、他の使い方も学びますAWSStorage Gateway リソースのモニタリングや保護に役立つサービス。

トピックス

でのデータ保護AWSStorage Gateway

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

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

- 各アカウントで多要素認証(MFA)を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 以降が推奨されています。
- AWS CloudTrail で API とユーザーアクティビティログをセットアップします。
- AWS暗号化ソリューションをAWSサービス内のすべてのデフォルトのセキュリティ管理と一緒に使用します。
- Amazon Macieなどのアドバンストマネージドセキュリティサービスを使用します。これは、Amazon S3に保存されている個人データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API を使用して AWS にアクセスするときに FIPS 140-2 の検証を受けた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、[Federal Information Processing Standard (FIPS) 140-2] (連邦情報処理規格 (FIPS) 140-2) を参照してください。

顧客のメールアドレスなどの機密または注意を要する情報は、タグや [Name] (名前) フィールドなど自由形式のフィールドに配置しないことを強くお勧めします。これには、Storage Gateway などを使用する場合も同様です。AWSコンソール、API、を使用したサービスAWS CLI, またはAWSSDK。タグまたは名前に使用する自由記入欄に入力したデータは、課金や診断ログに使用される場合があります。外部サーバーへの URL を提供する場合は、そのサーバーへのリクエストを検証するための認証情報を URL に含めないように強くお勧めします。q

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。デフォルトでは、Storage Gateway は Amazon S3 で管理された暗号化キー (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側で暗号化します。Storage Gateway API を使用して、でサーバー側の暗号化を使用してクラウドに保存されているデータを暗号化するようにゲートウェイを設定することもできます。AWS Key Management Service(SSE-KMS) カスタマーマスターキー (CMK)。

> **Important**
>
> を使用したときAWS KMSCMK サーバー側の暗号化を行うには、対称 CMK を選択する必要があります。Storage Gateway では、非対称 CMK はサポートされていません。詳細については、AWS Key Management Service デベロッパーガイドの対称キーと非対称キーの使用を参照してください。

ファイル共有を暗号化する

ファイル共有の場合、オブジェクトを暗号化するようにゲートウェイを構成できます。AWS KMS — SSE-KMS を使用してキーを管理します。Storage Gateway API を使用してファイル共有に書き込むデータを暗号化するには、「」を参照してください。CreateNFSFileShareのAWS Storage GatewayAPI リファレンス。

ファイルシステムの暗号化

詳細については、「」を参照してください。Amazon FSx でのデータ暗号化のAmazon FSx for Windows File Server ユーザーガイド。

AWS KMS を使用してデータを暗号化する場合は、次のこと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 ユーザーは、を呼び出すには、必要なアクセス権限が必要です。AWS KMSAPI オペレーション。詳細については、「」を参照してください。での IAM ポリシーの使用AWS KMSのAWS Key Management Serviceデベロッパーガイド。
- CMK を削除または無効にするか、許可トークンを取り消した場合、ボリュームまたはテープ上のデータにアクセスすることはできません。詳細については、「」を参照してください。カスタマーマスターキーを削除するのAWS Key Management Serviceデベロッパーガイド。

- KMS で暗号化されたボリュームからスナップショットを作成すると、スナップショットは暗号化されます。スナップショットは、ボリュームの KMS キーを継承します。
- KMS で暗号化されたスナップショットから新しいボリュームを作成すると、ボリュームは暗号化されます。新しいボリュームに別の KMS キーを指定できます。

> **Note**
>
> Storage Gateway は、KMS で暗号化されたボリュームやスナップショットの復旧ポイントからの暗号化されていないボリュームの作成をサポートしていません。

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

Storage Gateway の認証とアクセスコントロール

AWS Storage Gateway へのアクセスには、AWS によってリクエストの認証に使用される認証情報が必要です。それらの認証情報を取得したユーザーにAWSゲートウェイ、ファイル共有、ボリューム、テープなどのリソース。以下のセクションでは、使用方法の詳細を示します。AWS Identity and Access Management(IAM)Storage Gateway を使用すると、リソースにアクセスできるユーザーを制御してリソースを保護できます。

- 認証
- アクセスコントロール

認証

AWS には、次のタイプのアイデンティティでアクセスできます。

- AWS アカウント ルートユーザー - AWS アカウントを初めて作成するときは、このアカウント内のすべての AWS のサービスとリソースに対する完全なアクセス権を持つシングルサインインアイデンティティを使って作成を開始します。このアイデンティティは AWS アカウント ルートユーザー と呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることによってアクセスできます。強くお勧めするのは、日常的なタスクには、それが管理者タスクであっても、ルートユーザーを使用しないことです。代わりに、初期の IAM ユーザーを作成するためにのみ、ルートユーザーを使用するというベストプラクティスに従います。その後、ルートユーザーの認証情報を安全な場所に保管し、それらを使用して少数のアカウントおよびサービス管理タスクのみを実行します。

- IAM ユーザー— あんIAM ユーザーあなたの中の身元ですかAWS アカウントには、特定のカスタムアクセス許可 (たとえば、Storage Gateway でゲートウェイを作成するアクセス権限など) があります。IAM のユーザー名とパスワードは、AWS Management Console、AWS ディスカッションフォーラム、または AWS Support センターなどのセキュアな AWS ウェブページへのサインインに使用できます。

  ユーザー名とパスワードに加えて、各ユーザーの アクセスキー を生成することもできます。これらのキーは、 SDK の 1 つ または AWS Command Line Interface (CLI)を使用してプログラム的に AWS サービスにアクセスするときに使用できます。SDK と CLI ツールでは、アクセスキーを使用してリクエストが暗号で署名されます。AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。Storage Gateway署名バージョン 4では、インバウンド API リクエストを認証するためのプロトコルです。リクエストの認証の詳細については、 AWS 一般参照の 署名バージョン 4 署名プロセス を参照してください。

- IAM ロール - IAM ロールは、アカウントで作成して特定のアクセス権限を付与できる IAM アイデンティティです。IAM ロールは、アイデンティティが AWS で実行できることとできないことを決定するアクセス許可ポリシーを持つ AWS アイデンティティであるという点で IAM ユーザーと似ています。ただし、ユーザーは 1 人の特定の人に一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。また、ロールには標準の長期認証情報 (パスワードやアクセスキーなど) も関連付けられません。代わりに、ロールを引き受けると、ロールセッション用の一時的なセキュリティ認証情報が提供されます。IAM ロールと一時的な認証情報は、次の状況で役立ちます。

  - フェデレーティッドユーザーアクセス – IAM ユーザーを作成する代わりに、 AWS Directory Service、エンタープライズユーザーディレクトリ、またはウェブアイデンティティプロバイダーからの既存のアイデンティティを使用できます。このようなユーザーは フェデレーティッドユーザー と呼ばれます。AWS では、ID プロバイダーを通じてアクセスがリクエストされたとき、フェデレーティッドユーザーにロールを割り当てます。フェデレーティッドユーザーの詳細については、 IAM ユーザーガイドの フェデレーティッドユーザーとロール を参照してください。

  - AWS のサービスアクセス - サービスロールは、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 のサービスにアクセス権限を委任するロールの作成」を参照してください。

- Amazon EC2 で実行されているアプリケーション - EC2 インスタンスで実行され、 AWS CLI または AWS API 要求を行っているアプリケーションのテンポラリ認証情報を管理するには、IAM ロールを使用できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。AWS ロールを EC2 インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスに添付されたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムはテンポラリ認証情報を取得することができます。詳細については、 IAM ユーザーガイドの IAM ロールを使用して、Amazon EC2 インスタンスで実行されるアプリケーションにアクセス許可を付与する を参照してください。

アクセスコントロール

リクエストを認証するための有効な認証情報があっても、アクセス許可がなければ Storage Gateway リソースの作成やアクセスはできません。たとえば、Storage Gateway でゲートウェイを作成する権限が必要です。

以下のセクションでは、Storage Gateway のアクセス許可を管理する方法について説明します。最初に概要のセクションを読むことをお勧めします。

- Storage Gateway に対するアクセス許可の管理の概要
- アイデンティティベースのポリシー (IAM ポリシー)

Storage Gateway に対するアクセス許可の管理の概要

EVERYAWSリソースは Amazon Web Services アカウントによって所有され、リソースの作成またはアクセスは、アクセス権限のポリシーによって管理されます。アカウント管理者は、アクセス許可ポリシーを IAM アイデンティティ（ユーザー、グループ、ロール）にアタッチできます。一部のサービス（ AWS Lambdaなど）では、アクセス許可ポリシーをリソースに添付することもできます。

> **Note**
>
> アカウント管理者（または管理者ユーザー）は、管理者権限を持つユーザーです。詳細については、IAM ユーザーガイドの「IAM のベストプラクティス」を参照してください。

アクセス権限を付与する場合、アクセス権限を取得するユーザー、取得するアクセス権限の対象となるリソース、およびそれらのリソースに対して許可される特定のアクションを決定します。

トピック

- Storage Gateway のリソースと操作
- リソース所有権について
- リソースへのアクセスの管理
- ポリシー要素の指定: アクション、効果、リソース、プリンシパル
- ポリシーでの条件を指定する

Storage Gateway のリソースと操作

Storage Gateway では、プライマリリソースがゲートウェイ。Storage Gateway では、追加リソースタイプとしてファイル共有、ボリューム、仮想テープ、iSCSI ターゲット、仮想テープライブラリ (VTL) デバイスもサポートされています。これらは、サブリソースと呼ばれ、ゲートウェイに関連付けられている場合にのみ存在します。

これらのリソースとサブリソースには、次の表に示すとおり、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`*
ファイルシステム ARN	`arn:aws:fsx:` *`region`*`:`*`account-id`* `:file-system/` *`filesystem-id`*

> **Note**
>
> Storage Gateway リソース ID は大文字です。Amazon EC2 API でこれらのリソース ID を使用するとき、Amazon EC2 は小文字のリソース ID を必要とします。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。たとえば、ボリュームの ID が Storage Gateway では `vol-1122AABB` であるとします。この ID を EC2 API で使用するには、`vol-1122aabb` に変更する必要があります。これを行わなければ、EC2 API が正常に動作しない場合があります。
> 2015 年 9 月 2 日より前にアクティベートされたゲートウェイの ARN には、ゲートウェイ ID ではなくゲートウェイ名が含まれています。ゲートウェイの ARN を取得するには、`DescribeGatewayInformation` API オペレーションを使用します。

テープの作成などの特定の API オペレーションに対するアクセス権限を付与するために、Storage Gateway には、これらのリソースとサブリソースを作成および管理するための一連の API アクションが用意されています。API アクションのリストについては、「」を参照してくださいアクションのAWS Storage GatewayAPI リファレンス。

テープの作成などの特定のAPIオペレーションに対するアクセス権限を付与するために、Storage Gateway ではアクセス権限ポリシーで指定できる一連のアクションが定義されています。1 つの API オペレーションに複数のアクションを定義して、それらのアクションのためのアクセス権限を付与することが必要になる場合があります。Storage Gateway API のすべてのアクションとそれらが適用されるリソースを示す表については、「」を参照してください。Storage Gateway API のアクセス許可: アクション、リソース、条件リファレンス。

リソース所有権について

あるリソース所有者リソースを作成したAmazon Web Services アカウントです。つまり、リソース所有者はAmazon Web Services アカウントでプリンシパルエンティティリソースの作成リクエストを認証する (ルートアカウント、IAM ユーザー、または IAM ロール)。以下の例は、このしくみを示しています。

- Amazon Web Services アカウントのルートアカウントの認証情報を使用してゲートウェイをアクティベートする場合、Amazon Web Services アカウントはリソースの所有者です (Storage Gateway では、リソースはゲートウェイです)。
- Amazon Web Services アカウントに IAM ユーザーを作成し、アクセス権限を付与する場合`ActivateGateway`そのユーザーにアクションを実行する場合、そのユーザーはゲートウェイをアクティベートできます。ただし、ゲートウェイリソースを所有しているのは、このユーザーが属するAmazon Web Services アカウントです。
- ゲートウェイをアクティベートするためのアクセス権限を持つ IAM ロールをAmazon Web Services アカウントで作成する場合、そのロールを引き受けることのできるいずれのユーザーもゲートウェイをアクティベートできます。ゲートウェイリソースを所有しているのは、このロールが属するAmazon Web Services アカウントです。

リソースへのアクセスの管理

アクセスポリシーでは、誰が何にアクセスできるかを記述します。以下のセクションで、アクセス許可ポリシーを作成するために使用可能なオプションについて説明します。

> **Note**
>
> このセクションでは、Storage Gateway コンテキストでの IAM の使用について説明します。これは、IAM サービスに関する詳細情報を取得できません。完全な IAM ドキュメントについては、「」を参照してくださいIAM とはのIAM ユーザーガイド。IAM ポリシー構文の詳細と説明については、『IAM ユーザーガイド』の「AWS IAM ポリシーの参照」を参照してください。

IAM アイデンティティに添付されたポリシーは アイデンティティベース のポリシー (IAM ポリシー) と呼ばれ、リソースに添付されたポリシーは リソースベース のポリシーと呼ばれます。Storage Gateway では、アイデンティティベースのポリシー (IAM ポリシー) のみサポートされます。

トピック

- アイデンティティベースのポリシー (IAM ポリシー)
- リソースベースのポリシー

アイデンティティベースのポリシー (IAM ポリシー)

