ボリュームゲートウェイユーザーガイド

AWS Storage Gateway

API バージョン 2013-06-30

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスはAmazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

ボリュームゲートウェイについて 1
ボリュームゲートウェイの仕組み 2
ボリュームゲートウェイ 2
の開始方法 AWS Storage Gateway 8
にサインアップする AWS Storage Gateway 8
管理者権限を持つ IAM ユーザーを作成する 9
アクセス AWS Storage Gateway 11
AWS リージョン Storage Gateway をサポートする 11
ボリュームゲートウェイのセットアップ要件 13
ハードウェアとストレージの要件 13
VM のハードウェア要件 13
Amazon EC2 インスタンスタイプでの要件 14
..... 14
ストレージの要件 14
ネットワークとファイアウォールの要件 15
ポート要件 16
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 30
ファイアウォールとルーターを介したゲートウェイアクセスの許可 33
セキュリティグループの設定 35
サポートされているハイパーバイザーとホストの要件 36
サポートされている iSCSI イニシエータ 37
ハードウェアアプライアンスの使用 38
ハードウェアアプライアンスのセットアップ 39
ハードウェアアプライアンスの物理的なインストール 41
ハードウェアアプライアンスコンソールへのアクセス 43
ハードウェアアプライアンスのネットワークパラメータの設定 44
ハードウェアアプライアンスのアクティブ化 46
ハードウェアアプライアンスでゲートウェイを作成する 47
ハードウェアアプライアンスのゲートウェイ IP アドレスの設定 48
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 51
ハードウェアアプライアンスの削除 52
ゲートウェイを作成する 54
概要 - ゲートウェイのアクティブ化 54
ゲートウェイをセットアップする 54

に接続する AWS 54
確認してアクティブ化する 55
概要 - ゲートウェイの設定 55
概要 - ストレージリソース 55
ボリュームゲートウェイの作成 55
ボリュームゲートウェイをセットアップする 56
ボリュームゲートウェイを AWSに接続する 57
設定を確認してボリュームゲートウェイをアクティブ化する 58
ボリュームゲートウェイを設定する 59
ボリュームの作成 62
ボリューム用の CHAP 認証の設定 64
クライアントへのボリュームの接続 65
Microsoft Windows クライアントへの接続 65
Red Hat Enterprise Linux クライアントへの接続 66
ボリュームの初期化とフォーマット 67
Windows での初期化とフォーマット 67
RHEL での初期化とフォーマット 69
ゲートウェイのテスト 70
ボリュームのバックアップ 72
Storage Gateway を使用してボリュームをバックアップする 72
AWS Backup を使用してボリュームをバックアップする 72
次のステップ 75
実際のワークロードに対する、ボリュームゲートウェイストレージのサイズ設定 76
仮想プライベートクラウドでのゲートウェイのアクティブ化 78
Storage Gateway 用の VPC エンドポイントの作成 78
ボリュームゲートウェイの管理 80
ゲートウェイ情報の編集 82
ボリュームの追加と拡大 83
ボリュームをクローンする 83
ボリュームの使用量の表示 85
ストレージボリュームの削除 86
別のゲートウェイにボリュームを移動する 87
復旧スナップショットの作成 89
スナップショットスケジュールの編集 90
スナップショットの削除 91
AWS SDK for Java の使用 91

AWS SDK for .NET の使用 95
の使用 AWS Tools for Windows PowerShell 102
ボリュームステータスと移行について 104
ボリュームのステータスについて 105
ボリュームのステータスについて 110
キャッシュ型ボリュームステータスの遷移を理解する 110
保管型ボリュームステータスの遷移を理解する 113
新しいゲートウェイへのデータの移動 116
保管型ボリュームの新しい保管型ボリュームゲートウェイへの移動 116
キャッシュ型ボリュームを新しいゲートウェイの仮想マシンに移動する 119
Storage Gateway のモニタリング 123
ゲートウェイメトリクスについて 123
Storage Gateway メトリクスのディメンション 129
アップロードバッファのモニタリング 130
キャッシュストレージのモニタリング 133
CloudWatch アラームの説明 134
CloudWatch 推奨アラームの作成 136
カスタム CloudWatch アラームの作成 137
ボリュームゲートウェイのモニタリング 139
ボリュームゲートウェイのヘルスログの取得 140
Amazon CloudWatch メトリクスを使用する 141
アプリケーションとゲートウェイの間のパフォーマンスの測定 142
ゲートウェイと AWSの間のパフォーマンスの測定 144
ボリュームメトリクスについて 148
ゲートウェイの維持 156
ローカルディスクの管理 156
ローカルディスクストレージの容量の決定 157
アップロードバッファまたはキャッシュストレージを追加する 160
帯域幅の管理 162
Storage Gateway コンソールを使用して帯域幅スロットリングを変更する 163
帯域幅スロットリングのスケジューリング 163
の使用 AWS SDK for Java 165
の使用 AWS SDK for .NET 167
の使用 AWS Tools for Windows PowerShell 169
ゲートウェイアップデートの管理 170
更新頻度と予想される動作 170

メンテナンスアップデートをオンまたはオフにする 171
ゲートウェイのメンテナンスウィンドウのスケジュールを変更する 172
更新を手動で適用する 173
ゲートウェイ VM のシャットダウン 174
ボリュームゲートウェイを起動および停止する 175
ゲートウェイおよびリソースの削除 176
Storage Gateway コンソールを使用したゲートウェイの削除 176
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 178
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削除 178
ローカルコンソールを使用したメンテナンスタスクの実行 180
ゲートウェイローカルコンソールへのアクセス 180
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 181
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 181
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 182
VM ローカルコンソールでのタスクの実行 183
ボリュームゲートウェイのローカルコンソールへのログイン 184
オンプレミスゲートウェイの SOCKS5 プロキシの設定 186
ゲートウェイのネットワークの設定 187
ゲートウェイのインターネット接続のテスト 194
オンプレミスゲートウェイの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 195
ゲートウェイシステムリソースのステータスの表示 198
EC2 ローカルコンソールでのタスクの実行 199
EC2 ゲートウェイのローカルコンソールへのログイン 200
HTTP プロキシの設定 200
ゲートウェイのネットワーク接続をテストする 201
ゲートウェイシステムリソースのステータスの表示 202
ローカルコンソールでの Storage Gateway コマンドの実行 203
ボリュームゲートウェイのパフォーマンスと最適化 206
ゲートウェイのパフォーマンスの最適化 206
推奨設定 206
ゲートウェイへのリソースの追加 207
iSCSI 設定を最適化する 210
アプリケーション環境へのリソースの追加 210
セキュリティ 212
データ保護 213

データ暗号化 ... 214
CHAP 認証の設定 ... 215
Identity and Access Management ... 217
対象者 ... 217
アイデンティティを使用した認証 ... 218
ポリシーを使用したアクセスの管理 ... 222
How AWS Storage Gateway と IAM の連携 ... 224
アイデンティティベースのポリシーの例 ... 231
トラブルシューティング ... 234
コンプライアンス検証 ... 236
耐障害性 ... 237
インフラストラクチャセキュリティ ... 238
AWS セキュリティのベストプラクティス ... 239
ログ記録とモニタリング ... 239
CloudTrail での Storage Gateway の情報 ... 239
Storage Gateway のログファイルエントリを理解する ... 240
ゲートウェイ問題のトラブルシューティング ... 243
トラブルシューティング: ゲートウェイのオフライン問題 ... 244
関連付けられたファイアウォールまたはプロキシを確認する ... 244
ゲートウェイのトラフィックの継続的な SSL またはディープパケット検査を確認する ... 244
ハイパーバイザーホストで停電やハードウェア障害がないか確認する ... 244
関連付けられたキャッシュディスクの問題を確認する ... 245
トラブルシューティング: ゲートウェイのアクティベーションの問題 ... 245
パブリックエンドポイントを使用してゲートウェイをアクティブ化する際のエラーを解決する ... 246
Amazon VPC エンドポイントを使用してゲートウェイをアクティブ化する際のエラーを解決する ... 249
パブリックエンドポイントを使用してゲートウェイをアクティブ化し、同じ VPC に Storage Gateway VPC エンドポイントがある場合のエラーを解決する ... 253
オンプレミスゲートウェイの問題のトラブルシューティング ... 254
ゲートウェイ サポート のトラブルシューティングに役立つ のアクティブ化 ... 258
Microsoft Hyper-V セットアップの問題のトラブルシューティング ... 259
Amazon EC2 ゲートウェイの問題のトラブルシューティング ... 263
少し時間が経ってもゲートウェイのアクティベーションが実行されない ... 263
インスタンスリストに EC2 ゲートウェイインスタンスがない ... 264
EC2 ゲートウェイインスタンスに Amazon EBS ボリュームをアタッチできない ... 264

EC2 ゲートウェイのボリュームターゲットにイニシエータをアタッチできない 264
ストレージボリュームを追加するときに利用可能なディスクがないというメッセージ 265
アップロードバッファ領域を削減するために、アップロードバッファ領域として割り当てられたディスクを削除する方法 265
EC2 ゲートウェイとの間のスループットがゼロに低下する 265
ゲートウェイのトラブルシューティング サポート に役立つ のアクティブ化 266
シリアルコンソールを使用して Amazon EC2 ゲートウェイに接続する 268
ハードウェアアプライアンスの問題のトラブルシューティング 268
サービスの IP アドレスを特定する方法 268
ファクトリーリセットを実行する方法 268
リモート再起動を実行する方法 268
Dell iDRAC サポートを受ける方法 268
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方法 269
ハードウェアアプライアンスのサポートを受ける方法 269
ボリュームの問題のトラブルシューティング 270
ボリュームが設定されていないとコンソールに表示される 270
ボリュームは復旧不可能であるとコンソールに表示される 271
ゲートウェイキャッシュ型が到達不可能なためデータを復旧する場合 271
ボリュームのステータスが PASS THROUGH であるとコンソールに表示される 272
ボリュームの整合性を確認し、エラーがある場合は修正する 273
ボリュームの iSCSI ターゲットが Windows のディスク管理コンソールに表示されない 273
ボリュームの iSCSI ターゲット名を変更したい 273
スケジュールしたボリュームのスナップショットが実行されなかった 273
障害が発生したディスクの取り外しまたは交換が必要な場合 273
アプリケーションからボリュームへのスループットがゼロに低下した 274
ゲートウェイのキャッシュディスクでエラーが発生する 275
ボリュームのスナップショットのステータスが予想以上に長い時間にわたって PENDING のままである 275
高可用性のヘルス通知 276
高可用性に関する問題のトラブルシューティング 276
ヘルス通知 276
メトリクス 278
ベストプラクティス 279
ベストプラクティス: データの復旧 279
予期しない VM のシャットダウンからの復旧 280
正しく機能していないゲートウェイまたは VM からのデータの復旧 280

回復不可能なボリュームからのデータの復旧 281
正しく機能していないキャッシュディスクからのデータの復旧 281
破損したファイルシステムからのデータの復旧 281
アクセス不能なデータセンターからのデータの復旧 283
不要なリソースのクリーンアップ 283
ボリュームで課金されるストレージ量を削減する 284
その他のリソース 285
ホストセットアップ 285
ボリュームゲートウェイ用のデフォルトの Amazon EC2 ホストをデプロイする 287
ボリュームゲートウェイ用にカスタマイズされた Amazon EC2 インスタンスをデプロイする 289
Amazon EC2 インスタンスメタデータオプションの変更 293
VM の時刻を Hyper-V または Linux KVM ホストの時刻と同期する 294
VM の時刻と VMware ホストの時刻を同期する 295
準仮想化ディスクコントローラーの設定 296
ゲートウェイのネットワークアダプタの設定 297
Storage Gateway での VMware High Availability の使用 302
ボリュームゲートウェイのストレージリソースの使用 307
ゲートウェイからのディスクの削除 308
EC2 ゲートウェイの EBS ボリューム 309
アクティベーションキーの取得 311
Linux (curl) 312
Linux (bash/zsh) 312
Microsoft Windows PowerShell 313
ローカルコンソールを使用する 314
iSCSI イニシエータの接続 314
Windows クライアントからボリュームへの接続 315
ボリュームから Linux クライアントへの接続 319
iSCSI 設定のカスタマイズ 321
CHAP 認証の設定 327
Storage Gateway AWS Direct Connect での の使用 332
ゲートウェイ IP アドレスの取得 333
Amazon EC2 のホストから IP アドレスを取得する 334
リソースとリソース ID の理解 335
リソース ID の使用 336
リソースのタグ付け 336

タグの操作 337
オープンソースコンポーネント 338
Storage Gateway のクォータ 339
ボリュームのクォータ 339
ゲートウェイのローカルディスクの推奨サイズ 340
API リファレンス 341
必須リクエストヘッダー 341
リクエストへの署名 344
署名の計算例 345
エラーレスポンス 346
例外 347
オペレーションエラーコード 349
エラーレスポンス 369
オペレーション 371
ドキュメント履歴 372
以前の更新 392
リリースノート 412
..... cdxvii

ボリュームゲートウェイについて

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

Storage Gateway は、VMware ESXi、KVM、または Microsoft Hyper-V ハイパーバイザーで実行されている VM アプライアンスとしてオンプレミスでデプロイすることも、ハードウェアアプライアンスとしてデプロイすることも、Amazon EC2 インスタンス AWS として にデプロイすることもできます。EC2 インスタンスでホストされているゲートウェイは、災害対策やデータミラーリングのために使用できます。また、Amazon EC2 でホストされているアプリケーションにストレージを提供する用途にも使用が可能です。

を可能にするさまざまなユースケースについては、 AWS Storage Gateway 「」を参照してくださいAWS Storage Gateway。料金に関する最新の情報については、 詳細ページの料金表 AWS Storage Gateway を参照してください。

AWS Storage Gateway は、ファイルベース (S3 File Gateway および FSx File Gateway)、ボリュームベース (Volume Gateway)、テープベース (Tape Gateway) のストレージソリューションを提供します。

このユーザーガイドでは、ボリュームゲートウェイに関する情報を提供します。

ボリュームゲートウェイは、オンプレミスのアプリケーションサーバーから Internet Small Computer System Interface (iSCSI) デバイスとしてマウントできる、クラウドベースのストレージボリュームを提供します。

ボリュームゲートウェイがサポートするボリューム構成は以下のとおりです。

- キャッシュ型ボリューム – データを Amazon Simple Storage Service (Amazon S3) に保存し、頻繁にアクセスするデータのサブセットのコピーはローカルに保持します。プライマリストレージのコストを大幅に削減し、ストレージをオンプレミスで拡張する必要を最小限に抑えます。また、頻繁にアクセスするデータへのアクセスを低レイテンシーに保つことができます。
- 保管型ボリューム – データセット全体への低レイテンシーアクセスが必要な設定は、すべてのデータをローカルに保存するように、最初にオンプレミスのゲートウェイを設定します。次に、このデータのポイントインタイムスナップショットを非同期的に Amazon S3 にバックアップしま

す。この構成では、ローカルデータセンターや Amazon EC2 (Amazon Elastic Compute Cloud) への復元が可能な、耐久性が高く低コストのオフサイトバックアップを実現できます。例えば、障害復旧のための代替容量が必要な場合は、Amazon EC2 にバックアップを復元できます。

アーキテクチャの概要については、ボリュームゲートウェイの仕組み を参照してください。

このユーザーガイドには、すべてのゲートウェイタイプに共通するセットアップ情報を説明する入門セクションがあります。また、ボリュームゲートウェイのセットアップ要件、およびボリュームゲートウェイをデプロイ、アクティブ化、設定、管理する方法を説明するセクションを見つけることができます。

このユーザーガイドの手順では、主に AWS Management Consoleを使用してゲートウェイオペレーションを実行することに重点を置いています。プログラムによってこれらのオペレーションを実行する場合は、AWS Storage Gateway API リファレンスを参照してください。

ボリュームゲートウェイの仕組み

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

ボリュームゲートウェイ

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

トピック

- キャッシュ型ボリュームのアーキテクチャ
- 保管型ボリュームのアーキテクチャ

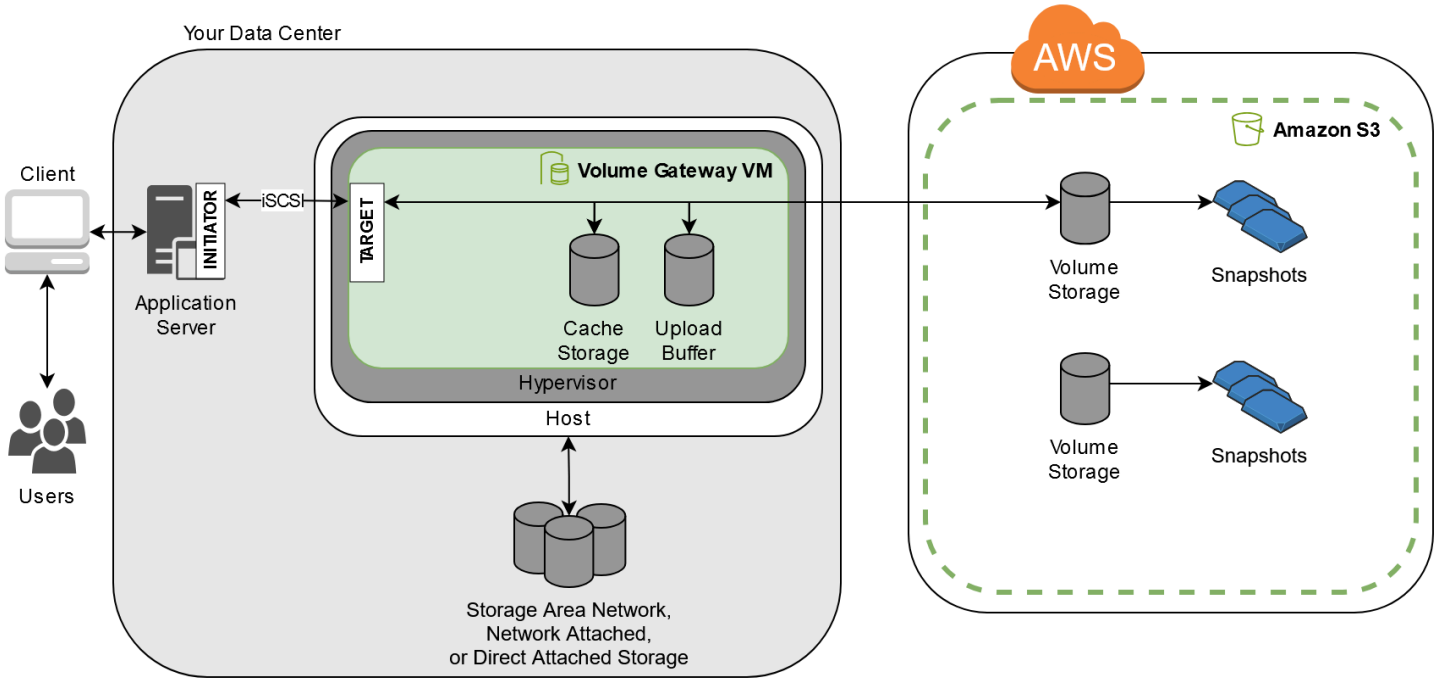
キャッシュ型ボリュームのアーキテクチャ

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

み込まれたデータはオンプレミスのストレージゲートウェイのキャッシュとアップロードバッファストレージに保持します。

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

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



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

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

- ゲートウェイがキャッシュストレージとして使用するディスク – アプリケーションがストレージボリュームにデータを書き込むと AWS、ゲートウェイはまずキャッシュストレージに使用されるオンプレミスディスクにデータを保存します。その上で、ゲートウェイはデータを Amazon S3 に

アップロードします。キャッシュストレージは、オンプレミスで耐久性の高い保存場所として機能し、アップロードバッファから Amazon S3 へのアップロードを待機しているデータを保存します。

また、キャッシュストレージはアプリケーションが最近アクセスしたデータをオンプレミスに保存し、低レイテンシーでアクセスできるようにもします。アプリケーションがデータをリクエストすると、ゲートウェイはまずキャッシュストレージでそのデータを検索し、見つからなければ Amazon S3 内を検索します。

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

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

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

データのバックアップからの復元が必要な場合には、Amazon EBS スナップショットをゲートウェイのストレージボリュームに復元できます。また、サイズが 16 TiB までのスナップショットであれば、新しい Amazon EBS ボリュームの開始点としてスナップショットを使用できます。その上で、この新しい Amazon EBS ボリュームを Amazon EC2 インスタンスにアタッチできます。

キャッシュ型ボリューム用のすべてのゲートウェイデータとスナップショットデータは、Amazon S3 に保存され、サーバー側の暗号化 (SSE) 機能を使用して保管時の暗号化が行われます。ただし、このデータには Amazon S3 API や Amazon S3 マネジメントコンソールなどのツールでアクセスすることはできません。

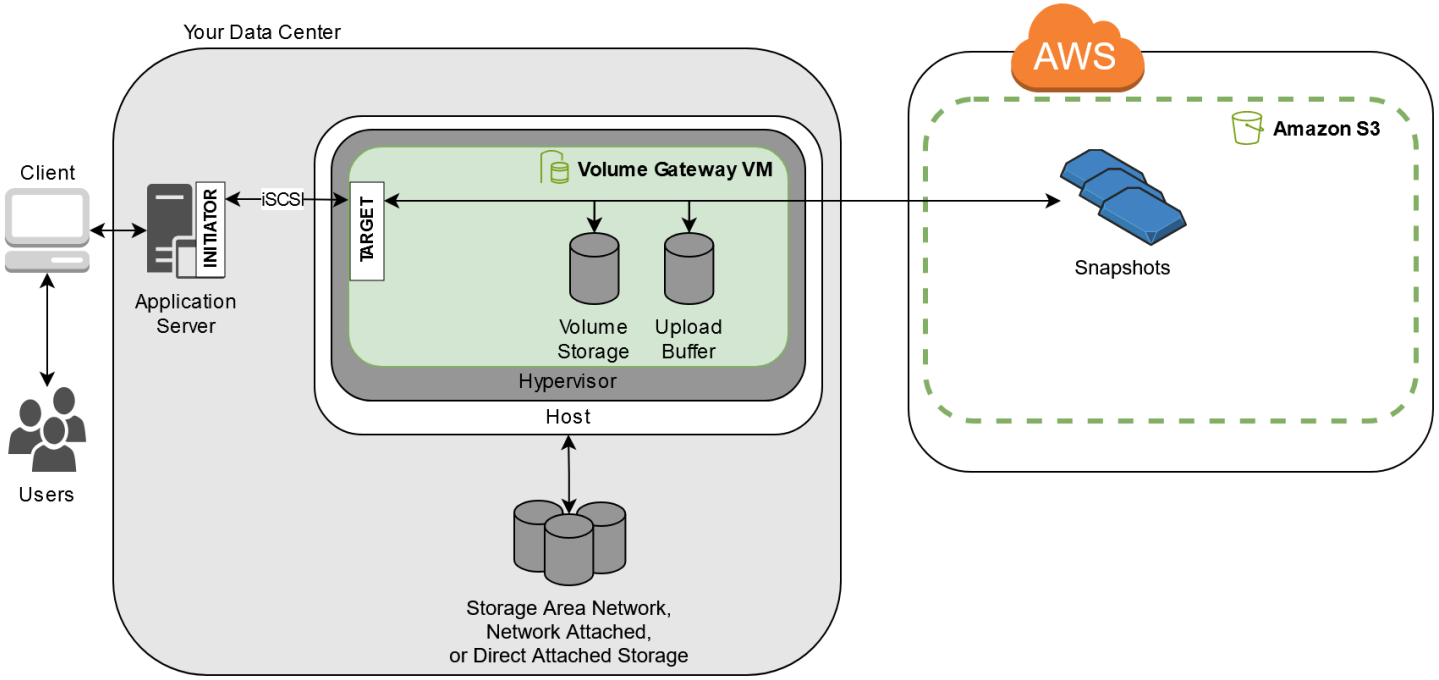
保管型ボリュームのアーキテクチャ

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

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

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

下の図は、保管型ボリュームのデプロイの概要を示しています。



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

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

ストレージボリュームは、増分バックアップ (スナップショットと呼びます) をとることができます。ゲートウェイは、これらのスナップショットを Amazon S3 に Amazon EBS スナップショットとして保存します。新たにスナップショットをとる際には、前回のスナップショット以降に変更されたデータのみが保存されます。スナップショットの作成時には、ゲートウェイがスナップショットポイントまでの変更内容をアップロードし、Amazon EBS を使用して新しいスナップショットを作成します。スナップショットは、スケジュールに基づいて、または 1 回のみ実行可能です。1 つのボ

リュームで複数のスナップショットを連続してキューに入れることができますが、各スナップショットの作成が完了しないと、次のスナップショットは作成されません。スナップショットを削除する場合、他のスナップショットが必要ないデータのみが削除されます。

データのバックアップからの復元が必要な場合には、Amazon EBS スナップショットをオンプレミスのゲートウェイストレージボリュームに復元できます。このスナップショットは、新しい Amazon EBS ボリュームの開始点としても利用できます。このボリュームは、Amazon EC2 インスタンスにアタッチすることが可能です。

の開始方法 AWS Storage Gateway

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

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

トピック

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

にサインアップする AWS Storage Gateway

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

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

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

   サインアップ手順の一環として、電話またはテキストメッセージを受け取り、電話キーパッドで検証コードを入力します。

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

また、 にアクセスするときは、ユーザーに一時的な認証情報の使用を求めることをお勧めします AWS。一時的な認証情報を提供するには、フェデレーションと IAM Identity Center などの ID AWS プロバイダーを使用できます。会社が既に ID プロバイダーを使用している場合は、フェデレーションでこれを使用して、 AWS アカウントのリソースへのアクセスを提供する方法を簡素化できます。

管理者権限を持つ IAM ユーザーを作成する

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

管理者ユーザーを作成するには、以下のいずれかのオプションを選択します。

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

Warning

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

アクセス AWS Storage Gateway

AWS Storage Gateway コンソールを使用して、Storage Gateway ハードウェアアプライアンスのデプロイからのアクティブ化または削除、さまざまなタイプのゲートウェイの作成、管理、削除、ストレージボリュームの作成、管理、削除、Storage Gateway サービスのさまざまな要素のヘルスとステータスのモニタリングなどを含む、さまざまなゲートウェイ設定とメンテナンスタスクを実行できます。わかりやすさと使いやすさのために、このガイドでは、Storage Gateway コンソールのウェブインターフェイスを使用してタスクを実行することに焦点を当てています。Storage Gateway コンソールには、ウェブブラウザから https://console.aws.amazon.com/storagegateway/home/ でアクセスできます。

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

AWS SDKs を使用して、Storage Gateway とやり取りするアプリケーションを開発することもできます。Java、.NET、PHP 用の AWS SDKs、基盤となる Storage Gateway API をラップして、プログラミングタスクを簡素化します。SDK ライブラリのダウンロードについては、「AWS デベロッパーセンター」を参照してください。

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

AWS リージョン Storage Gateway をサポートする

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

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

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

ボリュームゲートウェイのセットアップ要件

以下に挙げる要件は、特記がない限り、すべてのゲートウェイ構成に共通です。

トピック

- ハードウェアとストレージの要件
- 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
- サポートされている iSCSI イニシエータ

ハードウェアとストレージの要件

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

VM のハードウェア要件

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

- VM に割り当てられた仮想プロセッサ 4 個。
- ボリュームゲートウェイの場合、ハードウェアの RAM に次の容量の専用領域を確保する必要があります。
  - 16 TiB までのキャッシュ容量が使用可能な、ゲートウェイ用に予約された 16 GiB の RAM 領域
  - 16 TiB ~ 32 TiB のキャッシュ容量が使用可能な、ゲートウェイ用に予約された 32 GiB の RAM 領域
  - 32 TiB ~ 64 TiB のキャッシュ容量が使用可能な、ゲートウェイ用に予約された 48 GiB の RAM 領域
- ディスクの空き容量 80 GiB (VM イメージとシステムデータのインストール用)。

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

Amazon EC2 インスタンスタイプでの要件

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

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

ボリュームゲートウェイの場合、Amazon EC2 インスタンスはゲートウェイに使用する予定のキャッシュサイズに応じて、次の量の RAM を割り当てる必要があります。

- 16 TiB までのキャッシュ容量が使用可能な、ゲートウェイ用に予約された 16 GiB の RAM 領域
- 16 TiB ~ 32 TiB のキャッシュ容量が使用可能な、ゲートウェイ用に予約された 32 GiB の RAM 領域
- 32 TiB ~ 64 TiB のキャッシュ容量が使用可能な、ゲートウェイ用に予約された 48 GiB の RAM 領域

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

キャッシュ型ボリュームに推奨

- 汎用インスタンスファミリー – m4、m5、または m6 インスタンスタイプ。
- コンピューティング最適化インスタンスファミリー – c4、c5、c6、または c7 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、r5、r6、または r7 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、i4、または i7 インスタンスタイプ。

ストレージの要件

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

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

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

> **Note**
>
> キャッシュおよびアップロードバッファ用として、1 つ以上のローカルドライブを、最大容量まで構成することができます。
> 既存のゲートウェイにキャッシュやアップロードバッファを追加する場合、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やアップロードバッファとして割り当て済みである場合は、既存のディスクサイズを変更しないでください。

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

ネットワークとファイアウォールの要件

ゲートウェイには、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。以下は、必要なポートと、ファイアウォールとルーターを経由してアクセスを許可する方法についての情報です。

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

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

トピック

- ポート要件
- Storage Gateway ハードウェアアプライアンスのネットワークとファイアウォールに関する要件
- ファイアウォールとルーターを介した AWS Storage Gateway アクセスの許可
- Amazon EC2 ゲートウェイインスタンスでのセキュリティグループの設定

ポート要件

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

ボリュームゲートウェイのポート要件

ネットワーク要素	From	To	プロトコル	ポート	インバウンド	アウトバウンド	必須	メモ
ウェブブラウザ	ウェブブラウザ	Storage Gateway VM	TCP HTTP	80	✓	✓	✓	Storage Gateway アクティベーションキーを取得するためにローカルシステムによって使用されます。ポート 80 は Storage Gateway アプライアンスのアクティベーション時にのみ使用されます。Storage Gateway

ネットワーク要素	From	To	プロトコル	ポート	インバウンド	アウトバウンド	必須	メモ
								VM には、ポート 80 へのパブリックアクセスは不要です。ポート 80 へのアクセスに必要なレベルはネットワークの設定によって決まります。Storage Gateway マネジメントコンソールからゲートウェイをアクティ