ポリシーを IAM アイデンティティに添付できます。例えば、次の操作を実行できます。

- アカウントのユーザーまたはグループにアクセス権限ポリシーをアタッチする：アカウント管理者は、特定のユーザーに関連付けられるアクセス権限ポリシーを使用して、そのユーザーにゲートウェイ、ボリューム、テープなどのStorage Gateway リソースの作成を許可するアクセス権限を付与できます。
- アクセス許可ポリシーをロールに添付する (クロスアカウントのアクセス許可を付与) – アイデンティティベースのアクセス許可ポリシーを IAM ロールにアタッチして、クロスアカウントのアクセス許可を付与することができます。たとえば、アカウント A の管理者は、次のように別の Amazon Web Services アカウント (たとえば、アカウント B) または AWS のサービスにクロスアカウントアクセス許可を付与するロールを作成できます。
  1. アカウント A の管理者は、IAM ロールを作成して、アカウント A のリソースに権限を付与するロールに権限ポリシーをアタッチします。
  2. アカウント A の管理者は、アカウント B をそのロールを引き受けるプリンシパルとして識別するロールに、信頼ポリシーをアタッチします。
  3. アカウント B の管理者は、アカウント B のユーザーにロールを引き受ける権限を委任できるようになります。これにより、アカウント B のユーザーにアカウント A のリソースの作成とアクセスが許可されます。 AWS サービスのアクセス許可を付与してロールを引き受けさせたい場合は、信頼ポリシー内のプリンシパルも、 AWS サービスのプリンシパルとなることができます。

  IAM を使用した許可委任の詳細については、IAM ユーザーガイドのアクセス 管理を参照してください。

すべてのリソースのすべての `List*` アクションにアクセス権限を付与するポリシーの例を次に示します。このアクション読み取り専用アクションです。したがって、ポリシーでは、ユーザーによるリソースの状態の変更が許可されません。

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "AllowAllListActionsOnAllResources",
            "Effect": "Allow",
            "Action": [
                "storagegateway:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Storage Gateway でアイデンティティベースのポリシーを使用する方法の詳細については、「」を参照してください。Storage Gateway でのアイデンティティベースのポリシー (IAM ポリシー) の使用。ユーザー、グループ、ロール、アクセス許可の詳細については、IAM ユーザーガイドの「アイデンティティ (ユーザー、グループ、ロール)」を参照してください。

リソースベースのポリシー

Amazon S3 などの他のサービスでは、リソースベースのアクセス権限ポリシーもサポートされています。例えば、ポリシーを S3 バケットに添付して、そのバケットに対するアクセス許可を管理できます。Storage Gateway では、リソースベースのポリシーはサポートされていません。

ポリシー要素の指定: アクション、効果、リソース、プリンシパル

Storage Gateway リソースごとに (を参照) Storage Gateway API のアクセス許可: アクション、リソース、条件リファレンス) では、このサービスは、一連の API オペレーションを定義します (「」を参照してくださいアクション). これらの API 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ために、Storage Gateway ではポリシーに一連のアクションを定義できます。たとえば、Storage Gateway Gateway リソースの場合、アクションは次のとおりです。`ActivateGateway`,`DeleteGateway`, および`DescribeGatewayInformation`。API オペレーションを実行する場合に、複数のアクションで権限が必要となる場合があることに注意してください。

以下は、最も基本的なポリシーの要素です。

- リソース – ポリシーで Amazon リソースネーム (ARN) を使用して、ポリシーを適用するリソースを識別します。Storage Gateway リソースの場合、必ずワイルドカード文字を使用します。(*)IAM ポリシー内。詳細については、「Storage Gateway のリソースと操作」を参照してください。

- アクション - アクションのキーワードを使用して、許可または拒否するリソースオペレーションを識別します。たとえば、指定に応じてEffectとすると、storagegateway:ActivateGatewayアクセス権限では、Storage Gateway の実行をユーザーに許可または拒否します。ActivateGatewayオペレーション.
- 効果 – ユーザーが特定のアクションを要求する際の効果を指定します。許可または拒否のいずれかになります。リソースへのアクセスを明示的に許可していない場合、アクセスは暗黙的に拒否されます。また、明示的にリソースへのアクセスを拒否すると、別のポリシーによってアクセスが許可されている場合でも、ユーザーはそのリソースにアクセスできなくなります。
- プリンシパル - アイデンティティベースのポリシー（IAM ポリシー）で、ポリシーが添付されているユーザーが黙示的なプリンシパルとなります。リソースベースのポリシーでは、権限（リソースベースのポリシーにのみ適用）を受け取りたいユーザー、アカウント、サービス、またはその他のエンティティを指定します。Storage Gateway では、リソースベースのポリシーはサポートされていません。

IAM ポリシーの構文と記述の詳細については、IAM ユーザーガイドの AWS IAM ポリシーリファレンスを参照してください。

Storage Gateway API のすべてのアクションを示す表については、「」を参照してください。Storage Gateway API のアクセス許可: アクション、リソース、条件リファレンス。

ポリシーでの条件を指定する

アクセス権限を付与するとき、IAM ポリシー言語を使用して、ポリシーが有効になるために必要とされる条件を指定できます。たとえば、特定の日付の後にのみ適用されるポリシーが必要になる場合があります。ポリシー言語での条件の指定の詳細については、IAM ユーザーガイドの「条件」を参照してください。

条件を表すには、あらかじめ定義された条件キーを使用します。Storage Gateway に固有の条件キーはありません。ただし、必要に応じて使用できる AWS 全体の条件キーがあります。AWS 全般的なすべてのキーのリストについては、『IAM ユーザーガイド』の「利用可能なキー」を参照してください。

Storage Gateway でのアイデンティティベースのポリシー (IAM ポリシー) の使用

このトピックでは、アカウント管理者が IAM アイデンティティ（ユーザー、グループ、ロール）へのアクセス権限ポリシーをアタッチする、アイデンティティベースのポリシーの例を示します。

> **Important**
>
> 初めに、Storage Gateway リソースへのアクセスを管理するための基本概念と使用可能なオプションについて説明する概要トピックを読むことをお勧めします。詳細については、「Storage Gateway に対するアクセス許可の管理の概要」を参照してください。

このセクションでは、次のトピックを対象としています。

- Storage Gateway コンソールを使用するために必要なアクセス許可
- AWSStorage Gateway の管理ポリシー
- お客様のマネージドポリシーの例

以下に示しているのは、アクセス権限ポリシーの例です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsSpecifiedActionsOnAllGateways",
            "Effect": "Allow",
            "Action": [
                "storagegateway:ActivateGateway",
                "storagegateway:ListGateways"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowsSpecifiedEC2ActionsOnAllGateways",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSnapshots",
                "ec2:DeleteSnapshot"
            ],
            "Resource": "*"
        }
    ]
}
```

このポリシーには 2 つのステートメントがあります (両方のステートメントに Action および Resource 要素があることに注意してください)。

- 最初のステートメントでは、2 つのStorage Gateway アクション (storagegateway:ActivateGatewayそしてstoragegateway:ListGateways) をゲートウェイリソースに入力します。

  ワイルドカード文字 (*) は、このステートメントはどのリソースとも一致する可能性があることを意味します。この場合、ステートメントは許可しますstoragegateway:ActivateGatewayそしてstoragegateway:ListGateways任意のゲートウェイでのアクション。ゲートウェイを作成するまでリソース ID はわからないため、ここではワイルドカード文字が使用されます。ポリシーでワイルドカード文字 (*) を使用する方法については、「例 2: ゲートウェイへの読み取り専用アクセスを許可する」を参照してください。

  > **Note**
  >
  > ARN は AWS リソースを一意に識別します。詳細については、AWS 全般のリファレンスの「Amazon リソースネーム (ARN) と AWS のサービスの名前空間」を参照してください。

  特定のアクションに対するアクセス権限を特定のゲートウェイのみに制限するには、ポリシーでそのアクションのステートメントを個別に作成し、そのステートメントでゲートウェイ ID を指定します。

- 2 つ目のステートメントは、ec2:DescribeSnapshots および ec2:DeleteSnapshot アクションに対するアクセス権限を付与します。これらの Amazon Elastic Compute Cloud (Amazon EC2) アクションは、アクセス権限を必要とします。これは、Storage Gateway から生成されたスナップショットは Amazon Elastic Block Store (Amazon EBS) に保存され、Amazon EC2 リソースとして管理されるため、対応する EC2 アクションが必要になります。詳細については、「」を参照してください。アクションのAmazon EC2 API リファレンス。これらの Amazon EC2 アクションではリソースレベルのアクセス権限はサポートされていないため、ポリシーではワイルドカード文字 (*) がResourceゲートウェイ ARN を指定する代わりに値。

すべてのStorage Gateway API アクションとそれらが適用されるリソースの表については、「」を参照してください。Storage Gateway API のアクセス許可: アクション、リソース、条件リファレンス。

Storage Gateway コンソールを使用するために必要なアクセス許可

Storage Gateway コンソールを使用するには、読み取り専用アクセス権限を付与する必要があります。スナップショットの詳細を表示する場合は、次のアクセス権限ポリシーに示すように、追加のアクションに対するアクセス権限を付与する必要もあります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsSpecifiedEC2ActionOnAllGateways",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Resource": "*"
        }
    ]
}
```

Storage Gateway から生成された Amazon EBS スナップショットは Amazon EC2 リソースとして管理されるため、この追加のアクセス許可が必要になります。

Storage Gateway コンソールを使用するために必要な最小限のアクセス権限を設定するには、「」を参照してください。例 2: ゲートウェイへの読み取り専用アクセスを許可する。

AWSStorage Gateway の管理ポリシー

Amazon Web Services、によって作成され管理されるスタンドアロンの IAM ポリシーを提供することで、多くの一般的ユースケースに対応します。AWS。管理ポリシーは、一般的ユースケースに必要なアクセス権限を付与することで、どの権限が必要なのかをユーザーが調査する必要をなくすることができます。の詳細AWS管理ポリシー。「」を参照してください。AWS管理ポリシーのIAM ユーザーガイド。

以下のようになりますAWSアカウントのユーザーにアタッチ可能な管理ポリシーは、Storage Gateway に固有のものです。

- AWS Storage Gateway 読み取り専用アクセス— への読み取り専用アクセス権を付与します。AWS Storage Gatewayリソースの使用料金を見積もることができます。
- AWS Storage Gateway フルアクセス— へのフルアクセス権を付与します。AWS Storage Gatewayリソースの使用料金を見積もることができます。

> **Note**
>
> IAM コンソールにサインインし、特定のポリシーを検索することで、これらのアクセス許可ポリシーを確認できます。

独自のカスタム IAM ポリシーを作成して、AWS Storage Gateway API アクションにアクセス権限を付与することもできます。これらのカスタムポリシーは、それらのアクセス許可が必要な IAM ユーザーまたはグループに添付できます。

お客様のマネージドポリシーの例

このセクションでは、さまざまな Storage Gateway アクションのアクセス権限を付与するユーザーポリシー例を示しています。これらのポリシーは、AWS SDK または AWS CLI を使用しているときに機能します。コンソールを使用している場合は、「Storage Gateway コンソールを使用するために必要なアクセス許可」で説明しているコンソールに固有の追加のアクセス権限を付与する必要があります。

> **Note**
>
> 各例は全て、米国西部 (オレゴン) リージョン (us-west-2) を使用し、架空のアカウント ID を使用しています。

トピック

- 例 1: すべてのゲートウェイでStorage Gateway のアクションを許可する
- 例 2: ゲートウェイへの読み取り専用アクセスを許可する
- 例 3: 特定のゲートウェイへのアクセスを許可する
- 例 4: 特定のボリュームへのアクセスをユーザーに許可する
- 例 5: 特定のプレフィクスを持つゲートウェイですべてのアクションを許可する

例 1: すべてのゲートウェイでStorage Gateway のアクションを許可する

次のポリシーを使用すると、ユーザーはすべてのStorage Gateway アクションを実行できます。このポリシーでは、ユーザーが Amazon EC2 アクション (DescribeSnapshotsそしてDeleteSnapshot) は、Storage Gateway から生成された Amazon EBS スナップショットで確認できます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAllAWSStorageGatewayActions",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {You can use Windows ACLs only with file shares that are enabled for Active
 Directory.
            "Sid": "AllowsSpecifiedEC2Actions",
            "Action": [
                "ec2:DescribeSnapshots",
                "ec2:DeleteSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

例 2: ゲートウェイへの読み取り専用アクセスを許可する

次のポリシーでは、すべてのリソースに対して List* および Describe* アクションを実行することを許可します。これらのアクションは読み取り専用アクションであることに注意してください。したがって、ポリシーでは、ユーザーによるリソースの状態の変更が許可されません。つまり、ポリシーではユーザーに次のようなアクションの実行が許可されません。DeleteGateway,ActivateGateway, およびShutdownGateway。

また、このポリシーでは、Amazon EC2 の DescribeSnapshots アクションも許可されます。詳細については、「」を参照してください。DescribeSnapshotsのAmazon EC2 API リファレンス。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowReadOnlyAccessToAllGateways",
            "Action": [
                "storagegateway:List*",
                "storagegateway:Describe*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "AllowsUserToDescribeSnapshotsOnAllGateways",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

上記のポリシーでは、ワイルドカード文字 (*) を使用する代わりに、以下の例に示すように、ポリシーの対象となるリソースの範囲を特定のゲートウェイに設定できます。そのため、このポリシーでは、特定のゲートウェイでのみアクションを実行できます。

```
"Resource": [
             "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
             "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
            ]
```

ゲートウェイ内では、以下の例に示すように、リソースの範囲をさらにゲートウェイボリュームのみに制限できます。

```
"Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/volume/
*"
```