ネットワーク要素	From	To	プロトコル	ポート	インバウンド	アウトバウンド	必須	メモ
								ブ化する場合、コンソールに接続するホストはゲートウェイのポート 80 にアクセスできる必要があります。
ウェブブラウザ	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓	AWS マネジメントコンソール (その他すべてのオペレーション)

ネットワーク要素	From	To	プロトコル	ポート	インバウンド	アウトバウンド	必須	メモ
DNS	Storage Gateway VM	ドメインネームサービス (DNS) サーバー	TCP および UDP DNS	53	✓	✓	✓	IP 名解決のために Storage Gateway VM と DNS サーバー間の通信に使用されます。

ネットワーク要素	From	To	プロトコル	ポート	インバウンド	アウトバウンド	必須	メモ
NTP	Storage Gateway VM	Network Time Protocol (NTP) サーバー	TCP および UDP NTP	123	✓	✓	✓	VM 時間をホスト時間に同期するためにオンプレミスシステムで使用されます。Storage Gateway VM は、以下の NTP サーバーを使用するように設定されています。 • 0.amazon.pool.ntp.org

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

ネットワーク要素	From	To	プロトコル	ポート	インバウンド	アウトバウンド	必須	メモ
								りません。

ネットワーク要素	From	To	プロトコル	ポート	インバウンド	アウトバウンド	必須	メモ
Storage Gateway	Storage Gateway VM	サポート エンドポイント	TCP SSH	22	✓	✓	✓	サポート ゲートウェイの問題のトラブルシューティングに役立つゲートウェイへのアクセスを に許可します。このポートは、ゲートウェイの通常のオペレーションでは開いておく必要はありませんが、トラブル

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

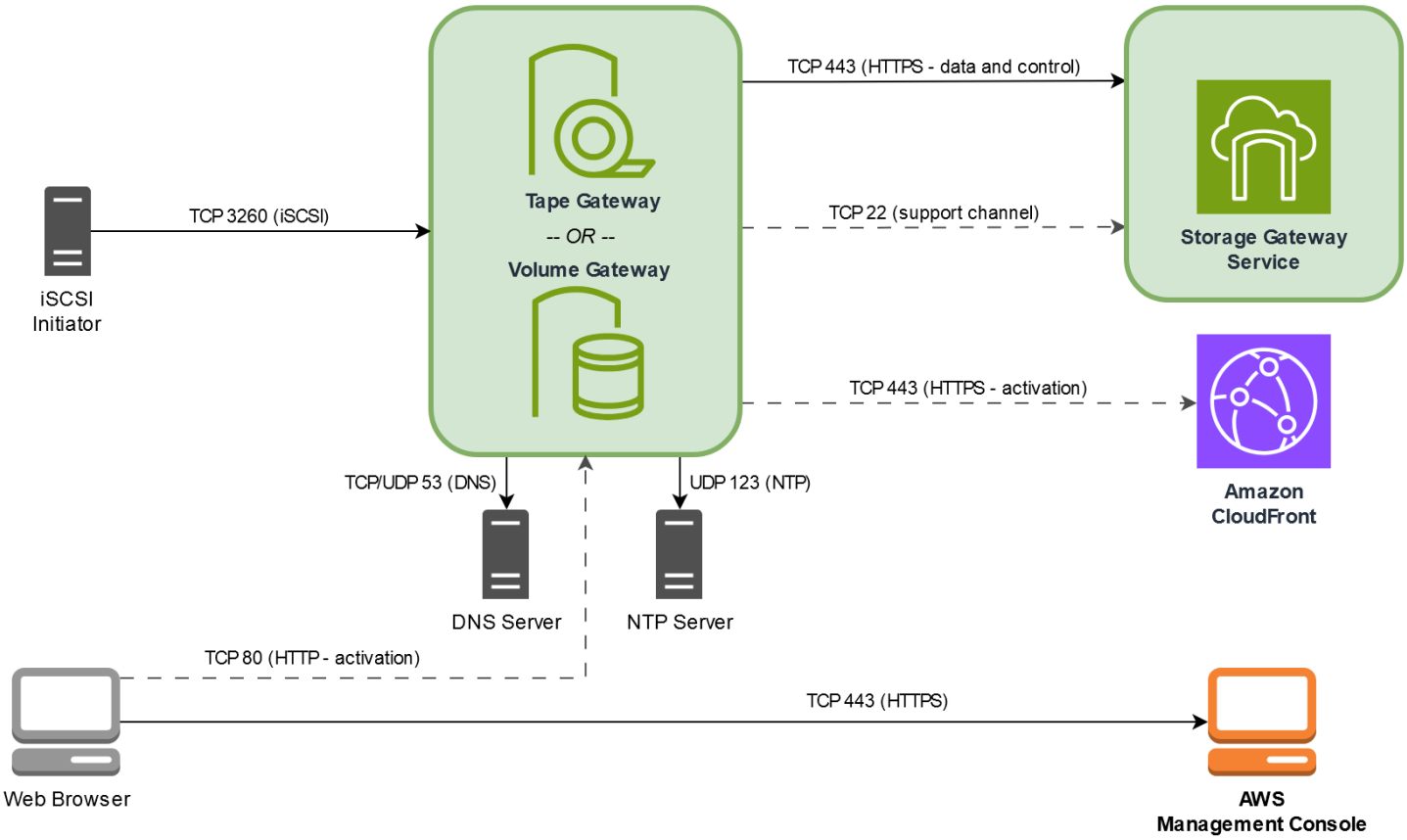
ネットワーク要素	From	To	プロトコル	ポート	インバウンド	アウトバウンド	必須	メモ
VPC	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓*	管理コントロール *VPC エンドポイントを使用する場合にのみ必須
VPC	Storage Gateway VM	AWS	TCP HTTPS	1026		✓	✓*	コントロールプレーンエンドポイント *VPC エンドポイントを使用する場合にのみ必須

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

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

ネットワーク要素	From	To	プロトコル	ポート	インバウンド	アウトバウンド	必須	メモ
VPC	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓*	管理コントロール *VPC エンドポイントを使用する場合にのみ必須
iSCSI クライアント	iSCSI クライアント	Storage Gateway VM	TCP	3260	✓	✓	✓	ローカルシステムがゲートウェイによって公開されている iSCSI ターゲットに接続できるようにするため。

次の図は、基本的なボリュームゲートウェイのデプロイのネットワークトラフィックフローを示しています。



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

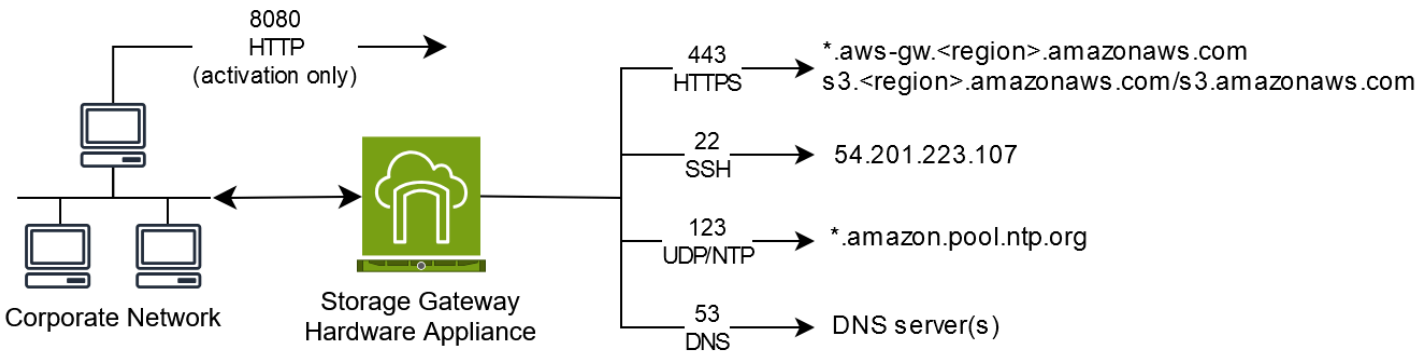
それぞれの Storage Gateway ハードウェアアプライアンスには、以下のネットワークサービスが必要です。

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

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

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

iDRAC ポートをリモートサーバー管理に使用できます。



ハードウェアアプライアンスでは、以下のポートの操作が必要です。

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

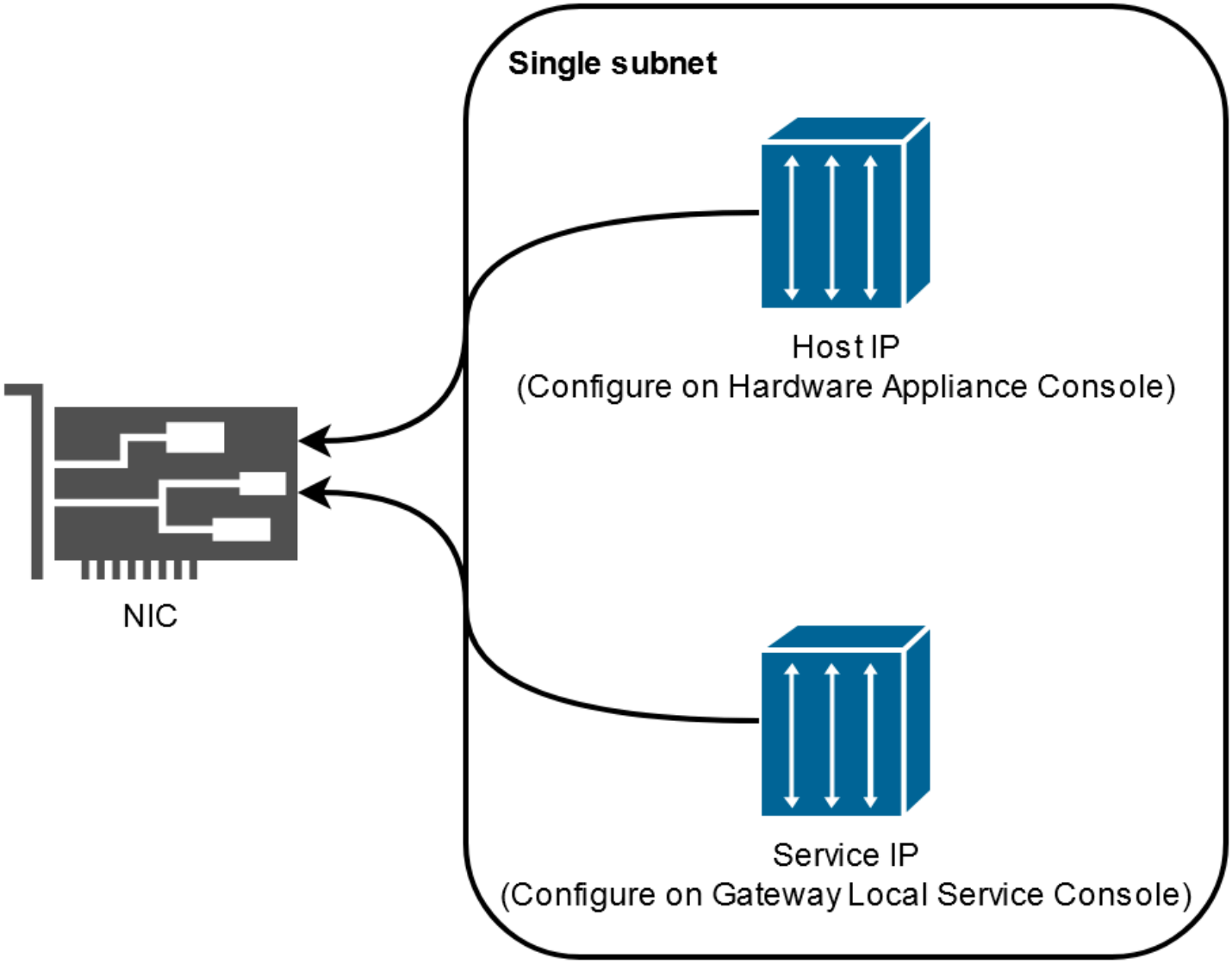
プロトコル	ポート	[Direction] (方向)	ソース	デスティネーション	用途
HTTP	8080	インバウンド	AWS	ハードウェアアプライアンス	アクティベーション (短時間のみ)

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、「ハードウェアアプライアンスのネットワークパラメータの設定」を参照してください。

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

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、Storage Gateway ハードウェアアプライアンスの使用 を参照してください。

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

ゲートウェイは、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に対し AWSへのアウトバウンド通信を許可するように、対象のファイアウォールおよびルーターを設定する必要があります。

> **Note**
>
> Storage Gateway との接続とデータ転送に使用するようにプライベート VPC エンドポイントを設定する場合 AWS、ゲートウェイはパブリックインターネットにアクセスする必要はありません。詳細については、「仮想プライベートクラウドでのゲートウェイのアクティブ化」を参照してください。

> **Important**
>
> ゲートウェイの AWS リージョンに応じて、サービスエンドポイントの*#####*を正しいリージョン文字列に置き換えます。

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

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

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

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

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

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

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

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

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

Amazon EC2 ゲートウェイインスタンスでのセキュリティグループの設定

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

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

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

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

ゲートウェイで開くポートについては、「ポート要件」を参照してください。

サポートされているハイパーバイザーとホストの要件

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

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

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

- VMware ESXi Hypervisor (バージョン 7.0 または 8.0) – このセットアップには、ホストに接続するための VMware vSphere クライアントも必要です。
- Microsoft Hyper-V Hypervisor (バージョン 2012 R2、2016、2019、または 2022) – Hyper-V の無料スタンドアロン版を Microsoft Download Center から入手できます。このセットアップでは、ホストに接続する Microsoft Windows クライアントコンピュータには Microsoft Hyper-V Manager が必要になります。
- Linux カーネルベースの仮想マシン (KVM) – これは無料のオープンソースの仮想化テクノロジーです。KVM は、Linux バージョン 2.6.20 以降のすべてのバージョンに同梱されています。Storage Gateway は、CentOS/RHEL 7.7、Ubuntu 16.04 LTS、および Ubuntu 18.04 LTS の各ディストリビューションでテストされ動作が確認されています。他の最新の Linux ディストリビューションは動作しますが、機能やパフォーマンスは保証されません。既に KVM 環境が稼働しており、KVM の仕組みに精通している場合は、このオプションをお勧めします。
- Amazon EC2 インスタンス – Storage Gateway では、ゲートウェイ の VM イメージを含む Amazon マシンイメージ (AMI) を提供します。Amazon EC2 に対してはファイル、キャッシュ型ボリューム、テープゲートウェイのテープのみがデプロイ可能です。Amazon EC2 にゲートウェイをデプロイする方法については、「ボリュームゲートウェイ用にカスタマイズされた Amazon EC2 インスタンスをデプロイする」を参照してください。
- Storage Gateway ハードウェアアプライアンス – Storage Gateway では、仮想マシンによるインフラストラクチャが制限されている場所のためのオンプレミス用デプロイオプションとして、物理ハードウェアアプライアンスが提供されています。

> **Note**
>
> Storage Gateway では、スナップショットから作成された VM、または別のゲートウェイ VM のクローン、または Amazon EC2 AMI からのゲートウェイの復元はサポートされていません。ゲートウェイ VM が正しく機能しない場合は、新しいゲートウェイをアクティブ化し、データをそのゲートウェイに復旧します。詳細については、「予期しない仮想マシンのシャットダウンからの復旧」を参照してください。
> Storage Gateway は動的メモリと仮想メモリのバルーニングをサポートしていません。

サポートされている iSCSI イニシエータ

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

これらの iSCSI デバイスに接続するために、Storage Gateway では、以下の iSCSI イニシエータがサポートされています。

- Microsoft Windows Server 2022
- Red Hat Enterprise Linux 8
- Red Hat Enterprise Linux 9
- VM のゲストオペレーティングシステムでのイニシエータの使用に代わる、VMware ESX イニシエータ

> **Important**
>
> Storage Gateway では、Windows クライアントからの Microsoft Multipath I/O (MPIO) はサポートされていません。
> ホストが Windows Server Failover Clustering (WSFC) を使用してアクセスを調整する場合には、Storage Gatewayによる同じボリューム内の複数のホストへの接続がサポートされます。ただし、WSFC を使用せずに複数のホストを同じボリュームに接続すること (非クラスター NTFS/ext4 ファイルシステムの共有など) はできません。

Storage Gateway ハードウェアアプライアンスの使用

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

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

ハードウェアアプライアンスは、高性能な 1U サーバであり、データセンターや、企業ファイアウォール内のオンプレミス環境でデプロイすることができます。ハードウェアアプライアンスを購入してアクティブ化を行うと、アクティブ化プロセスによって、ハードウェアアプライアンスは AWS アカウントに関連付けられます。アクティブ化が完了すると、ハードウェアアプライアンスはコンソールの [ハードウェアアプライアンスの概要] ページに表示されます。ハードウェアアプライアンスは、S3 ファイルゲートウェイ、FSx ファイルゲートウェイ、テープゲートウェイ、またはボリュームゲートウェイタイプとして設定できます。ハードウェアアプライアンスでこれらのゲートウェイタイプをデプロイする手順は、仮想プラットフォームでの手順と同じです。

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

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

トピック

- Storage Gateway ハードウェアアプライアンスのセットアップ
- ハードウェアアプライアンスの物理的なインストール
- ハードウェアアプライアンスコンソールへのアクセス

- ハードウェアアプライアンスのネットワークパラメータの設定
- Storage Gateway ハードウェアアプライアンスのアクティブ化
- ハードウェアアプライアンスでゲートウェイを作成する
- ハードウェアアプライアンスのゲートウェイ IP アドレスの設定
- ハードウェアアプライアンスからゲートウェイソフトウェアを削除する
- Storage Gateway ハードウェアアプライアンスの削除

Storage Gateway ハードウェアアプライアンスのセットアップ

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

Storage Gateway ハードウェアアプライアンスを受け取ったら、ハードウェアアプライアンスのローカルコンソールを使用して、 への常時オン接続を提供し AWS 、アプライアンスをアクティブ化するようにネットワークを設定します。アクティベーションは、アプライアンスをアクティベーションプロセス中に使用される AWS アカウントと関連付けます。アプライアンスをアクティブ化した後は、Storage Gateway コンソールから、S3 File Gateway、FSx File Gateway、テープゲートウェイ、またはボリュームゲートウェイを起動できます。

ハードウェアアプライアンスをインストールして設定するには

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

4. ハードウェアアプライアンスでゲートウェイを作成します。詳細については、「ボリュームゲートウェイの作成」を参照してください。

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

使用可能なキャッシュストレージの増加

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

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

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

ネットワークインターフェイスカードのオプション

注文したアプライアンスのモデルによっては、10G-Base-T RJ45 銅線または 10G DA/SFP+ ネットワークカードが付属している場合があります。

- 10G-Base-T NIC の構成:
  - 10G には CAT6 のケーブルを使用し、1G には CAT5(e) を使用
- 10G DA/SFP+ NIC の構成:
  - 最長 5 メートルの、Twinax 銅線ダイレクトアタッチケーブルを使用
  - デル/インテル互換の SFP+ 光モジュール (SR または LR)
  - 1G-Base-T または 10G-Base-T 向け SFP/SFP+ 銅線トランシーバ

ハードウェアアプライアンスの物理的なインストール

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

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

前提条件

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

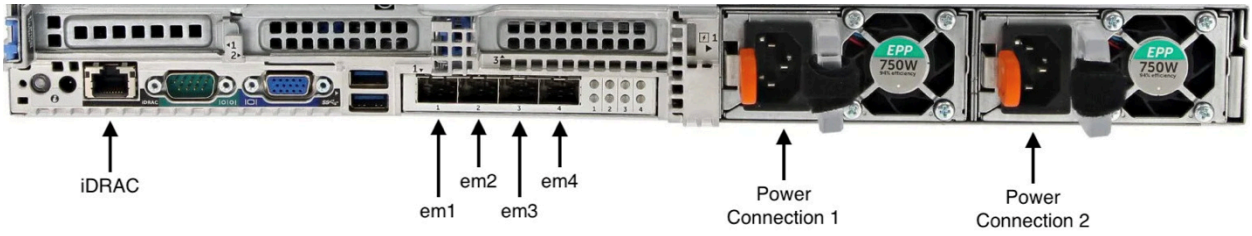
- 電源ケーブル: 1 つは必須です。2 つを推奨します。
- サポートされているネットワークケーブル (ハードウェアアプライアンスに組み込まれているネットワークインターフェイスカード (NIC) によって異なります)。Twinax 銅線 DAC、SFP+ 光モジュール (インテル互換)、または Base-T 向け SFP 銅線トランシーバ。
- キーボードとモニター、またはキーボード、ビデオ、マウス (KVM) スイッチソリューション。

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

ハードウェアアプライアンスを物理的にインストールするには

1. ハードウェアアプライアンスを開梱し、同梱されている指示に従いサーバーをラックにマウントします。

次の図は、電源、イーサネット、モニター、USB キーボード、iDRAC を接続するためのポートを備えたハードウェアアプライアンスの背面を示しています。
ハードウェアアプライアンス 1 の背面。ネットワークや電源のコネクタのラベルが表示されています。

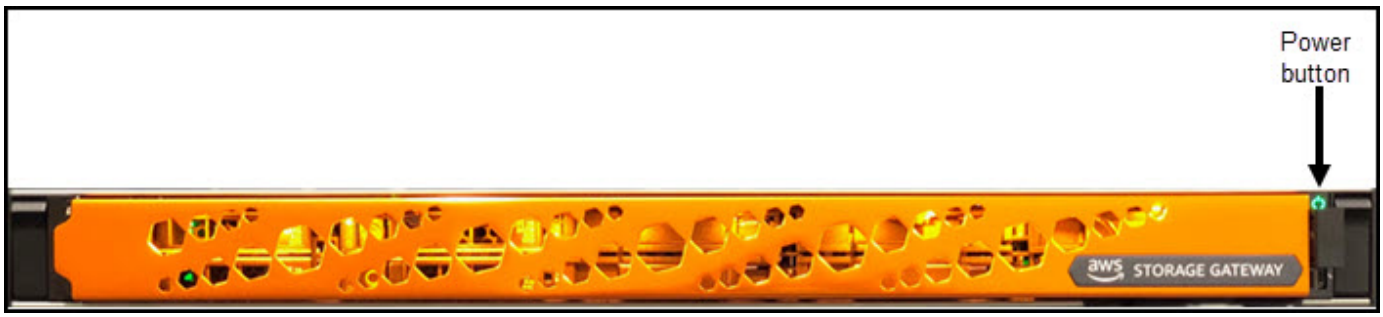


ハードウェアアプライアンス 1 の背面。ネットワークや電源のコネクタのラベルが表示されています。

2. 2 つの電源装置のそれぞれに電源を接続します。1 つの電源接続のみを使用することも可能ですが、冗長性を確保するために両方の電源への接続を推奨します。
3. イーサネットケーブルを em1 ポートに接続し、インターネットの常時接続を提供します。em1 ポートは、背面で左から右に並ぶ 4 つの物理ネットワークポートの 1 つめのポートです。

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

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



ハードウェアアプライアンスの前面。電源ボタンのラベルが表示されています。

次のステップ

ハードウェアアプライアンスコンソールへのアクセス

ハードウェアアプライアンスコンソールへのアクセス

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

ハードウェアアプライアンスの電源を入れると、ハードウェアアプライアンスコンソールがモニタに表示されます。ハードウェアアプライアンスコンソールには、管理者パスワードの設定、初期ネットワークパラメータの設定、サポートチャネルのオープン AWS に使用できる 固有のユーザーインターフェイスが表示されます AWS。

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

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

管理者パスワードを設定するには

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

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

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

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

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

次のステップ

ハードウェアアプライアンスのネットワークパラメータの設定

ハードウェアアプライアンスのネットワークパラメータの設定

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

ハードウェアアプライアンスが起動し、「ハードウェアアプライアンスコンソールへのアクセス」の説明に従ってハードウェアコンソールで管理者ユーザーのパスワードを設定したら、次の手順を使用してネットワークパラメータを設定して、ハードウェアアプライアンスが AWSに接続できるようにします。

ネットワークアドレスを設定するには

1. [ホーム] ページから、[ネットワークを設定] を選択し、Enter を押します。[ネットワークを設定] ページが表示されます。[ネットワークを設定] ページには、ハードウェアアプライアンス上の 4 つのネットワークインターフェイスの IP と DNS 情報が表示され、それぞれに [DHCP] または [静的] アドレスを設定するメニューオプションが含まれています。

2. [em1] インターフェイス内で、次のいずれかを実行します。

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

     このアドレスを記録し、それを後のアクティベーション手順で使用します。

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

     [em1] ネットワークインターフェイスの有効な [IP アドレス]、[サブネットマスク]、[ゲートウェイ]、[DNS] サーバーアドレスを入力します。

     完了したら、[保存] を選択し、Enter を押して設定を保存します。

> **Note**
>
> この手順を使用して、[em1] に加えて他のネットワークインターフェイスを設定できます。他のインターフェイスを設定する場合は、要件に記載されている AWS エンドポイントへの同じ常時オン接続を提供する必要があります。
> ネットワークボンディングと Link Aggregation Control Protocol (LACP) は、ハードウェアアプライアンスまたは Storage Gateway ではサポートされていません。
> ルーティングの問題が発生する可能性があるため、同じサブネットに複数のネットワークインターフェイスを設定することはお勧めしません。

ハードウェアコンソールからログアウトするには

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

次のステップ

Storage Gateway ハードウェアアプライアンスのアクティブ化

Storage Gateway ハードウェアアプライアンスのアクティブ化

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

IP アドレスを設定したら、 AWS Storage Gateway コンソールのハードウェアページにこの IP アドレスを入力して、ハードウェアアプライアンスをアクティブ化します。アクティベーションプロセスは、アプライアンスを AWS アカウントに登録します。

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

ストレージゲートウェイハードウェアアプライアンスをアクティブ化するには

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

   > **Note**
   >
   > アクティベーションを行う場合のみは、次の条件が満たされている必要があります。
   >
   > - ブラウザは、ハードウェアアプライアンスと同じネットワーク上になければなりません。
   > - ファイアウォールは、アプライアンスへインバウンドトラフィックのためのポート 8080 への HTTP アクセスを許可する必要があります。

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

IP アドレス設定の詳細については、「ネットワークパラメータの設定」を参照してください。

5. [名前] に、ハードウェアアプライアンスの名前を入力します。255 文字以内で名前を指定します。スラッシュ文字を含むことはできません。
6. [ハードウェアアプライアンスのタイムゾーン] には、ゲートウェイのほとんどのワークロードが生成されるローカルタイムゾーンを入力し、[次へ] を選択します。

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

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

これで、アプライアンスはアカウントに関連付けられました。次のステップは、新しいアプライアンスで S3 File Gateway、FSx File Gateway、テープゲートウェイ、またはボリュームゲートウェイを設定して起動することです。

次のステップ

ハードウェアアプライアンスでゲートウェイを作成する

ハードウェアアプライアンスでゲートウェイを作成する

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

デプロイ内の任意の Storage Gateway ハードウェアアプライアンスに、S3 ファイルゲートウェイ、FSx ファイルゲートウェイ、テープゲートウェイ、またはボリュームゲートウェイを作成できます。

ハードウェアアプライアンスでゲートウェイを作成するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/storagegateway/home で Storage Gateway コンソールを開きます。
2. 「ゲートウェイを作成する」で説明されている手順に従って、デプロイする Storage Gateway のタイプをセットアップ、接続、設定します。

Storage Gateway コンソールでゲートウェイを作成し終わると、ハードウェアアプライアンスへの Storage Gateway ソフトウェアのインストールが自動的に開始します。動的ホスト設定プロトコル (DHCP) を使用する場合、ゲートウェイがコンソールでオンラインとして表示されるまでに 5～10 分かかることがあります。インストールされたゲートウェイに静的 IP アドレスを割り当てるには、「ゲートウェイの IP アドレスの設定」を参照してください。

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

次のステップ

ハードウェアアプライアンスのゲートウェイ IP アドレスの設定

ハードウェアアプライアンスのゲートウェイ IP アドレスの設定

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

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

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

1. ハードウェアコンソールで、[オープンサービスコンソール] を選択し、`Enter` を押して、ゲートウェイのローカルコンソールのログインページを開きます。
2. AWS Storage Gateway ローカルコンソールのログインページでは、ログインしてネットワーク設定やその他の設定を変更するように求められます。

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

   > **Note**
   >
   > デフォルトのパスワードは変更することを推奨します。変更するには、[AWS Appliance Activation - Configuration] メインメニューで [Gateway Console] に対応する番号を入力し、`passwd` コマンドを実行してください。このコマンドを実行する方法については、「オンプレミスゲートウェイの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、「Storage Gateway コンソールからのローカルコンソールパスワードの設定」を参照してください。

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

   - HTTP/SOCKS プロキシ設定
   - ネットワーク構成
   - ネットワーク接続のテスト
   - システムリソースチェックの表示
   - システム時刻の管理

- ライセンス情報
- コマンドプロント

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

対応する番号を入力して [ネットワーク構成] を選択します。

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

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

     > **Note**
     >
     > ここで指定する IP アドレスは、ハードウェアアプライアンスのアクティベーション中に使用された IP アドレスと同じサブネット上になければなりません。

ゲートウェイのローカルコンソールを終了するには

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

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

ハードウェアアプライアンスのアクティベーションと設定が行われると、アプライアンスがコンソールに表示されます。これで、Storage Gateway コンソールでゲートウェイのセットアップと設定手順を続行できます。手順については、「」を参照してください。

ハードウェアアプライアンスからゲートウェイソフトウェアを削除する

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

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

ハードウェアアプライアンスからゲートウェイを削除するには

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. コンソールページの左側にあるナビゲーションペインから [ハードウェア] を選択し、ゲートウェイソフトウェアを削除する [アプライアンスのハードウェアアプライアンス名] を選択します。
3. [アクション] ドロップダウンメニューから、[ゲートウェイを削除] を選択します。

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

   > **Note**
   >
   > ゲートウェイソフトウェアを削除した後で、その操作を元に戻すことはできません。特定のゲートウェイタイプでは、削除されたデータ、特にキャッシュされたデータが失わ

れる場合があります。ゲートウェイの削除の詳細については、「ゲートウェイおよび関連リソースの削除」を参照してください。

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

Storage Gateway ハードウェアアプライアンスの削除

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

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

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

ハードウェアアプライアンスを削除するには

1. ゲートウェイをハードウェアアプライアンスにインストールしている場合は、アプライアンスを削除する前に、まずゲートウェイを削除する必要があります。ハードウェアアプライアンスからゲートウェイを削除する方法については、「ハードウェアアプライアンスからゲートウェイソフトウェアを削除する」を参照してください。