例 3: 特定のゲートウェイへのアクセスを許可する

次のポリシーでは、特定のゲートウェイ上でのすべてのアクションを許可します。ユーザーはデプロイ済みの他のゲートウェイにはアクセスできません。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowReadOnlyAccessToAllGateways",
            "Action": [
                "storagegateway:List*",
                "storagegateway:Describe*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "AllowsUserToDescribeSnapshotsOnAllGateways",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "AllowsAllActionsOnSpecificGateway",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
            ]
        }
    ]
}
```

上記のポリシーは、ポリシーがアタッチされているユーザーが API またはAWSゲートウェイにアクセスするための SDK。ただし、ユーザーがStorage Gateway コンソールを使用する場合は、`ListGateways`次の例に示すように、アクション。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "AllowsAllActionsOnSpecificGateway",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
                "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
            ]
        },
        {
            "Sid": "AllowsUserToUseAWSConsole",
            "Action": [
                "storagegateway:ListGateways"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

例 4: 特定のボリュームへのアクセスをユーザーに許可する

次のポリシーでは、ユーザーはゲートウェイ上の特定のボリュームに対してすべてのアクションを実行できます。ユーザーにはデフォルトでアクセス権限が付与されないため、このポリシーでは、ユーザーは特定のボリュームにしかアクセスできません。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GrantsPermissionsToSpecificVolume",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-
id/volume/volume-id"
        },
        {
            "Sid": "GrantsPermissionsToUseStorageGatewayConsole",
            "Action": [
                "storagegateway:ListGateways"
```

```
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

上記のポリシーは、ポリシーがアタッチされているユーザーが API またはAWSボリュームにアクセスするための SDK。ただし、このユーザがAWS Storage Gatewayコンソールで許可するためのアクセス権限も付与する必要があります。`ListGateways`次の例に示すように、アクション。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GrantsPermissionsToSpecificVolume",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/volume/volume-id"
        },
        {
            "Sid": "GrantsPermissionsToUseStorageGatewayConsole",
            "Action": [
                "storagegateway:ListGateways"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

例 5: 特定のプレフィクスを持つゲートウェイですべてのアクションを許可する

以下のポリシーでは、名前がで始まるゲートウェイに対するすべてのStorage Gateway アクションの実行をユーザーに許可しています。`DeptX`。また、このポリシーでは、`DescribeSnapshots`Amazon EC2 アクション。スナップショットを記述する場合に必要です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsActionsGatewayWithPrefixDeptX",
            "Action": [
                "storagegateway:*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/DeptX"
        },
        {
            "Sid": "GrantsPermissionsToSpecifiedAction",
            "Action": [
                "ec2:DescribeSnapshots"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

上記のポリシーは、ポリシーがアタッチされているユーザーが API またはAWSゲートウェイにアクセスするための SDK。ただし、このユーザがAWS Storage Gatewayコンソールを使用する場合は、の説明に従って追加のアクセス権限を付与する必要があります。例 3: 特定のゲートウェイへのアクセスを許可する。

タグを使用したゲートウェイとリソースへのアクセスのコントロール

ゲートウェイリソースとアクションへのアクセスをコントロールするには、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 つの方法で可能です：

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。

```
{
  "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:region:account-id:*/*"
      }
  ]
}
```

IAM リクエスト内のタグに基づいたアクセスの制御

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、タグに基づいて IAM ポリシーの条件を使用できます。たとえば、IAM ユーザーが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) 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。**Department**そして**Finance**。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。

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

Storage Gateway API のアクセス許可: アクション、リソース、条件リファレンス

アクセスコントロールを設定し、IAM アイデンティティにアタッチできるアクセス許可ポリシー (アイデンティティベースのポリシー) を作成するときは、以下の表をリファレンスとして使用できます。この表には、各 Storage Gateway API オペレーション、およびその実行のためのアクセス権限を付与できる対応するアクション、AWSアクセス許可を付与できるリソース。ポリシーの `Action` フィールドでアクションを指定し、ポリシーの `Resource` フィールドでリソースの値を指定します。

次を使用できます。AWSStorage Gateway ポリシーで全体の条件キーを使用して、条件を表現します。AWS 全般的なすべてのキーのリストについては、『IAM ユーザーガイド』の「利用可能なキー」を参照してください。

> **Note**
>
> アクションを指定するには、API オペレーション名 (`storagegateway:ActivateGateway`など) の前に `storagegateway:` プレフィックスを使用します。Storage Gateway アクションごとに、ワイルドカード文字 (*) をリソースとして指定できます。

ARN 形式を使用したStorage Gateway リソースのリストについては、「」を参照してください。Storage Gateway のリソースと操作。

Storage Gateway API、およびアクションに必要なアクセス許可は以下のとおりです。

ActivateGateway

アクション: `storagegateway:ActivateGateway`

リソース: *

AddCache

アクション: storagegateway:AddCache

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

AddTagsToResource

アクション: storagegateway:AddTagsToResource

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

または

arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

または

arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

AddUploadBuffer

アクション: storagegateway:AddUploadBuffer

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

AddWorkingStorage

アクション: storagegateway:AddWorkingStorage

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

CancelArchival

アクション: storagegateway:CancelArchival

リソース: arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

CancelRetrieval

アクション: storagegateway:CancelRetrieval

リソース: arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

CreateCachediSCSIVolume

アクション: storagegateway:CreateCachediSCSIVolume

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

CreateSnapshot

アクション: storagegateway:CreateSnapshot

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

CreateSnapshotFromVolumeRecoveryPoint

アクション: storagegateway:CreateSnapshotFromVolumeRecoveryPoint

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

CreateStorediSCSIVolume

アクション: storagegateway:CreateStorediSCSIVolume

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

CreateTapes

アクション: storagegateway:CreateTapes

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DeleteBandwidthRateLimit

アクション: storagegateway:DeleteBandwidthRateLimit

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DeleteChapCredentials

アクション: storagegateway:DeleteChapCredentials

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/target/*iSCSItarget*

DeleteGateway

アクション: storagegateway:DeleteGateway

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DeleteSnapshotSchedule

アクション: storagegateway:DeleteSnapshotSchedule

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

DeleteTape

アクション: storagegateway:DeleteTape

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DeleteTapeArchive

アクション: storagegateway:DeleteTapeArchive

リソース: *

DeleteVolume

アクション: storagegateway:DeleteVolume

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

DescribeBandwidthRateLimit

アクション: storagegateway:DescribeBandwidthRateLimit

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeCache

アクション: storagegateway:DescribeCache

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeCachediSCSIVolumes

アクション: storagegateway:DescribeCachediSCSIVolumes

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

DescribeChapCredentials

アクション: storagegateway:DescribeChapCredentials

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/target/*iSCSItarget*

DescribeGatewayInformation

アクション: storagegateway:DescribeGatewayInformation

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeMaintenanceStartTime

アクション: storagegateway:DescribeMaintenanceStartTime

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeSnapshotSchedule

アクション: storagegateway:DescribeSnapshotSchedule

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

DescribeStorediSCSIVolumes

アクション: storagegateway:DescribeStorediSCSIVolumes

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

DescribeTapeArchives

アクション: storagegateway:DescribeTapeArchives

リソース: *

DescribeTapeRecoveryPoints

アクション: storagegateway:DescribeTapeRecoveryPoints

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeTapes

アクション: storagegateway:DescribeTapes

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeUploadBuffer

アクション: storagegateway:DescribeUploadBuffer

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeVTLDevices

アクション: storagegateway:DescribeVTLDevices

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeWorkingStorage

アクション: storagegateway:DescribeWorkingStorage

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DisableGateway

アクション: storagegateway:DisableGateway

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ListGateways

アクション: storagegateway:ListGateways

リソース: *

ListLocalDisks

アクション: storagegateway:ListLocalDisks

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ListTagsForResource

アクション: storagegateway:ListTagsForResource

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

または

arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

または

arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

ListTapes

アクション: storagegateway:ListTapes

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ListVolumeInitiators

アクション: storagegateway:ListVolumeInitiators

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

ListVolumeRecoveryPoints

アクション: storagegateway:ListVolumeRecoveryPoints

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ListVolumes

アクション: storagegateway:ListVolumes

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

RemoveTagsFromResource

アクション: storagegateway:RemoveTagsFromResource

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

または

arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

または

arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

ResetCache

アクション: storagegateway:ResetCache

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

RetrieveTapeArchive

アクション: storagegateway:RetrieveTapeArchive

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

RetrieveTapeRecoveryPoint

アクション: `storagegateway:RetrieveTapeRecoveryPoint`

リソース: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

ShutdownGateway

アクション: `storagegateway:ShutdownGateway`

リソース: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

StartGateway

アクション: `storagegateway:StartGateway`

リソース: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

UpdateBandwidthRateLimit

アクション: `storagegateway:UpdateBandwidthRateLimit`

リソース: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

UpdateChapCredentials

アクション: `storagegateway:UpdateChapCredentials`

リソース: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*`/target/`*`iSCSItarget`*

UpdateGatewayInformation

アクション: `storagegateway:UpdateGatewayInformation`

リソース: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

UpdateGatewaySoftwareNow

アクション: `storagegateway:UpdateGatewaySoftwareNow`

リソース: `arn:aws:storagegateway:`*`region`*`:`*`account-id`*`:gateway/`*`gateway-id`*

UpdateMaintenanceStartTime

アクション: `storagegateway:UpdateMaintenanceStartTime`

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

UpdateSnapshotSchedule

アクション: storagegateway:UpdateSnapshotSchedule

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

UpdateVTLDeviceType

アクション: storagegateway:UpdateVTLDeviceType

リソース: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/device/*vtldevice*

関連トピック

- アクセスコントロール
- お客様のマネージドポリシーの例

Storage Gateway のサービスにリンクされたロールの使用

Storage GatewayAWS Identity and Access Management(IAM)サービスにリンクされたロール。サービスにリンクされたロールは、Storage Gateway に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは、Storage Gateway によって事前定義されており、サービスから other を呼び出すために必要なすべてのアクセス許可が含まれされます。AWSお客様に代わってのサービス。

サービスにリンクされたロールを使用することで、必要なアクセス許可を手動で追加する必要がなくなるため、Storage Gateway の設定が簡単になります。Storage Gateway は、サービスにリンクされたロールのアクセス許可を定義します。特に定義されている場合を除き、Storage Gateway のみがそのロールを引き受けることができます。定義される許可には、信頼ポリシーと許可ポリシーが含まれており、その許可ポリシーを他のIAM エンティティに添付することはできません。

サービスリンクロールをサポートする他のサービスについては、「AWS Services That Work with IAM」を参照して、[Service-Linked Role] (サービスにリンクされたロール) 列が[Yes] (はい) になっているサービスを見つけてください。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、リンク付きの [Yes] (はい) を選択します。

Storage Gateway のサービスにリンクされたロールのアクセス許可

Storage Gateway では、という名前のサービスにリンクされたロールを使用します。ストレージゲートウェイの AWS サービスロール— ストレージゲートウェイの AWS サービスロール。

サービスにリンクされたロール AWSServiceRoleForStorageGateWay サービスにリンクされたロールは、ロールを引き受ける上で次のサービスを信頼します。

- `storagegateway.amazonaws.com`

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

- アクション: `arn:aws:fsx:*:*:backup/*` の `fsx:ListTagsForResource`

サービスにリンクされたロールの作成と編集を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、アクセス権限を設定する必要があります。詳細については、IAM ユーザーガイド の「サービスにリンクされたロールのアクセス許可」を参照してください。

Storage Gateway のサービスにリンクされたロールの作成

サービスリンクロールを手動で作成する必要はありません。Storage Gateway を作成するときAssociateFileSystemでの API コールAWS Management Consoleとすると、AWS CLI、またはAWSAPI、Storage Gateway は、サービスにリンクされたロールを作成します。

> **Important**
>
> このサービスリンクロールがアカウントに表示されるのは、このロールでサポートされている機能を使用する別のサービスでアクションが完了した場合です。また、サービスにリンクされたロールのサポートが開始された2021 年 3 月 31 日以前に Storage Gateway サービスを使用していた場合、Storage Gateway は AWSServiceRoleForStorageGateWay ロールをアカウントに作成済みです。詳細については、「IAM アカウントに新しいロールが表示される」を参照してください。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は、同じ方法でアカウントにロールを再作成できます。Storage Gateway を作成するときAssociateFileSystemAPI 呼び出しを行うと、Storage Gateway によってサービスにリンクされたロールが再度作成されます。

IAM コンソールを使用して、サービスにリンクされたロールをストレージゲートウェイの AWS サービスロールユースケース。AWS CLI または AWS API で、`storagegateway.amazonaws.com` サービス名を使用してサービスリンクロールを作成します。詳細については、IAM ユーザーガイドの「サービスにリンクされたロールの作成」を参照してください。このサービスリンクロールを削除する場合、この同じプロセスを使用して、もう一度ロールを作成できます。

Storage Gateway のサービスにリンクされたロールの編集

Storage Gateway では、AWSServiceRoleForStorageGateWay サービスにリンクされたロールを編集することはできません。サービスリンクロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAMを使用したロールの説明の編集はできます。詳細については、IAM ユーザーガイドの「サービスリンクロールの編集」を参照してください。

Storage Gateway のサービスにリンクされたロールの削除

Storage Gateway では、AWSServiceRoleForStorageGateWay ロールが自動的に削除されません。AWSServiceRoleforStorageGateWay ロールを削除するには、`iam:DeleteSLR`アピ。サービス· リンク· ロールに依存するストレージ· ゲートウェイ· リソースがない場合、削除は成功します。そうしないと、削除は失敗します。サービスにリンクされたロールを削除する場合は、IAM API を使用する必要があります`iam:DeleteRole`または`iam:DeleteServiceLinkedRole`。この場合、Storage Gateway APIを使用して、アカウント内のゲートウェイまたはファイルシステムの関連付けを最初に削除し、次にサービスにリンクされたロールを削除する必要があります。`iam:DeleteRole`または`iam:DeleteServiceLinkedRole`アピ。IAM を使用してサービスにリンクされたロールを削除する場合は、Storage Gateway を使用する必要があります。`DisassociateFileSystemAssociation`API は、アカウント内のすべてのファイルシステムの関連付けを最初に削除します。そうしないと、削除操作は失敗します。

> **Note**
>
> リソースを削除する際に、Storage Gateway サービスでそのロールが使用されている場合、削除は失敗することがあります。失敗した場合は、数分待ってから操作を再試行してください。

AWSServiceRoleForStorageGateWay で使用されているStorage Gateway リソースを削除するには

1. サービスコンソール、CLI、または API を使用して、リソースをクリーンアップしてロールを削除する呼び出しを行うか、IAM コンソール、CLI、または API を使用して削除を実行します。こ

の場合、Storage Gateway APIを使用して、アカウント内のゲートウェイとファイルシステムの関連付けをまず削除する必要があります。

2. IAM コンソール、CLI、または API を使用する場合は、IAM を使用してサービスにリンクされたロールを削除します。`DeleteRole`または`DeleteServiceLinkedRole`アピ。

IAM を使用して、サービスにリンクされたロールを手動で削除するには

IAM コンソールを使用して、AWS CLI、またはAWSAWS ServiceRoleForStorageGateWay サービスにリンクされたロールを削除するには API。詳細については、IAM ユーザーガイドの「サービスにリンクされたロールの削除」を参照してください。

Storage Gateway サービスリンクロールでサポートされるリージョン

Storage Gateway は、サービスを利用できるすべてのリージョンで、サービスにリンクされたロールの使用をサポートします。詳細については、「AWS サービスエンドポイント」を参照してください。

Storage Gateway は、サービスを利用できるすべてのリージョンで、サービスにリンクされたロールの使用をサポートしているわけではありません。AWSServiceRoleForStorageGateWay ロールは、以下のリージョンで使用できます。

リージョン名	リージョン識別子	Storage Gateway でのSupport
米国東部 (バージニア北部)	us-east-1	はい
米国東部 (オハイオ)	us-east-2	はい
米国西部 (北カリフォルニア)	us-west-1	はい
米国西部 (オレゴン)	us-west-2	はい
アジアパシフィック (ムンバイ)	ap-south-1	はい
アジアパシフィック (大阪)	ap-northeast-3	はい
アジアパシフィック (ソウル)	ap-northeast-2	はい
アジアパシフィック (シンガポール)	ap-southeast-1	はい

リージョン名	リージョン識別子	Storage Gateway でのSupport
アジアパシフィック (シドニー)	ap-southeast-2	はい
アジアパシフィック (東京)	ap-northeast-1	はい
カナダ (中部)	ca-central-1	はい
欧州 (フランクフルト)	eu-central-1	はい
欧州 (アイルランド)	eu-west-1	はい
欧州 (ロンドン)	eu-west-2	はい
欧州 (パリ)	eu-west-3	はい
南米 (サンパウロ)	sa-east-1	はい
AWS GovCloud (US)	us-gov-west-2	はい

でのログ記録とモニタリングAWS Storage Gateway

Storage Gateway はAWS CloudTrail、ユーザー、ロール、またはAWSStorage Gateway 内のサービス。CloudTrail は、Storage Gateway のすべての API 呼び出しをイベントとしてキャプチャします。キャプチャされた呼び出しには、Storage Gateway コンソールからの呼び出しと、Storage Gateway API オペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、Storage Gateway のイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。証跡を設定しない場合でも、CloudTrail コンソールの [Event history] (イベント履歴) で最新のイベントを表示できます。CloudTrail で収集された情報を使用して、Storage Gateway に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時、追加の詳細を確認できます。

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 情報

CloudTrailは、アカウントを作成すると AWS アカウントで有効になります。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 [他の] とともに CloudTrail イベントに記録され

ます。AWSでのサービスイベントイベント履歴。最近のイベントは、AWS アカウントで表示、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。

でのイベントの継続的な記録についてAWSStorage Gateway のイベントなどのアカウントは、証跡を作成します。証跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで追跡を作成するときに、追跡がすべてのAWSリージョンに適用されます。追跡は、AWSパーティションのすべてのリージョンからのイベントをログに記録し、明記した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail· ログで収集したイベントデータをより詳細に分析し、それに基づく対応するためにその他の AWS サービスを設定できます。詳細については、以下を参照してください:

- [Overview for Creating a Trail] (追跡を作成するための概要)
- CloudTrailのサポート対象サービスと統合
- Amazon SNSのCloudTrailの通知の設定
- 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 のすべてのアクションが記録されます。これらのアクションについては、を参照してください。アクショントピック。例えば、`ActivateGateway` 、`ListGateways`、および `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。同一性情報は以下の判断に役立ちます:

- リクエストが、ルート または AWS Identity and Access Management(IAM)ユーザー認証情報の 認証情報で行われたか。
- リクエストが、ロールとフェデレーティッドユーザーの一時的なセキュリティ認証情報で行われたか。
- リクエストが、別の AWS サービスによって送信されたかどうか。

詳細については、[CloudTrail userIdentity Element] (CloudTrail ユーザーアイデンティティ要素) 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

追跡は、指定したAmazon S3バケットにイベントをログファイルとして配信するように設定できるものです。CloudTrailのログファイルには、単一か複数のログエントリがあります。イベントはあらゆるソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストのパラメータなどの情報が含まれます。CloudTrail· ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

次は、 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": "2014-12-04T16:19:00Z",
                  "eventSource": "storagegateway.amazonaws.com",
                  "eventName": "ActivateGateway",
                  "awsRegion": "us-east-2",
                  "sourceIPAddress": "192.0.2.0",
                  "userAgent": "aws-cli/1.6.2 Python/2.7.6 Linux/2.6.18-164.el5",
                   "requestParameters": {
                                          "gatewayTimezone": "GMT-5:00",
                                          "gatewayName": "cloudtrailgatewayvtl",
                                          "gatewayRegion": "us-east-2",
                                          "activationKey": "EHFBX-1NDD0-P0IVU-PI259-
DHK88",
                                          "gatewayType": "VTL"
                                               },
                                               "responseElements": {
                                                                       "gatewayARN":
 "arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayvtl"
                                               },
                                               "requestID":
 "54BTFGNQI71987UJD2IHTCT8NF1Q8GLLE1QEU3KPGG6F0KSTAUU0",
                                               "eventID": "635f2ea2-7e42-45f0-
bed1-8b17d7b74265",
                                               "eventType": "AwsApiCall",
```

```
                                                    "apiVersion": "20130630",
                                                    "recipientAccountId": "444455556666"
            }]
}
```