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

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

ゲートウェイを作成する

このページの概要セクションでは、Storage Gateway の作成プロセスがどのように機能するかについて概説しています。Storage Gateway コンソールを使用して特定のタイプのゲートウェイを作成する手順については、以下のトピックを参照してください。

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

> **Important**
>
> 新規のお客様への Amazon FSx File Gateway の提供は終了しました。FSx File Gateway の既存のお客様は、通常どおりサービスを引き続き使用できます。FSx File Gateway に似た機能については、このブログ記事を参照してください。

概要 - ゲートウェイのアクティブ化

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

ゲートウェイをセットアップする

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

に接続する AWS

次のステップでは、ゲートウェイを AWSに接続します。これを行うには、まずゲートウェイ仮想アプライアンスとクラウド内のサービス間の通信に使用する AWS サービスエンドポイントのタイプを

選択します。このエンドポイントには、パブリックインターネットからアクセスできます。または、ネットワークのセキュリティ設定を完全に制御できる Amazon VPC 内からのみアクセスできます。次に、ゲートウェイの IP アドレスまたはアクティベーションキーを指定します。これらは、ゲートウェイアプライアンスのローカルコンソールに接続することで取得できます。

確認してアクティブ化する

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

概要 - ゲートウェイの設定

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

概要 - ストレージリソース

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

ボリュームゲートウェイの作成

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

トピック

- ボリュームゲートウェイをセットアップする

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

ボリュームゲートウェイをセットアップする

新しいボリュームゲートウェイをセットアップするには

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

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

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

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

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

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

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

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

6. [Next] (次へ) をクリックして先に進みます。

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

ボリュームゲートウェイを AWSに接続する

新しいボリュームゲートウェイを に接続するには AWS

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

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

   > **Note**
   >
   > コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-2 検証済み暗号化モジュールが必要な場合は、FIPS 準拠のエンドポイントを使用します。詳細については、連邦情報処理規格 (FIPS) 140-2 を参照してください。

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

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

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

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

     ゲートウェイの IP アドレスは、ハイパーバイザークライアントからゲートウェイのローカルコンソールにログインするか、Amazon EC2 インスタンスの詳細ページからコピーすることで取得できます。
   - アクティベーションキー - ゲートウェイのアクティベーションキーを、対応するフィールドに入力します。アクティベーションキーは、ゲートウェイのローカルコンソールを使用して生成できます。ゲートウェイの IP アドレスを使用できない場合は、このオプションを選択してください。

4. [Next] (次へ) をクリックして先に進みます。

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

設定を確認してボリュームゲートウェイをアクティブ化する

新しいボリュームゲートウェイをアクティブ化するには

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

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

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

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

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

4. [アクティブゲートウェイ] を選択して、先に進みます。

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

ボリュームゲートウェイを設定する

新しいボリュームゲートウェイで初回の設定を行うには

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

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

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

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

3. [CloudWatch ロググループ] セクションで、ゲートウェイの状態をモニタリングするための Amazon CloudWatch Logs の設定方法を選択します。次のオプションから選択できます。

   - 新しいロググループの作成 - ゲートウェイをモニタリングするための新しいロググループを設定します。
   - 既存のロググループの使用 - 対応するドロップダウンメニューから既存のロググループを選択します。
   - ログ記録の非アクティブ化 - ゲートウェイのモニタリングに Amazon CloudWatch Logs を使用しません。

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

4. [CloudWatch アラーム] セクションで、定義されている制限からゲートウェイのメトリクスが逸脱したときに通知する Amazon CloudWatch アラームの設定方法を選択します。次のオプションから選択できます。

- Storage Gateway の推奨アラームを作成 — ゲートウェイの作成時に、CloudWatch の推奨アラームをすべて自動的に作成します。推奨アラームの詳細については、「CloudWatch アラームの説明」を参照してください。

  > **Note**
  >
  > この機能を使用するには、CloudWatch ポリシーのアクセス権限が必要です。この権限は、事前設定済みの Storage Gateway のフルアクセスポリシーの一部として自動的に付与されるものではありません。CloudWatch の推奨アラームを作成する前に、セキュリティポリシーで次のアクセス権限が付与されていることを確認してください。
  >
  > - `cloudwatch:PutMetricAlarm` - アラームを作成する
  > - `cloudwatch:DisableAlarmActions` - アラームアクションをオフにする
  > - `cloudwatch:EnableAlarmActions` - アラームアクションをオンにする
  > - `cloudwatch:DeleteAlarms` - アラームを削除する

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

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

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

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

ストレージボリュームの作成

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

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

ボリュームを作成するには

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

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

   キャッシュ型ボリュームの場合、次のオプションがあります:

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

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

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

保管型ボリュームの場合、次のオプションがあります。

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

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

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

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

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

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

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

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

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

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

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

ボリューム用の CHAP 認証の設定

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

CHAP を設定するには

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

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

次のステップ

クライアントへのボリュームの接続

クライアントへのボリュームの接続

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

> **Important**
>
> Storage Gateway では、ホストが Windows Server Failover Clustering (WSFC) を使用してアクセスを調整する場合、複数のホストを同じボリュームに接続できます。WSFC を使用せずに (たとえば、非クラスター NTFS/ext4 ファイルシステムを共有して) 複数のホストを同じボリュームに接続することはできません。

トピック

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

Microsoft Windows クライアントへの接続

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

Windows クライアントに接続するには

1. iscsicpl.exe を開始します。
2. [iSCSI Initiator Properties (iSCSI イニシエータのプロパティ)] ダイアログボックスで、[検出] タブを選択し、[Discovery Portal (検出ポータル)] を選択します。
3. [Discover Target Portal (ターゲットポータルの検出)] ダイアログボックスで、IP アドレスまたは DNS 名の iSCSI ターゲットの IP アドレスを入力します。

4. ゲートウェイのストレージボリュームターゲットに新しいターゲットポータルを接続します。
5. ターゲットを選択し、[接続] を選択します。
6. [ターゲット] タブで、ターゲットのステータスが、ターゲットが接続されていることを示す値 [Connected (接続済み)] であることを確認し、[OK] を選択します。

Red Hat Enterprise Linux クライアントへの接続

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

Linux クライアントを iSCSI ターゲットに接続するには

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

   パッケージをインストールするには、以下のコマンドを使用できます。

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

2. iSCSI デーモンが実行していることを確認します。

   RHEL 5 または 6 を使用している場合は、次のコマンドを使用します。

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

   RHEL 7、8 または 9 を使用している場合は、次のコマンドを使用します。

   ```
   sudo service iscsid status
   ```

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

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

   discovery コマンドの出力は、次の出力例のようになります。

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

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

4. ターゲットに接続します。

   connect コマンドには、正しい *[GATEWAY_IP]* と IQN を指定する必要があります。

   以下のコマンドを使用します。

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

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

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

   コマンドの出力は、次の出力例のようになります。

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

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

ボリュームの初期化とフォーマット

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

トピック

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

Microsoft Windows でのボリュームの初期化とフォーマット

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

ストレージボリュームを初期化してフォーマットするには

1. **diskmgmt.msc** を起動し、[Disk Management] コンソールを開きます。

2. [Initialize Disk] ダイアログボックスで、[MBR (Master Boot Record)] パーティションの形式でボリュームを初期化します。パーティションの形式を選択する場合、接続先のボリュームのタイプ (キャッシュ型または保管型) を、次の表のように考慮する必要があります。

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

3. シンプルボリュームの作成

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

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

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

   c. 最大ディスクサイズを指定します。

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

   > **Important**
   >
   > キャッシュボリュームには [クリックフォーマットする] を使用することを強くお勧めします。これにより、初期化 I/O と初期スナップショットサイズが小さくなり、

使用可能なボリュームへの時間が最も高速になります。また、キャッシュボリュームスペースを使用したフルフォーマット処理を回避できます。

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

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

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

ストレージボリュームを初期化してフォーマットするには

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

   ```
   $ lsblk
   ```

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

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

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

MBR パーティションでは、次のコマンドを使用します: `sudo parted /dev/your volume mklabel msdos`

GPT パーティションでは、次のコマンドを使用します: `sudo parted /dev/your volume mklabel gpt`

5. パーティションを作成するには、次のコマンドを使用します。

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

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

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

7. 次のコマンドを使用して、ファイルシステムをマウントします。

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

ゲートウェイのテスト

次のタスクを実行して、ボリュームゲートウェイの設定をテストします。

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

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

> **Note**
>
> 暗号化された Amazon Elastic Block Store (Amazon EBS) ボリュームからデータを復元することはできません。

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

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

   この演習では、コピーするデータ量は問題ではありません。小さなファイルで十分に復元を確認することができます。
2. Storage Gateway コンソールのナビゲーションペインで、[Volumes] (ボリューム) を選択します。
3. ゲートウェイ用に作成したストレージボリュームを選択します。

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

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

スナップショットを別ボリュームに復元するには

「ストレージボリュームの作成」を参照してください。

ボリュームのバックアップ

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

トピック

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

Storage Gateway を使用してボリュームをバックアップする

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

- ゲートウェイのテスト
- 復旧スナップショットの作成
- 復旧ポイントからキャッシュされたボリュームのクローン

AWS Backup を使用してボリュームをバックアップする

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

- バックアップする AWS リソースを設定して監査します。
- バックアップスケジュールのオートメーション。
- 保持ポリシーの設定。
- 最近のすべてのバックアップと復元アクティビティのモニタリング。

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

AWS Backup では、Storage Gateway ボリュームのバックアップおよび復元オペレーションを管理できます。カスタムスクリプトを作成したり、ポイントインタイムのバックアップを手動で管理する必要はありません。を使用すると AWS Backup、1 つの AWS Backup ダッシュボードからクラウド内 AWS リソースとともにオンプレミスボリュームのバックアップをモニタリングすることもできます。 AWS Backup を使用して、1 回限りのオンデマンドバックアップを作成するか、 で管理されるバックアッププランを定義できます AWS Backup。

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

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

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

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

- バックアップ要件を満たすカスタマイズ可能なバックアップポリシーのスケジュールを設定します。
- バックアップ保持期間および有効期限切れルールを設定することで、ボリュームの特定時点におけるバックアップを手動で管理する必要がなくなります。

- 複数のゲートウェイ、およびその他の AWS リソース間のバックアップを一元的に管理およびモニタリングします。

AWS Backup を使用してボリュームのバックアップを作成するには

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

1. Storage Gateway コンソールを開き、左のナビゲーションペインから [Volumes] (ボリューム) を選択します。
2. アクション で、 でオンデマンドバックアップを作成する AWS Backup または AWS バックアッププランを作成する を選択します。

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

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

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

AWS Backupからボリュームを検索して復元する

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

ボリュームを見つけて復元するには

1. AWS Backup コンソールを開き、復元する Storage Gateway ボリュームのバックアップを見つけます。Storage Gateway ボリュームのバックアップは、Amazon EBS ボリュームまたは Storage Gateway ボリュームに復元できます。復元要件に適したオプションを選択します。
2. [Restore type] (復元の種類) で、保存済みあるいはキャッシュ済みの Storage Gateway ボリュームを復元し、必要な情報を入力します。
   - 保存済みのボリュームでは、[ゲートウェイ名]、[ディスク ID]、[iSCSI ターゲット名] に関する情報を入力します。
   - キャッシュ済みのボリュームでは、[ゲートウェイ名]、[容量]、[iSCSI ターゲット名] に関する情報を入力します。
3. [Restore resource (リソースの復元)] を選択してボリュームを復元します。

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

次のステップ

前のセクションでは、ゲートウェイの作成とプロビジョニングを行い、ホストをゲートウェイのストレージボリュームに接続しました。また、ゲートウェイの iSCSI ボリュームへのデータの追加、ボリュームのスナップショットの作成、新しいボリュームへのスナップショットの復元、新しいボリュームへの接続、ボリュームのデータが表示されることの確認を行いました。

演習を終了したら、以下の点を考慮します。

- ゲートウェイを引き続き使用するのであれば、実際のワークロードに合わせてアップロードバッファのサイズを設定します。詳細については、「実際のワークロードに対する、ボリュームゲートウェイストレージのサイズ設定」を参照してください。

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

- ストレージボリュームとその管理方法の詳細については、「ボリュームゲートウェイの管理」を参照してください。

- ゲートウェイを引き続き使用する予定がないのであれば、料金が発生しないようにするために、ゲートウェイを削除することを検討します。詳細については、「不要なリソースのクリーンアップ」を参照してください。
- ゲートウェイの問題をトラブルシューティングする方法については、「ゲートウェイのトラブルシューティング」を参照してください。
- ゲートウェイを最適化するには、「ゲートウェイのパフォーマンスの最適化」を参照してください。
- Storage Gateway メトリクスの概要と、ゲートウェイの動作のモニタリング方法については、「Storage Gateway のモニタリング」を参照してください。
- データを保存するためのゲートウェイの iSCSI ターゲットの設定については、「Windows クライアントからボリュームへの接続」を参照してください。

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

実際のワークロードに対する、ボリュームゲートウェイストレージのサイズ設定

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

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

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

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

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

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

保管型のセットアップに対して、アップロードバッファのサイズを設定するには

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

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

アップロードバッファを監視するには

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

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

仮想プライベートクラウドでのゲートウェイのアクティブ化

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

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

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

トピック

- Storage Gateway 用の VPC エンドポイントの作成

Storage Gateway 用の VPC エンドポイントの作成

これらの手順に従って、VPC エンドポイントを作成します。Storage Gateway 用に VPC エンドポイントがすでに用意されている場合には、そのエンドポイントを使用してゲートウェイをアクティブ化できます。

Storage Gateway 用の VPC エンドポイントを作成するには

1. にサインイン AWS Management Console し、Amazon VPC コンソールを https://console.aws.amazon.com/vpc/://www.com で開きます。
2. ナビゲーションペインで [エンドポイント] を選択し、[Create endpoint (エンドポイントの作成)] を選択します。

3. [エンドポイントの作成] ページで、[サービスカテゴリ] の [AWS サービス] を選択します。
4. [Service Name] (サービス名)には `com.amazonaws.region.storagegateway` を選択します。たとえば、 です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. 選択したストレージゲートウェイエンドポイントの [詳細] タブの [DNS 名] で、アベイラビリティーゾーン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。詳細については、「ゲートウェイを作成する」を参照してください。

ボリュームゲートウェイの管理

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

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

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

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

キャッシュ型ボリュームの全データとスナップショットデータは、サーバーサイド暗号化 (SSE) 機能を使用して Amazon S3に保管されます。ただし、このデータには Amazon S3 API や、他のツール (Amazon S3 マネジメントコンソールなど) を使用してアクセスすることはできません。

以下は、ボリュームゲートウェイリソースを管理する方法についての情報です。

トピック

- 基本的なゲートウェイ情報の編集 - Storage Gateway コンソールを使用して、ゲートウェイ名、タイムゾーン、CloudWatch ロググループなどを含む、既存のゲートウェイの基本情報を編集する方法について説明します。
- ボリュームの追加と拡大 - ゲートウェイにボリュームを追加する方法、またはアプリケーションのニーズが大きくなるにつれて既存のボリュームのサイズを拡大する方法について説明します。
- 復旧ポイントからキャッシュされたボリュームのクローン - 既存のボリュームの復旧ポイントから新しいボリュームを作成する方法について説明します。復旧ポイントは、ボリュームのすべてのデータが一貫しているときに保存されるポイントです。
- ボリュームの使用量の表示 - Storage Gateway コンソールを使用して、ボリュームに保存されているデータ量を表示する方法について説明します。
- ストレージボリュームの削除 - より大きなストレージボリュームを使用するようにアプリケーションを移行する場合など、アプリケーションに変更が必要な場合にボリュームを削除する方法について説明します。
- 別のゲートウェイにボリュームを移動する - ボリュームをデタッチおよび再アタッチする方法について説明します。これは、パフォーマンスニーズの変化に応じてボリュームを別のボリュームゲートウェイに移動する必要がある場合に役立ちます。
- 復旧スナップショットの作成 - ゲートウェイのボリューム復旧ポイントから復旧スナップショットを作成する方法と、作成後に Storage Gateway コンソールでそのスナップショットを見つける方法について説明します。
- スナップショットスケジュールの編集 - スナップショットが毎日発生する時刻またはスナップショットが撮影される頻度を変更して、スナップショットスケジュールをカスタマイズする方法について説明します。
- ストレージボリュームのスナップショットの削除 - 不要になったスナップショットを削除する方法について説明します。
- ボリュームステータスと移行について - Storage Gateway が報告するさまざまなボリュームステータス値について説明します。これらの値は、ボリュームが正常に機能しているかどうか、またはユーザー側でアクションを必要とする可能性のある問題があるかどうかを判断するのに役立ちます。
- 新しいゲートウェイへのデータの移動 - データやパフォーマンスに対するニーズの増大に対応するため、またはゲートウェイを移行するための AWS 通知を受け取った場合などに、ゲートウェイ間でデータを移動する方法について説明します。

基本的なゲートウェイ情報の編集

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

既存のゲートウェイの基本情報を編集するには

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. [ゲートウェイ] を選択し、基本情報を編集するゲートウェイを選択します。
3. [アクション] ドロップダウンメニューから [ゲートウェイ情報の編集] を選択します。
4. [ゲートウェイ名] に、ゲートウェイの名前を入力します。この名前を検索して、Storage Gateway コンソールのリストページでゲートウェイを見つけることができます。

   > **Note**
   >
   > ゲートウェイ名は 2 ~ 255 文字で、スラッシュ (\ または /) を含めることはできません。
   > ゲートウェイの名前を変更すると、ゲートウェイのモニタリング用に設定された CloudWatch アラームがすべて接続解除されます。アラームを再接続するには、CloudWatch コンソールで各アラームの GatewayName を更新してください。

5. [ゲートウェイのタイムゾーン] では、ゲートウェイをデプロイしたい地域のローカルタイムゾーンを選択します。
6. [ロググループのセットアップ方法の選択] では、ゲートウェイのヘルスをモニタリングするための Amazon CloudWatch Logs の設定方法を選択します。次のオプションから選択できます。

   - 新しいロググループを作成 - ゲートウェイをモニタリングするための新しいロググループを設定します。
   - [既存のロググループの使用] - 対応するドロップダウンリストから既存のロググループを選択します。
   - ログ記録の非アクティブ化 - ゲートウェイのモニタリングに Amazon CloudWatch Logs を使用しません。

7. 変更する設定の変更が完了したら、[変更を保存] を選択します。

ボリュームの追加と拡大

アプリケーションのニーズが大きくなるにつれて、ゲートウェイにボリュームを追加したり、既存のボリュームのサイズを拡大したりする必要がある場合があります。ボリュームを追加または拡大する場合、ゲートウェイに割り当てたキャッシュストレージとアップロードバッファのサイズを考慮する必要があります。ゲートウェイには、新しいボリュームに十分なバッファとキャッシュスペースが必要です。詳細については、「割り当てるアップロードバッファのサイズの決定」を参照してください。

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

既存のボリュームのサイズは、次のいずれかの方法を使用して拡大できます。

- 拡大するボリュームのスナップショットを作成し、そのスナップショットを使用して、より大きいサイズの新しいボリュームを作成します。スナップショットの作成方法については、「復旧スナップショットの作成」を参照してください。スナップショットを使用した新しいボリュームの作成方法については、「ストレージボリュームの作成」を参照してください。
- 拡大するキャッシュ型ボリュームを使用して、より大きいサイズの新しいボリュームのクローンを作成します。ボリュームのクローン方法については、「復旧ポイントからキャッシュされたボリュームのクローン」を参照してください。ボリュームを作成する方法については、「ストレージボリュームの作成」を参照してください。

復旧ポイントからキャッシュされたボリュームのクローン

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

既存のボリュームからのクローンは、Amazon EBS スナップショットを作成するより短時間で完了でき、コスト効率にも優れています。クローン作成では、ソースボリュームの最新の復旧ポイントを使用して、ソースボリュームから新しいボリュームにデータを 1 バイトずつコピーします。Storage

Gateway は、キャッシュ型ボリュームのためにリカバリポイントを自動的に作成します。最新の復旧ポイントがいつ作成されたかは、Amazon CloudWatch の `TimeSinceLastRecoveryPoint` メトリクスで確認できます。

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

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

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

到達不可能なゲートウェイからボリュームをクローンして使用する

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

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

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

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

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

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

ボリュームの使用量の表示

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

ボリュームに書き込まれるデータ量を表示するには

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

   以下のフィールドには、ボリュームに関する情報が示されます。

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

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

ストレージボリュームの削除

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

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

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

ボリュームを削除するには

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

別のゲートウェイにボリュームを移動する

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

ボリュームのデタッチおよびアタッチすると、以下を実行できます。

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

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

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

> **Note**
>
> ボリュームのアタッチおよびデタッチにはいくつかの制限があります。
>
> - ボリュームのデタッチには長い時間がかかる場合があります。ボリュームをデタッチすると、ゲートウェイはボリューム上のすべてのデータを にアップロード AWS してから、ボリュームをデタッチします。アップロードが完了するまでにかかる時間は、アップロードする必要のあるデータ量と AWSへのネットワーク接続によって異なります。
> - キャッシュ済みのボリュームをデタッチする場合、これを保存済みのボリュームとして再アタッチすることはできません。
> - 保存済みのボリュームをデタッチする場合、これをキャッシュ済みのボリュームとして再アタッチすることはできません。

- デタッチされたボリュームは、これがゲートウェイにアタッチされるまで使用することはできません。
- 保存済みのボリュームをアタッチする場合、ゲートウェイにアタッチする前に完全に復元する必要があります。
- ボリュームのアタッチあるいはデタッチを開始したら、ボリュームを使用する前にオペレーションが完了するまで待機する必要があります。
- 現在のところ、ボリュームの強制的な削除は API のみでサポートされています。
- ゲートウェイからボリュームをデタッチしている間にこのゲートウェイを削除すると、データは喪失されます。ゲートウェイを削除する前に、ボリュームのデタッチオペレーションが完了するまで待ってください。
- 保存済みのゲートウェイが復元状態にある場合、このゲートウェイからボリュームをデタッチすることはできません。

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

ゲートウェイからボリュームをデタッチするには

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

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

別のゲートウェイにボリュームをアタッチできるようになりました。

ゲートウェイにボリュームをアタッチするには

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. ナビゲーションペインで [ボリューム] を選択します。デタッチした各ボリュームのステータスは [デタッチ済み] と示されます。
3. デタッチ済みのボリュームのリストから、アタッチするボリュームを選択します。一度にアタッチできるボリュームは 1 つのみです。
4. [アクション] で [ボリュームのアタッチ] を選択します。
5. [ボリュームのアタッチ] ダイアログボックスで、ボリュームをアタッチするゲートウェイを選択し、ボリュームを接続する iSCSI ターゲットを入力します。

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

復旧スナップショットの作成

次の手順では、ゲートウェイのボリューム復旧ポイントから復旧スナップショットを作成する方法と、作成後に Storage Gateway コンソールでそのスナップショットを見つける場所を示します。復旧スナップショットを 1 回だけ、アドホックベースで作成することも、指定した定期的な間隔でボリュームのスナップショットを作成するようにスナップショットスケジュールを設定することもできます。

既存のゲートウェイからボリュームの復旧スナップショットを作成し、使用するには

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

2. コンソールページの左側のナビゲーションペインで、[ゲートウェイ] を選択します。
3. スナップショットを作成するゲートウェイを選択し、[詳細] タブを選択します。

   [詳細] タブには、選択したゲートウェイの復旧スナップショットメッセージが表示されます。
4. [Create recovery snapshot] を選択して、[Create recovery snapshot] ダイアログボックスを開きます。
5. 表示されるボリュームのリストから、復旧するボリュームを選択し、[スナップショットを作成する] を選択します。

   Storage Gateway は、指定されたボリュームのスナップショットプロセスを開始します。スナップショットプロセスが完了すると、Storage Gateway コンソールの [ボリューム] ページでボリュームを表示するときに、[スナップショット] 列にリストされているスナップショットを確認できます。

スナップショットスケジュールの編集

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

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

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

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

ボリュームのスナップショットスケジュールを編集するには

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

ストレージボリュームのスナップショットの削除

ストレージボリュームのスナップショットを削除できます。たとえば、長期間に渡ってストレージボリュームの多数のスナップショットを作成し、古いスナップショットが不要になった場合などは、これを実行できます。スナップショットは増分バックアップなので、スナップショットを削除すると、他のスナップショットで必要とされていないデータのみが削除されます。

トピック

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

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

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

AWS SDK for Java を使用したスナップショットの削除

ボリュームに関連付けられている多数のスナップショットを削除するには、プログラム的な方法を使用します。次の例で、 AWS SDK for Java を使用してスナップショットを削除する方法を示しま

す。サンプルコードを使用するには、Java コンソールアプリケーションの実行について理解している必要があります。手順については、AWS SDK for Java デベロッパーガイドの「Getting Started」を参照してください。いくつかのスナップショットだけを削除する必要がある場合は、ストレージボリュームのスナップショットの削除 で説明されているように、コンソールを使用します。

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

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

サービスエンドポイント、ゲートウェイの Amazon リソースネーム (ARN) およびスナップショットを保存する日数を提供するコードを更新します。スナップショットは、この期限が削除される前に取得されます。また、`viewOnly` というブール値も指定する必要があります。この値は、削除されるスナップショットを表示するかどうかや、実際に削除を行うかどうかを示します。まずは、表示オプションだけで (つまり、`viewOnly` を `true` に設定して) コードを実行して、コードによって何が削除されるかを確認します。Storage Gateway で使用できる AWS サービスエンドポイントのリストについては、のAWS Storage Gateway 「エンドポイントとクォータ」を参照してくださいAWS 全般のリファレンス。

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

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

```
public class ListDeleteVolumeSnapshotsExample {

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

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

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

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

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

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

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

        sgClient.setEndpoint(serviceURLSG);

        ec2Client = new AmazonEC2Client(new PropertiesCredentials(

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

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

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

        String marker = null;
        do {
```

```
            ListVolumesRequest request = new
ListVolumesRequest().withGatewayARN(gatewayARN);
            ListVolumesResult result = sgClient.listVolumes(request);
            marker = result.getMarker();

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

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

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

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

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

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

                sb.append(", meets criteria for delete? " + meetsCriteria);
                sb.append(", deleted? ");
                if (!viewOnly & meetsCriteria) {
                    sb.append("yes");
                    DeleteSnapshotRequest deleteSnapshotRequest =
```

```
                        new DeleteSnapshotRequest().withSnapshotId(s.getSnapshotId());
                    ec2Client.deleteSnapshot(deleteSnapshotRequest);
                }
                else {
                    sb.append("no");
                }
                System.out.println(sb.toString());
            }
        }
    }

    private static String OutputVolumeInfo(VolumeInfo vi) {

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

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

}
```

AWS SDK for .NET を使用したスナップショットの削除

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

ある場合は、ストレージボリュームのスナップショットの削除 で説明されているように、コンソールを使用します。

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

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

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

サービスエンドポイント、ゲートウェイの Amazon リソースネーム (ARN) およびスナップショットを保存する日数を提供するコードを更新します。スナップショットは、この期限が削除される前に取得されます。また、`viewOnly` というブール値も指定する必要があります。この値は、削除されるスナップショットを表示するかどうかや、実際に削除を行うかどうかを示します。まずは、表示オプションだけで (つまり、`viewOnly` を `true` に設定して) コードを実行して、コードによって何が削除されるかを確認します。Storage Gateway で使用できる AWS サービスエンドポイントのリストについては、のAWS Storage Gateway 「エンドポイントとクォータ」を参照してくださいAWS 全般のリファレンス。

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

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

JSON

```
{
      "Version": "2012-10-17",
      "Statement": [
          {
              "Sid": "StmtEC2Snapshots",
              "Effect": "Allow",
              "Action": [
```

```
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "StmtSgwListVolumes",
            "Effect": "Allow",
            "Action": [
                "storagegateway:ListVolumes"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

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

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

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

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

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

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

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

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

        static String SnapshotStatus = "completed";

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

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

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

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

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

            List<VolumeInfo> StorageGatewayVolumes = ListVolumesForGateway();
```

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

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

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

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

```
                    String volumeID = volumeARN.Substring(volumeARN.LastIndexOf("/") +
1).ToLower();

                    DescribeSnapshotsRequest describeSnapshotsRequest = new
DescribeSnapshotsRequest();

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

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

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

                    DescribeSnapshotsResponse describeSnapshotsResponse =
                      ec2Client.DescribeSnapshots(describeSnapshotsRequest);

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

```
            {
                Console.WriteLine(ex.Message);
            }
            return SelectedSnapshots;
        }

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

                    DeleteSnapshotRequest deleteSnapshotRequest = new
DeleteSnapshotRequest(s.SnapshotId);
                    DeleteSnapshotResponse response =
ec2Client.DeleteSnapshot(deleteSnapshotRequest);
                    Console.WriteLine("Volume: " +
                              s.VolumeId +
                              " => Snapshot: " +
                              s.SnapshotId +
                              " Response: "
                              + response.HttpStatusCode.ToString());
                }
            }
            catch (AmazonEC2Exception ex)
            {
                Console.WriteLine(ex.Message);
            }
        }

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

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

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

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

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

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

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

```
<#
```

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

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

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

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

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

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

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

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

    $snapshots = get-EC2Snapshot -Filter $filter
    Write-Output("`nFor volume-id = " + $volumeId)
    foreach ($s in $snapshots)
    {
```

```
        $d = ([DateTime]::Now).AddDays(-$daysBack)
        $meetsCriteria = $false
        if ([DateTime]::Compare($d, $s.StartTime) -gt 0)
        {
             $meetsCriteria = $true
        }

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

ボリュームステータスと移行について

各ボリュームには、ボリュームの状態をわかりやすく示すステータスが関連付けられています。ほぼ常に、ステータスは、ボリュームが正常に機能しており、ユーザーによる対応は不要であることを示しています。まれに、ボリュームで問題が発生していることをステータスが示すことがあり、ユーザーによる対応が必要かどうかは問題によって異なります。このセクションでは、ユーザーによる対応が必要かどうかを判断するために役立つ情報を示します。ボリュームステータスは、Storage Gateway コンソールで、または Storage Gateway API オペレーション (DescribeCachediSCSIVolumes や DescribeStorediSCSIVolumes など) のいずれかを使用して確認できます。

トピック

- ボリュームのステータスについて
- アタッチメントステータスについて
- キャッシュ型ボリュームステータスの遷移を理解する
- 保管型ボリュームステータスの遷移を理解する

ボリュームのステータスについて

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

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

ステータス	意味
[使用可能]	ボリュームは使用できます。このステータスは、ボリュームが正常に実行中であることを示すステータスです。 [ブートストラッピング] フェーズが完了すると、ボリュームは [Available (使用可能)] ステータスに戻ります。つまり、ゲートウェイは最初に [Pass Through (パススルー)] ステータスになってからボリュームに生じたすべての変更を同期します。
ブートストラッピング	ゲートウェイは、保存されたデータのコピーとローカルでデータを同期しています AWS。ほとんどの場合、ストレージボリュームのステータスは自動的に [Available (使用可能)] になるため、通常このステータスに対しては何もする必要はありません。 ボリュームのステータスが [ブートストラッピング] の場合、以下のシナリオが考えられます。 • ゲートウェイが予期せずシャットダウンした。 • ゲートウェイのアップロードバッファの容量を超えた。このシナリオでは、ボリュームのステータスが [Pass Through (パススルー)] で、アップロードバッファの空き容量が十分に増設されたときに、ブートストラップが発生します。アップロードバッファの空き領域の割合を増やす 1 つの方法として、追加のアップロードバッファ領域を用意できます。特にこのシナリオでは、ストレージボリュームのステータスが [Pass Through (パススルー)] から [ブートストラッピング] に変わっ

ステータス	意味
	てから、[Available (使用可能)] に変わります。ブートストラップの間もこのボリュームを使い続けることができます。ただし、この時点でボリュームのスナップショットを作成することはできません。 • 保管型ボリュームゲートウェイを作成していて、既存のローカルディスクデータを保存しています。このシナリオでは、ゲートウェイがすべてのデータのアップロードを開始します AWS。ボリュームは、ローカルディスクのすべてのデータがコピーされるまでブートストラップステータスになります AWS。ブートストラップの間もボリュームを使用できます。ただし、この時点でボリュームのスナップショットを作成することはできません。
[作成中]	ボリュームは現在作成中であり、使用準備ができていません。[Creating (作成中)] は過渡的なステータスです。アクションは必要ありません。
削除	ボリュームは削除中です。[Deleting (削除中)] ステータスは過渡的なものです。アクションは必要ありません。
回復不可能	エラーが発生し、ボリュームは回復できません。この場合の操作については、「ボリュームの問題のトラブルシューティング」を参照してください。

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

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

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

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

アタッチメントステータスについて

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

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

キャッシュ型ボリュームステータスの遷移を理解する

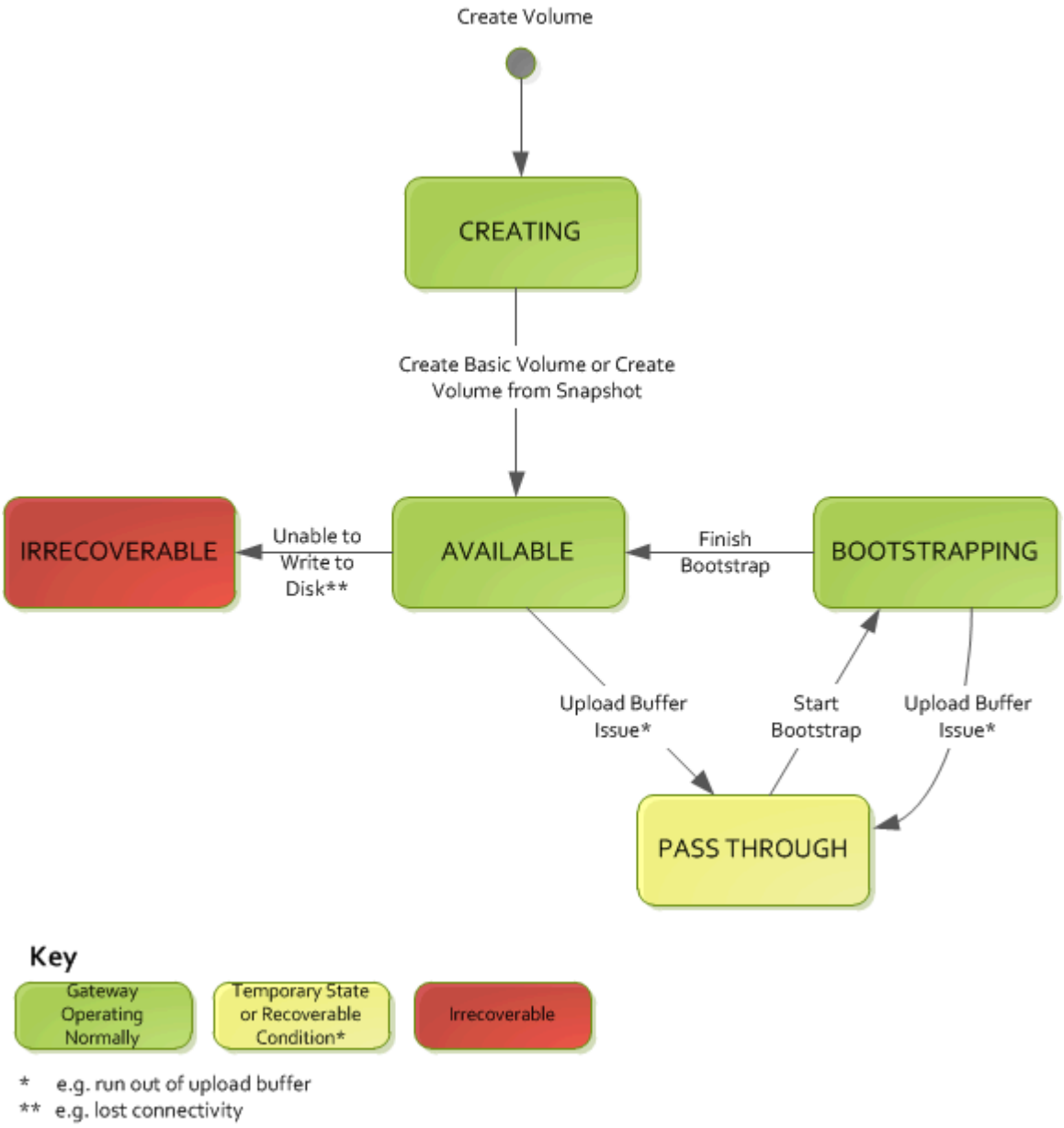
次の図を使用して、キャッシュ型ゲートウェイのボリュームでよく発生するステータス間の遷移を理解します。ゲートウェイを効果的に使用するために、この図を詳しく理解する必要はありません。むしろ、ボリュームゲートウェイの仕組みについて、この図で詳しく知ることができます。

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

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

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

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



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

保管型ボリュームステータスの遷移を理解する

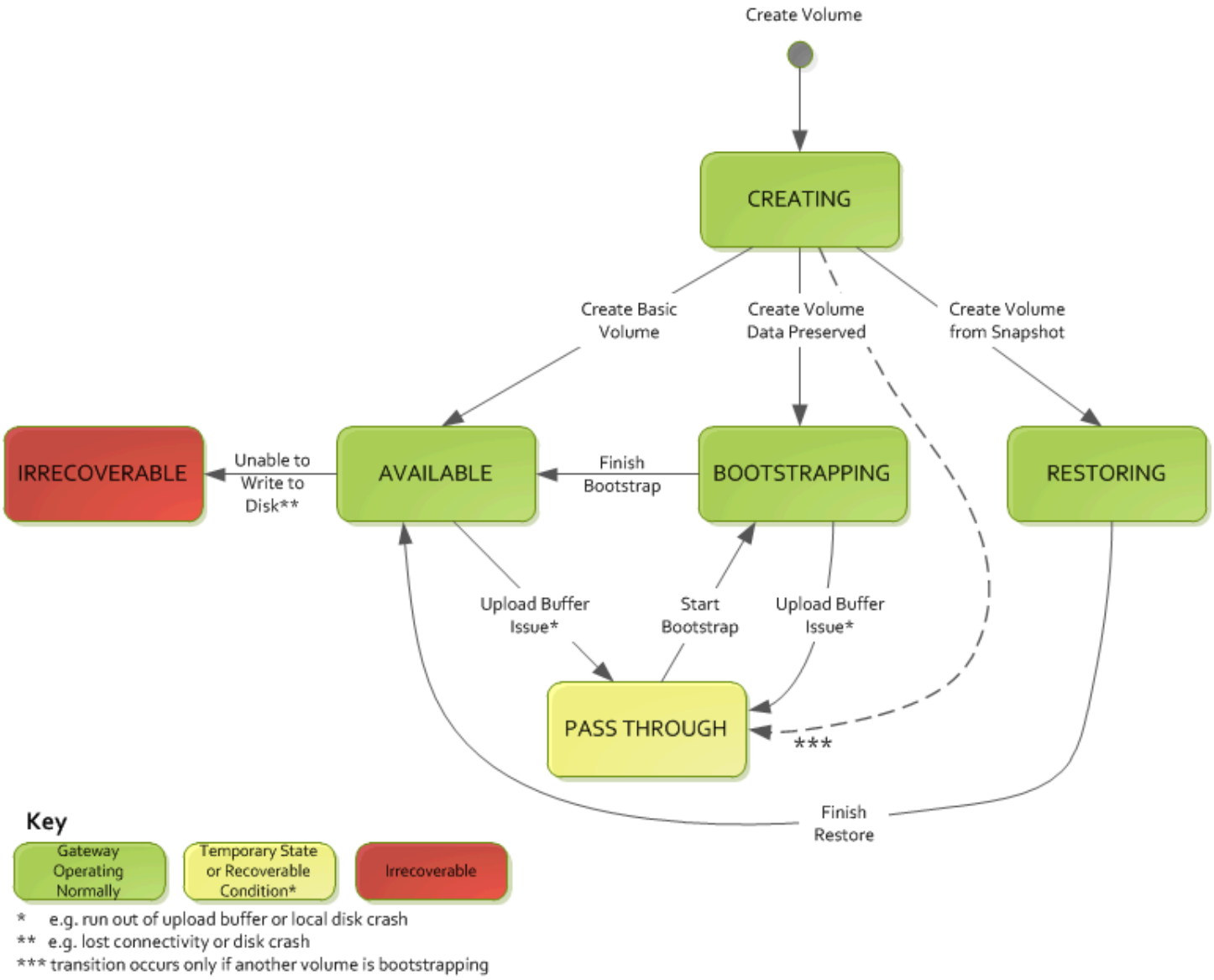
次の図を使用して、保管型ゲートウェイのボリュームでよく発生するステータス間の遷移を理解します。ゲートウェイを効果的に使用するために、この図を詳しく理解する必要はありません。むしろ、ボリュームゲートウェイの仕組みについて、この図で詳しく知ることができます。

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

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

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

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



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

新しいゲートウェイへのデータの移動

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

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

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

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

保管型ボリュームの新しい保管型ボリュームゲートウェイへの移動

保管型ボリュームを新しい保管型ボリュームゲートウェイに移動するには

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

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

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

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

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

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

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

3. 次の手順に従って、古い保管型ボリュームゲートウェイを停止します。

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

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

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

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

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

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

5. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) から、利用可能な新しいハイパーバイザー VM イメージを使用して、新しい保管型ボリュームゲートウェイをアクティブ化します。

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

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

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

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

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

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

ボリュームの作成方法については、「ストレージボリュームの作成」を参照してください。

8. (オプション) [Configure CHAP authentication] (CHAP 認証設定) ウィザードが表示されたら、[Initiator name] (イニシエータ名)、[Initiator secret] (イニシエータのシークレット)、[Target secret] (ターゲットのシークレット) をそれぞれ入力し、[Save] (保存) をクリックします。

   チャレンジハンドシェイク認証プロトコル (CHAP) 認証を操作する詳細については、「iSCSI ターゲットの CHAP 認証の設定」を参照してください。

9. 保存したボリュームに書き込むアプリケーションを起動します。

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

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

次のステップに従って、古い保管型ボリュームゲートウェイを削除します。

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

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

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

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

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

キャッシュ型ボリュームを新しいゲートウェイの仮想マシンに移動する

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

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

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

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

   c. [アクション] で [スナップショットを作成] を選択します。

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

      スナップショットがコンソールを使用して作成されたことを確認できます。依然としてデータがボリュームにアップロード中である場合は、アップロードが完了するのを待ってから、次のステップに進みます。保留中のスナップショットがなくなったことを、そのステータスにより確認するには、対象のボリュームのスナップショットへのリンクを選択します。

      コンソールでのボリュームステータスの確認については、「ボリュームステータスと移行について」を参照してください。キャッシュ型ボリュームのステータスについては、「キャッシュ型ボリュームステータスの遷移を理解する 」を参照してください。
4. 古いキャッシュ型ボリュームゲートウェイを停止するには、以下のステップに従います。

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

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

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

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

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

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

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

キャッシュ型ボリュームゲートウェイの VM として Amazon EC2 インスタンスを使用している場合は、「Amazon EC2 ユーザーガイド」の「Linux インスタンスからの Amazon EBS ボリュームのデタッチ」を参照してください。KVM、VMware、または Hyper-V VM からのディスクのデタッチについては、ハイパーバイザーからのドキュメントを参照してください。

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

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

7. 新しい Storage Gateway ハイパーバイザー VM インスタンスでも、古い VM と同じネットワーク構成を使用する必要があります。ゲートウェイのデフォルトのネットワーク設定は、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。

   新しい VM の静的 IP アドレスを手動で設定する必要がある場合は、「ゲートウェイのネットワークの設定」を参照して詳細をご確認ください。ゲートウェイが、インターネットに接続するために Socket Secure バージョン 5 (SOCKS5) プロキシを使用する必要がある場合は、「オンプレミスゲートウェイの SOCKS5 プロキシの設定」で詳細をご確認ください。
8. 新しい VM を起動します。
9. ステップ 5 で古いキャッシュ型ボリュームゲートウェイ VM からデタッチしたディスクを、新しいキャッシュ型ボリュームゲートウェイにアタッチします。古いゲートウェイ VM の場合と同じ順序で、これらを新しいゲートウェイ VM にアタッチします。

   すべてのディスクを変更なしで移行する必要があります。ボリュームサイズを変更しないでください。変更するとメタデータの整合性がなくなります。
10. 次の形式の URL により新しい VM に接続して、ゲートウェイ移行プロセスを開始します。

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

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

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

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

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

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

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

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

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

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

Storage Gateway のモニタリング

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

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

ボリュームゲートウェイとその関連リソースのモニタリングに固有の情報については、「ボリューム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

- ゲートウェイメトリクスについて
- アップロードバッファのモニタリング
- キャッシュストレージのモニタリング
- CloudWatch アラームの説明
- ゲートウェイ用の CloudWatch 推奨アラームの作成
- ゲートウェイのカスタム CloudWatch アラームの作成
- ボリュームゲートウェイのモニタリング

ゲートウェイメトリクスについて

このトピックの説明では、ゲートウェイメトリクスを、ゲートウェイの範囲内にあるメトリクス、つまり、ゲートウェイに関する何かを測定するメトリクスと定義しています。ゲートウェイには 1 つ

以上のボリュームが含まれているので、ゲートウェイ固有のメトリクスは、ゲートウェイにあるすべてのボリュームの代表です。たとえば、CloudBytesUploaded メトリクスは、レポート期間中にゲートウェイがクラウドに送信した総バイト数です。このメトリクスには、ゲートウェイのすべてのボリュームのアクティビティが含まれます。

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

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

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

メトリクス	説明
	単位: パーセント
CachePercentDirty	永続化されていないゲートウェイキャッシュの全体的な割合 AWS。サンプリングは、レポート期間の最後に行われます。 このメトリクスを Sum 統計とともに使用します。 理想的には、このメトリクスを低く維持する必要があります。 単位: パーセント
CacheUsed	ゲートウェイのキャッシュストレージで使用されている総バイト数。サンプリングは、レポート期間の最後に行われます。 単位: バイト
IoWaitPercent	ゲートウェイがローカルディスクからの応答を待機している時間の割合。 単位: パーセント
MemTotalBytes	ゲートウェイ VM にプロビジョニングされた RAM の量 (バイト単位)。 単位: バイト

メトリクス	説明	
MemUsedBytes	ゲートウェイ VM で現在使用されている RAM の量 (バイト単位)。 単位: バイト	
QueuedWrites	通常、この値は書き込みを待機しているローカルに保存されたバイト数を表しますが AWS、ゲートウェイが再起動するたびに発生する「ブートストラップ」中にローカルデータとクラウドデータの間で発生する同期プロセスも反映します。 単位: バイト	
ReadBytes	ゲートウェイにあるすべてのボリュームを対象としたレポートの期間中に内部設置型のアプリケーションから読み取られた総バイト数。 このメトリクスを Sum 統計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
ReadTime	ゲートウェイにあるすべてのボリュームを対象としたレポートの期間中にオンプレミスのアプリケーションからの読み込みオペレーションにかかった合計時間 (ミリ秒)。 このメトリクスを Average 統計と共に使用してレイテンシーを測定します。 単位: ミリ秒
TimeSinceLastRecoveryPoint	使用可能な最新の復旧ポイントからの時間。詳細については、「ゲートウェイキャッシュ型が到達不可能なためデータを復旧する場合」を参照してください。 単位: 秒
TotalCacheSize	キャッシュの総バイト数。サンプリングは、レポート期間の最後に行われます。 単位: バイト
UploadBufferPercentUsed	ゲートウェイのアップロードバッファの使用率。サンプリングは、レポート期間の最後に行われます。 単位: パーセント

メトリクス	説明
UploadBufferUsed	ゲートウェイのアップロードバッファで使用されている総バイト数。サンプリングは、レポート期間の最後に行われます。 単位: バイト
UserCpuPercent	ゲートウェイ処理にかかった CPU 時間の割合 (すべてのコアの平均)。 単位: パーセント
WorkingStorageFree	ゲートウェイの作業ストレージの未使用領域の量。サンプリングは、レポート期間の最後に行われます。 単位: バイト
WorkingStoragePercentUsed	ゲートウェイのアップロードバッファの使用率。サンプリングは、レポート期間の最後に行われます。 単位: パーセント
WorkingStorageUsed	ゲートウェイのアップロードバッファで使用されている総バイト数。サンプリングは、レポート期間の最後に行われます。 単位: バイト

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

Storage Gateway メトリクスのディメンション

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

ディメンション	説明
GatewayId , GatewayName	このディメンションを指定すると、リクエストしたデータがフィルタリングされて、ゲートウェイ固有のメトリクスのもの

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

アップロードバッファのモニタリング

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

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

> **Note**
>
> WorkingStoragePercentUsed、WorkingStorageUsed、および WorkingStorageFree メトリクスは、Storage Gateway のキャッシュ型ボリューム機能がリリースされる前にのみ、保存されたボリュームのアップロードバッファについて表していました。現在は、同等のアップロードバッファメトリクスとして

UploadBufferPercentUsed、UploadBufferUsed、および UploadBufferFree を使用します。これらのメトリクスは、両方のゲートウェイアーキテクチャに適用されます。

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

使用されるアップロードバッファの割合を測定するには

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

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

CloudWatch コンソールを使用してアラームを作成するには、次の手順を実行します。アラームとしきい値の詳細については、Amazon CloudWatch ユーザーガイドの「Amazon CloudWatch でのアラームの使用」を参照してください。

ゲートウェイのアップロードバッファの上限アラームを設定するには

1. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
2. [Create Alarm (アラームの作成)] を選択して、アラームの作成ウィザードを起動します。
3. アラームのメトリクスを指定します。

a. Create Alarm ウィザードの [Select Metric] (メトリクスの選択) ページで、[AWS/StorageGateway:GatewayId,GatewayName] ディメンションを選択し、対象のゲートウェイを見つけます。

b. `UploadBufferPercentUsed` メトリクスを選択します。`Average` 統計および 5 分の期間を使用します。

c. [Continue] (続行) を選択します。

4. アラームの名前、説明、しきい値を定義します。

a. Create Alarm Wizard の [Define Alarm (アラームの定義)] ページで、[Name (名前)] ボックスにアラームの名前を、[Description (説明)] ボックスにアラームの説明を入力して、アラームを指定します。

b. アラームのしきい値を定義します。

c. [Continue] (続行) を選択します。

5. アラームの E メールアクションを設定します。

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

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

E メールトピックを作成することは、Amazon SNS トピックをセットアップするということです。詳細については、Amazon CloudWatch ユーザーガイドの「Amazon SNS 通知の設定」を参照してください。

c. [トピック] に、トピックを示すわかりやすい名前を入力します。

d. [Add Action] (アクションの追加) を選択します。

e. [Continue] (続行) を選択します。

6. アラーム設定を確認してアラームを作成します。

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

b. アラームの要約を確認したら、[Save Alarm] を選択します。

7. アラームトピックの受信登録を確認します。

a. トピックの作成時に指定した E メールアドレス宛に送信されている、Amazon SNS の E メールを開きます。

b. メール内のリンクをクリックして、受信登録を確認します。

サブスクリプションの確認が表示されます。

キャッシュストレージのモニタリング

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

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

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

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

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

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

ボリュームのダーティなキャッシュの割合を測定するには

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

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

CloudWatch アラームの説明

CloudWatch アラームは、メトリクスと式に基づいてゲートウェイに関する情報をモニタリングします。ゲートウェイ用の CloudWatch アラームを追加し、Storage Gateway コンソールでそのステータスを表示できます。ボリュームゲートウェイのモニタリングに使用されるメトリクスの詳細については、「ゲートウェイメトリクスについて」および「ボリュームメトリクスについて」を参照してください。アラームごとに、ALARM 状態が開始する条件を指定します。ALARM 状態になると、Storage Gateway コンソールのアラーム状態のインジケータが赤に変わるため、先を見越した状態のモニタリングがしやすくなります。状態の継続的な変化に応じて自動的にアクションを呼び出すようにア

ラームを設定できます。CloudWatch アラームの使用の詳細については、Amazon CloudWatch ユーザーガイドの「Amazon CloudWatch アラームの使用」を参照してください。

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

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

- 高い IO 待機率: `IoWaitpercent` >= 20、3 つのデータポイント、15 分以内
- キャッシュのダーティ率: `CachePercentDirty` > 80、4 つのデータポイント、20 分以内
- ヘルス通知: `HealthNotifications` >= 1、1 つのデータポイント、5 分以内 このアラームを設定するときは、[欠落データの処理] を [notBreaching] に設定してください。

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

HA モードが有効になっている VMware ホストプラットフォーム上のゲートウェイでは、次の追加の CloudWatch アラームも推奨します。

- 可用性通知: `AvailabilityNotifications` >= 1、1 つのデータポイント、5 分以内 このアラームを設定するときは、[欠落データの処理] を [notBreaching] に設定してください。

次の表に、アラームの状態を示します。

状態	説明
OK	メトリクスや式は、定義されているしきい値の範囲内です。
アラーム	メトリクスまたは式が、定義されているしきい値を超えています。

状態	説明
不十分なデータ	アラームが開始直後であるか、メトリクスが利用できないか、メトリクス用のデータが不足しているため、アラームの状態を判定できません。
[なし]	ゲートウェイのアラームが作成されていません。新しいアラームを作成する方法については、「ゲートウェイのカスタム CloudWatch アラームの作成」を参照してください。
使用不可	アラームの状態が不明です。[Monitoring] (モニタリング) タブでエラー情報を表示するには、[Unavailable] (使用不可) を選択します。

ゲートウェイ用の CloudWatch 推奨アラームの作成

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

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

> **Note**
>
> この機能を使用するには、CloudWatch ポリシーのアクセス権限が必要です。この権限は、事前設定済みの Storage Gateway のフルアクセスポリシーの一部として自動的に付与されるものではありません。CloudWatch の推奨アラームを作成する前に、セキュリティポリシーで次のアクセス権限が付与されていることを確認してください。
>
> - `cloudwatch:PutMetricAlarm` - アラームを作成する
> - `cloudwatch:DisableAlarmActions` - アラームアクションをオフにする
> - `cloudwatch:EnableAlarmActions` - アラームアクションをオンにする
> - `cloudwatch:DeleteAlarms` - アラームを削除する

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

   [アラーム] セクションには、特定のゲートウェイの CloudWatch アラームがすべて一覧表示されます。ここから、1 つ以上のアラームを選択して削除したり、アラームアクションをオンまたはオフにしたり、新しいアラームを作成したりできます。

ゲートウェイのカスタム CloudWatch アラームの作成

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

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

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

   - 静的しきい値アラーム: 指定のメトリクスに応じて設定されたしきい値に基づくアラーム。指定した評価期間数にわたってメトリクスがしきい値を超えると、アラームが ALARM 状態に移行します。

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

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

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

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

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

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

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

     [アラーム] セクションには、特定のゲートウェイの CloudWatch アラームがすべて一覧表示されます。ここから、1 つ以上のアラームを選択して削除したり、アラームアクションをオンまたはオフにしたり、新しいアラームを作成したりできます。
   - ナビゲーションペインで [ゲートウェイ] を選択し、アラームを表示したいゲートウェイのアラーム状態を選択します。

アラームを編集または削除するには、「CloudWatch アラームの編集または削除」を参照してください。

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

ボリュームゲートウェイのモニタリング

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

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

トピック

- Amazon CloudWatch Logs を使用したボリュームゲートウェイのヘルスログの取得 - Amazon CloudWatch Logs を使用して、ボリュームゲートウェイと関連リソースのヘルスに関する情報を取得する方法について説明します。
- Amazon CloudWatch メトリクスを使用する - AWS Management Console または CloudWatch API を使用してゲートウェイのモニタリングデータを取得する方法について説明します。
- アプリケーションとゲートウェイの間のパフォーマンスの測定 - アプリケーションとゲートウェイの間のパフォーマンスを理解するために、データスループット、データレイテンシー、1 秒あたりのオペレーション数を測定する方法について説明します。
- ゲートウェイと AWSの間のパフォーマンスの測定 - ゲートウェイと AWS クラウド間のパフォーマンスを理解するために、データスループット、データレイテンシー、および 1 秒あたりのオペレーションを測定する方法について説明します。

- ボリュームメトリクスについて - ゲートウェイに関連付けられたボリュームに関するデータを提供するメトリクスを測定する方法について説明します。

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

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

例えば、VMware High Availability (HA) が有効なクラスターにゲートウェイがデプロイされ、エラーについて把握する必要があるとします。ゲートウェイをモニタリングし、ゲートウェイでエラーが発生したときに通知を表示するように 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、「ボリュームゲートウェイを設定する」を参照してください。CloudWatch ロググループの一般的情報については、Amazon CloudWatch Logs ユーザーガイドの「ロググループとログストリームの操作」を参照してください。

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

次の手順では、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。

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

1. にサインイン AWS Management Console し、https://https://console.aws.amazon.com/storagegateway/home.https://www.com で Storage Gateway コンソールを開きます。
2. ナビゲーションペインで [ゲートウェイ] を選択してから、CloudWatch ロググループを設定するゲートウェイを選択します。
3. [アクション] で [ゲートウェイ情報の編集] を選択するか、[詳細] タブの [ヘルスログ] および [有効になっていません] で [ロググループを設定] を選択して、[***CustomerGatewayName*** を編集] ダイアログボックスを開きます。

4. [Gateway health log group] (ゲートウェイヘルスロググループ) で、次のいずれかを選択します。

   - [Disable logging] (ログの無効化) CloudWatch ロググループを使用してゲートウェイをモニタリングしない場合。
   - [Create a new log group] (新しいロググループの作成) 新しい CloudWatch ロググループを作成する場合。
   - [Use an existing log group] (既存のロググループの使用) 既に存在している CloudWatch ロググループを使用する場合。[Existing log group list] (既存のロググループのリスト) から、ロググループを選択します。

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

   1. ナビゲーションペインで [ゲートウェイ] を選択してから、CloudWatch ロググループが設定されているゲートウェイを選択します。
   2. [Details] (詳細) タブを選択し、[Health logs] (ヘルスログ) で、[CloudWatch Logs] を選択します。Amazon CloudWatch コンソールで [ロググループの詳細] ページが開きます。

Amazon CloudWatch メトリクスを使用する

ゲートウェイのモニタリングデータは、 AWS Management Console または CloudWatch API を使用して取得できます。コンソールには、CloudWatch API の raw データに基づいて一連のグラフが表示されます。CloudWatch API は、AWS ソフトウェア開発キット (SDK) または Amazon CloudWatch API ツールでも使用できます。必要に応じて、コンソールに表示されるグラフまたは API から取得したグラフを使用できます。

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

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

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

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

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

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

アプリケーションとゲートウェイの間のパフォーマンスの測定

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

統計とは、指定した期間を対象としたメトリックスの集計を意味します。CloudWatch でメトリクスの値を表示するとき、データレイテンシー (ミリ秒) には Average 統計、データスループット (バイト/秒) には Sum 統計、1 秒あたりの入力/出力オペレーション数 (IOPS) には Samples 統計を使用します。詳細については、Amazon CloudWatch ユーザーガイドの「統計」を参照してください。

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

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

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

アプリケーションからボリュームへのデータスループットを測定するには

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

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

例えば、読み取りスループットが 300 秒の期間で、2,384,199,680 バイトの場合、そのデータポイントの概算スループットレートは 7.9 メガバイト/秒です。

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

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

例えば、300 秒の期間の書き込みオペレーションの数が 24,373 の場合、そのデータポイントの IOPS は 1 秒あたり 81 回の書き込みオペレーションです。