次の例は、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"
              }]
}
```

のコンプライアンス検証AWSStorage Gateway

サードパーティーの監査担当者は、セキュリティとコンプライアンスを評価します。AWS 複数の一部としてのStorage GatewayAWSコンプライアンスプログラム。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、コンプライアンスプログラムによる AWS 対象範囲内のサービスを参照してください。一般的な情報については、AWS コンプライアンスプログラム を参照してください。

サードパーティーの監査レポートをダウンロードするには、AWS Artifact を使用します。詳細については、「におけるレポートのAWS Artifactダウンロードにおけるレポートのダウンロードレポート」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上の責任は、お客様のデータの機密性、会社のコンプライアンス目的、適用される法令および規制に応じて判断されます。AWSでは、コンプライアンスに役立つ以下のリソースを提供しています。

- セキュリティ＆コンプライアンスクイックリファレンスガイド – これらのデプロイガイドには、アーキテクチャ上の考慮事項の説明と、AWS で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ためのステップが記載されています。
- HIPAA セキュリティおよびコンプライアンスのためのアーキテクチャの設計ホワイトペーパー – このホワイトペーパーは、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を説明します。
- AWS コンプライアンスのリソース - このワークブックおよびガイドのコレクションは、ユーザーの業界や地域で使用できる場合があります。
- 『AWS Config デベロッパーガイド』の「Evaluating resources with rules」- AWS Config サービスは、リソース設定が社内の慣行、業界のガイドライン、および規制にどの程度準拠しているかを評価します。
- AWS Security Hub: この AWS のサービスでは、AWS 内のセキュリティ状態を包括的に表示しており、セキュリティ業界の標準およびベストプラクティスへの準拠を確認するのに役立ちます。

での耐障害性AWSStorage Gateway

AWSのグローバルインフラストラクチャはAWSリージョンとアベイラビリティーゾーンを中心に構築されます。AWSリージョンには、低レイテンシー、高いスループット、そして高度の冗長ネット

ワークで接続されている複数の物理的に独立・隔離されたアベイラビリティーゾーンがあります。アベイラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、耐障害性、および拡張性が優れています。

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

に加えて、AWSグローバルインフラストラクチャでは、Storage Gateway は、データの耐障害性とバックアップのニーズに対応できるように複数の機能を提供しています。

- VMware vSphere 高可用性 (VMware HA) を使用して、ハードウェア、ハイパーバイザー、またはネットワーク障害からストレージワークロードを保護します。詳細については、「」を参照してください。Storage Gateway での VMware vSphere High Availabil。
- AWS Backup を使用してボリュームをバックアップします。詳細については、「」を参照してください。を使用するAWS Backupボリュームをバックアップするには。
- 復旧ポイントからボリュームのクローンを作成します。詳細については、「」を参照してください。ボリュームのクローンを作成する。
- Amazon S3 Glacier で仮想テープをアーカイブします。詳細については、「」を参照してください。仮想テープのアーカイブ。

でのインフラストラクチャセキュリティAWSStorage Gateway

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

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

また、リクエストは、アクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token Service (AWS STS) を使用して、テンポラリ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。

Storage Gateway のセキュリティベストプラクティス

AWSStorage Gateway 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る必要のあるいくつかのセキュリティ機能が用意されています。以下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に相当するものではありません。これらのベストプラクティスはお客様の環境に適切ではないか、十分ではない場合があるため、これらは処方箋ではなく、有用な考慮事項と見なしてください。詳細については、「」を参照してください。AWSセキュリティのベストプラクティス。

ゲートウェイのトラブルシューティング

次に、ゲートウェイ、ファイル共有、ボリューム、仮想テープ、およびスナップショットに関連する問題のトラブルシューティングについて説明します。オンプレミスのゲートウェイのトラブルシューティング情報では、VMware ESXi および Microsoft Hyper-V クライアントの両方にデプロイされているゲートウェイを扱います。ファイル共有のトラブルシューティング情報は、Amazon S3 ファイルゲートウェイタイプに適用されます。ボリュームのトラブルシューティング情報は、ボリュームゲートウェイタイプに適用されます。テープのトラブルシューティング情報は、Tape Gateway タイプに適用されます。ゲートウェイの問題のトラブルシューティング情報は CloudWatch メトリクスの使用に適用されます。高可用性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ているゲートウェイが含まれます。

トピック

オンプレミスのゲートウェイの問題のトラブルシューティング

オンプレミスのゲートウェイを使用しているときに遭遇する可能性がある典型的な問題と、有効にする方法について、以下の情報を取扱います。AWS Supportゲートウェイのトラブルシューティングに役立ちます。

次の表は、オンプレミスのゲートウェイを使用しているときに遭遇する可能性がある典型的な問題を一覧にしたものです。

問題	実行するアクション
ゲートウェイの IP アドレスが見つかりません。	ハイパーバイザークライアントを使用してホストに接続し、ゲートウェイの IP アドレスを見つけます。

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 [Summary] 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 • 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、へのアウトバウンド通信でこれらのサービスエンドポイントを許可するように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。AWS。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
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。アクティベーションに進みます[Storage Gateway 管理コンソール] の [] ボタンをクリックします。	• 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、「ゲートウェイエンドポイントへの FSx ファイルゲートウェイゲートウェイ接続のテスト」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ることと、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の時間の同期に関する詳細については、ゲートウェイのネットワークタイムプロトコル (NTP) サーバーの構成 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。 • VM の RAM が 7.5 GB 以上であることを確認します。RAM が 7.5 GB 未満の場合、ゲートウェイの割り当てが失敗します。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。
アップロードバッファ領域として割り当てられているディスクを削除する必要があります。たとえば、ゲートウェイのアップロードバッファ領域の量を減らしたり、エラーが発生したアップロードバッファとして使用されているディスクを置き換えたりする必要が生じる場合があります。	

問題	実行するアクション
ゲートウェイとゲートウェイの間の帯域幅を改善する必要がありますAWS。	アプリケーションとゲートウェイ VM の間の接続とは別に、ネットワークアダプタ (NIC) で AWS へのインターネット接続を設定することで、ゲートウェイから AWS への帯域幅を改善できます。この方法は、高帯域で AWS に接続しているときに帯域幅の競合を回避する場合に便利です (特にスナップショット復旧時)。高スループットのワークロードのニーズについては、AWS Direct Connectオンプレミスのゲートウェイとの間に専用ネットワーク接続を確立するにはAWS。ゲートウェイから AWS への接続の帯域幅を計測するには、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」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。	• リポジトリの []ゲートウェイ[Storage Gateway] コンソールの [] タブで、ゲートウェイ仮想マシンの 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 マネージャ) 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。同じではない場合、「」の図のようにStorage Gateway コンソールを再起動します。ゲートウェイ VM のシャットダウン。再起動後、IP アドレスStorage Gateway コンソールのリストゲートウェイタブは、ハイパーバイザークライアントから決定するゲートウェイの IP アドレスと一致する必要があります。
	  • VMware ESXi の場合、VM の IP アドレスは vSphere クライアントの [Summary] 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.
	• 「ゲートウェイエンドポイントへの FSx ファイルゲートウェイゲートウェイ接続のテスト」で説明されているように、ゲートウェイと AWS の接続を確認します。
	• ゲートウェイのネットワークアダプタ設定を確認し、ゲートウェイに対して有効にする予定のすべてのインターフェイスが有効になっていることを確認します。ゲートウェイのネットワークアダプタ設定を表示するには、「ゲートウェイのネットワークアダプタの設定」の指示に従い、ゲートウェイのネットワーク設定を表示するためのオプションを選択します。
	
	ゲートウェイと AWS の間のスループットは、Amazon CloudWatch コンソールから表示できます。ゲートウェイと AWS の間のスループットを計測する方法については、「パフォーマンス」を参照してください。

Microsoft Hyper-V に Storage Gateway をインポート (デプロイ) できません。	「Microsoft Hyper-V セットアップのトラブルシューティング」を参照してください。ここでは、Microsoft Hyper-V でゲートウェイをデプロイするための一般的な問題を説明しています。

問題	実行するアクション
次のようなメッセージが届きます。「ゲートウェイのボリュームに書き込まれたデータが、AWS「。	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、お問い合わせください。AWS Support。

の有効化AWS Supportオンプレミスでホストされているゲートウェイのトラブルシューティングに役立つ

Storage Gateway には、複数のメンテナンスタスクの実行に使用するローカルコンソールが用意されています。これらのタスクには、AWS Supportゲートウェイの問題のトラブルシューティングに利用するためにゲートウェイにアクセスしてください。デフォルトでは、次のようになります。AWS Supportゲートウェイへのアクセスは無効化されています。このアクセスは、ホストのローカルコンソールを通して有効にします。与えるにはAWS Supportゲートウェイにアクセスする場合は、最初にホストのローカルコンソールにログインし、ストレージゲートウェイのコンソールに移動してから、サポートサーバーに接続します。

を有効化するにはAWS Supportゲートウェイへのアクセス

1. ホストのローカルコンソールにログインします。

   - VMware ESXi — 詳細については、「」を参照してください。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 — 詳細については、「」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。

   ローカルコンソールは次のようになっています。

2. のプロンプトに従って、「」と入力します。**5**をクリックして、[] を開きます。AWS Support チャンネルコンソール。
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. 以下の いずれかを 実行します。

   - 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、使用できるコマンドウィンドウで、次のように入力します。**`open-support-channel`**をクリックして、Storage

Gateway のカスタマーサポートに接続します。TCP ポート 22 を許可して、次のサポートチャネルを開くことができます。AWS。カスタマーサポートに接続する際、Storage Gateway はサポート番号を割り当てます。サポート番号を書き留めます。

- ゲートウェイが VPC エンドポイントを使用している場合は、[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ブ化されていない場合は、VPC エンドポイントまたは IP アドレスを指定して、Storage Gateway のカスタマーサポートに接続します。TCP ポート 22 を許可して、次のサポートチャネルを開くことができます。AWS。カスタマーサポートに接続する際、Storage Gateway はサポート番号を割り当てます。サポート番号を書き留めます。

> **Note**
>
> チャネル番号は 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、次の場所にサポートサービス番号を指定します。AWS SupportそうAWS Supportは、トラブルシューティング支援を提供できます。
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。Support セッションが完了したことをAmazon Web Services サポートから通知するまで、セッションを閉じないでください。
7. Enter**`exit`**をクリックして、Storage Gateway コンソールをログアウトします。
8. プロンプトに従ってローカルコンソールを終了します。

Microsoft Hyper-V セットアップのトラブルシューティング

次の表は、Microsoft Storage Gateway にストレージゲートウェイ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	このエラーは、次の原因で発生することがあります。

問題	実行するアクション
れます。「インポートに失敗しました。場所 ... では、仮想マシンのインポートファイルが見つかりません。」というエラーメッセージが表示されます。	• 解凍されていないゲートウェイソースファイルのルートをポイントしている場合。[Import Virtual Machine] ダイアログボックスで指定した場所の最後のパートは、次の例が示すように、`AWS-Storage-Gateway` となっている必要があります。 • ゲートウェイをすでにデプロイしていて、仮想マシンをコピーします。オプションを選択し、すべてのファイルを複製するオプションの仮想マシンのインポートダイアログボックスが表示されたら、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、この場所から再度インポートすることはできません。この問題を解決するには、未解凍のゲートウェイソースファイルの最新コピーを入手して、新しい場所にコピーします。インポートのソースとして新しい場所を使用します。次の例は、未解凍ソースファイルが置かれている 1 つの場所から複数のゲートウェイを作成する場合にオンにすべきオプションを示しています。
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。「インポートに失敗しました。ファイルをコピーできませんでした。」というエラーメッセージが表示されます。	既にゲートウェイをデプロイしていて、仮想ハードディスクファイルと仮想マシン構成ファイルを保存するデフォルトのフォルダを再利用しようとすると、このエラーが発生します。この問題を解決するには、[Hyper-V Settings] ダイアログボックスで新しい場所を指定します。

問題	実行するアクション
ゲートウェイをインポートしようとすると、次のエラーメッセージが表示されます。「インポートに失敗しました。仮想マシンに新しい識別子が必要です。新しい識別子を選択して、インポートを再試行してください。」というエラーメッセージが表示されます。	ゲートウェイをインポートするときは、仮想マシンをコピーします。オプションを選択し、すべてのファイルを複製するオプションの仮想マシンのインポートダイアログボックスを使用して、仮想マシンの新しい一意の ID を作成します。次の例は、使用する必要がある [Import Virtual Machine] ダイアログボックスのオプションを示しています。
ゲートウェイ VM を起動しようとすると、「子パーティションのプロセッサの設定が親パーティションと互換性がありません。」というエラーメッセージが表示されます。	このエラーは通常、ゲートウェイで必要とされる CPU と、ホストで使用可能な CPU の不一致が原因で発生します。VM の CPU 数が、基本ハイパーバイザーでサポートされていることを確認します。 Storage Gateway の要件の詳細については、「」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。
ゲートウェイ VM を起動しようとすると、「パーティションを作成できませんでした。要求されたサービスを完了するためのリソースが不足しています。」	このエラーは通常、ゲートウェイで必要とされる RAM と、ホストで使用可能な RAM の不一致が原因で発生します。 Storage Gateway の要件の詳細については、「」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。
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、「ゲートウェイのネットワークタイムプロトコル (NTP) サーバーの構成」を参照してください。

問題	実行するアクション
解凍された 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。

Amazon EC2 ゲートウェイ問題のトラブルシューティング

以下のセクションでは、Amazon 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遭遇する可能性がある典型的な問題を取扱います。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、を参照してください。Amazon EC2 ホストへのファイルゲートウェイのデプロイ。

トピック

- ゲートウェイのアクティベーションがしばらくしても発生しない
- インスタンスリストに EC2 ゲートウェイインスタンスが見つかりません
- 君が欲しいAWS SupportEC2 ゲートウェイのトラブルシューティングに役立つ

ゲートウェイのアクティベーションがしばらくしても発生しない

Amazon EC2 コンソールで以下を確認します。

- インスタンスに関連付けられているセキュリティグループでポート 80 が有効になっています。セキュリティグループルールの追加の詳細については、「」を参照してください。セキュリティグループルールを追加するのLinux インスタンス用 Amazon EC2 ユーザーガイド。
- 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、状態インスタンスの値が 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「」で説明する最低要件を満たしているを確認します。ストレージの要件。

問題を修正したら、ゲートウェイを再度アクティブ化してみてください。これを行うには、Storage Gateway コンソールを開き、Amazon EC2 に新しいゲートウェイをデプロイするをクリックし、インスタンスの IP アドレスを再入力します。

インスタンスリストに EC2 ゲートウェイインスタンスが見つかりません

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 [Description (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、「」というテキストで始まります。**`aws-storage-gateway-ami`**。
- 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。

君が欲しいAWS SupportEC2 ゲートウェイのトラブルシューティングに役立つ

Storage Gateway には、複数のメンテナンスタスクの実行に使用するローカルコンソールが用意されています。これらのタスクには、AWS Supportゲートウェイの問題のトラブルシューティングに利用するためにゲートウェイにアクセスしてください。デフォルトでは、次のようになります。AWS Supportゲートウェイへのアクセスは無効化されています。このアクセスは Amazon EC2 ローカルコンソールを通じて有効にします。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の詳細と、セキュリティグループルールの追加方法については、「」を参照してください。Amazon EC2 セキュリティグループのAmazon EC2 ユーザーガイド。

できるようにするにはAWS Supportゲートウェイに接続し、最初に Amazon EC2 インスタンスのローカルコンソールにログインし、ストレージゲートウェイのコンソールに移動してから、アクセス許可を付与します。

を有効化するにはAWS SupportAmazon EC2 インスタンスにデプロイされているゲートウェイへのアクセス

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。方法については、「」を参照してください。インスタンスへの接続のAmazon EC2 ユーザーガイド。

   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**
   >
   > *-########*ですか .pemファイル。このファイルは、Amazon EC2 インスタンスを起動するために使用した EC2 key pair プライベート証明書を含みます。詳細については、「」を参照してください。キーペアのパブリックキーを取得するのAmazon EC2 ユーザーガイド。
   >
   > *-######-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、説明タブ。

2. のプロンプトに従って、「」と入力します。**6 - Command Prompt**をクリックして、[] を開きます。AWS Supportチャンネルコンソール。
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. 以下の いずれかを 実行します。

   - 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、使用できるコマンドウィンドウで、次のように入力します。**open-support-channel**をクリックして、Storage Gateway のカスタマーサポートに接続します。TCP ポート 22 を許可して、次のサポートチャネルを開くことができます。AWS。カスタマーサポートに接続する際、Storage Gateway はサポート番号を割り当てます。サポート番号を書き留めます。
   - ゲートウェイが VPC エンドポイントを使用している場合は、[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ブ化されていない場合は、VPC エンドポイントまたは IP アドレスを指定し

て、Storage Gateway のカスタマーサポートに接続します。TCP ポート 22 を許可して、次のサポートチャネルを開くことができます。AWS。カスタマーサポートに接続する際、Storage Gateway はサポート番号を割り当てます。サポート番号を書き留めます。

> **Note**
>
> チャネル番号は 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、次の場所にサポートサービス番号を指定します。AWS SupportそうAWS Supportは、トラブルシューティング支援を提供できます。
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。Support セッションが完了したことをAmazon Web Services サポートから通知するまで、セッションを閉じないでください。
7. Enter**exit**をクリックして、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。

ハードウェアアプライアンスの問題をトラブルシューティングする

以下のトピックでは、Storage Gateway ハードウェアアプライアンスで発生する可能性がある問題と、そのトラブルシューティング対策を示します。

サービスの IP アドレスを特定できない

サービスに接続するときは、ホストの IP アドレスではなく、サービスの IP アドレスを使用していることを確認します。サービスのコンソールでサービスの IP アドレスを設定し、ハードウェアコンソールでホストの IP アドレスを設定します。ハードウェアコンソールは、ハードウェアアプライアンスを起動すると表示されます。ハードウェアコンソールからサービスコンソールにアクセスするには、[Open Service Console (サービスコンソールを開く)] を選択します。

工場出荷時リセットはどのように実行しますか？

アプライアンスでファクトリのリセットを実行する必要がある場合は、Support セクションの説明に従って、Storage Gateway ハードウェアアプライアンスのチームにお問い合わせください。

Dell iDRAC サポートはどこで入手できますか。

Dell PowerEdge R640 サーバーには、Dell iDRAC 管理インターフェイスが搭載されています。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 の認証情報の詳細については、「」を参照してください。Dell PowerEdge-iDRAC デフォルトのユーザー名とパスワードは何ですか?。
- 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りません

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、ハードウェアページを Storage Gateway コンソールに表示します。

ハードウェアアプライアンスのサポートを受ける場所

Storage Gateway ハードウェアアプライアンスのサポートに連絡するには、を参照してください。AWS Support。

-AWS Support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には、サポートチャネルをアクティブ化する必要があることがあります。このポートは、ゲートウェイの通常のオペレーションでは開いておく必要はありませんが、トラブルシューティングでは必要です。以下の手順に示すように、ハードウェアコンソールからサポートチャネルをアクティブ化することができます。

のサポートチャンネルを開くにはAWS

1. ハードウェアコンソールを開きます。
2. 次に示すように、[Open Support Channel (サポートチャネルを開く)] を選択します。

   ネットワーク接続やファイアウォールに問題がなければ、割り当てられたポート番号が 30 秒以内に表示されます。
3. ポート番号を記録して、AWS Support。

ファイルゲートウェイ問題のトラブルシューティング

ファイルゲートウェイを VMware vSphere High Availability (HA) を実行するときに、Amazon CloudWatch ロググループを設定できます。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、ファイル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。これらのエラー通知とヘルス通知については、CloudWatch Logs で確認できます。

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: ObjectMissing

おれは手に入れることができる`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 Amazon FSX から削除すると、エラーが発生します。以降、Amazon FSx へのオブジェクトのアップロードまたは Amazon FSx からのオブジェクトの取得は失敗します。

ObjectMissing エラーを解決するには

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

Notification 再起動

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。メンテナンス期間外に著しく再起動が発生した場合は、ゲートウェイを手動で再起動したかどうかを確認します。

Notification 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 アプリケーションのモニタリングによるリセットにより、このイベントがトリガーされることがあります。

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。

Notification 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。

`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、AWS Support。

Notification AvailabilityMonitorTest

あなたが手に入れるAvailabilityMonitorTestあなたがいるときに通知するテストを実行するの可用性とアプリケーションの監視VMware vSphere HA プラットフォームで実行されているゲートウェイ上のシステム。

エラー: RoleTrustRelationshipInvalid

このエラーは、ファイル共有の IAM ロールで IAM 信頼関係が正しく設定されていない (つまり、IAM ロールが、という名前のStorage Gateway プリンシパルを信頼していない) 場合に発生します。storagegateway.amazonaws.com). その結果、ファイルゲートウェイは、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

- IAM コンソールまたは IAM API を使用して含めます。storagegateway.amazonaws.comファイル共有の iamRole によって信頼されているプリンシパルとして指定します。IAM ロールの詳細については、「」を参照してください。チュートリアル:アクセス権の委任AWSIAM ロールを使用するアカウント。

CloudWatch メトリクスを使用したトラブルシューティング

以下では、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説明します。

トピック

- ディレクトリを参照すると、ゲートウェイの反応が遅くなります。
- ゲートウェイが応答しない
- Amazon FSx ファイルシステムにはファイルが表示されない
- ゲートウェイで Amazon FSx へのデータ転送が遅いです
- 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

ディレクトリを参照すると、ゲートウェイの反応が遅くなります。

ファイルゲートウェイの実行時に反応が遅い場合はlsコマンドまたはディレクトリを参照する場合は、IndexFetchそしてIndexEvictionCloudWatch メトリクス:

- そのファイルにIndexFetch実行すると、メトリックが 0 より大きくなります。lsコマンドまたはディレクトリの閲覧を行うと、影響を受けるディレクトリのコンテンツに関する情報なしでファイルゲートウェイが起動し、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。
- そのファイルにIndexEvictionメトリクスが 0 より大きい場合、ファイルゲートウェイがその時点でキャッシュで管理できる制限に達したことを意味します。この場合、ファイルゲートウェイは、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。これが頻繁に発生し、パフォーマンスに影響がある場合は、AWS Support。

  ディスカッション方法AWS Support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に、関連する Amazon FSX ファイルシステムのコンテンツと推奨事項。

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は RAM にインデックスキャッシュを再構築するため、低速のルートディスクが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。
- そのファイルにMemUsedBytesメトリックは、MemTotalBytesメトリクスを指定すると、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ます。すでにある場合は、ワークロードとユースケースに基づいて、さらに RAM をファイルゲートウェイに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は、ファイルゲートウェイへの RAM の追加が必要になることがあります。

Amazon FSx ファイルシステムにはファイルが表示されない

ゲートウェイ上のファイルが Amazon FSx ファイルシステムに反映されないことに気付いた場合は、FilesFailingUploadのメトリクス. メトリックで一部のファイルがアップロードに失敗していると報告された場合は、ヘルス通知を確認してください。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含むヘルス通知を生成します。

ゲートウェイで Amazon FSx へのデータ転送が遅いです

ファイルゲートウェイで Amazon S3 へのデータ転送が遅い場合は、次の操作を行います。

- そのファイルにCachePercentDirtyメトリクスが 80 以上の場合、ファイルゲートウェイは、データを Amazon S3 にアップロードするよりも高速にデータをディスクに書き込んでいます。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。
- そのファイルにCachePercentDirtyメトリクスが低い場合は、IoWaitPercentのメトリクス. もしIoWaitPercentが 10 より大きい場合、ファイルゲートウェイでローカルキャッシュディスクの速度がボトルネックになっている可能性があります。キャッシュには、ローカルソリッドステートドライブ (SSD) ディスク (できれば NVM Express (NVMe)) をお勧めします。このようなディスクが使用できない場合は、パフォーマンスを向上させるために、別々の物理ディスクから複数のキャッシュディスクを使用してみてください。

ゲートウェイ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

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

- そのファイルに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が Amazon FSx または Amazon S3 にアップロードされている速度を確認するには、CloudBytesUploadedのメトリクス. そのメトリックをWriteBytesメトリクス。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度を示します。ファイルゲートウェイが Amazon FSx または Amazon S3 にアップロードできる速度よりも高速に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も、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がクライアント側のセッションタイムアウトに達している可

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。

高可用性のヘルス通知

VMware vSphere High Availability (HA) プラットフォームでゲートウェイを実行すると、ヘルス通知が表示される場合があります。ヘルス通知の詳細については、「高可用性問題のトラブルシューティング」を参照してください。

高可用性問題のトラブルシューティング

可用性の問題が発生した場合の対処方法については、以下を参照してください。

トピック

- Health 通知
- メトリクス

Health 通知

VMware vSphere HA でゲートウェイを実行すると、すべてのゲートウェイが、設定済みの Amazon CloudWatch ロググループに対して次のヘルス通知を生成します。これらの通知は、`AvailabilityMonitor` と呼ばれるログストリームに入ります。

トピック

- Notification 再起動
- Notification HardReboot
- Notification HealthCheckFailure
- Notification AvailabilityMonitorTest

Notification 再起動

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 ハイパーバイザー管理コンソールまたは Storage Gateway コンソールを使用して、ゲートウェイ VM を再起動できます。また、ゲートウェイのメンテナンスサイクル中にゲートウェイソフトウェアを使用して再起動することもできます。

実行するアクション

再起動の時間がゲートウェイで設定されたメンテナンス開始時間から 10 分以内である場合、これは通常の発生であり、問題の兆候ではありません。メンテナンス期間外に著しく再起動が発生した場合は、ゲートウェイを手動で再起動したかどうかを確認します。

Notification 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 アプリケーションのモニタリングによるリセットにより、このイベントがトリガーされることがあります。

実行するアクション

ゲートウェイがこのような環境で実行されている場合は、HealthCheckFailure 通知の有無を確認し、VM の VMware イベントログを調べます。

Notification 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、AWS Support。

Notification AvailabilityMonitorTest

VMware vSphere HA のゲートウェイでは、AvailabilityMonitorTestあなたがいるときに通知するテストを実行するの可用性とアプリケーションの監視VMware のシステム。

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、設定されている CloudWatch ロググループに問い合わせてください。

データをリカバリするためのベストプラクティス

まれに、ゲートウェイで回復不可能な障害が発生する場合があります。そのような障害は、仮想マシン (VM)、ゲートウェイ自体、ローカルストレージなどの場所で発生する可能性があります。障害が発生した場合、データの回復に関する以下の該当するセクションの手順に従うことをお勧めします。

> **Important**
>
> Storage Gateway では、ハイパーバイザーによって作成されたスナップショット、または Amazon EC2 Amazon マシンイメージ (AMI) からのゲートウェイ VM の復元はサポートされていません。ゲートウェイ VM が正しく機能しない場合、新しいゲートウェイをアクティブ化し、以下の手順を使用してデータをそのゲートウェイに復旧します。

トピック

- 予期しない仮想マシンのシャットダウンからのリカバリ
- 誤動作しているキャッシュディスクからデータを復元する
- アクセス無効なデータセンターからデータを復旧する

予期しない仮想マシンのシャットダウンからのリカバリ

VM が予期せずにシャットダウンした場合 (停電時など)、ゲートウェイは到達不可能になります。電源とネットワーク接続が復旧されると、ゲートウェイは到達可能になり、通常の動作を開始します。データを回復するためにその時点で実行可能ないくつかのステップを以下に示します。

- 停止によりネットワーク接続の問題が発生した場合、問題をトラブルシューティングできます。ネットワーク接続をテストする方法については、「ゲートウェイエンドポイントへの FSx ファイルゲートウェイゲートウェイ接続のテスト」を参照してください。
- ゲートウェイが正しく機能せず、予期しないシャットダウンの結果としてボリュームまたはテープに問題が発生した場合、データを回復できます。データの復旧方法については、シナリオに当てはまる以下のクションを参照してください。

誤動作しているキャッシュディスクからデータを復元する

キャッシュディスクで障害が発生した場合、以下のステップを使用し、状況に応じてデータを復旧することをお勧めします。

- キャッシュディスクがホストから削除されたために障害が発生した場合は、ゲートウェイをシャットダウンし、ディスクを再追加してゲートウェイを再起動します。
- キャッシュディスクが破損したかアクセスできない場合、ゲートウェイをシャットダウンしてキャッシュディスクをリセットし、キャッシュストレージ用にディスクを再設定してゲートウェイを再起動します。

詳細については、「誤動作しているキャッシュディスクからデータを復元する」を参照してください。

アクセス無効なデータセンターからデータを復旧する

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、別のデータセンターのゲートウェイにデータを復元するか、Amazon EC2 インスタンスにホストされているゲートウェイに復元することができます。別のデータセンターへのアクセス権がない場合は、Amazon EC2 インスタンスにゲートウェイを作成することをお勧めします。手順は、データ復旧元のゲートウェイの種類によって異なります。

アクセス無効なデータセンターの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で、復旧するデータを含む Amazon S3 バケットに新しいファイル共有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有効化します。詳細については、「Amazon EC2 ホストへのファイルゲートウェイのデプロイ」を参照してください。
2. 作成した EC2 ゲートウェイに新しいファイル共有を作成します。詳細については、「」を参照してください。ファイル共有の作成。
3. ファイル共有をクライアントにマウントし、復旧するデータを含む S3 バケットにマッピングします。詳細については、「」を参照してください。ファイル共有をマウントして使用する。

Storage Gateway に関するその他のリソース

このセクションでは、についての情報を説明します。AWSと、ゲートウェイをセットアップまたは管理するために役立つサードパーティーのソフトウェア、ツール、リソースに加え、Storage Gateway のクォータについても説明します。

トピック

ホストセットアップ

トピック

Storage Gateway 用の VMware の設定

Storage Gateway の VMware を設定する際、VM タイムとホストタイムを同期し、ストレージのプロビジョニングで準仮想化ディスクを使用するように VM を設定し、ゲートウェイ VM をサポートするインフラストラクチャレイヤーにおける障害からの保護を提供することを確認します。

トピック

VM の時刻とホストの時刻の同期

ゲートウェイを正常にアクティブ化するには、VM の時刻をホストの時刻と同期し、ホストの時刻を正しく設定する必要があります。このセクションでは、最初に VM の時刻をホストの時刻に同期します。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 クライアントでゲートウェイ VM のコンテキスト (右クリック) メニューを開き、[Edit Settings] を選択します。

      [Virtual Machine Properties] ダイアログボックスが開きます。

   b. [Options] タブを選択し、オプションリストで [VMware Tools] を選択します。
   c. [Synchronize guest time with host] オプションをチェックして、[OK] を選択します。

      VM の時刻がホストと同期されます。

2. ホストの時刻を構成します。

   ホストの時計が正しい時刻に設定されてかを確認するのは重要です。ホスト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、左側のペインの vSphere ホストノードを選択し、[Configuration] タブを選択します。
   b. Select時刻設定のソフトウェア] パネルを選択し、プロパティ[] リンク。

      [Time Configuration] ダイアログボックスが表示されます。

c. [Date and Time] パネルで、日付と時刻を設定します。

d. 時刻を NTP サーバーに自動的に同期するように、ホストを設定します。

   i. 選択Optionsの時刻設定ダイアログボックスを開き、NTP Daemon (ntpd) Options] ダイアログボックスで、[] を選択します。NTP 設定[] 左ペインの [] をクリックします。

   ii. [Add] を選択して、新しい NTP サーバーを追加します。

   iii. [Add NTP Server] 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。

   次の例のように、`pool.ntp.org` を使用することができます。

   iv. [NTP Daemon (ntpd) Options] ダイアログボックスで、左側のペインの [General] を選択します。

   v. [Service Commands] ペインで、[Start] を選択してサービスを開始します。

   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 Daemon (ntpd) Options] ダイアログボックスを閉じます。

f. [OK] を選択して [Time Configuration] ダイアログボックスを閉じます。

VMware HA を使用したStorage Gateway の使用

VMware High Availability (HA) は、ゲートウェイ VM をサポートしているインフラストラクチャレイヤーの障害から保護するための vSphere コンポーネントです。そのため、VMware HA は複数のホストをクラスターとして設定し、ゲートウェイ VM を実行しているホストが失敗すると、クラスター内の別のホストでゲートウェイ VM が自動的に再開されます。VMware HA の詳細については、「」を参照してください。VMware HA: コンセプトとベストプラクティスVMware のウェブサイトを参照してください。

VMware HA でStorage Gateway を使用するには、次の操作を実行することをお勧めします。

- VMware ESX をデプロイする .ovaクラスター内の 1 つのホストだけに Storage Gateway VM が含まれている、ダウンロード可能なパッケージ。
- .ova パッケージをデプロイする場合は、1 つのホストだけにローカルではないデータストアを選択してください。代わりに、クラスターのすべてのホストにアクセスできるデータストアを使用します。1 つのホストだけにローカルなデータストアを選択し、そのホストに障害が発生した場合、データソースはクラスター内の他のホストからアクセスできない可能性があります。また、他のホストへのフェイルオーバーが成功しない可能性があります。
- クラスタリングを利用して .ova パッケージをクラスターにデプロイした場合、プロンプトが表示されたら、ホストを選択します。その他の方法として、クラスター内のホストに直接デプロイすることもできます。

ゲートウェイ VM の時刻の同期

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 の時刻とホストの時刻の同期」を参照してください。Microsoft Hyper-V にデプロイされたゲートウェイの場合は、次の手順を使用して定期的に VM の時刻を確認する必要があります。

ハイパーバイザーゲートウェイ VM の時刻を表示して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。

   - 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 カーネルベースの仮想マシン (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. リポジトリの []Storage Gateway 設定メインメニュー、**4**にとってシステム時刻管理。

3. リポジトリの []システム時刻管理メニューの「」と入力します。**1**にとってシステム時刻の表示と同期。

4. VM の時刻と NTP の時刻を同期させる必要があるという結果が示された場合は、「**y**」と入力します。それ以外の場合は、「**n**」と入力します。

   同期するために「**y**」と入力した後で、同期にしばらく時間がかかることがあります。

   次のスクリーンショットでは、時刻の同期が必要ない VM を示します。

   次のスクリーンショットでは、時刻の同期が必要な VM を示します。

Amazon EC2 ホストへのファイルゲートウェイのデプロイ

ファイルゲートウェイは、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにデプロイしてアクティベーションできます。ファイルゲートウェイ 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。

Amazon EC2 インスタンスにゲートウェイをデプロイする

1. [ホストプラットフォームの選択] ページで、[Amazon EC2] を選択します。
2. [インスタンスの起動] を選択して、ストレージゲートウェイ EC2 AMI を起動します。インスタンスタイプを選択できる Amazon EC2 コンソールにリダイレクトされます。
3. リポジトリの []ステップ 2: インスタンスタイプの選択ページで、インスタンスのハードウェア構成を選択します。Storage Gateway は、特定の最小要件を満たしているインスタンスタイプでサポートされます。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る、m4.xlarge インスタンスタイプから始めることをお勧めします。詳細については、「オンプレミス VM のハードウェア要件」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、「」を参照してください。インスタンスのサイズ変更のLinux インスタンス用 Amazon EC2 ユーザーガイド。

   > **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。のモニタリングCachePercentDirtyAmazon CloudWatch メトリクスを設定し、パラメータがの場合に限り、システムを開始または停止してください。0。ゲートウェイのメトリクスのモニタリングの詳細については、「」を参照してください。Storage Gatewayのメトリクスおよびディメンションを参照してくださいCloudWatch のドキュメント。Amazon EC2 インスタンスタイプの要件の詳細については、「」を参照してください。the section called “Amazon EC2 インスタンスタイプの要件”。

4. [Next: (次へ:)] を選択します インスタンスの詳細の設定。
5. リポジトリの []ステップ 3: インスタンスの詳細の設定[] ページで、[] の値を選択します。パブリックIPの自動割り当て。インスタンスをパブリックインターネットからアクセス可能にする場合は、[自動割り当てパブリック IP] が [有効化] に設定されていることを確認します。インターネットからインスタンスにアクセス可能にしない場合は、[自動割り当てパブリック IP] で [無効化] を選択します。
6. を使用する場合IAM ロールで、AWS Identity and Access Managementゲートウェイに使用する (IAM) ロール。
7. [Next: (次へ:)] を選択します ストレージの追加。
8. リポジトリの []ステップ 4: ストレージの追加[] ページで、新しいボリュームを追加をクリックして、ファイルゲートウェイインスタンスにストレージを追加します。キャッシュストレージ用に設定するには、少なくとも 1 つの Amazon EBS ボリュームが必要です。

   推奨ディスクサイズ: キャッシュ (最小) 150 GiB とキャッシュ (最大) 64 TiB
9. リポジトリの []ステップ 5: タグの追加ページで、オプションのタグをインスタンスに追加できます。続いて、[次へ] を選択します。セキュリティグループの設定。
10. リポジトリの []ステップ 6: セキュリティグループの設定ページで、インスタンスに到達するための特定のトラフィックにファイアウォールのルールを追加します。新しいセキュリティグループを作成することも、既存のセキュリティグループを選択することもできます。

    > **Important**
    >
    > Storage Gateway のアクティベーションと Secure Shell (SSH) のアクセスポートに加えて、NFS クライアントに追加のポートへのアクセスが必要です。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。
11. [確認と作成] を選択して設定を確認します。
12. リポジトリの []ステップ 7: インスタンス作成の確認[] ページで、を起動する。

13. [Select an existing key pair or create a new key pair] ダイアログボックスで、[既存のキーペアの選択] を選択し、セットアップ時に作成したキーペアを選択します。準備ができたら、確認ボックスを選択してから、[インスタンスの作成] を選択します。

    確認ページに、インスタンスが起動中であることが示されます。

14. [View Instances] を選択して確認ページを閉じ、コンソールに戻ります。[Instances] 画面でインスタンスのステータスを表示できます。インスタンスはすぐに起動します。インスタンスを起動した直後のステータスは [pending (保留中)] です。インスタンスが開始されると、ステータスは running に変わり、インスタンスはパブリック DNS 名を取得します

15. インスタンスを選択し、にパブリック IP アドレスを書き留めます。説明タグを付けて、に接続します。AWS[Storage Gateway] コンソールで、ゲートウェイの設定を続行します。

Storage Gateway ゲートウェイコンソールを使用するか、にクエリを実行して、ファイルゲートウェイの起動に使用する AMI ID を確認できます。AWS Systems Managerパラメータストア。

AMI ID を確認するには

1. にサインインします。AWS Management Consoleで、Storage Gateway コンソールを開きます。https://console.aws.amazon.com/storagegateway/home。
2. [ゲートウェイの作成]、[ファイルゲートウェイ] の順に選択してから、[次へ] をクリックします。
3. [Choose host platform] ページで、[Amazon EC2] を選択します。
4. 選択インスタンスを起動するをクリックして、Storage Gateway EC2 AMI を起動します。EC2 コミュニティ AMI ページにリダイレクトされ、の AMI ID が表示されます。AWSURL 内のリージョン。

   または、Systems Manager パラメータストアにクエリを実行することもできます。♪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を実行します。`/aws/service/storagegateway/ami/FILE_S3/latest`。たとえば、以下の CLI コマンドを使用すると、現在の AMI の ID が返されます。AWSリージョン。

   ```
   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_FSX/latest",
        "Name": "/aws/service/storagegateway/ami/FILE_S3/latest",
        "Value": "ami-123c45dd67d891000"
    }
}
```

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取得するには、ゲートウェイ VM にウェブリクエストを行います。アクティベーションキーが格納されているリダイレクトが返されます。このアクティベーションキーは、ActivateGateway API アクションにパラメータの 1 つとしてが渡され、ゲートウェイの設定を指定します。詳細については、「」を参照してください。ActivateGatewayのStorage Gateway API のリファレンス。

ゲートウェイ VM へのリクエストには、AWSアクティベーションが発生するリージョン。応答のリダイレクトで返される URL には、activationkey と呼ばれるクエリ文字列パラメータが含まれています。このクエリ文字列パラメータが、アクティベーションキーです。クエリ文字列の形式は次のようになります。 http://*gateway_ip_address*/?activationRegion=*activation_region*。

トピック

- AWS CLI
- Linux (bash/zsh)
- Microsoft Windows PowerShell

AWS CLI

まだ AWS CLI をインストールして設定していない場合は、インストールして設定する必要があります。これを行うには、AWS Command Line Interface のユーザーガイドの手順に従います。

- インストール:AWS Command Line Interface
- 設定:AWS Command Line Interface

次の例は、を使用する方法を示しています。AWS CLIHTTP レスポンスをフェッチするには、HTTP ヘッダーを解析してアクティベーションキーを取得します。