ゲートウェイと AWSの間のパフォーマンスの測定

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

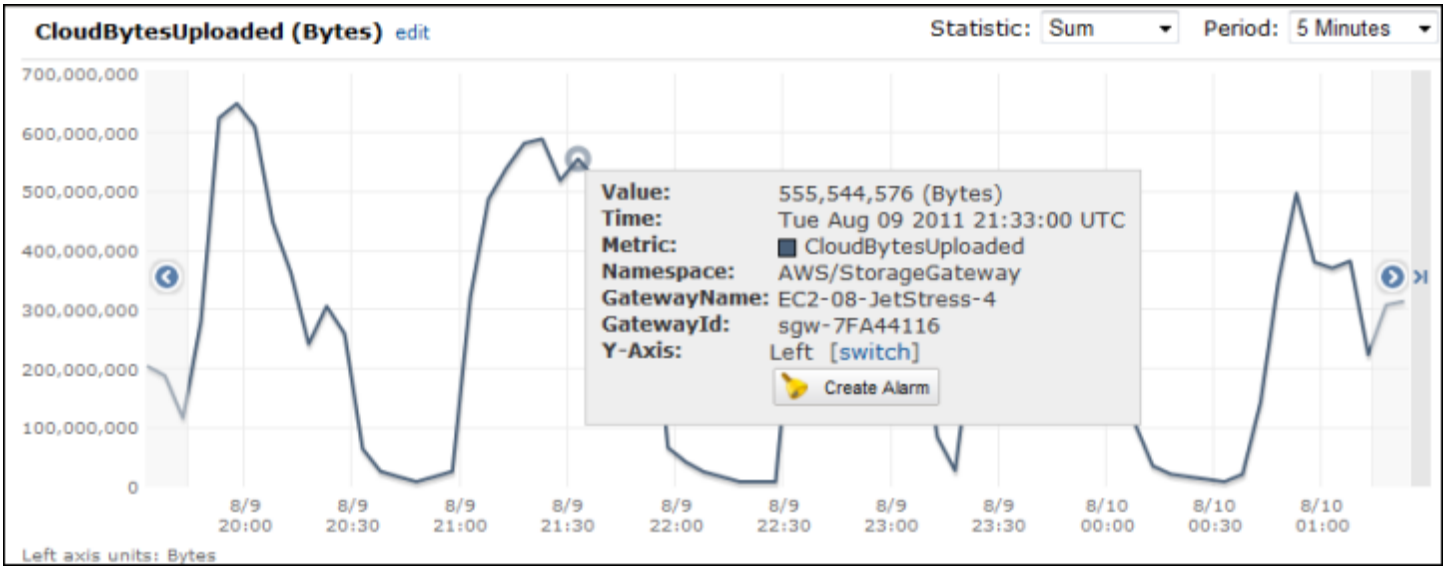
対象となる項目	測定方法
スループット	ReadBytes および WriteBytes メトリクスを Sum CloudWatch 統計と共に使用します。たとえば、5 分間のサンプル期間に対する

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

ゲートウェイから へのアップロードデータスループットを測定するには AWS

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

データポイントにカーソルを移動すると、そのデータポイントに関する情報 (データポイントの値やアップロードしたバイト数など) が表示されます。この値を [Period] の値 (5 分) で割ると、そのサンプルポイントのスループットがわかります。例えば、ゲートウェイから へのスループット AWS が 300 秒間で 555,544,576 バイトの場合、1 秒あたりのおおよそのスループットは 1.85 メガバイト/秒です。



ゲートウェイのオペレーションあたりのレイテンシーを測定するには

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

ゲートウェイから へのデータレイテンシーを測定するには AWS

1. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
2. [Metrics] を選択し、[All metrics] タブを選択して、[Storage Gateway] を選択します。

3. [Gateway metrics] ディメンションを選択し、対象のボリュームを見つけます。
4. `CloudDownloadLatency` メトリクスを選択します。
5. [Time Range] で値を選択します。
6. `Average` 統計を選択します。
7. [Period] で、デフォルトのレポート時間に合わせて 5 分を選択します。

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

ゲートウェイのスループットの上限しきい値アラームを に設定するには AWS

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

からデータを読み取るためのしきい値上限アラームを設定するには AWS

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

7. アラームの作成(アラームの作成) を選択します。

ボリュームメトリクスについて

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

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

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

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

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

メトリクス	説明	キャッシュボリューム	保管型ボリューム
	ト期間の最後に行われます。 ボリュームからのアプリケーション読み込みオペレーションがない割合、このメトリックにより 100 パーセントが報告されます。 単位: パーセント		

メトリクス	説明	キャッシュボリューム	保管型ボリューム
CachePercentDirty	AWSに保持されていないゲートウェイのキャッシュの割合全体に対するボリュームの割合。サンプリングは、レポート期間の最後に行われます。 ゲートウェイの CachePercentDirty メトリクスを使用して、AWSに保持されていないゲートウェイのキャッシュの割合全体を表示します。詳細については、「ゲートウェイメトリクスについて」を参照してください。 単位: パーセント	あり	あり

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

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

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

メトリクス	説明	キャッシュボリューム	保管型ボリューム
UserCpuPercent	ボリュームで現在使用されている、割り当てられた CPU コンピューティングユニットの割合。 単位: パーセント	あり	あり
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	あり	あり

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

ゲートウェイの維持

ボリュームゲートウェイのメンテナンスには、キャッシュストレージ用のローカルディスクのサイズ設定と構成、バッファスペースのアップロード、更新の管理と更新スケジュールの設定、帯域幅使用量の管理、必要に応じてゲートウェイおよび関連するリソースのシャットダウンまたは削除などのタスクが含まれます。これらのタスクは、すべてのゲートウェイの種類に共通です。ゲートウェイをまだ作成していない場合は、「ゲートウェイを作成する」を参照してください。

トピック

- Storage Gateway のローカルディスクの管理 - ディスクサイズ要件を評価し、キャッシュ容量を追加して、バッファリングとストレージのためにボリュームゲートウェイに割り当てるローカルディスクを管理する方法について説明します。
- ボリュームゲートウェイの帯域幅管理 - ゲートウェイから へのアップロードスループットを制限 AWS して、ゲートウェイが使用するネットワーク帯域幅の量を制御する方法について説明します。
- ゲートウェイアップデートの管理 - メンテナンスの更新をオンまたはオフにする、およびボリュームゲートウェイのメンテナンスウィンドウスケジュールを変更する方法について説明します。
- ゲートウェイ VM のシャットダウン - ハイパーバイザーにパッチを適用する場合など、メンテナンスのためにゲートウェイ仮想マシンをシャットダウンまたは再起動する必要がある場合の対処方法について説明します。
- ゲートウェイおよび関連リソースの削除 - AWS Storage Gateway コンソールを使用してゲートウェイを削除し、関連するリソースをクリーンアップして、継続的な使用に対して課金されないようにする方法について説明します。

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容量の決定
- 追加のアップロードバッファとキャッシュストレージの設定

ローカルディスクストレージの容量の決定

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

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

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

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

ローカルストレージ	説明	
	リケーションがボリュームまたはテープに対してデータを要求すると、ゲートウェイは、 AWSからデータをダウンロードする前に、まずキャッシュストレージにデータがあるかどうかをチェックします。	

> **Note**
>
> ディスクをプロビジョニングするとき、同じ物理リソース (同じディスク) を使用しているアップロードバッファとキャッシュストレージのローカルディスクはプロビジョニングしないことを強くお勧めします。基になる物理ストレージリソースは、VMware でデータストアとして表されます。ゲートウェイ VM をデプロイする場合は、VM ファイルを保存するデータストアを選択します。たとえば、キャッシュストレージまたはアップロードバッファとして使用するなど、ローカルディスクをプロビジョニングする場合は、VM と同じデータストアまたは別のデータストアに仮想ディスクを保存することもできます。
> 複数のデータストアがある場合は、キャッシュストレージ用とアップロードバッファ用でデータストアの場所を分けることを強くお勧めします。基になる物理ディスクが 1 つのみのデータストアを、キャッシュストレージとアップロードバッファの両方に使用すると、パフォーマンスが低下する場合があります。これは、バックアップが 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。

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

割り当てるアップロードバッファのサイズの決定

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

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

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

受信データレート

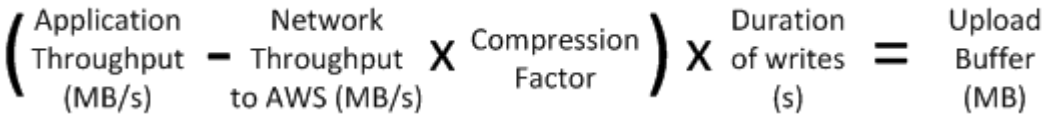
これはアプリケーションスループットです。つまり、オンプレミスアプリケーションが一定期間にゲートウェイにデータを書き込むレートです。

送信データレート

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

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

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



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

Example

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

最初にこの概算値を使うことで、アップロードバッファ容量としてゲートウェイに割り当てるディスクサイズを判断できます。必要に応じて、Storage Gateway コンソールを使用してアップロードバッファ領域を追加します。また、Amazon CloudWatch オペレーションメトリクスを使用してアップロードバッファ使用率をモニタリングし、ストレージ追加の必要性を判断できます。メトリックとアラームの設定については、アップロードバッファのモニタリング を参照してください。

割り当てるキャッシュストレージのサイズの決定

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

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

追加のアップロードバッファとキャッシュストレージの設定

アプリケーションのニーズの変化に応じて、ゲートウェイのアップロードバッファやキャッシュストレージの容量を増やすことができます。機能を中断したりダウンタイムを発生させたりすることな

く、ゲートウェイにストレージ容量を追加できます。容量を追加する場合は、ゲートウェイ VM を有効にした状態で行います。

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

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

1. ゲートウェイホストのハイパーバイザーまたは Amazon EC2 インスタンスで 1 つ以上の新しいディスクをプロビジョニングします。ハイパーバイザーでディスクをプロビジョニングする方法については、ハイパーバイザーのドキュメントを参照してください。Amazon EC2 インスタンス用の Amazon EBS ボリュームのプロビジョニングについては、「Amazon Elastic Compute Cloud Linux インスタンス用ユーザーガイド」の「Amazon EBS ボリューム」を参照してください。次の手順では、このディスクをアップロードバッファまたはキャッシュストレージとして設定します。
2. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
3. ナビゲーションペインで、[Gateways] を選択します。
4. ゲートウェイを検索し、リストから選択します。
5. [アクション] メニューから [ストレージの設定] を選択します。
6. [ストレージの設定] セクションで、プロビジョニングしたディスクを特定します。ディスクが表示されない場合は、更新アイコンを選択してリストを更新します。ディスクごとに、[割り当て済み] ドロップダウンメニューから [アップロードバッファ] または [キャッシュストレージ] を選択します。

   > **Note**
   >
   > 保管型ボリュームゲートウェイにディスクを割り当てる際に使用できるオプションは、[アップロードバッファ] だけです。

7. [変更を保存] を選択して設定を保存します。

ボリュームゲートウェイの帯域幅管理

ゲートウェイから へのアップロードスループット AWS 、または からゲートウェイ AWS へのダウンロードスループットを制限 (またはスロットリング) できます。帯域幅のスロットル機能は、ゲートウェイによるネットワーク帯域幅の使用量の制御に役立ちます。デフォルトでは、アクティブ化されたゲートウェイのレート制限は、アップロードまたはダウンロード時には設定されていません。

レート制限は、 を使用するか AWS Management Console、Storage Gateway API (UpdateBandwidthRateLimit を参照) または AWS Software Development Kit (SDK) を使用してプログラムで指定できます。帯域幅をプログラムでスロットリングすることで (例えば、帯域幅を変更するようにタスクをスケジュールすることで)、制限を 1 日を通して自動的に変更することができます。

スケジュールベースでゲートウェイの帯域幅スロットリングを定義することもできます。帯域幅スロットリングをスケジュールするには、帯域幅レート制限期間を 1 つ以上定義します。詳細については、「Storage Gateway コンソールを使用したスケジュールベースの帯域幅スロットリング」を参照してください。

帯域幅スロットリングの設定を 1 つにする場合、機能的には、[毎日]、[開始時刻] = 00:00、[終了時刻] = 23:59 という単一の帯域幅レート制限期間でスケジュールを定義することと同じです。

> **Note**
>
> このセクションの情報は、テープゲートウェイとボリュームゲートウェイに固有の情報です。Amazon S3 ファイルゲートウェイの帯域幅を管理するには、「Managing Bandwidth for Your Amazon S3 File Gateway」を参照してください。Amazon FSx ファイルゲートウェイでは、現時点では、帯域幅レート制限はサポートされていません。

トピック

- Storage Gateway コンソールを使用して帯域幅スロットリングを変更する
- Storage Gateway コンソールを使用したスケジュールベースの帯域幅スロットリング
- を使用したゲートウェイ帯域幅レート制限の更新 AWS SDK for Java
- を使用したゲートウェイ帯域幅レート制限の更新 AWS SDK for .NET
- を使用したゲートウェイ帯域幅レート制限の更新 AWS Tools for Windows PowerShell

Storage Gateway コンソールを使用して帯域幅スロットリングを変更する

次の手順は、Storage Gateway コンソールを使用してゲートウェイの帯域幅スロットリングを変更する方法を示しています。

コンソールを使用してゲートウェイの帯域幅スロットルを変更するには

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. 左側のナビゲーションペインで [ゲートウェイ] を選択してから、管理対象のゲートウェイを選択します。
3. [アクション] で、[帯域幅レート制限の編集] を選択します。
4. [速度制限の編集] ダイアログボックスで、新しい制限値を入力し、[保存] をクリックします。変更はゲートウェイの [Details] タブに表示されます。

Storage Gateway コンソールを使用したスケジュールベースの帯域幅スロットリング

次の手順は、Storage Gateway コンソールを使用してゲートウェイの帯域幅スロットリングのスケジュールを変更する方法を示しています。

ゲートウェイ帯域幅スロットリングのスケジュールを追加または変更するには

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

   ゲートウェイの帯域幅レート制限スケジュールは、[帯域幅レート制限スケジュールの編集] ダイアログボックスに表示されます。デフォルトでは、新しいゲートウェイ帯域幅レート制限スケジュールは空です。
4. [帯域幅レート制限スケジュールの編集] ダイアログボックスで、[新しいエントリの追加] を選択して、新しい帯域幅レート制限の期間を追加します。帯域幅レート制限期間ごとに次の情報を入力します。

- [曜日] – 平日 (月曜日から金曜日)、週末 (土曜日と日曜日)、すべての曜日、または 1 つ以上の特定の曜日について、帯域幅レート制限期間を作成できます。
- [開始時刻] – ゲートウェイのローカルタイムゾーンを使用して、帯域幅期間の開始時刻を HH:MM 形式で入力します。

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

- [終了時刻] – ゲートウェイのローカルタイムゾーンを使用して、帯域幅レート制限の期間の終了時刻を HH:MM 形式で入力します。

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

- [ダウンロード速度] – ダウンロードのレート制限をキロビット/秒 (Kbps) で入力するか、[無制限] を選択して、ダウンロードの帯域幅スロットリングを無効にします。ダウンロード速度の最小値は 100 Kbps です。
- [アップロード速度] – アップロードのレート制限をキロビット/秒 (Kbps) で入力するか、[無制限] を選択して、アップロードの帯域幅スロットリングを無効にします。アップロード速度の最小値は 50 Kbps です。

帯域幅レート制限期間を変更するには、期間パラメータの変更後の値を入力します。

帯域幅レート制限期間を削除するには、削除対象の期間の右側にある [削除] をクリックします。

変更が完了したら、[保存] をクリックします。

5. 引き続き帯域幅レート制限期間を追加するには、[新しいエントリの追加] を選択し、曜日、開始時刻と終了時刻、ダウンロードおよびアップロードのレート制限を入力します。

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

6. すべての帯域幅レート制限期間を入力したら、[保存] をクリックして、帯域幅レート制限スケジュールを保存します。

帯域幅レート制限スケジュールが正常に更新されると、現在のダウンロードおよびアップロードのレート制限がゲートウェイの [詳細] パネルに表示されます。

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

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

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

次の Java コードの例では、ゲートウェイの帯域幅レート制限を更新します。このサンプルコードを使用するには、サービスエンドポイント、ゲートウェイ Amazon リソースネーム (ARN) 、およびアップロード制限とダウンロード制限を指定する必要があります。Storage Gateway で使用できる AWS サービスエンドポイントのリストについては、のAWS Storage Gateway 「エンドポイントとクォータ」を参照してくださいAWS 全般のリファレンス。

```
import java.io.IOException;

import com.amazonaws.AmazonClientException;
import com.amazonaws.auth.PropertiesCredentials;
import com.amazonaws.services.storagegateway.AWSStorageGatewayClient;
import com.amazonaws.services.storagegateway.model.UpdateBandwidthRateLimitRequest;
import com.amazonaws.services.storagegateway.model.UpdateBandwidthRateLimitResult;


public class UpdateBandwidthExample {

    public static AWSStorageGatewayClient sgClient;
```

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

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

   // Rates
   static long uploadRate = 51200;  // Bits per second, minimum 51200
   static long downloadRate = 102400;   // Bits per second, minimum 102400

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

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

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

       UpdateBandwidth(gatewayARN, uploadRate, downloadRate);

   }

   private static void UpdateBandwidth(String gatewayARN2, long uploadRate2,
           long downloadRate2) {
       try
       {
           UpdateBandwidthRateLimitRequest updateBandwidthRateLimitRequest =
               new UpdateBandwidthRateLimitRequest()
               .withGatewayARN(gatewayARN)
               .withAverageDownloadRateLimitInBitsPerSec(downloadRate)
               .withAverageUploadRateLimitInBitsPerSec(uploadRate);

           UpdateBandwidthRateLimitResult updateBandwidthRateLimitResult =
sgClient.updateBandwidthRateLimit(updateBandwidthRateLimitRequest);
           String returnGatewayARN = updateBandwidthRateLimitResult.getGatewayARN();
           System.out.println("Updated the bandwidth rate limits of " +
returnGatewayARN);
           System.out.println("Upload bandwidth limit = " + uploadRate + " bits per
second");
           System.out.println("Download bandwidth limit = " + downloadRate + " bits
per second");
       }
       catch (AmazonClientException ex)
```

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

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

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

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

次の C# コードの例では、ゲートウェイの帯域幅レート制限を更新します。このサンプルコードを使用するには、サービスエンドポイント、ゲートウェイ Amazon リソースネーム (ARN) 、およびアップロード制限とダウンロード制限を指定する必要があります。Storage Gateway で使用できる AWS サービスエンドポイントのリストについては、のAWS Storage Gateway 「エンドポイントとクォータ」を参照してくださいAWS 全般のリファレンス。

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

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

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

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

```
        // Rates
        static long uploadRate = 51200;  // Bits per second, minimum 51200
        static long downloadRate = 102400;   // Bits per second, minimum 102400

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

            UpdateBandwidth(gatewayARN, uploadRate, downloadRate);

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

        public static void UpdateBandwidth(string gatewayARN, long uploadRate, long
downloadRate)
        {
            try
            {
                UpdateBandwidthRateLimitRequest updateBandwidthRateLimitRequest =
                    new UpdateBandwidthRateLimitRequest()
                    .WithGatewayARN(gatewayARN)
                    .WithAverageDownloadRateLimitInBitsPerSec(downloadRate)
                    .WithAverageUploadRateLimitInBitsPerSec(uploadRate);

                UpdateBandwidthRateLimitResponse updateBandwidthRateLimitResponse =
sgClient.UpdateBandwidthRateLimit(updateBandwidthRateLimitRequest);
                String returnGatewayARN =
updateBandwidthRateLimitResponse.UpdateBandwidthRateLimitResult.GatewayARN;
                Console.WriteLine("Updated the bandwidth rate limits of " +
returnGatewayARN);
                Console.WriteLine("Upload bandwidth limit = " + uploadRate + " bits per
second");
                Console.WriteLine("Download bandwidth limit = " + downloadRate + " bits
per second");
            }
            catch (AmazonStorageGatewayException ex)
            {
                Console.WriteLine("Error updating gateway bandwith.\n" +
ex.ToString());
            }
```

```
        }
    }
}
```

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

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

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

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

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

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


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

$UploadBandwidthRate = 51200
$DownloadBandwidthRate = 102400
$gatewayARN = "*** provide gateway ARN ***"

#Update Bandwidth Rate Limits
```

```
Update-SGBandwidthRateLimit -GatewayARN $gatewayARN `
                            -AverageUploadRateLimitInBitsPerSec $UploadBandwidthRate `
                            -AverageDownloadRateLimitInBitsPerSec
 $DownloadBandwidthRate

$limits =  Get-SGBandwidthRateLimit -GatewayARN $gatewayARN

Write-Output("`nGateway: " + $gatewayARN);
Write-Output("`nNew Upload Rate: " + $limits.AverageUploadRateLimitInBitsPerSec)
Write-Output("`nNew Download Rate: " + $limits.AverageDownloadRateLimitInBitsPerSec)
```

ゲートウェイアップデートの管理

Storage Gateway は、マネージドクラウドサービスコンポーネントと、オンプレミスまたは AWS クラウド内の Amazon EC2 インスタンスにデプロイするゲートウェイアプライアンスコンポーネントで構成されます。どちらのコンポーネントも定期的に更新されます。このセクションのトピックでは、これらの更新の頻度、適用方法、デプロイ内のゲートウェイで更新関連の設定を行う方法について説明します。

> **Important**
>
> Storage Gateway アプライアンスは、マネージド型の仮想マシンとして扱い、インストールへのアクセスや変更を試みるべきではありません。通常の AWS ゲートウェイ更新メカニズム (SSM やハイパーバイザーツールなど) 以外の方法を使用してソフトウェアパッケージをインストールまたは更新しようとすると、ゲートウェイが誤動作する可能性があります。

更新頻度と予想される動作

AWS は、デプロイされたゲートウェイを中断することなく、必要に応じてクラウドサービスコンポーネントを更新します。デプロイされたゲートウェイアプライアンスは、毎月のメンテナンス更新を受け取ります。毎月のメンテナンス更新には、オペレーティングシステムとソフトウェアのアップグレード、安定性、パフォーマンス、セキュリティに対処するための修正、新機能へのアクセスが含まれます。すべての更新は累積的であり、適用時にゲートウェイを現在のバージョンにアップグレードします。各更新に含まれる特定の変更の詳細については「ボリュームゲートウェイアプライアンスソフトウェアのリリースノート」を参照してください。

毎月のメンテナンス更新により、サービスが短時間中断される可能性があります。ゲートウェイの VM ホストは更新中に再起動する必要はありませんが、ゲートウェイアプライアンスが更新および

再起動している間は、ゲートウェイが短期間使用できなくなります。ゲートウェイの再起動によってアプリケーションが中断される可能性を最小限に抑えるには、iSCSI イニシエータのタイムアウトを延長します。Windows と Linux の iSCSI イニシエータタイムアウト延長の詳細については、「Windows iSCSI 設定のカスタマイズ」および「Linux iSCSI 設定のカスタマイズ」を参照してください。

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ウィンドウスケジュールが設定されます。メンテナンスウィンドウスケジュールはいつでも変更できます。毎月のメンテナンス更新をオフにすることもできますが、オンのままにしておくことをお勧めします。

> **Note**
>
> 緊急の更新は、定期的なメンテナンス更新がオフになっていても、メンテナンスウィンドウのスケジュールに従って適用されることがあります。

更新がゲートウェイに適用される前に、 は Storage Gateway コンソールと にメッセージで AWS 通知します AWS Health Dashboard。詳細については、「AWS Health Dashboard」を参照してください。ソフトウェア更新通知の送信先の E メールアドレスを変更するには、AWS 「 アカウント管理リファレンスガイド」の「アカウントの代替連絡先の更新」を参照してください。 AWS

更新が利用可能な場合は、ゲートウェイの [詳細] タブにメンテナンスメッセージが表示されます。また、[詳細] タブには、最後に更新が正常に適用された日時が表示されます。

メンテナンスアップデートをオンまたはオフにする

メンテナンスアップデートがオンになっている場合、ゲートウェイは設定されたメンテナンスウィンドウのスケジュールに従ってこれらのアップデートを自動的に適用します。詳細については、「」を参照してください。

メンテナンスアップデートがオフになっている場合、ゲートウェイはこれらのアップデートを自動的に適用しませんが、Storage Gateway コンソール、API、または CLI を使用していつでも手動で適用できます。この設定に関係なく、設定されたメンテナンスウィンドウ中に緊急の更新が適用されることがあります。

> **Note**
>
> 次の手順では、Storage Gateway コンソールを使用してゲートウェイの更新をオンまたはオフにする方法について説明します。API を使用してプログラムでこの設定を変更するには、

「Storage Gateway API リファレンス」の「UpdateMaintenanceStartTime」を参照してください。

Storage Gateway コンソールを使用してメンテナンスアップデートをオンまたはオフにするには:

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. ナビゲーションペインで、[ゲートウェイ] を選択してから、メンテナンス更新を設定するゲートウェイを選択します。
3. [アクション] を選択し、[メンテナンス設定を編集] を選択します。
4. [メンテナンスアップデート] では、[オン] または [オフ] を選択します。
5. 完了したら、[変更を保存] を選択します。

Storage Gateway コンソールの選択したゲートウェイの [詳細] タブで、更新された設定を確認できます。

ゲートウェイのメンテナンスウィンドウのスケジュールを変更する

メンテナンス更新が有効になっている場合、ゲートウェイはメンテナンスウィンドウのスケジュールに従ってこれらの更新を自動的に適用します。緊急更新は、メンテナンス更新の設定に関係なく、設定されたメンテナンスウィンドウ中に適用されることがあります。

> **Note**
>
> 次の手順では、Storage Gateway コンソールを使用してメンテナンスウィンドウのスケジュールを変更する方法について説明します。API を使用してプログラムでこの設定を変更するには、「Storage Gateway API リファレンス」の「UpdateMaintenanceStartTime」を参照してください。

Storage Gateway コンソールを使用してメンテナンスウィンドウのスケジュールを変更するには:

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. ナビゲーションペインで、[ゲートウェイ] を選択してから、メンテナンス更新を設定するゲートウェイを選択します。

3. [アクション] を選択し、[メンテナンス設定を編集] を選択します。
4. [メンテナンスウィンドウの開始時刻] で、次の操作を行います。

   a. [スケジュール] では、[毎週] または [毎月] を選択してメンテナンスウィンドウの頻度を設定します。

   b. [毎週] を選択した場合は、[曜日] と [時刻] の値を変更して、メンテナンスウィンドウが始まる各週の特定のポイントを設定します。

      [毎月] を選択した場合は、[日付] と [時刻] の値を変更して、メンテナンスウィンドウが始まる各月の特定のポイントを設定します。

      > **Note**
      >
      > 月の中の日として設定できる最大値は 28 です。メンテナンススケジュールを 29 日目から 31 日目に開始するように設定することはできません。
      > この設定を構成中にエラーが表示された場合は、ゲートウェイソフトウェアが古くなっている可能性があります。まずゲートウェイを手動で更新してから、メンテナンスウィンドウのスケジュールを再度設定することを検討してください。

5. 完了したら、[変更を保存] を選択します。

Storage Gateway コンソールの選択したゲートウェイの [詳細] タブで、更新された設定を確認できます。

更新を手動で適用する

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

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

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

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. ナビゲーションペインで [ゲートウェイ] を選択してから、更新するゲートウェイを選択します。

   更新が利用可能な場合、コンソールはゲートウェイの [詳細] タブに青い通知バナーを表示します。これには、更新を適用するオプションが含まれます。
3. [アップデートを今すぐ適用する] を選択して、ゲートウェイをすぐに更新します。

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

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

ゲートウェイ VM のシャットダウン

ハイパーバイザーにパッチを適用するときなど、メンテナンスのために VM をシャットダウンまたは再起動する必要がある場合があります。VM をシャットダウンする前に、まずゲートウェイを停止する必要があります。このセクションでは、Storage Gateway マネジメントコンソールを使用したゲートウェイの開始および停止について主に取り上げますが、VM ローカルコンソールまたは Storage Gateway API でもゲートウェイを開始および停止できます。VM の電源をオンにするときは、必ずゲートウェイを再起動します。

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

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

- Gateway VM ローカルコンソール – 「ボリュームゲートウェイのローカルコンソールへのログイン」を参照してください。
- Storage Gateway API – 「ShutdownGateway」を参照してください。

ボリュームゲートウェイを起動および停止する

ボリュームゲートウェイを停止するには

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

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

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

ボリュームゲートウェイを起動するには

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

2. ナビゲーションペインで [Gateways] を選択してから、起動するゲートウェイを選択します。ゲートウェイのステータスは [シャットダウン] です。
3. [詳細] を選択します。それから、[ゲートウェイの起動] を選択します。

ゲートウェイおよび関連リソースの削除

ゲートウェイを引き続き使用する予定がない場合は、ゲートウェイとそれに関連付けられているリソースを削除することを検討してください。リソースを除去することで、引き続き使用する予定がないリソースに対する課金を回避し、月額利用料金を削減できます。

ゲートウェイを削除すると、そのゲートウェイは AWS Storage Gateway マネジメントコンソールに表示されなくなり、イニシエータへの iSCSI 接続は閉じられます。ゲートウェイを削除する手順は、すべてのゲートウェイタイプで同じです。ただし、関連付けられているリソースを除去するには、削除するゲートウェイのタイプとそれがデプロイされているホストに応じた手順に従います。

ゲートウェイは、Storage Gateway コンソールを使用して、またはプログラムによって削除できます。以下では、Storage Gateway コンソールを使用してゲートウェイを削除する方法について説明します。プログラムによってゲートウェイを削除する場合は、「AWS Storage Gateway API Reference」を参照してください。

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削除

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 (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. [ゲートウェイ] を選択し、削除対象のゲートウェイを 1 つ以上選択します。
3. [Actions (アクション)] の [Delete gateway (ゲートウェイを削除)] を選択します。確認のダイアログボックスが表示されます。

   Warning

   このステップを行う前に、ゲートウェイのボリュームに現在書き込んでいるアプリケーションがないことを確認してください。使用中のゲートウェイを削除すると、データが失われる場合があります。ゲートウェイを削除すると、復元できなくなります。

4. 指定したゲートウェイを削除することを確認し、確認ボックスに「delete」と入力して [削除] を選択します。
5. (オプション) 削除されたゲートウェイに関するフィードバックを提供する場合は、フィードバックダイアログボックスに入力してから [送信] をクリックします。それ以外の場合は、[スキップ] を選択します。

Important

ゲートウェイを削除すると、ソフトウェア料金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 インスタンスと Amazon EBS スナップショットは、Amazon EC2 サブスクリプションをキャンセルすることによって削除できます。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。手順については、Storage Gateway コンソールを使用したゲートウェイの削除 を参照してください。
- 不要な Amazon EBS スナップショットをすべて削除します。手順については、「Amazon EC2 ユーザーガイド」の「Amazon EBS スナップショットの削除」を参照してください。

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削除

Amazon EC2 インスタンスにデプロイしたゲートウェイを削除する場合は、ゲートウェイで使用された AWS リソース、特に Amazon EC2 インスタンス、Amazon EBS ボリューム、テープゲートウェイをデプロイした場合はテープをクリーンアップすることをお勧めします。クリーンアップによって、意図しない使用に対する課金を回避できるためです。

Amazon 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削除

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. 「Storage Gateway コンソールを使用したゲートウェイの削除」で示されているように、Storage Gateway コンソールでゲートウェイを削除します。
2. EC2 インスタンスを再度使用する予定がある場合は、Amazon EC2 コンソールでその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. インスタンスにアタッチされている Amazon EBS ボリュームを再度使用する予定がない場合は、Amazon EC2 コンソールですべて削除します。詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスとボリュームのクリーンアップ」を参照してください。