```
wget 'ec2_instance_ip_address/?activationRegion=eu-west-2' 2>&1 | \
grep -i location | \
grep -i key | \
cut -d'=' -f2 |\
cut -d'&' -f1
```

Linux (bash/zsh)

次の例では、Linux (bash/zsh) を使用して HTTP レスポンスを取得し、HTTP ヘッダーを解析してアクティベーションキーを取得する方法を示します。

```
function get-activation-key() {
  local ip_address=$1
  local activation_region=$2
  if [[ -z "$ip_address" || -z "$activation_region" ]]; then
    echo "Usage: get-activation-key ip_address activation_region"
    return 1
  fi
  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region"); 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 レスポンスを取得し、HTTP ヘッダーを解析してアクティベーションキーを取得する方法を示します。

```
function Get-ActivationKey {
  [CmdletBinding()]
  Param(
    [parameter(Mandatory=$true)][string]$IpAddress,
    [parameter(Mandatory=$true)][string]$ActivationRegion
  )
  PROCESS {
```

```
    $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion" -MaximumRedirection 0 -ErrorAction SilentlyContinue
    if ($request) {
      $activationKeyParam = $request.Headers.Location | Select-String -Pattern
 "activationKey=([A-Z0-9-]+)"
      $activationKeyParam.Matches.Value.Split("=")[1]
    }
  }
}
```

を使用するAWS Direct ConnectStorage Gateway

AWS Direct Connectは、お客様の内部ネットワークをAmazon Web Services ラウドにリンクします。を使用することによりAWS Direct ConnectStorage Gateway を使用すると、高スループットのワークロードが要求される場合に備えた接続を作成し、オンプレミスのゲートウェイとAWS。

Storage Gateway ではパブリックエンドポイントを使用します。とあるAWS Direct Connect接続を設定すると、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 の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、同じ場所に配置できます。AWS地域としてのAWS Direct Connect場所、または別の場所にある可能性がありますAWSリージョン。

次の図に例を示します。AWS Direct ConnectStorage Gateway で動作します。

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。

を使用するにはAWS Direct ConnectStorage Gateway

1. 作成して確立するAWS Direct Connectオンプレミスデータセンターと Storage Gateway エンドポイントの間の接続。接続の作成方法の詳細については、「」を参照してください。の使用開始 AWS Direct ConnectのAWS Direct Connectユーザーガイド。
2. Connect スのStorage Gateway アプライアンスをにAWS Direct Connectルーター。
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、「」を参照してください。仮想インターフェイスの作成のAWS Direct Connectユーザーガイド。

についての詳細AWS Direct Connect「」を参照してください。とはAWS Direct Connect?のAWS Direct Connectユーザーガイド。

ゲートウェイへの接続

ホストを選択してゲートウェイ VM をデプロイしたら、ゲートウェイを接続してアクティブ化します。これを行うには、ゲートウェイ VM の IP アドレスが必要です。ゲートウェイのローカルコンソールから IP アドレスを取得します。ローカルコンソールにログインし、コンソールページの先頭から IP アドレスを取得します。

オンプレミスでデプロイされているゲートウェイでは、ハイパーバイザーでも IP アドレスを取得できます。Amazon EC2 ゲートウェイでは、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 カーネルベースの仮想マシン (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 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。その後、Storage Gateway コンソールに戻り、コンソールに IP アドレスを入力します。

Amazon EC2 ホストから IP アドレスを取得する

ゲートウェイがデプロイされている Amazon EC2 インスタンスの IP アドレスを取得するには、EC2 インスタンスのローカルコンソールにログインします。コンソールページの先頭から IP アドレスを取得します。手順については、「」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 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 (https://console.aws.amazon.com/ec2/) を開きます。
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 (https://console.aws.amazon.com/ec2/) を開きます。
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。
4. ゲートウェイをアクティブ化した後、アクティブ化したゲートウェイを選択し、次にパネル下部から [VTL デバイス] タブを選択します。
5. すべての VTL デバイスの名前を取得します。
6. 各ターゲットでは、以下のコマンドを実行してターゲットを設定します。

   ```
   iscsiadm -m node -o new -T [$TARGET_NAME] -p [$Elastic_IP]:3260
   ```
7. 各ターゲットで、以下のコマンドを実行してログインします。

   ```
   iscsiadm -m node -p [$ELASTIC_IP]:3260 --login
   ```

   ゲートウェイはこれで EC2 インスタンスの elastic IP アドレスを使用して接続するようになりました。

Storage Gateway リソースとリソース ID の理解

Storage Gateway では、プライマリリソースはゲートウェイただし、その他のリソースタイプは次のとおりです。ボリューム,仮想テープ,iSCSI ターゲット, およびvtl デバイス。これらは、サブリソースと呼ばれ、ゲートウェイに関連付けられている場合にのみ存在します。

これらのリソースとサブリソースには、次の表に示すとおり、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`*

リソースタイプ	ARN 形式
ファイル共有 ARN	arn:aws:storagegateway: *region*:*account-id* :share/*share-id*
ボリューム ARN	arn:aws:storagegateway: *region*:*account-id* :gateway/ *gateway-id* /volume/*volume-id*
テープ ARN	arn:aws:storagegateway: *region*:*account-id* :tape/*tapebarcode*
ターゲット ARN (iSCSI ターゲット)	arn:aws:storagegateway: *region*:*account-id* :gateway/ *gateway-id* /target/*iSCSItarget*
VTL デバイス ARN	arn:aws:storagegateway: *region*:*account-id* :gateway/ *gateway-id* /device/*vtldevice*

また、Storage Gateway は EC2 インスタンスと EBS ボリュームとスナップショットをサポートします。これらのリソースは、Storage Gateway で使用される Amazon EC2 リソースです。

リソース 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。ボリューム ID は `vol-3344CCDD` という形式であり、この `vol` がボリュームのリソース ID です。

仮想テープの場合は、最大 4 文字のプレフィックスをバーコード ID の先頭につけてテープを整理できます。

Storage Gateway リソース ID は大文字です。ただし、Amazon EC2 API でこれらのリソース ID を使用する場合、Amazon EC2 は小文字のリソース ID を必要とします。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。たとえば、ボリュームの ID が Storage Gateway では `vol-1122AABB` であるとします。この ID を EC2 API で使用するには、`vol-1122aabb` に変更する必要があります。これを行わなければ、EC2 API が正常に動作しない場合があります。

> **Important**
>
> ストレージゲートウェイボリュームと、ゲートウェイボリュームから作成された Amazon EBS スナップショットの ID は、長い形式に変更されています。2016 年 12 月から、すべての新しいボリュームとスナップショットは、17 文字の文字列で作成されます。2016 年 4 月からこれらの長い ID を使用できるので、新しい形式でシステムをテストできます。詳細については、「長い EC2 および EBS リソース ID」を参照してください。
> たとえば、長いボリューム ID 形式のボリューム ARN は次のようになります。`arn:aws:storagegateway:us-west-2:111122223333:gateway/sgw-12A3456B/volume/vol-1122AABBCCDDEEFFG`.
> 長い ID 形式のスナップショット ID は次のようになります。`snap-78e226633445566ee`。詳細については、「」を参照してください。お知らせ: Heads-up — Lenger Storage Gateway ボリュームとスナップショット ID が登場 2016。