ローカルコンソールを使用したメンテナンスタスクの実行

このセクションでは、ゲートウェイアプライアンスのローカルコンソールを使用してメンテナンスタスクを実行する方法に関する情報を提供する次のトピックが含まれています。ローカルコンソールは、ゲートウェイアプライアンスをホストする仮想化ホストプラットフォームで直接実行されます。オンプレミスゲートウェイの場合、VMware、Hyper-v、または Linux KVM 仮想化ホストを介してローカルコンソールにアクセスします。Amazon EC2 ゲートウェイの場合は、SSH を使用して Amazon EC2 インスタンスに接続してコンソールにアクセスします。ほとんどのタスクはさまざまなホストプラットフォーム間で共通していますが、異なる点もいくつかあります。

トピック

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

ゲートウェイローカルコンソールへのアクセス

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

Linux KVM でゲートウェイのローカルコンソールにアクセスする

KVM で実行する仮想マシンを構成する方法は、使用する Linux ディストリビューションによって異なります。コマンドラインから KVM 構成オプションにアクセスする手順は次のとおりです。手順は KVM の実装によって異なる場合があります。

KVM でゲートウェイのローカルコンソールにアクセスするには

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

   ```
   # virsh list
   ```

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

2. ローカルコンソールにアクセスするには、次のコマンドを使用します。

   ```
   # virsh console Id
   ```

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

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

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

   ログインすると、[AWS アプライアンスのアクティベーション - 設定] メニューが表示されます。メニューオプションから選択して、ゲートウェイ設定タスクを実行できます。詳細については、「仮想マシンのローカルコンソールでのタスクの実行」を参照してください。

VMware ESXi でゲートウェイのローカルコンソールにアクセスする

VMware ESXi でゲートウェイのローカルコンソールにアクセスするには

1. VMware vSphere クライアントで、ゲートウェイの VM を選択します。
2. ゲートウェイ VM がオンになっていることを確認します。

> **Note**
>
> ゲートウェイ VM がオンになっている場合、アプリケーションウィンドウの左側にある VM ブラウザパネルに、VM アイコンと共に緑色の矢印アイコンが表示されます。ゲートウェイ VM がオンになっていない場合は、アプリケーションウィンドウの上部にある [ツールバー] の緑の [電源オン] アイコンをクリックしてオンにすることができます。

3. アプリケーションウィンドウの右側にあるメイン情報パネルの [コンソール] タブを選択します。

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

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

4. ユーザー名とパスワードを入力して、ゲートウェイローカルコンソールにログインします。詳細については、「ボリュームゲートウェイローカルコンソールへのログイン」を参照してください。

   ログインすると、[AWS アプライアンスのアクティベーション - 設定] メニューが表示されます。メニューオプションから選択して、ゲートウェイ設定タスクを実行できます。詳細については、「仮想マシンのローカルコンソールでのタスクの実行」を参照してください。

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

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

1. Microsoft Hyper-V Manager アプリケーションウィンドウの左側にある [仮想マシン] パネルからゲートウェイアプライアンス VM を選択します。
2. ゲートウェイの電源がオンになっていることを確認します。

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

3. [アクション] パネルから [接続] を選択します。

   [Virtual Machine Connection] ウィンドウが表示されます。認証ウィンドウが表示されたら、ハイパーバイザー管理者から提供されたサインイン認証情報を入力します。

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

4. ユーザー名とパスワードを入力して、ゲートウェイローカルコンソールにログインします。詳細については、「ボリュームゲートウェイローカルコンソールへのログイン」を参照してください。

   ログインすると、[AWS アプライアンスのアクティベーション - 設定] メニューが表示されます。メニューオプションから選択して、ゲートウェイ設定タスクを実行できます。詳細については、「仮想マシンのローカルコンソールでのタスクの実行」を参照してください。

VM ローカルコンソールでのタスクの実行

オンプレミスにデプロイするボリュームゲートウェイの場合、仮想マシンホストプラットフォームからアクセスするゲートウェイ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。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

- ボリュームゲートウェイのローカルコンソールへのログイン - ゲートウェイネットワーク設定を構成し、デフォルトのパスワードを変更できるゲートウェイローカルコンソールにログインする方法について説明します。
- オンプレミスゲートウェイの SOCKS5 プロキシの設定 - ソケットセキュアバージョン 5 (SOCKS5) プロキシサーバーを介してすべての AWS エンドポイントトラフィックをルーティングするように Storage Gateway を設定する方法について説明します。

- ゲートウェイのネットワークの設定 - DHCP を使用するようにゲートウェイを設定する方法、または静的 IP アドレスを割り当てる方法について説明します。
- ゲートウェイのインターネット接続のテスト - ゲートウェイローカルコンソールを使用してゲートウェイとインターネット間の接続をテストする方法について説明します。
- オンプレミスゲートウェイの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 - ルーティングテーブルの保存、 への接続などの追加のタスクを実行できるようにするローカルコンソールコマンドを実行する方法について説明します サポート。
- ゲートウェイシステムリソースのステータスの表示 - ゲートウェイアプライアンスで使用できる仮想 CPU コア、ルートボリュームサイズ、RAM を確認する方法について説明します。

ボリュームゲートウェイのローカルコンソールへのログイン

VM にログインできるようになると、ログイン画面が表示されます。ローカルコンソールに初めてログインする場合は、デフォルトのサインイン認証情報を使用してログインします。これらのデフォルトのログイン認証情報を使用することで、ゲートウェイのネットワーク設定を構成したり、ローカルコンソールからパスワードを変更したりできるメニューにアクセスできます。Storage Gateway では、ローカル AWS Storage Gateway コンソールからパスワードを変更する代わりに、コンソールから独自のパスワードを設定できます。新しいパスワードを設定するためにデフォルトパスワードを知っている必要はありません。詳細については、「Storage Gateway コンソールからのローカルコンソールパスワードの設定」を参照してください。

ゲートウェイのローカルコンソールにログインするには

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

  初めてではない場合は、認証情報を使用してログインします。

  > **Note**
  >
  > デフォルトのパスワードは変更することを推奨します。変更するには、[AWS Appliance Activation - Configuration] メインメニューで [Gateway Console] に対応する番号を入力し、`passwd` コマンドを実行してください。このコマンドを実行する方法については、「オンプレミスゲートウェイの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。 AWS Storage Gateway コンソールから独自のパス

ワードを設定することもできます。詳細については、「Storage Gateway コンソールからのローカルコンソールパスワードの設定」を参照してください。

> **Important**
>
> 古いバージョンのボリュームまたはテープゲートウェイでは、ユーザー名は `sguser`、パスワードは `sgpassword` です。パスワードをリセットし、ゲートウェイが新しいバージョンに更新された場合、ユーザー名は admin に変更されますが、パスワードは維持されます。

Storage Gateway コンソールからのローカルコンソールパスワードの設定

ローカルコンソールに初めてログインするとき、デフォルトの認証情報 (ユーザー名 `admin` およびパスワード `password`) を使用して VM にログインします。新しいゲートウェイを作成した直後に必ず新しいパスワードを設定することをお勧めします。このパスワードは、必要に応じてローカルコンソールではなく AWS Storage Gateway コンソールから設定できます。新しいパスワードを設定するためにデフォルトパスワードを知っている必要はありません。

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

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. ナビゲーションペインで、[Gateways] を選択し、新しいパスワードを設定するゲートウェイを選択します。
3. [Actions] で、[Set Local Console Password] を選択します。
4. [Set Local Console Password] ダイアログボックスで、新しいパスワードを入力し、確認のためにパスワードを再入力してから、[Save] を選択します。新しいパスワードを設定すると、デフォルトのパスワードが置き換えられます。Storage Gateway にはパスワードが保存されず、VM に安全に送信されます。

> **Note**
>
> パスワードには、キーボードの任意の文字を使用することができ、長さは 1 ~ 512 文字です。

オンプレミスゲートウェイの SOCKS5 プロキシの設定

ボリュームゲートウェイとテープゲートウェイは、オンプレミスゲートウェイと AWSの間で Socket Secure バージョン 5 (SOCKS5) プロキシの設定をサポートします。

> **Note**
>
> サポート対象のプロキシ設定は SOCKS5 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、SOCKS 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。その後、Storage Gateway はすべてのトラフィックをプロキシサーバー経由でルーティングします。ゲートウェイのネットワーク要件の詳細については、ネットワークとファイアウォールの要件を参照してください。

次の手順では、ボリュームゲートウェイとテープゲートウェイの SOCKS プロキシを設定する方法を示します。

ボリュームゲートウェイとテープゲートウェイの SOCKS5 プロキシを設定するには

1. ゲートウェイのローカルコンソールにログインします。
   - VMware ESXi – 詳細については、「VMware ESXi でゲートウェイのローカルコンソールにアクセスする」を参照してください。
   - Microsoft Hyper-V – 詳細については、「Microsoft Hyper-V でゲートウェイのローカルコンソールにアクセスする」を参照してください。
   - KVM – 詳細については、「Linux KVM でゲートウェイのローカルコンソールにアクセスする」を参照してください。
2. [AWS Storage Gateway - Configuration] メインメニューから、対応する番号を入力して [SOCKS Proxy Configuration] を選択します。
3. [AWS Storage Gateway SOCKS Proxy Configuration] メニューから、対応する番号を入力して、以下のいずれかのタスクを実行します。

このタスクを実行するには	操作
SOCKS プロキシを設定する	

このタスクを実行するには	操作
	対応する番号を入力して [Configure SOCKS Proxy] を選択します。 設定を完了するには、ホスト名とポートを指定する必要があります。
SOCKS プロキシの現在の設定を表示する	対応する番号を入力して [View Current SOCKS Proxy Configuration] を選択します。 SOCKS プロキシが設定されていない場合は、"`SOCKS Proxy not configured`" というメッセージが表示されます。SOCKS が設定されている場合は、プロキシのホスト名とポートが表示されます。
SOCKS プロキシの設定を削除する	対応する番号を入力して [Remove SOCKS Proxy Configuration] を選択します。 "`SOCKS Proxy Configuration Removed`" というメッセージが表示されます。

4. VM を再起動して HTTP 設定を適用します。

ゲートウェイのネットワークの設定

ゲートウェイのデフォルトのネットワーク設定は、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 – 詳細については、「VMware ESXi でゲートウェイのローカルコンソールにアクセスする」を参照してください。

- Microsoft Hyper-V – 詳細については、「Microsoft Hyper-V でゲートウェイのローカルコンソールにアクセスする」を参照してください。
- KVM – 詳細については、「Linux KVM でゲートウェイのローカルコンソールにアクセスする」を参照してください。

2. [AWS Storage Gateway - Configuration] メインメニューから、対応する番号を入力して [Network Configuration] を選択します。
3. [AWS Storage Gateway Network Configuration] メニューから、以下のいずれかのタスクを実行します。

このタスクを実行するには	操作
ネットワークアダプタの詳細を表示する	対応する番号を入力して [Describe Adapter] を選択します。 アダプタ名のリストが表示され、「**eth0**」などのアダプタ名の入力を求めるプロンプトが表示されます。指定したアダプタが使用中の場合、アダプタに関する次の情報が表示されます。 • メディアアクセスコントロール (MAC) アドレス • IP アドレス • ネットマスク • ゲートウェイ IP アドレス • DHCP アクティブ化ステータス 静的 IP アドレスを設定したり、ゲートウェイのデフォルトアダプタを設定したりするとき

このタスクを実行するには	操作
	は、ここに記載されているアダプタ名を使用します。
DHCP を設定する	対応する番号を入力して [Configure DHCP] を選択します。 DHCP を使用するようにネットワークインターフェイスを設定するように求められます。

このタスクを実行するには	操作
ゲートウェイの静的 IP アドレスを設定する	対応する番号を入力して [Configure Static IP] を選択します。 静的 IP アドレスを設定するために、以下の情報の入力を求められます。 • ネットワークアダプタ名 • IP アドレス • ネットマスク • デフォルトゲートウェイアドレス • プライマリドメインネームサービス (DNS) アドレス • セカンダリ DNS アドレス **Important** ゲートウェイが既にアクティブになっている場合、設定を有効にするには、Storage Gateway コンソールでゲートウェイをシャットダウンして再起動する必要があります。詳細については、「ゲートウェイ VM のシャットダウン」を参照してください。 ゲートウェイ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、有効になって

このタスクを実行するには	操作
	いるインターフェイスのすべてで、DHCP または静的 IP アドレスを使用するように設定する必要があります。 たとえば、ゲートウェイ VM で DHCP として設定された 2 つのインターフェイスを使用するとします。後で 1 つのインターフェイスを静的 IP に設定すると、もう 1 つのインターフェイスは無効になります。この場合、そのインターフェイスを有効にするには、静的 IP を設定する必要があります。 最初に両方のインターフェイスが静的 IP アドレスを使用するように設定されている場合、DHCP を使用するようにゲートウェイを設定すると、どちらのインターフェイスも DHCP を使用するようになります。

このタスクを実行するには	操作
ゲートウェイのホスト名を設定する	対応する番号を入力して [Configure Hostname] を選択します。 指定した静的ホスト名をゲートウェイで使用するか、DHCP または RDN を通じて自動的に取得するかを選択するように求められます。 [静的] を選択すると、`testgateway.example.com` などの静的ホスト名を指定するように求められます。y を入力して設定を適用します。 **Note** ゲートウェイに静的ホスト名を設定する場合は、指定されたホスト名がゲートウェイが結合されているドメインにあることを確認します。また、ゲートウェイの IP アドレスを静的ホスト名にポイントする A レコードを DNS システム内に作成する必要があります。

このタスクを実行するには	操作
ゲートウェイのすべてのネットワーク設定を DHCP にリセットする	対応する番号を入力して [Reset all to DHCP] を選択します。 すべてのネットワークインターフェイスが、DHCP を使用するように設定されます。 **Important** ゲートウェイがすでにアクティブになっている場合、設定を有効にするには、Storage Gateway コンソールでゲートウェイをシャットダウンして再起動する必要があります。詳細については、「ゲートウェイ VM のシャットダウン」を参照してください。
ゲートウェイのデフォルトルートアダプタを設定する	対応する番号を入力して [Set Default Adapter] を選択します。 ゲートウェイで使用できるアダプタが表示され、「**eth0**」など、いずれかのアダプタを選択するよう求めるプロンプトが表示されます。
ゲートウェイの DNS 設定を表示する	対応する番号を入力して [View DNS Configuration] を選択します。 プライマリとセカンダリの DNS ネームサーバーの IP アドレスが表示されます。

このタスクを実行するには	操作
ルーティングテーブルを表示する	対応する番号を入力して [View Routes] を選択します。 ゲートウェイのデフォルトルートが表示されます。

ゲートウェイのインターネット接続のテスト

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

インターネットに対するゲートウェイの接続をテストするには

1. ゲートウェイのローカルコンソールにログインします。
   - VMware ESXi – 詳細については、「VMware ESXi でゲートウェイのローカルコンソールにアクセスする」を参照してください。
   - Microsoft Hyper-V – 詳細については、「Microsoft Hyper-V でゲートウェイのローカルコンソールにアクセスする」を参照してください。
   - KVM – 詳細については、「Linux KVM でゲートウェイのローカルコンソールにアクセスする」を参照してください。
2. [AWS Storage Gateway - Configuration] メインメニューから、対応する番号を入力して [Test Network Connectivity] を選択します。

   ゲートウェイがすでにアクティブ化されている場合は、接続テストがすぐに開始します。まだアクティブ化されていないゲートウェイの場合は、次の手順で説明 AWS リージョン するように、エンドポイントタイプ と を指定する必要があります。
3. ゲートウェイがまだアクティブ化されていない場合は、対応する番号を入力して、ゲートウェイのエンドポイントタイプを選択します。
4. パブリックエンドポイントタイプを選択した場合は、対応する数字を入力して、テスト AWS リージョン する を選択します。サポートされているサービスエンドポイント AWS リージョン と Storage Gateway で使用できる AWS サービスエンドポイントのリストについては、「」のAWS Storage Gateway 「エンドポイントとクォータ」を参照してくださいAWS 全般のリファレンス。

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

メッセージ	説明
[PASSED]	Storage Gateway がネットワークに接続されています。
[FAILED]	Storage Gateway はネットワークに接続されていません。

オンプレミスゲートウェイの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コマンドを使用して、ルーティングテーブルの保存、 への接続などのメンテナンスタスクを実行できます サポート。

設定または診断コマンドを実行するには

1. ゲートウェイのローカルコンソールにログインします。

   - VMware ESXi ローカルコンソールへのログインの詳細については、「VMware ESXi でゲートウェイのローカルコンソールにアクセスする」を参照してください。
   - Microsoft Hyper-V ローカルコンソールへのログインの詳細については、「Microsoft Hyper-V でゲートウェイのローカルコンソールにアクセスする」を参照してください。
   - KVM ローカルコンソールへのログインの詳細については、「Linux KVM でゲートウェイのローカルコンソールにアクセスする」を参照してください。

2. [AWS Appliance Activation - Configuration] メインメニューから、対応する番号を入力して「Gateway Console」を選択します。
3. ゲートウェイコンソールのコマンドプロンプトから、「**h**」と入力します。

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

コマンド	関数
dig	DNS のトラブルシューティング用に、dig からの出力を収集します。
exit	コンソール設定メニューに戻ります。
h	使用可能なコマンドリストを表示します。
ifconfig	ネットワークインターフェイスを表示または設定します。 **Note** Storage Gateway コンソールまたは専用のローカルコンソールメニューオプションを使用して、ネットワークまたは IP 設定を構成することをお勧めします。手順については、「ゲートウェイネットワークの設定」を参照してください。
ip	ルーティング、デバイス、トンネルを表示または操作します。 **Note** Storage Gateway コンソールまたは専用のローカルコンソールメニューオプションを使用して、ネットワークまたは IP 設定を構成することをお勧めします。手順については、「ゲートウェイネットワークの設定」を参照してください。

コマンド	関数
iptables	IPv4 パケットフィルタリングおよび NAT の管理ツール。
ncport	ネットワーク上の特定の TCP ポートへの接続をテストします。
nping	ネットワークのトラブルシューティング用に、nping からの出力を収集します。
open-support-channel	AWS サポートに接続します。
passwd	認証トークンを更新します。
save-iptables	IP テーブルを永続化します。
save-routing-table	新しく追加されたルーティングテーブルエントリーを保存します。
sslcheck	証明書発行者の出力を返します。 **Note** Storage Gateway は証明書発行者の検証を使用し、SSL 検査をサポートしていません。このコマンドが aws-appliance@amazon.com 以外の発行者を返す場合、アプリケーションが SSL 検査を実行する可能性があります。この場合、Storage Gateway アプライアンスの SSL 検査をバイパスすることをお勧めします。
tcptraceroute	送信先への TCP トラフィックに関する traceroute 出力を収集します。

4. ゲートウェイコンソールのコマンドプロンプトから、使用したい機能に対応するコマンドを入力し、指示に従います。

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

ゲートウェイシステムリソースのステータスの表示

ゲートウェイの開始時に、その仮想 CPU コア、ルートボリュームサイズ、RAM がチェックされます。その後、ゲートウェイが適切に機能するためにこれらのシステムリソースが十分であるかどうかが確認されます。このチェックの結果は、ゲートウェイのローカルコンソールで表示できます。

システムリソースチェックのステータスを表示するには

1. ゲートウェイのローカルコンソールにログインします。

   - VMware ESXi コンソールへのログインの詳細については、「VMware ESXi でゲートウェイのローカルコンソールにアクセスする」を参照してください。
   - Microsoft Hyper-V ローカルコンソールへのログインの詳細については、「Microsoft Hyper-V でゲートウェイのローカルコンソールにアクセスする」を参照してください。
   - KVM ローカルコンソールへのログインの詳細については、「Linux KVM でゲートウェイのローカルコンソールにアクセスする」を参照してください。

2. [AWS Appliance Activation - Configuration] メインメニューで、対応する番号を入力して「View System Resource Check」を選択します。

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

メッセージ	説明
[OK]	リソースはシステムリソースチェックに合格しました。
[WARNING]	リソースは推奨される要件を満たしていませんが、ゲートウェイは引き続き機能します。Storage Gateway は、リソースチェックの結果について説明するメッセージを表示します。
[FAIL]	リソースは最小要件を満たしていません。ゲートウェイ は適切に機能していない可能性があります。Storage Gateway は、リソースチェッ

メッセージ	説明
	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。

Amazon EC2 ローカルコンソールでのタスクの実行

一部の Storage Gateway メンテナンスタスクでは、Amazon EC2 インスタンスにデプロイしたゲートウェイのゲートウェイローカルコンソールにログインする必要があります。Secure Shell (SSH) クライアントを使用して、Amazon EC2 インスタンス上のゲートウェイローカルコンソールに接続できます。このセクションのトピックでは、ゲートウェイローカルコンソールにログインして、メンテナンスタスクを実行する方法について説明します。

トピック

- Amazon EC2 ゲートウェイのローカルコンソールへのログイン - Secure Shell (SSH) クライアントを使用して Amazon EC2 インスタンスをゲートウェイローカルコンソールに接続してログインする方法について説明します。
- EC2 にデプロイされたゲートウェイの HTTP プロキシ経由のルーティング - ソケットセキュアバージョン 5 (SOCKS5) プロキシサーバーを介してすべての AWS エンポイントトラフィックを Amazon EC2 ゲートウェイインスタンスにルーティングするように Storage Gateway を設定する方法について説明します。
- ゲートウェイのネットワーク接続をテストする - ゲートウェイローカルコンソールを使用して、ゲートウェイとさまざまなネットワークリソース間のネットワーク接続をテストする方法について説明します。
- ゲートウェイシステムリソースのステータスの表示 - ゲートウェイローカルコンソールを使用して、ゲートウェイアプライアンスで使用できる仮想 CPU コア、ルートボリュームサイズ、および RAM を確認する方法について説明します。
- ローカルコンソールでの Storage Gateway コマンドの実行 - ルーティングテーブルの保存、 への接続などの追加のタスクを実行できるようにするローカルコンソールコマンドを実行する方法について説明します サポート。

Amazon EC2 ゲートウェイのローカルコンソールへのログイン

Secure Shell (SSH) クライアントを使用して、Amazon EC2 インスタンスに接続できます。詳細については、Amazon EC2 Linux インスタンス用 ユーザーガイドの「Linux インスタンスへの接続」を参照してください。この方法で接続するには、インスタンスを起動したときに指定した SSH キーペアが必要です。Amazon EC2 キーペアについては、Amazon EC2 Linux インスタンス用 ユーザーガイドの「Amazon EC2 のキーペアと Linux インスタンス」を参照してください。

ゲートウェイのローカルコンソールにログインするには

1. 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. ログインすると、[AWS Storage Gateway - Configuration] メインメニューが表示されます。このメニューから、さまざまなタスクを実行できます。

実行するタスク	参照先のトピック
ゲートウェイ用に SOCKS プロキシを設定する	EC2 にデプロイされたゲートウェイの HTTP プロキシ経由のルーティング
ネットワークの接続をテストする	ゲートウェイのネットワーク接続をテストする
Storage Gateway コンソールコマンドを実行する	ローカルコンソールでの Storage Gateway コマンドの実行
システムリソースチェックを表示する	ゲートウェイシステムリソースのステータスの表示.

ゲートウェイをシャットダウンするには、「**0**」と入力します。

設定セッションを終了するには、「**X**」と入力します。

EC2 にデプロイされたゲートウェイの HTTP プロキシ経由のルーティング

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

ゲートウェイがプロキシサーバーを使用してインターネットと通信する必要がある場合は、HTTP プロキシをゲートウェイ用に設定する必要があります。そのためには、プロキシを実行しているホストの IP アドレスとポート番号を指定します。これを行うと、Storage Gateway はプロキシサーバーを介してすべての AWS エンドポイントトラフィックをルーティングします。HTTP プロキシを使用している場合でも、ゲートウェイとエンドポイント間の通信は暗号化されます。

ローカルプロキシサーバー経由でゲートウェイのインターネットトラフィックをルーティングするには

1. ゲートウェイのローカルコンソールにログインします。手順については、Amazon EC2 ゲートウェイのローカルコンソールへのログイン を参照してください。
2. [AWS Appliance Activation - Configuration] メインメニューから、対応する番号を入力して [Configure HTTP Proxy] を選択します。
3. [AWS Appliance Activation HTTP Proxy Configuration] メニューから、実行するタスクに対応する番号を入力します。

   - Configure HTTP proxy - 設定を完了するには、ホスト名とポートを指定する必要があります。
   - View current HTTP proxy configuration - HTTP プロキシが設定されていない場合、メッセージ「`HTTP Proxy not configured`」が表示されます。HTTP が設定されている場合は、プロキシのホスト名とポートが表示されます。
   - Remove an HTTP proxy configuration - メッセージ「`HTTP Proxy Configuration Removed`」が表示されます。

ゲートウェイのネットワーク接続をテストする

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

ゲートウェイの接続をテストするには

1. ゲートウェイのローカルコンソールにログインします。手順については、Amazon EC2 ゲートウェイのローカルコンソールへのログイン を参照してください。
2. [AWS Appliance Activation - Configuration] メインメニューから、対応する番号を入力して [Test Network Connectivity] を選択します。

ゲートウェイがすでにアクティブ化されている場合は、接続テストがすぐに開始します。まだアクティブ化されていないゲートウェイの場合は、次の手順で説明 AWS リージョン するように、エンドポイントタイプ と を指定する必要があります。

3. ゲートウェイがまだアクティブ化されていない場合は、対応する番号を入力して、ゲートウェイのエンドポイントタイプを選択します。
4. パブリックエンドポイントタイプを選択した場合は、対応する数字を入力して、テスト AWS リージョン する を選択します。サポートされているサービスエンドポイント AWS リージョン と Storage Gateway で使用できる AWS サービスエンドポイントのリストについては、「」のAWS Storage Gateway 「エンドポイントとクォータ」を参照してくださいAWS 全般のリファレンス。

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

メッセージ	説明
[PASSED]	Storage Gateway がネットワークに接続されています。
[FAILED]	Storage Gateway はネットワークに接続されていません。

ゲートウェイシステムリソースのステータスの表示

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へのログイン を参照してください。
2. [AWS Appliance Activation - Configuration] メインメニューで、対応する番号を入力して「View System Resource Check」を選択します。

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

メッセージ	説明
[OK]	リソースはシステムリソースチェックに合格しました。
[WARNING]	リソースは推奨される要件を満たしていませんが、ゲートウェイは引き続き機能します。Storage Gateway は、リソースチェックの結果について説明するメッセージを表示します。
[FAIL]	リソースは最小要件を満たしていません。ゲートウェイ は適切に機能していない可能性があります。Storage Gateway は、リソースチェックの結果について説明するメッセージを表示します。

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

ローカルコンソールでの Storage Gateway コマンドの実行

AWS Storage Gateway コンソールは、ゲートウェイの問題を設定および診断するための安全な環境を提供します。コンソールコマンドを使用して、ルーティングテーブルの保存や への接続などのメンテナンスタスクを実行できます サポート。

設定または診断コマンドを実行するには

1. ゲートウェイのローカルコンソールにログインします。手順については、Amazon EC2 ゲートウェイのローカルコンソールへのログイン を参照してください。
2. [AWS Appliance Activation - Configuration] メインメニューから、対応する番号を入力して「Gateway Console」を選択します。
3. ゲートウェイコンソールのコマンドプロンプトから、「h」と入力します。

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

コマンド	関数
dig	DNS のトラブルシューティング用に、dig からの出力を収集します。
exit	コンソール設定メニューに戻ります。
h	使用可能なコマンドリストを表示します。
ifconfig	ネットワークインターフェイスを表示または設定します。 **Note** Storage Gateway コンソールまたは専用のローカルコンソールメニューオプションを使用して、ネットワークまたは IP 設定を構成することをお勧めします。
ip	ルーティング、デバイス、トンネルを表示または操作します。 **Note** Storage Gateway コンソールまたは専用のローカルコンソールメニューオプションを使用して、ネットワークまたは IP 設定を構成することをお勧めします。
iptables	IPv4 パケットフィルタリングおよび NAT の管理ツール。

コマンド	関数
ncport	ネットワーク上の特定の TCP ポートへの接続をテストします。
nping	ネットワークのトラブルシューティング用に、nping からの出力を収集します。
open-support-channel	AWS サポートに接続します。
save-iptables	IP テーブルを永続化します。
save-routing-table	新しく追加されたルーティングテーブルエントリーを保存します。
sslcheck	ネットワークのトラブルシューティングのため、SSL の有効性を確認します。
tcptraceroute	送信先への TCP トラフィックに関する traceroute 出力を収集します。

4. ゲートウェイコンソールのコマンドプロンプトから、使用したい機能に対応するコマンドを入力し、指示に従います。

コマンドについて知るには、コマンド名の後に -h オプションを入力します (例: `sslcheck -h`)。

ボリュームゲートウェイのパフォーマンスと最適化

このセクションでは、Storage Gateway のパフォーマンスについて説明します。

トピック

- ゲートウェイのパフォーマンスの最適化

ゲートウェイのパフォーマンスの最適化

ゲートウェイサーバーの推奨構成

ゲートウェイのパフォーマンスを最大限に引き出せるように、Storage Gateway では、ゲートウェイのホストサーバーに対して以下のゲートウェイ構成を推奨しています。

- 24 個以上の専用の物理 CPU コア
- ボリュームゲートウェイの場合、ハードウェアの RAM に次の容量の専用領域を確保する必要があります。
  - キャッシュ容量が 16 TiB までのゲートウェイの場合、16 GiB 以上の RAM の予約領域
  - キャッシュ容量が 16 TiB ~ 32 TiB のゲートウェイの場合、32 GiB 以上 の RAM の予約領域
  - キャッシュ容量が 32 TiB ~ 64 TiB のゲートウェイの場合、48 GiB 以上の RAM の予約領域
- ディスク 1。ゲートウェイキャッシュとして次のように使用します。
  - NVMe コントローラーを使用する SSD。
- ディスク 2。ゲートウェイアップロードバッファとして次のように使用します。
  - NVMe コントローラーを使用する SSD。
- ディスク 3。ゲートウェイアップロードバッファとして次のように使用します。
  - 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。

ゲートウェイへのリソースの追加

次のボトルネックにより、ボリュームゲートウェイのパフォーマンスが理論上の最大持続スループット (AWS クラウドへの帯域幅) を下回る可能性があります。

- CPU コアの数
- キャッシュ/アップロードバッファのディスクスループット
- RAM の合計容量
- へのネットワーク帯域幅 AWS
- イニシエータからゲートウェイまでのネットワーク帯域幅

このセクションでは、ゲートウェイのパフォーマンスを最適化するための対策について説明します。以下のガイダンスは、ゲートウェイまたはアプリケーションサーバーへのリソースの追加を前提としています。