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。

たとえば、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、「タグを使用したゲートウェイとリソースへのアクセスのコントロール」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。

- タグのキーと値は大文字と小文字が区別されます。
- 1 つのリソースに付けることができるタグの最大数は 50 です。
- タグキーを aws: で始めることはできません。このプレフィックスは以下のために予約されています。AWSを使用するを使用する。
- 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

タグを操作するには、ストレージゲートウェイコンソール、Storage Gateway API、またはCLI (Storage Gateway コマンドラインインターフェイス) 。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. でStorage Gateway コンソールを開きます。https://console.aws.amazon.com/storagegateway/home。
2. ナビゲーションペインで、タグを付けるリソースを選択します。

   たとえば、ゲートウェイにタグを付ける場合は、[Gateways] を選択してから、ゲートウェイのリストからタグを付けるゲートウェイを選択します。
3. [Tags] を選択してから、[Add/edit tags] を選択します。
4. [Add/edit tags] ダイアログボックスで、[Create tag] を選択します。
5. [Key] でキーを、[Value] で値を入力します。たとえば、キーに [**Department**] を、値に [**Accounting**] を入力できます。

   > **Note**
   >
   > [Value] ボックスは空白のままにすることができます。

6. [Create Tag] を選択してタグを追加します。1 つのリソースに複数のタグを追加できます。
7. タグの追加が終了したら、[Save] を選択します。

タグを編集するには

1. でStorage Gateway コンソールを開きます。https://console.aws.amazon.com/storagegateway/home。
2. タグを編集するリソースを選択します。
3. [Tags] を選択して、[Add/edit tags] ダイアログボックスを開きます。
4. 編集するタグの横にある鉛筆アイコンを選択し、タグを編集します。
5. タグの編集が終了したら、[Save] を選択します。

タグを削除するには

1. でStorage Gateway コンソールを開きます。https://console.aws.amazon.com/storagegateway/home。
2. タグを削除するリソースを選択します。
3. [Tags] を選択してから、[Add/edit tags] を選択して [Add/edit tags] ダイアログボックスを開きます。
4. 削除するタグの横にある [X] アイコンを選択してから、[Save] を選択します。

以下の資料も参照してください。

タグを使用したゲートウェイとリソースへのアクセスのコントロール

のオープンソースコンポーネントの操作AWS Storage Gateway

このセクションでは、Storage Gateway の機能を提供するために依存しているサードパーティー製のツールとライセンスについて説明しています。

トピック

- Storage Gateway のオープンソースコンポーネント
- Amazon FSx ファイルゲートウェイのオープンソースコンポーネント

Storage Gateway のオープンソースコンポーネント

ボリュームゲートウェイ、テープゲートウェイ、および 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のツールとライセンスが使用されます。

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するには、以下のリンクを使用します。AWS Storage Gatewayソフトウェア:

- VMware ESXi にデプロイされたゲートウェイの場合:sources.tar
- Microsoft Hyper-V にデプロイされたゲートウェイの場合:sources_hyperv.tar
- Linux カーネルベースの仮想マシン (KVM) にデプロイされたゲートウェイの場合:sources_KVM.tar

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ー製ツールの関連ライセンスについては、サードパーティーのライセンスを参照してください。

Amazon FSx ファイルゲートウェイのオープンソースコンポーネント

Amazon FSx ファイルゲートウェイ (FSx ファイルゲートウェイ) 機能を提供するために、いくつかのサードパーティ製のツールとライセンスが使用されています。

FSX File 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するには、以下のリンクを使用します。

- Amazon FSx ファイルゲートウェイ 2021 年 7 月 7 日sgw-file-Fsx-smb-opensource.tgz
- Amazon FSx ファイルゲートウェイ 2021-04-06 リリースの場合:sgw-file-Fsx-smb-20210406-opensource.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。依存しているすべてのサードパーティー製のツールの関連ライセンスについては、以下のリンクを参照してください。

- Amazon FSx ファイルゲートウェイ 2021 年 7 月 7 日 サードパーティーライセンス。
- Amazon FSx ファイルゲートウェイ 2021-04-06 リリースの場合: サードパーティーライセンス。

クォータ

ファイルシステムのクォータ

次の表は、ファイルシステムのクォータの一覧です。

リソース	ファイルシステムあたりの制限
タグの最大数	50
自動バックアップの最大保持期間	90 日間
アカウントあたり 1 つの宛先リージョンに対して、進行中のバックアップコピーリクエストの最大数。	5
最小ストレージ容量、SSD ファイルシステム	32 GiB
最小ストレージ容量、HDD ファイルシステム	2,000 GiB
最大ストレージ容量、SSD、HDD	64 TiB
最小スループット容量	8 MBps
最大スループット容量	2,048 MBps
ファイル共有の最大数	100,000

ゲートウェイの推奨ローカルディスクサイズ

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)	その他の必要なローカルディスク
FSx ファイルゲートウェイ	150 GiB	64 TiB	—

> **Note**
>
> 最大容量まで、キャッシュに対して 1 つ以上のローカルドライブを設定できます。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

キャッシュとして割り当て済みである場合は、既存のディスクサイズを変更しないでください。

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 を使用してゲートウェイをプログラミングで設定し、管理できます。このセクションでは、AWS Storage Gateway のオペレーション、認証のための署名要求、エラー処理について説明します。Storage Gateway で使用可能なリージョンとエンドポイントの詳細については、「」を参照してください。AWS Storage Gatewayエンドポイントとクォータのの全般のリファレンス。

> **Note**
>
> また、 を使用することもできますAWSStorage Gateway でアプリケーションを開発するときの SDK。-AWSSDK for Java、.NET、PHP は、基盤となるStorage Gateway API をラップして、プログラミング作業を簡素化します。SDK ライブラリのダウンロードについては、「サンプルコードライブラリ」を参照してください。

トピックス

- AWS Storage Gateway必須リクエストヘッダー
- リクエストへの署名
- エラーレスポンス
- アクション

AWS Storage Gateway必須リクエストヘッダー

このセクションでは、すべての POST リクエストで送信する必要がある必須のヘッダーについて説明します。AWS Storage Gateway。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
```

次に示すのは、の POST リクエストに含める必要があるヘッダーです。AWS Storage Gateway。次に示す「x-amz」で始まっているヘッダーは次のとおりです。AWS固有のヘッダー。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	認証ヘッダーには、有効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。AWS Storage Gatewayを使用して、リクエストがリクエスタに対して有効なアクションかどうかを判別します。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。認証ヘッダーの形式は、AWSV4 署名プロセス。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	を使用するapplication/x-amz-json-1.1　に対するすべてのリクエストのコンテンツタイプとしてAWS Storage Gateway。 `Content-Type: application/x-amz-json-1.1`
Host	ホストヘッダーを使用して、AWS Storage Gatewayリクエストを送信するエンドポイント。たとえば、storagegateway.us-east-2.am

ヘッダー	説明
	azonaws.com　は、米国東部 (オハイオ) リージョンのエンドポイントです。で利用可能なエンドポイントの詳細については、を参照してください。AWS Storage Gateway「」を参照してください。AWS Storage Gatewayエンドポイントとクォータのリファレンス。 `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)。ときx-amz-date　ヘッダーが存在する場合、AWS Storage Gateway無視します。Dateリクエスト認証中のヘッダー。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」など) は、API リストにあります。Storage Gateway の API リファレンス。

リクエストへの署名

Storage Gateway では、リクエストに署名することで、送信するすべてのリクエストを認証する必要があります。リクエストに署名するには、暗号化ハッシュ関数を使用してデジタル署名を計算します。暗号化ハッシュは、入力データから一意のハッシュ値生成して返す関数です。ハッシュ関数に

渡される入力データとしては、リクエストのテキスト、およびシークレットアクセスキーが該当します。ハッシュ関数から返されるハッシュ値をリクエストに署名として含めます。署名は、リクエストの `Authorization` ヘッダーの一部です。

Storage Gateway は、リクエストを受け取ると、リクエスト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 は認証をサポートしていますAWS署名バージョン 4。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。正規形式を使用する必要がある理由は、送信した署名と比較するために署名を再計算するときに正規形式が使用されるので、同じ正規形式を使用する必要があります。
- タスク 2: 署名文字列を作成する

  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: 署名の作成

  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。その他の参考計算例については、アマゾン ウェブ サービス用語集の「Signature Version 4 Test Suite」を参照してください。

例では、次のように想定しています。

- リクエストのタイムスタンプは「Mon, 10 Sep 2012 00:00:00" 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 (またはStorage Gateway API) のクエリパラメータがないためです。

-署名対象の文字列にとってタスク 2: 署名文字列を作成するは:

```
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: 署名の作成 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 が使用されている場合、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

次の表は、AWS Storage Gateway API の例外を表示しています。AWS Storage Gateway オペレーションがエラーレスポンスを返す場合、レスポンス本文には、次の例外のいずれかが含まれます。InternalServerError と InvalidGatewayRequestException は、特定のオペレーションエラーコードを表示するオペレーションエラーコード オペレーションエラーコード メッセージの 1 つを返します。

Exception	メッセージ	HTTP ステータスコード
IncompleteSignatureException	指定された署名は不完全です。	400 Bad Request
InternalFailure	リクエストの処理は、不明なエラー、例外、または失敗により実行できませんでした。	500 Internal Server Error
InternalServerError	オペレーションエラーコードメッセージの 1 つ オペレーションエラーコード.	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	X.509 証明書、またはAWS指定されたアクセスキー ID が見つかりません。	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。確認方法AWSアクセスキーと署名方法。	400 Bad Request

Exception	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 (登録済み) のいずれか一方が含まれている必要があります。AWSアクセスキー ID または X.509 証明書。	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	リクエストは、サーバーの一時的障害のために実行に失敗しました。	503 Service Unavailable
SubscriptionRequiredException	-AWSサービスを利用するためには、アクセスキー ID を取得する必要があります。	400 Bad Request
ThrottlingException	速度を超過しました。	400 Bad Request
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 でのオペレーション に示します。	400 Bad Request

Exception	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

次のテーブルに、AWS Storage Gateway オペレーションエラーコードと、そのコードを返す API の対応を示します。すべての操作エラーコードは、2 つの一般的な例外のいずれかとともに返されます。InternalServerErrorそしてInvalidGatewayRequestException—で説明しています。例外。

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
ファイルシステムの関連付けエンドポイント構成の競合	既存のファイルシステムの関連付けエンドポイント構成は、指定された構成と競合しています。	ファイルシステムを関連付ける
ファイルシステムの関連付けエンドポイント IP アドレスはすでに使用中です	指定されたエンドポイント IP アドレスはすでに使用されています。	ファイルシステムを関連付ける
ファイルシステムの関連付けエンドポイントヒントアドレスがありません	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。	ファイルシステムを関連付ける
ファイルシステムの関連付けが見つかりません	指定されたファイルシステムの関連付けは、見つかりませんでした。	ファイルシステムの関連付けを更新 ファイルシステムの関連付けを解除する ファイルシステムの関連付けを記述する
ファイルシステムが見つかりません	指定されたファイルシステムが見つかりません。	ファイルシステムを関連付ける

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。

Type: 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。

Type: Collection

errorCode

オペレーションエラーコードの 1 つ。

Type: 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。

Type: 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 .

Type: 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 が計算した署名とリクエストで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 でのオペレーション

Storage Gateway オペレーションのリストについては、「」を参照してください。アクションのAWS Storage GatewayAPI リファレンス。

Amazon FSx ファイルゲートウェイユーザーガイドのドキュメント履歴

- API バージョン: 2013-06-30
- ドキュメント最新更新日: 2021 年 7 月 07 日

以下の表は、Amazon FSx File Gateway のドキュメントリリースを示します。このドキュメントの更新に関する通知については、RSS フィードでサブスクライブできます。

更新履歴の変更	update-history-description	update-history-date
複数のファイルシステムサポート	Amazon FSx ファイルゲートウェイでは、最大 5 つのアタッチされた Amazon FSx ファイルシステムがサポートされるようになりました。詳細については、「」を参照してください。Amazon FSx for Windows File Server ファイルシステムをアタッチする。	2021 年 7 月 7 日
Amazon FSx ソフトストレージクォータのサポート	Amazon FSx ファイルゲートウェイは、ストレージクォータが設定されている接続された Amazon FSx ファイルシステムに書き込むときに、ソフトストレージクォータ (ユーザーがデータ制限を超えた場合に警告する) をサポートするようになりました。ハードクォータ (書き込みアクセスを拒否してデータ制限を強制する) はサポートされていません。ソフトクォータは、Amazon FSx 管理者ユー	2021 年 7 月 7 日

	ザーを除くすべてのユーザーに対して機能します。ストレージクォータのセットアップの詳細については、「」を参照してください。ストレージクォータのAmazon FSx for Windows File Server ユーザーガイド。	
新規ガイド	Storage Gateway ゲートウェイは、元のファイルゲートウェイ（現在はAmazon S3 ファイルゲートウェイとして知られている）に加えて、Amazon FSx ファイルゲートウェイ（FSx File）を提供しています。FSx ファイルは、オンプレミス施設から Windows ファイルサーバーファイル共有のためのクラウド内 FSx に低レイテンシーと効率的なアクセスを提供します。詳細については、「」を参照してください。Amazon FSx ファイルゲートウェイとは何ですか?	2021 年 4 月 27 日

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