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

より高性能なディスクの使用

キャッシュとアップロードバッファのディスクスループットによって、ゲートウェイのアップロードとダウンロードのパフォーマンスが制限される可能性があります。ゲートウェイのパフォーマンスが予想を大幅に下回っている場合は、キャッシュとアップロードバッファのディスクスループットを次の方法で改善することを検討してください。

- RAID 10 などのストライプ RAID を使用してディスクスループットを向上させる。理想的には、ハードウェア RAID コントローラを使用します。

  > **Note**
  >
  > RAID (独立した複数のディスクから成る冗長アレイ)、具体的には RAID 10 などのディスクストライプ RAID 構成は、データをブロックに分割し、そのデータブロックを複数のストレージデバイスに分散させるプロセスです。使用する RAID レベルによって、実現できる速度と耐障害性が変わります。IO ワークロードを複数のディスクに分散することで、RAID デバイスの全体的なスループットは、1 台 1 台のメンバーディスクのスループットをはるかに上回ります。

- 高性能ディスクを直接接続して使用する。

ゲートウェイのパフォーマンスを最適化するには、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。

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

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

アップロードバッファディスクをさらに追加する

書き込みスループットを高めるには、少なくとも 2 つのアップロードバッファディスクを追加します。データがゲートウェイに書き込まれると、アップロードバッファディスクにローカルに書き込まれて保存されます。その後、保存されたローカルデータはディスクから非同期的に読み取られ、処理と AWSへのアップロードが行われます。アップロードバッファディスクをさらに追加すると、個別のディスクに対して実行される同時 I/O 操作の量が減る可能性があります。これにより、ゲートウェイへの書き込みスループットが増える可能性があります。

別の物理ディスクを使用したゲートウェイ仮想ディスクのバックアップ

ゲートウェイのディスクをプロビジョニングする場合は、同じ物理ストレージディスクを基盤として使用しているアップロードバッファおよびキャッシュストレージ用にローカルディスクをプロビジョニングしないことを強くお勧めします。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 や RAID 6 のような比較的パフォーマンスの低い RAID 構成で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。

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各仮想プロセッサが、それぞれ専用の CPU コアでサポートされてい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 Amazon S3 へのこのデータのアップロードの両方を並行して処理できます。また、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。

ゲートウェイと AWS クラウドの間の帯域幅を広げる

帯域幅を との間で増やす AWS と、ゲートウェイへのデータ進入と AWS クラウドへのデータ進入の最大レートが増加します。低速のディスクや、ゲートウェイとイニシエータ間の接続帯域幅不足といった他の要因ではなく、ネットワーク速度がゲートウェイ構成における制限要因となっている場合は、これでゲートウェイのパフォーマンスを向上させることができます。

> **Note**
>
> キャッシュ/アップロードバッファのディスクスループット、CPU コア数、RAM の合計容量、イニシエータとゲートウェイ間の帯域幅など、ここに記載されているその他の制限要因により、ゲートウェイのパフォーマンスの実測値がネットワーク帯域幅を下回る可能性があります。また、ゲートウェイの通常運用に際しては、データ保護のために多くの対策が実施されるため、ネットワーク帯域幅よりもパフォーマンスの実測値が低くなる場合があります。

ボリュームの設定を変更する

ボリュームゲートウェイを使用している場合に、ゲートウェイにストレージボリュームを追加するとゲートウェイへのスループットが低下する場合は、別のゲートウェイにボリュームを追加す

ることを検討してください。特に、ボリュームが高スループットのアプリケーションに使用されている場合は、高スループットのアプリケーション用に別のゲートウェイを作成することを検討してください。ただし、一般的なルールとして、すべての高スループットのアプリケーションに一方のゲートウェイを使用し、すべての低スループットのアプリケーションにもう一方のゲートウェイを使用するといった方法は避けてください。ボリュームのスループットを測定するには、`ReadBytes` および `WriteBytes` メトリクスを使用します。

これらのメトリクスの詳細については、「アプリケーションとゲートウェイの間のパフォーマンスの測定」を参照してください。

iSCSI 設定を最適化する

iSCSI イニシエータの iSCSI 設定を最適化して、I/O パフォーマンスを向上させることができます。`MaxReceiveDataSegmentLength` と `FirstBurstLength` には 256 KiB、`MaxBurstLength` には 1 MiB を選択することをお勧めします。iSCSI 設定の詳細については、「iSCSI 設定のカスタマイズ」を参照してください。

> **Note**
>
> これらの推奨設定により、全体的なパフォーマンスが向上します。ただし、パフォーマンスを最適化するために必要な特定の iSCSI 設定は、使用するバックアップソフトウェアによって異なります。詳細については、バックアップソフトウェアのドキュメントを参照してください。

アプリケーション環境へのリソースの追加

アプリケーションサーバーとゲートウェイの間の帯域幅を増やす

iSCSI イニシエータとゲートウェイ間の接続のせいで、アップロードとダウンロードのパフォーマンスが制限されることがあります。ゲートウェイのパフォーマンスが予想よりも著しく低く、CPU コア数とディスクスループットを既に改善している場合は、次の点を検討してください。

- ネットワークケーブルをアップグレードして、イニシエータとゲートウェイ間の帯域幅を広げる。

ゲートウェイのパフォーマンスを最適化するには、アプリケーションとゲートウェイ間のネットワーク帯域幅が、アプリケーションのニーズを満たすようにしてください。ゲートウェイの

ReadBytes メトリクスと WriteBytes メトリクスを使用して、データの合計スループットを測定できます。

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

アプリケーション環境への 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。

セキュリティイン AWS Storage Gateway

のクラウドセキュリティが最優先事項 AWS です。 AWS カスタマーは、最もセキュリティの影響を受けやすい組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャを活用できます。

セキュリティは、 AWS とユーザーの間で共有される責任です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ – AWS は、Amazon Web Services Cloud で AWS サービスを実行するインフラストラクチャを保護する責任を担います。 AWS また、 では、安全に使用できるサービスも提供しています。サードパーティーの監査者は、AWS コンプライアンスプログラムコンプライアンスプログラムの一環として、当社のセキュリティの有効性を定期的にテストおよび検証。AWS Storage Gateway「コンプライアンスプログラムAWS による対象範囲内のサービスコンプライアンスプログラム」を参照してください。
- クラウド内のセキュリティ – お客様の責任は、使用する AWS サービスによって決まります。また、ユーザーは、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、Storage Gateway を使用する際の責任共有モデルの適用方法を理解するのに役立ちます。次のトピックでは、セキュリティおよびコンプライアンスの目的を満たすように Storage Gateway を設定する方法について説明します。また、Storage Gateway リソースのモニタリングや保護に役立つ他の AWS サービスの使用方法についても説明します。

トピック

- In AWS Storage Gateway でのデータ保護
- AWS Storage Gatewayの Identity and Access Management
- AWS Storage Gateway のコンプライアンス検証
- In AWS Storage Gateway の耐障害性
- AWS Storage Gateway でのインフラストラクチャセキュリティ
- AWS セキュリティのベストプラクティス
- での口グ記録とモニタリング AWS Storage Gateway

In AWS Storage Gateway でのデータ保護

責任 AWS 共有モデル、 AWS Storage Gateway でのデータ保護に適用されます。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を維持する責任があります。また、使用する「 AWS のサービス 」のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、データプライバシーに関するよくある質問を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿された AWS 責任共有モデルおよび GDPR のブログ記事を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント 、 AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「 AWS CloudTrail ユーザーガイド」のCloudTrail 証跡の使用」を参照してください。
- AWS 暗号化ソリューションと、 内のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度な管理されたセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-3 検証済み暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-3」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報を、タグ、または [名前] フィールドなどの自由形式のテキストフィールドに含めないことを強くお勧めします。これは、コンソール、API、または SDK を使用して Storage Gateway AWS CLIまたは他の AWS のサービス を操作する場合も同様です。 AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

を使用したデータ暗号化 AWS KMS

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

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

ファイル共有の暗号化

ファイル共有では、SSE-KMS を使用して AWS KMSマネージドキーでオブジェクトを暗号化するようにゲートウェイを設定できます。Storage Gateway API を使用したファイル共有に書き込まれるデータの暗号化についての詳細は、AWS Storage Gateway API リファレンスの「CreateNFSFileShare」を参照してください。

ボリュームの暗号化

キャッシュ型ボリュームと保存型ボリュームの場合、Storage Gateway API を使用して、クラウドに保存されているボリュームデータを AWS KMSマネージドキーで暗号化するようにゲートウェイを設定できます。 Storage Gateway マネージドキーの 1 つを KMS キーとして指定することができます。ボリュームの暗号化に使用するキーは、ボリュームの作成後に変更することはできません。Storage Gateway API を使用したキャッシュ型ボリュームまたは保管型ボリュームに書き込まれるデータの暗号化についての詳細は、AWS Storage Gateway API リファレンスの「CreateCachediSCSIVolume」または「CreateStorediSCSIVolume」を参照してください。

テープの暗号化

仮想テープの場合、Storage Gateway API を使用して、クラウドに保存されているテープデータを AWS KMSマネージドキーで暗号化するようにゲートウェイを設定できます。 Storage Gateway マ

ネージドキーの 1 つを KMS キーとして指定することができます。テープデータの暗号化に使用するキーは、テープの作成後に変更することはできません。Storage Gateway API を使用した仮想テープに書き込まれるデータの暗号化についての詳細は、AWS Storage Gateway API リファレンスの「CreateTapes」を参照してください。

AWS KMS を使用してデータを暗号化する場合は、次の点に注意してください。

- データはクラウドでの保管時に暗号化されます。つまり、Amazon S3 内でデータが暗号化されます。
- IAM ユーザーには、 AWS KMS API オペレーションを呼び出すために必要なアクセス許可が必要です。詳細については、「AWS Key Management Service 開発者ガイド」の「AWS KMSで IAM ポリシーを使用する」を参照してください。
- AWS AWS KMS キーを削除または非アクティブ化するか、許可トークンを取り消すと、ボリュームまたはテープ上のデータにアクセスできなくなります。詳細については、「AWS Key Management Service デベロッパーガイド」の「KMS keys を削除する」を参照してください。
- 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 では、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暗号化されていないボリュームを作成することはできません。

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

ボリューム用の CHAP 認証の設定

Storage Gateway では、iSCSI イニシエータが iSCSI ターゲットとしてボリュームに接続されます。Storage Gateway では、チャレンジハンドシェイク認証プロトコル (CHAP) を使用して iSCSI とイニシエータの接続が認証されます。CHAP は、ストレージボリュームターゲットへのアクセスが試みられる際に認証を要求することによって、プレイバック攻撃に対する保護を提供します。ボリュームターゲットごとに、1 つまたは複数の CHAP 認証情報を定義できます。さまざまなイニシエーター用のこれらの認証情報は、[Configure CHAP credentials] ダイアログボックスで表示、編集できます。

CHAP 認証情報を設定するには

1. Storage Gateway コンソールで [Volumes] (ボリューム) を選択し、CHAP 認証情報を設定するボリュームを選択します。
2. [アクション] メニューで、[CHAP 認証の設定] を選択します。
3. [イニシエータ名] にイニシエータの名前を入力します。この名前は 1 文字以上、255 文字以内にしてください。
4. [イニシエータのシークレット] に、iSCSI イニシエータを認証するために使用する秘密のフレーズを入力します。イニシエータの秘密のフレーズは、12 ~ 16 文字である必要があります。
5. [Target secret] で、相互 CHAP のターゲットを認証するために使用する秘密のフレーズを入力します。ターゲットの秘密のフレーズは、12 ~ 16 文字である必要があります。
6. [Save] を選択してエントリを保存します。

CHAP 認証情報を表示または更新するには、そのオペレーションを実行するために必要な IAM ロールのアクセス許可を割り当てられている必要があります。

CHAP 認証情報の表示および編集

各ユーザーの CHAP 認証情報を追加、削除、または更新できます。CHAP 認証情報を表示または編集するために必要な IAM ロールのアクセス許可を割り当てられている必要があります。また、イニシエーターゲットが、機能しているゲートウェイにアタッチされていることも必要です。

CHAP 認証情報を追加するには

1. Storage Gateway コンソールで [Volumes] (ボリューム) を選択し、CHAP 認証情報を追加するボリュームを選択します。
2. [アクション] メニューで、[CHAP 認証の設定] を選択します。
3. [Configure CHAPS] ページで、各ボックスに [イニシエータ名]、[イニシエータのシークレット]、および [ターゲットのシークレット] を指定し、[保存] を選択します。

CHAP 認証情報を削除するには

1. Storage Gateway コンソールで [Volumes] (ボリューム) を選択し、CHAP 認証情報を削除するボリュームを選択します。
2. [アクション] メニューで、[CHAP 認証の設定] を選択します。
3. 削除する認証情報の横にある [X] をクリックし、[保存] を選択します。

CHAP 認証情報を更新するには

1. Storage Gateway コンソールで [Volumes] (ボリューム) を選択し、CHAP を更新するボリュームを選択します。
2. [アクション] メニューで、[CHAP 認証の設定] を選択します。
3. [Configure CHAP credentials] ページで、更新する認証情報のエントリを変更します。
4. [Save] を選択します。

AWS Storage Gatewayの Identity and Access Management

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、誰を認証 (サインイン) し、誰に SGW AWS リソースの使用を許可する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで AWS のサービス 使用できる です。

トピック

- 対象者
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- How AWS Storage Gateway と IAM の連携
- Storage Gateway のアイデンティティベースのポリシーの例
- Troubleshooting AWS Storage Gateway のアイデンティティとアクセス

対象者

AWS Identity and Access Management (IAM) の使用方法は、SGW AWS で行う作業によって異なります。

サービスユーザー – ジョブを実行するために SGW AWS サービスを使用する場合、管理者から必要な認証情報とアクセス許可が提供されます。さらに多くの SGW AWS 機能を使用して作業を行う場合は、追加のアクセス許可が必要になる場合があります。アクセスの管理方法を理解すると、管理者に適切なアクセス許可をリクエストするのに役に立ちます。 AWS SGW の機能にアクセスできない場合は、「Troubleshooting AWS Storage Gateway のアイデンティティとアクセス」を参照してください。

サービス管理者 – 社内の SGW AWS リソースを担当している場合は、通常、SGW AWS へのフルアクセスがあります。サービスユーザーがどの SGW AWS 機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。SGW で IAM AWS を使用する方法の詳細については、「」を参照してくださいHow AWS Storage Gateway と IAM の連携。

IAM 管理者 - IAM 管理者は、 AWS SGW へのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります。IAM で使用できる AWS SGW アイデンティティベースのポリシーの例を表示するには、「」を参照してください Storage Gateway のアイデンティティベースのポリシーの例。

アイデンティティを使用した認証

認証は、ID 認証情報 AWS を使用して にサインインする方法です。として、IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けることによって、認証 (にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM Identity Center （ IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook 認証情報は、フェデレーティッド ID の例です。フェデレーティッド ID としてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーの種類に応じて、 AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、 AWS サインイン ユーザーガイドの「 へのサインイン方法 AWS アカウント」を参照してください。

AWS プログラムで にアクセスする場合、 はソフトウェア開発キット (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストを暗号化して署名します。AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。リクエストに自分で署名する推奨方法の使用については、「IAM ユーザーガイド」の「API リクエストに対するAWS Signature Version 4」を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、 AWS では、多要素認証 (MFA) を使用してアカウントのセキュリティを向上させることをお勧めします。詳細については、「AWS IAM Identity Center ユーザーガイド」の「多要素認証」および「IAM ユーザーガイド」の「IAM のAWS 多要素認証」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての およびリソースへの AWS のサービス 完全なアクセス権を持つ 1 つのサインイン ID から始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「IAM ユーザーガイド」の「ルートユーザー認証情報が必要なタスク」を参照してください。

フェデレーティッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、一時的な認証情報を使用して にアクセスするために ID プロバイダーとのフェデレーション AWS のサービス を使用することを要求します。

フェデレーティッド ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、AWS Directory Service、アイデンティティセンターディレクトリ、または ID ソースを介して提供された認証情報 AWS のサービス を使用して にアクセスするすべてのユーザーです。フェデレーティッド ID がアクセスすると AWS アカウント、ロールを引き受け、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、 AWS IAM Identity Centerを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成するか、独自の ID ソースのユーザーとグループのセットに接続して同期し、すべての AWS アカウント とアプリケーションで使用できます。IAM Identity Center の詳細については、「AWS IAM Identity Center ユーザーガイド」の「What is IAM Identity Center?」(IAM Identity Center とは) を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「IAM ユーザーガイド」の「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できま

す。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する許可を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。で IAM ロールを一時的に引き受けるには AWS Management Console、ユーザーから IAM ロール (コンソール) に切り替えることができます。ロールを引き受けるには、 または AWS API オペレーションを AWS CLI 呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロールについては、「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM Identity Center User Guide」の「Permission sets」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、 (プロキシとしてロールを使用する代わりに) リソースに直接ポリシーをアタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

- クロスサービスアクセス — 一部の は他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストリクエストリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービス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「AWS のサービスに許可を委任するロールを作成する」を参照してください。
  - サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、 サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許可を表示できますが、編集することはできません。
- Amazon EC2 で実行されているアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。EC2 インスタンスに AWS ロールを割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、「IAM ユーザーガイド」の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与する」を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、ID AWS またはリソースにアタッチします。ポリシーは AWS 、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義する のオブジェクトです。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、IAM ユーザーガイドの JSON ポリシー概要を参照してください。

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの許可を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 AWS Management Console、、 AWS CLIまたは AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「管理ポリシーとインラインポリシーのいずれかを選択する」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーでは、IAM の AWS マネージドポリシーを使用できません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、 AWS WAF、および Amazon VPC は、ACLs。ACL の詳細については、「Amazon Simple Storage Service デベロッパーガイド」の「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS は、追加のあまり一般的ではないポリシータイプをサポートしています。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」を参照してください。
- サービスコントロールポリシー (SCPs) – SCPsは、 の組織または組織単位 (OU) の最大アクセス許可を指定する JSON ポリシーです AWS Organizations。 AWS Organizations は、ビジネスが所

有する複数の をグループ化して一元管理するためのサービス AWS アカウント です。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各 を含むメンバーアカウントのエンティティのアクセス許可を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー (SCP)」を参照してください。

- リソースコントロールポリシー (RCP) – RCP は、所有する各リソースにアタッチされた IAM ポリシーを更新することなく、アカウント内のリソースに利用可能な最大数のアクセス許可を設定するために使用できる JSON ポリシーです。RCP は、メンバーアカウントのリソースに対するアクセス許可を制限し、組織に属するかどうかにかかわらず AWS アカウントのルートユーザー、 を含む ID に対する有効なアクセス許可に影響を与える可能性があります。RCP AWS のサービス をサポートする のリストを含む Organizations と RCPs「リソースコントロールポリシー (RCPs」を参照してください。 AWS Organizations
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。複数のポリシータイプが関係する場合にリクエストを許可するかどうか AWS を決定する方法については、IAM ユーザーガイドの「ポリシー評価ロジック」を参照してください。

How AWS Storage Gateway と IAM の連携

IAM を使用して SGW AWS へのアクセスを管理する前に、SGW で使用できる IAM AWS 機能について説明します。

AWS Storage Gatewayで使用できる IAM 機能

IAM 機能	AWS SGW サポート
アイデンティティベースポリシー	はい
リソースベースのポリシー	いいえ
ポリシーアクション	はい
ポリシーリソース	はい
ポリシー条件キー (サービス固有)	はい
ACL	いいえ
ABAC (ポリシー内のタグ)	部分的
一時的な認証情報	あり
転送アクセスセッション (FAS)	あり
サービスロール	はい
サービスリンクロール	はい

AWS SGW およびその他の AWS のサービスがほとんどの IAM 機能とどのように連携するかの概要については、IAM ユーザーガイドのAWS 「IAM と連携する のサービス」を参照してください。

SGW AWS のアイデンティティベースのポリシー

アイデンティティベースのポリシーのサポート: あり

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。ID ベースのポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。プリンシパルは、それが添付されている

ユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素について学ぶには、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

SGW AWS のアイデンティティベースのポリシーの例

AWS SGW アイデンティティベースのポリシーの例を表示するには、「」を参照してください Storage Gateway のアイデンティティベースのポリシーの例。

SGW AWS 内のリソースベースのポリシー

リソースベースのポリシーのサポート: なし

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

クロスアカウントアクセスを有効にするには、アカウント全体、または別のアカウントの IAM エンティティをリソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる場合 AWS アカウント、信頼されたアカウントの IAM 管理者は、プリンシパルエンティティ (ユーザーまたはロール) にリソースへのアクセス許可も付与する必要があります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーをさらに付与する必要はありません。詳細については、「IAM ユーザーガイド」の「IAM でのクロスアカウントリソースアクセス」を参照してください。

SGW AWS のポリシーアクション

ポリシーアクションのサポート:あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

JSON ポリシーの Action 要素にはポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連付けられた AWS API オペレーションと同じです。一致する API オペレーションのない許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは依存アクションと呼ばれます。

このアクションは関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

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

SGW AWS のポリシーアクションは、アクションの前に次のプレフィックスを使用します。

```
sgw
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

```
"Action": [
      "sgw:action1",
      "sgw:action2"
         ]
```

AWS SGW アイデンティティベースのポリシーの例を表示するには、「」を参照してください Storage Gateway のアイデンティティベースのポリシーの例。

SGW AWS のポリシーリソース

ポリシーリソースのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルが、どのリソースに対してどのような条件下でアクションを実行できるかということです。

Resource JSON ポリシー要素はアクションが適用されるオブジェクトを指定します。ステートメントにはResource または NotResource 要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

```
"Resource": "*"
```

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

AWS SGW アイデンティティベースのポリシーの例を表示するには、「」を参照してください Storage Gateway のアイデンティティベースのポリシーの例。

SGW AWS のポリシー条件キー

サービス固有のポリシー条件キーのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルが、どのリソースに対してどのような条件下でアクションを実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成して、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の Condition 要素を指定する場合、または 1 つの Condition 要素に複数のキーを指定する場合、 AWS では AND 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 は論理ORオペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与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 ポリシーの要素: 変数およびタグ」を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートしています。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「グローバル条件コンテキストキー」を参照してください。

AWS SGW 条件キーのリストを確認するには、「サービス認可リファレンス」の「Condition Keys for AWS Storage Gateway」を参照してください。条件キーを使用できるアクションとリソースについては、「Actions Defined by AWS Storage Gateway」を参照してください。

AWS SGW アイデンティティベースのポリシーの例を表示するには、「」を参照してください Storage Gateway のアイデンティティベースのポリシーの例。

SGW AWS ACLs

ACL のサポート: なし

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

SGW AWS での ABAC

ABAC (ポリシー内のタグ) のサポート: 一部

属性ベースのアクセス制御 (ABAC) は、属性に基づいてアクセス許可を定義する認可戦略です。では AWS、これらの属性はタグと呼ばれます。タグは、IAM エンティティ (ユーザーまたはロール) および多くの AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。その後、プリンシパルのタグがアクセスしようとしているリソースのタグと一致した場合にオペレーションを許可するように ABAC ポリシーをします。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、「IAM ユーザーガイド」の「ABAC 認可でアクセス許可を定義する」を参照してください。ABAC をセットアップする手順を説明するチュートリアルについては、「IAM ユーザーガイド」の「属性ベースのアクセスコントロール (ABAC) を使用する」を参照してください。

SGW AWS での一時的な認証情報の使用

一時的な認証情報のサポート: あり

一部の AWS のサービス は、一時的な認証情報を使用してサインインすると機能しません。一時的な認証情報 AWS のサービス を使用する などの詳細については、AWS のサービス IAM ユーザーガイドの「IAM と連携する」を参照してください。

ユーザー名とパスワード以外の AWS Management Console 方法で にサインインする場合、一時的な認証情報を使用します。たとえば、会社のシングルサインオン (SSO) リンク AWS を使用して にアクセスすると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えに関する詳細については、「IAM ユーザーガイド」の「ユーザーから IAM ロールに切り替える (コンソール)」を参照してください。

一時的な認証情報は、 AWS CLI または AWS API を使用して手動で作成できます。その後、これらの一時的な認証情報を使用して access. AWS recommends にアクセスすることができます AWS。長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成することをお勧めします。詳細については、「IAM の一時的セキュリティ認証情報」を参照してください。

SGW AWS の転送アクセスセッション

転送アクセスセッション (FAS) のサポート: あり

IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストリクエストリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

AWS SGW のサービスロール

サービスロールのサポート: あり

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細につい

ては、「IAM ユーザーガイド」の「AWS のサービスに許可を委任するロールを作成する」を参照してください。

> **Warning**
>
> サービスロールのアクセス許可を変更すると、SGW AWS 機能が破損する可能性があります。SGW AWS が指示する場合にのみ、サービスロールを編集します。

SGW AWS のサービスにリンクされたロール

サービスリンクロールのサポート: あり

サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、 サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

サービスにリンクされたロールの作成または管理の詳細については、「IAM と提携するAWS のサービス」を参照してください。表の「サービスリンクロール」列に Yes と記載されたサービスを見つけます。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[はい] リンクを選択します。

Storage Gateway のアイデンティティベースのポリシーの例

デフォルトでは、ユーザーとロールには SGW AWS リソースを作成または変更するアクセス許可はありません。また、、 AWS Command Line Interface （ AWS CLI ） AWS Management Console、または AWS API を使用してタスクを実行することはできません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

これらサンプルの JSON ポリシードキュメントを使用して、IAM アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーを作成する (コンソール)」を参照してください。

各リソースタイプの ARN の形式など、SGW AWS で定義されるアクションとリソースタイプの詳細については、「サービス認可リファレンス」のAWS Storage Gatewayのアクション、リソース、および条件キー」を参照してください。 ARNs

トピック

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

ポリシーに関するベストプラクティス

アイデンティティベースのポリシーは、アカウント内で誰かが SGW AWS リソースを作成、アクセス、または削除できるかどうかを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行 – ユーザーとワークロードにアクセス許可の付与を開始するには、多くの一般的なユースケースにアクセス許可を付与するAWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義することで、アクセス許可をさらに減らすことをお勧めします。詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」または「ジョブ機能の AWS マネージドポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、「IAM ユーザーガイド」の「IAM でのポリシーとアクセス許可」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、サービスアクションが などの特定の を通じて使用される場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素:条件」を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer でポリシーを検証する」を参照してください。

- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化するために MFA を有効にします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、「IAM ユーザーガイド」の「MFA を使用した安全な API アクセス」を参照してください。

IAM でのベストプラクティスの詳細については、IAM ユーザーガイドの IAM でのセキュリティのベストプラクティスを参照してください。

SGW AWS コンソールの使用

AWS Storage Gatewayコンソールにアクセスするには、最小限のアクセス許可のセットが必要です。これらのアクセス許可により、 の SGW AWS リソースの詳細を一覧表示および表示できます AWS アカウント。最小限必要な許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

ユーザーとロールが引き続き SGW AWS コンソールを使用できるようにするには、エンティティに AWS SGW *ConsoleAccess*または *ReadOnly* AWS 管理ポリシーもアタッチします。詳細については、「IAM ユーザーガイド」の「ユーザーへのアクセス許可の追加」を参照してください。

自分の権限の表示をユーザーに許可する

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI または AWS API を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
```

```
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

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

以下の情報は、SGW と IAM AWS の使用時に発生する可能性がある一般的な問題の診断と修正に役立ちます。

トピック

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

SGW AWS でアクションを実行する権限がありません

アクションを実行する権限がないというエラーが表示された場合は、そのアクションを実行できるようにポリシーを更新する必要があります。

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

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 sgw:GetWidget on resource: my-example-widget
```

この場合、sgw:*GetWidget* アクションを使用して *my-example-widget*リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

iam:PassRole を実行する権限がありません

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、SGW AWS にロールを渡すことができるようにポリシーを更新する必要があります。

一部の AWS のサービス では、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、そのサービスに既存のロールを渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

以下の例のエラーは、 marymajor という IAM ユーザーがコンソールを使用して AWS SGW でアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

この場合、Mary のポリシーを更新してメアリーに iam:PassRole アクションの実行を許可する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

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

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまた

はアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

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

AWS Storage Gateway のコンプライアンス検証

サードパーティーの監査者は、複数の コンプライアンスプログラムの一環として、 AWS Storage Gateway のセキュリティと AWS コンプライアンスを評価します。これらには、SOC、PCI、ISO、FedRAMP、HIPAA、MTSC、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AWS による対象範囲内のサービスコンプライアンスプログラム」を参照してください。一般的な情報については、AWS 「コンプライアンスプログラム」を参照してください。

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

Storage Gateway を使用する際のお客様のコンプライアンス責任は、データの機密性、企業のコンプライアンス目的、適用法規によって決まります。 AWS では、コンプライアンスに役立つ次のリソースが提供されています。

- セキュリティとコンプライアンスのクイックスタートガイド – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境をデプロイする手順について説明します AWS。
- HIPAA セキュリティとコンプライアンスのためのアーキテクチャホワイトペーパー – このホワイトペーパーでは、企業が AWS を使用して HIPAA 準拠のアプリケーションを作成する方法について説明します。
- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界と地域に適用される場合があります。
- 「 デベロッパーガイド」のルールによるリソースの評価 – この AWS Config サービスは、リソース設定が内部プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub – この AWS サービスは、 内のセキュリティ状態を包括的に把握 AWS し、セキュリティ業界標準とベストプラクティスへの準拠を確認するのに役立ちます。

In AWS Storage Gateway の耐障害性

AWS グローバルインフラストラクチャは、 AWS リージョン およびアベイラビリティーゾーンを中心に構築されています。

AWS リージョン は、データセンターがクラスター化されている世界中の物理的な場所です。論理的なデータセンターの各グループはアベイラビリティーゾーン (AZ) と呼ばれます。各 AWS リージョン は、1 つの地理的領域内にある、少なくとも 3 つの隔離され、物理的にも分かれている AZ で成り立っています。多くの場合、リージョンを単一のデータセンターとして定義する他のクラウドプロバイダーとは異なり、すべての の複数の AZ 設計 AWS リージョン には明確な利点があります。各 AZ には独立した電源、冷却、物理的セキュリティがあり、冗長で超低レイテンシーのネットワークを介して接続されます。デプロイで高可用性に重点を置く必要がある場合は、耐障害性を高めるために、複数の AZ でサービスとリソースを設定することができます。

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

AWS リージョン およびアベイラビリティーゾーンの詳細については、AWS 「 グローバルインフラストラクチャ」を参照してください。

Storage Gateway には、 AWS グローバルインフラストラクチャに加えて、データの耐障害性とバックアップのニーズをサポートするのに役立ついくつかの機能があります。

- VMware vSphere 高可用性 (VMware HA) を使用して、ハードウェア、ハイパーバイザー、またはネットワーク障害からストレージワークロードを保護します。詳細については、「Storage Gateway での VMware vSphere High Availability の使用」を参照してください。
- AWS Backup を使用してボリュームをバックアップします。詳細については、「ボリュームのバックアップ」を参照してください。
- 復旧ポイントからボリュームのクローンを作成します。詳細については、「復旧ポイントからキャッシュされたボリュームのクローン」を参照してください。

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

マネージドサービスである AWS Storage Gatewayは、ホワイトペーパー「Amazon Web Services: セキュリティプロセスの概要」に記載されている AWS グローバルネットワークセキュリティ手順で保護されています。

AWS 公開された API コールを使用して、ネットワーク経由で Storage Gateway にアクセスします。クライアントは Transport Layer Security (TLS) 1.2 をサポートしている必要があります。また、一時的ディフィー・ヘルマン Ephemeral Diffie-Hellman (DHE) や Elliptic Curve Ephemeral Diffie-Hellman (ECDHE) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートもクライアントでサポートされている必要があります。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。

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

> **Note**
>
> AWS Storage Gatewayアプライアンスはマネージド仮想マシンとして扱い、インストールへのアクセスや変更を試みないでください。通常のゲートウェイ更新メカニズム以外の方法を使用してスキャンソフトウェアをインストールしたり、ソフトウェアパッケージを更新しようとすると、ゲートウェイが誤動作し、ゲートウェイをサポートまたは修正する能力に影響を与える可能性があります。

AWS は CVEs を定期的にレビュー、分析、修正します。これらの問題の修正は、通常のソフトウェアリリースサイクルの一部として Storage Gateway に組み込まれます。これらの修正は、通常スケジュールされたメンテナンス期間中の通常のゲートウェイ更新プロセスの一部として適用されます。ゲートウェイの更新の詳細については、「コンソール。

AWS セキュリティのベストプラクティス

AWS には、独自のセキュリティポリシーを開発および実装する際に考慮すべき多くのセキュリティ機能が用意されています。これらのベストプラクティスは一般的なガイドラインであり、完全なセキュリティソリューションを提供するものではありません。これらのプラクティスは顧客の環境に必ずしも適切または十分でない可能性があるので、処方箋ではなく、あくまで有用な検討事項とお考えください。詳細については、「AWS Security Best Practices」を参照してください。

でのログ記録とモニタリング AWS Storage Gateway

Storage Gateway は AWS CloudTrail、Storage Gateway のユーザー、ロール、または のサービスによって実行されたアクションを記録する AWS サービスである と統合されています。CloudTrail は、Storage Gateway に対するすべての API コールをイベントとしてキャプチャします。キャプチャされる呼び出しには、Storage Gateway コンソールからの呼び出しと Storage Gateway API オペレーションへのコード呼び出しが含まれます。証跡を作成することで、Storage Gateway のイベントなど、Amazon S3 バケットへの CloudTrail イベントを継続的に配信できるようになります。証跡を設定しない場合でも、CloudTrail コンソールの [イベント履歴] で最新のイベントを表示できます。CloudTrail で収集された情報により、Storage Gateway に対するリクエスト、リクエスト元の IP アドレス、リクエストの実行者、リクエストの日時などの詳細を特定できます。

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

CloudTrail での Storage Gateway の情報

Amazon Web Services アカウントの作成時に、そのアカウントで CloudTrail が有効になります。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 [Event history] (イベント履歴) で、その他の AWS サービスのイベントと共に CloudTrail イベントに記録されます。AWS アカウントでの最近のイベントを表示、検索、ダウンロードできます。詳細については、「CloudTrail イベント履歴でのイベントの表示」を参照してください。

Storage Gateway のイベントなど、Amazon Web Services のアカウントのイベントを継続的に記録するには、証跡を作成します。証跡を作成すれば、CloudTrail でログファイルを Amazon S3バケッ

トに配信できます。デフォルトでは、コンソールで証跡を作成すると、証跡はすべての AWS リージョンに適用されます。証跡は、 AWS パーティションのすべてのリージョンからのイベントを口グに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集されたイベントデータをさらに分析して処理するように、他の AWS サービスを設定できます。詳細については、次を参照してください:

- 証跡の作成のための概要
- CloudTrail がサポートするサービスと統合
- CloudTrail 用 Amazon SNS 通知の構成
- 「複数のリージョンからCloudTrail口グファイルを受け取る」および「複数のアカウントからCloudTrail口グファイルを受け取る」

Storage Gateway のアクションはすべて記録され、[Actions] (アクション) トピックで説明されます。例えば、`ActivateGateway`、`ListGateways`、`ShutdownGateway` の各アクションを呼び出すと、CloudTrail ログファイルにエントリが生成されます。

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

- リクエストが root または AWS Identity and Access Management (IAM) ユーザー認証情報を使用して行われたかどうか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが別の AWS サービスによって行われたかどうか。

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

Storage Gateway のログファイルエントリを理解する

証跡とは、指定した Amazon S3 バケットに、イベントをログファイルとして配信できるようにする設定です。CloudTrail のログファイルは、単一か複数のログエントリを含みます。イベントは任意ソースからの単一リクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどの情報を含みます。CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

以下の例は、 アクションを示す CloudTrail ログエントリです。

```
{ "Records": [{
                "eventVersion": "1.02",
                "userIdentity": {
                "type": "IAMUser",
                "principalId": "AIDAII5AUEPBH2M7JTNVC",
                "arn": "arn:aws:iam::111122223333:user/StorageGateway-team/JohnDoe",
                "accountId": "111122223333",
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                 "userName": "JohnDoe"
               },
                  "eventTime": "2014-12-04T16:19:00Z",
                  "eventSource": "storagegateway.amazonaws.com",
                  "eventName": "ActivateGateway",
                  "awsRegion": "us-east-2",
                  "sourceIPAddress": "192.0.2.0",
                  "userAgent": "aws-cli/1.6.2 Python/2.7.6 Linux/2.6.18-164.el5",
                   "requestParameters": {
                                          "gatewayTimezone": "GMT-5:00",
                                          "gatewayName": "cloudtrailgatewayvtl",
                                          "gatewayRegion": "us-east-2",
                                          "activationKey": "EHFBX-1NDD0-P0IVU-PI259-
DHK88",
                                          "gatewayType": "VTL"
                                               },
                                               "responseElements": {
                                                                     "gatewayARN":
 "arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayvtl"
                                          },
                                          "requestID":
 "54BTFGNQI71987UJD2IHTCT8NF1Q8GLLE1QEU3KPGG6F0KSTAUU0",
                                          "eventID": "635f2ea2-7e42-45f0-
bed1-8b17d7b74265",
                                          "eventType": "AwsApiCall",
                                          "apiVersion": "20130630",
                                          "recipientAccountId": "444455556666"
             }]
}
```

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

```
{
 "Records": [{
               "eventVersion": "1.02",
```

```
               "userIdentity": {
                                "type": "IAMUser",
                                "principalId": "AIDAII5AUEPBH2M7JTNVC",
                                "arn": "arn:aws:iam::111122223333:user/StorageGateway-
team/JohnDoe",
                                "accountId:" 111122223333", " accessKeyId ":"
 AKIAIOSFODNN7EXAMPLE",
                                " userName ":" JohnDoe "
                                },

                                " eventTime ":" 2014 - 12 - 03T19: 41: 53Z ",
                                " eventSource ":" storagegateway.amazonaws.com ",
                                " eventName ":" ListGateways ",
                                " awsRegion ":" us-east-2 ",
                                " sourceIPAddress ":" 192.0.2.0 ",
                                " userAgent ":" aws - cli / 1.6.2 Python / 2.7.6
 Linux / 2.6.18 - 164.el5 ",
                                " requestParameters ":null,
                                " responseElements ":null,
                                "requestID ":"
 6U2N42CU37KAO8BG6V1I23FRSJ1Q8GLLE1QEU3KPGG6F0KSTAUU0 ",
                                " eventID ":" f76e5919 - 9362 - 48ff - a7c4 -
 d203a189ec8d ",
                                " eventType ":" AwsApiCall ",
                                " apiVersion ":" 20130630 ",
                                " recipientAccountId ":" 444455556666"
              }]
}
```

ゲートウェイのトラブルシューティング

以下は、ゲートウェイ、ホストプラットフォーム、ボリューム、高可用性、データ復旧、スナップショットに関連するベストプラクティスとトラブルシューティングの問題についての情報です。オンプレミスゲートウェイのトラブルシューティング情報は、サポートされている仮想化プラットフォームにデプロイされたゲートウェイを対象としています。高可用性の問題のトラブルシューティング情報には、VMware vSphere High Availability (HA) プラットフォームで実行されているゲートウェイが含まれます。

トピック

- トラブルシューティング: ゲートウェイのオフライン問題 - Storage Gateway コンソールでゲートウェイがオフラインになる原因となる問題を診断する方法について説明します。
- トラブルシューティング: ゲートウェイのアクティベーション中の内部エラー - Storage Gateway のアクティブ化を試みるときに内部エラーメッセージが表示された場合の対処方法について説明します。
- オンプレミスゲートウェイの問題のトラブルシューティング - オンプレミスゲートウェイの使用に伴って発生する可能性がある一般的な問題と、 がゲートウェイに接続 サポート してトラブルシューティングを支援する方法について説明します。
- Microsoft Hyper-V セットアップのトラブルシューティング - Microsoft Hyper-V プラットフォームに Storage Gateway をデプロイする際に発生する可能性がある一般的な問題について説明します。
- Amazon EC2 ゲートウェイの問題のトラブルシューティング - Amazon EC2 にデプロイされたゲートウェイを操作するときに発生する可能性のある一般的な問題に関する情報を確認します。
- ハードウェアアプライアンスの問題のトラブルシューティング - Storage Gateway ハードウェアアプライアンスで発生する可能性のある問題を解決する方法について説明します。
- ボリュームの問題のトラブルシューティング - ボリュームを使用しているときに発生する可能性のある最も一般的な問題と、これらを修正する際に推奨されるアクションに関する情報を確認します。
- 高可用性に関する問題のトラブルシューティング - VMware HA 環境にデプロイされているゲートウェイで問題が発生した場合の対処方法について説明します。

トラブルシューティング: ゲートウェイのオフライン問題

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

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

- ゲートウェイが Storage Gateway サービスエンドポイントに到達できません。
- ゲートウェイが予期せずシャットダウンしました。
- ゲートウェイに関連付けられたキャッシュディスクが切断または変更されたか、失敗しました。

ゲートウェイをオンラインに戻すには、ゲートウェイがオフラインになった原因となった問題を特定して解決します。

関連付けられたファイアウォールまたはプロキシを確認する

プロキシを使用するようにゲートウェイを設定した場合、またはファイアウォールの背後にゲートウェイを配置した場合は、プロキシまたはファイアウォールのアクセスルールを確認してください。プロキシまたはファイアウォールは、Storage Gateway に必要なネットワークポートとサービスエンドポイントとの間のトラフィックを許可する必要があります。詳細については、「ネットワークとファイアウォールの要件」を参照してください。

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

ゲートウェイと の間のネットワークトラフィックに対して SSL またはディープパケット検査が現在実行されている場合 AWS、ゲートウェイは必要なサービスエンドポイントと通信できない可能性があります。ゲートウェイをオンラインに戻すには、検査を無効にする必要があります。

ハイパーバイザーホストで停電やハードウェア障害がないか確認する

ゲートウェイのハイパーバイザーホストで停電やハードウェア障害が発生すると、ゲートウェイが予期せずシャットダウンし、アクセスできなくなる可能性があります。電源とネットワーク接続を復元すると、ゲートウェイに再びアクセスできるようになります。

ゲートウェイがオンラインに戻ったら、必ずデータを復旧する手順を実行してください。詳細については、「データの復旧に関するベストプラクティス」を参照してください。

関連付けられたキャッシュディスクの問題を確認する

ゲートウェイに関連付けられたキャッシュディスクの少なくとも 1 つが削除、変更、またはサイズ変更された場合、あるいは破損した場合、ゲートウェイはオフラインになる可能性があります。

ハイパーバイザーホストから動作キャッシュディスクが削除された場合:

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

> **Note**
> ディスクを同じディスクノードに追加していることを確認してください。

3. ゲートウェイを再起動します。

キャッシュディスクが破損しているか、置き換えられたか、またはサイズが変更された場合:

1. ゲートウェイをシャットダウンします。
2. キャッシュディスクをリセットします。
3. キャッシュストレージ用にディスクを再設定します。
4. ゲートウェイを再起動します。

トラブルシューティング: ゲートウェイのアクティベーション中の内部エラー

Storage Gateway のアクティベーションリクエストは、2 つのネットワークパスを通過します。クライアントによって送信される受信アクティベーションリクエストは、ポート 80 経由でゲートウェイの仮想マシン (VM) または Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに接続します。ゲートウェイがアクティベーションリクエストを正常に受信すると、ゲートウェイは Storage Gateway エンドポイントと通信してアクティベーションキーを受け取ります。ゲートウェイが Storage Gateway エンドポイントに到達できない場合、ゲートウェイは内部エラーメッセージでクライアントに応答します。

AWS Storage Gatewayをアクティブ化しようとしたときに内部エラーメッセージが表示された場合は、次のトラブルシューティング情報を使用して対処方法を決定します。

> **Note**
>
> - 必ず最新の仮想マシンイメージファイルまたは Amazon マシンイメージ (AMI) バージョンを使用して、新しいゲートウェイをデプロイしてください。古い AMI を使用するゲートウェイをアクティブ化しようとすると、内部エラーが表示されます。
> - AMI をダウンロードする前に、デプロイする正しいゲートウェイタイプを選択していることを確認してください。各ゲートウェイタイプの .ova ファイルと AMI は異なっており、互換性がありません。

パブリックエンドポイントを使用してゲートウェイをアクティブ化する際のエラーを解決する

パブリックエンドポイントを使用してゲートウェイをアクティブ化する際のアクティベーションエラーを解決するには、次のチェックと設定を実行します。

必要なポートを確認する

オンプレミスにデプロイされたゲートウェイの場合、ポートがローカルファイアウォールで開いていることを確認します。Amazon EC2 インスタンスにデプロイされたゲートウェイの場合、インスタンスのセキュリティグループでポートが開いていることを確認します。ポートが開いていることを確認するには、サーバーからパブリックエンドポイントで telnet コマンドを実行します。このサーバーは、ゲートウェイと同じサブネット内にある必要があります。例えば、次の telnet コマンドは、ポート 443 への接続をテストします。

```
telnet d4kdq0yaxexbo.cloudfront.net 443
telnet storagegateway.region.amazonaws.com 443
telnet dp-1.storagegateway.region.amazonaws.com 443
telnet proxy-app.storagegateway.region.amazonaws.com 443
telnet client-cp.storagegateway.region.amazonaws.com 443
telnet anon-cp.storagegateway.region.amazonaws.com 443
```

ゲートウェイ自体がエンドポイントに到達できることを確認するには、ゲートウェイのローカル VM コンソール (オンプレミスにデプロイされたゲートウェイの場合) にアクセスします。または、ゲートウェイのインスタンス (Amazon EC2 にデプロイされたゲートウェイの場合) に SSH 接続できます。次に、ネットワーク接続テストを実行します。テストで [PASSED] を返すことを確認します。詳細については、「ゲートウェイのインターネットへの接続のテスト」を参照してください。

> **Note**
>
> ゲートウェイコンソールのデフォルトのログインユーザー名は admin で、デフォルトのパスワードは password です。

ファイアウォールのセキュリティがゲートウェイからパブリックエンドポイントに送信されたパケットを変更しないことを確認する

SSL 検査、ディープパケット検査、またはその他の形式のファイアウォールセキュリティは、ゲートウェイから送信されるパケットに干渉する可能性があります。SSL 証明書がアクティベーションエンドポイントが期待する内容から変更されると、SSL ハンドシェイクは失敗します。進行中の SSL 検査がないことを確認するには、ポート 443 のメインアクティベーションエンドポイント (anon-cp.storagegateway.region.amazonaws.com) で OpenSSL コマンドを実行します。このコマンドは、ゲートウェイと同じサブネットにあるマシンから実行する必要があります。

```
$ openssl s_client -connect  anon-cp.storagegateway.region.amazonaws.com:443 -
servername anon-cp.storagegateway.region.amazonaws.com
```

> **Note**
>
> *region* を に置き換えます AWS リージョン。

SSL 検査が進行中でない場合、コマンドは次のような応答を返します。

```
$ openssl s_client -connect anon-cp.storagegateway.us-east-2.amazonaws.com:443 -
servername anon-cp.storagegateway.us-east-2.amazonaws.com
CONNECTED(00000003)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-2.amazonaws.com
verify return:1
---
Certificate chain
 0 s:/CN=anon-cp.storagegateway.us-east-2.amazonaws.com
   i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
 1 s:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
```

```
   i:/C=US/O=Amazon/CN=Amazon Root CA 1
 2 s:/C=US/O=Amazon/CN=Amazon Root CA 1
   i:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
 3 s:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
   i:/C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification Authority
---
```

SSL 検査が進行中の場合、応答には次のような変更された証明書チェーンが表示されます。

```
$ openssl s_client -connect  anon-cp.storagegateway.ap-southeast-1.amazonaws.com:443 -
servername anon-cp.storagegateway.ap-southeast-1.amazonaws.com
CONNECTED(00000003)
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.ap-southeast-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

アクティベーションエンドポイントは、SSL 証明書を認識した場合にのみ SSL ハンドシェイクを受け入れます。つまり、エンドポイントへのゲートウェイのアウトバウンドトラフィックは、ネットワーク内のファイアウォールによって実行される検査から除外される必要があります。これらの検査には、SSL 検査やディープパケット検査などがあります。

ゲートウェイの時刻同期を確認する

過剰な時刻のずれがあると、SSL ハンドシェイクエラーを引き起こす可能性があります。オンプレミスゲートウェイの場合、ゲートウェイのローカル VM コンソールを使用して、ゲートウェイの時刻同期を確認できます。時刻のずれは 60 秒以下にする必要があります。詳細については、「ゲートウェイ VM 時刻の同期」を参照してください。

[システム時刻管理] オプションは、Amazon EC2 インスタンスでホストされているゲートウェイでは使用できません。Amazon EC2 ゲートウェイが適切に時刻を同期できるようにするには、Amazon

EC2 インスタンスがポート UDP と TCP 123 経由で次の NTP サーバープールリストに接続できることを確認します。

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

Amazon VPC エンドポイントを使用してゲートウェイをアクティブ化する際のエラーを解決する

Amazon Virtual Private Cloud (Amazon VPC) エンドポイントを使用してゲートウェイをアクティブ化する際のアクティベーションエラーを解決するには、次のチェックと設定を実行します。

必要なポートを確認する

ローカルファイアウォール (オンプレミスにデプロイされたゲートウェイの場合) またはセキュリティグループ (Amazon EC2 にデプロイされたゲートウェイの場合) 内の必要なポートが開いていることを確認します。Storage Gateway VPC エンドポイントにゲートウェイを接続するために必要なポートは、ゲートウェイをパブリックエンドポイントに接続するときに必要なポートとは異なります。Storage Gateway VPC エンドポイントに接続するには、次のポートが必要です。

- TCP 443
- TCP 1026
- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

詳細については、「Storage Gateway 用の VPC エンドポイントの作成」を参照してください。

さらに、Storage Gateway VPC エンドポイントにアタッチされているセキュリティグループを確認します。エンドポイントにアタッチされたデフォルトのセキュリティグループでは、必要なポートが許可されない場合があります。ゲートウェイの IP アドレス範囲からのトラフィックを必要なポート経由で許可する新しいセキュリティグループを作成します。次に、そのセキュリティグループを VPC エンドポイントにアタッチします。

> **Note**
>
> Amazon VPC コンソールを使用して、VPC エンドポイントにアタッチされているセキュリティグループを検証します。コンソールから Storage Gateway VPC エンドポイントを表示し、[セキュリティグループ] タブを選択します。

必要なポートが開いていることを確認するには、Storage Gateway VPC エンドポイントで telnet コマンドを実行できます。これらのコマンドは、ゲートウェイと同じサブネットにあるサーバーから実行する必要があります。アベイラビリティーゾーンを指定していない最初の DNS 名でテストを実行できます。例えば、次の telnet コマンドは、DNS 名 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com を使用して必要なポート接続をテストします。

```
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 443
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1026
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1027
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1028
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1031
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 2222
```

ファイアウォールのセキュリティがゲートウェイから Storage Gateway Amazon VPC エンドポイントに送信されたパケットを変更しないことを確認します。

SSL 検査、ディープパケット検査、またはその他の形式のファイアウォールセキュリティは、ゲートウェイから送信されるパケットに干渉する可能性があります。SSL 証明書がアクティベーションエンドポイントが期待する内容から変更されると、SSL ハンドシェイクは失敗します。SSL 検査が進行中でないことを確認するには、Storage Gateway VPC エンドポイントで OpenSSL コマンドを実行します。このコマンドは、ゲートウェイと同じサブネットにあるマシンから実行する必要があります。必要なポートごとにコマンドを実行します。

```
$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:443 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1026 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

```
$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1028 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1031 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:2222 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

SSL 検査が進行中でない場合、コマンドは次のような応答を返します。

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-1.amazonaws.com
verify return:1
---
Certificate chain
 0 s:CN = anon-cp.storagegateway.us-east-1.amazonaws.com
   i:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
 1 s:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
   i:C = US, O = Amazon, CN = Amazon Root CA 1
 2 s:C = US, O = Amazon, CN = Amazon Root CA 1
   i:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
 3 s:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
   i:C = US, O = "Starfield Technologies, Inc.", OU = Starfield Class 2 Certification
 Authority
---
```

SSL 検査が進行中の場合、応答には次のような変更された証明書チェーンが表示されます。

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.us-
east-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.us-east-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

アクティベーションエンドポイントは、SSL 証明書を認識した場合にのみ SSL ハンドシェイクを受け入れます。つまり、必要なポートを介した VPC エンドポイントへのゲートウェイのアウトバウンドトラフィックは、ネットワークファイアウォールによって実行される検査から除外されます。これらの検査には、SSL 検査やディープパケット検査などがあります。

ゲートウェイの時刻同期を確認する

過剰な時刻のずれがあると、SSL ハンドシェイクエラーを引き起こす可能性があります。オンプレミスゲートウェイの場合、ゲートウェイのローカル VM コンソールを使用して、ゲートウェイの時刻同期を確認できます。時刻のずれは 60 秒以下にする必要があります。詳細については、「ゲートウェイ VM 時刻の同期」を参照してください。

[システム時刻管理] オプションは、Amazon EC2 インスタンスでホストされているゲートウェイでは使用できません。Amazon EC2 ゲートウェイが適切に時刻を同期できるようにするには、Amazon EC2 インスタンスがポート UDP と TCP 123 経由で次の NTP サーバープールリストに接続できることを確認します。

- 0.amazon.pool.ntp.org
- 1.amazon.pool.ntp.org
- 2.amazon.pool.ntp.org

- 3.amazon.pool.ntp.org

HTTP プロキシをチェックし、関連するセキュリティグループ設定を確認する

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

- Amazon EC2 の HTTP プロキシにアタッチされたセキュリティグループには、インバウンドルールが必要です。このインバウンドルールでは、ゲートウェイ VM の IP アドレスからのポート 3128 上の Squid プロキシトラフィックを許可する必要があります。
- Amazon EC2 VPC エンドポイントにアタッチされたセキュリティグループには、インバウンドルールが必要です。これらのインバウンドルールでは、Amazon EC2 の HTTP プロキシの IP アドレスからポート 1026-1028、1031、2222、443 へのトラフィックを許可する必要があります。

パブリックエンドポイントを使用してゲートウェイをアクティブ化し、同じ VPC に Storage Gateway VPC エンドポイントがある場合のエラーを解決する

同じ VPC に Amazon Virtual Private Cloud (Amazon VPC) エンポイントがある場合にパブリックエンドポイントを使用してゲートウェイをアクティブ化する際のエラーを解決するには、次のチェックと設定を実行します。

Storage Gateway VPC エンドポイントで [プライベート DNS 名を有効にする] 設定が有効になっていないことを確認します。

[プライベート DNS 名を有効にする] が有効になっている場合、その VPC からパブリックエンドポイントへのゲートウェイをアクティブ化することはできません。

プライベート DNS 名オプションを無効にするには:

1. Amazon VPC コンソールを開きます。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. Storage Gateway VPC エンドポイントを選択します。
4. [アクション] を選択します。
5. [プライベート DNS 名の管理] を選択します。

6. [プライベート DNS 名を有効にする] で、[このエンドポイントを有効にする] を選択します。
7. [プライベート DNS 名の変更] を選択して設定を保存します。

オンプレミスゲートウェイの問題のトラブルシューティング

オンプレミスゲートウェイで作業する際に発生する可能性のある一般的な問題と、ゲートウェイのトラブルシューティングに役立つ サポート ように をアクティブ化する方法についての情報を以下に示します。

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。 • 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。 • SSL 証明書の検証/検査は有効にしないでください。Storage Gateway は相互 TLS 認証を利用しますが、サードパーティのアプリケーションがいずれかの証明書を傍受/署名しようとすると認証が失敗します。

問題	実行するアクション
	• ファイアウォールまたはルーターを使用してネットワークトラフィックをフィルタリングまたは制限する場合は、これらのサービスエンドポイントに対し AWSへのアウトバウンド通信を許可するように、対象のファイアウォールおよびルーターを設定する必要があります。ネットワークおよびファイアウォールの要件の詳細については、ネットワークとファイアウォールの要件を参照してください。
Storage Gateway マネジメントコンソールで [Proceed to Activation] (アクティベーションに進む) ボタンをクリックすると、ゲートウェイのアクティベーションは失敗します。	• クライアントから VM に Ping を送信し、ゲートウェイ VM にアクセスできることを確認します。 • VM がインターネットに接続していることを確認します。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、「オンプレミスゲートウェイの SOCKS5 プロキシの設定」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、VM の時刻を Hyper-V または Linux KVM ホストの時刻と同期する を参照してください。 • 以上の手順を実行したら、Storage Gateway コンソールと [Setup and Activate Gateway] (ゲートウェイのセットアップとアクティベーション) ウィザードを使用して、ゲートウェイのデプロイを再試行できます。 • SSL 証明書の検証/検査は有効にしないでください。Storage Gateway は相互 TLS 認証を利用しますが、サードパーティのアプリケーションがいずれかの証明書を傍受/署名しようとすると認証が失敗します。 • 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、「ボリュームゲートウェイのセットアップ要件」を参照してください。

問題	実行するアクション
アップロードバッファ領域として割り当てられているディスクを削除する必要があります。たとえば、ゲートウェイのアップロードバッファ領域の量を減らしたり、エラーが発生したアップロードバッファとして使用されているディスクを置き換えたりする必要が生じる場合があります。	アップロードバッファ領域として割り当てられているディスクを削除する手順については、「ゲートウェイからのディスクの削除」を参照してください。
ゲートウェイと AWSの間の帯域幅を改善する必要があります。	アプリケーションとゲートウェイ VM を接続するネットワークアダプタ (NIC) AWS で へのインターネット接続を設定 AWS することで、ゲートウェイから への帯域幅を向上させることができます。このアプローチは、 への高帯域幅接続があり、特にスナップショットの復元中に帯域幅の競合を回避 AWS したい場合に便利です。高スループットのワークロードが要求される場合、AWS Direct Connect を使用して、オンプレミスのゲートウェイと AWSの間の専用ネットワーク接続を確立できます。ゲートウェイから への接続の帯域幅を測定するには AWS、ゲートウェイの `CloudBytesDownloaded` および `CloudBytesUploaded` メトリクスを使用します。この詳細については、「ゲートウェイと AWSの間のパフォーマンスの測定」を参照してください。インターネット接続を改善すれば、アップロードバッファがいっぱいになることがありません。

問題	実行するアクション

ゲートウェイへのスループットまたはゲートウェイからのスループットがゼロに落ちます。	• Storage Gateway コンソールの [Gateway] (ゲートウェイ) タブで、ゲートウェイ VM の IP アドレスが、ハイパーバイザークライアントソフトウェア (VMware vSphere クライアントまたは Microsoft Hyper-V Manager) を使用して表示されるものと同じであることを確認します。同じでない場合、「ゲートウェイ VM のシャットダウン」に示すように Storage Gateway コンソールからゲートウェイを再起動します。再起動後、Storage Gateway コンソールの [Gateway] (ゲートウェイ) タブにある [IP Addresses] (IP アドレス) リスト内のアドレスは、ゲートウェイの IP アドレスと一致するはずです。ゲートウェイの IP アドレスはハイパーバイザークライアントから判断します。
	  • VMware 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。
	• 「」の説明 AWS に従って、ゲートウェイの への接続を確認しますゲートウェイのインターネット接続のテスト。
	• ゲートウェイのネットワークアダプタ設定を確認し、ゲートウェイに対して有効にする予定のすべてのインターフェイスが有効になっていることを確認します。ゲートウェイのネットワークアダプタ設定を表示するには、「ゲートウェイのネットワークの設定」の指示に従い、ゲートウェイのネットワーク設定を表示するためのオプションを選択します。
	
	Amazon CloudWatch コンソールにゲートウェイとの双方向のスループットを表示できます。ゲートウェイと との間のスループットの測定の詳細については AWS、「」を参照してくださいゲートウェイと AWSの間のパフォーマンスの測定。

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

問題	実行するアクション
「ゲートウェイのボリュームに書き込まれたデータが AWS内に安全に保存されていません」というメッセージを受信する。	このメッセージを受信するのは、ゲートウェイ VM が別のゲートウェイ VM のクローンまたはスナップショットから作成された場合です。そうでない場合は、 サポートにお問い合わせください。

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

Storage Gateway には、ゲートウェイの問題のトラブルシューティングに役立つゲートウェイへのアクセス サポート のアクティブ化など、いくつかのメンテナンスタスクを実行するために使用できるローカルコンソールが用意されています。デフォルトでは、ゲートウェイ サポート へのアクセスは無効になっています。このアクセスは、ホストのローカルコンソールを通して有効にします。ゲートウェイ サポート へのアクセスを許可するには、まずホストのローカルコンソールにログインし、Storage Gateway のコンソールに移動してから、サポートサーバーに接続します。

ゲートウェイ サポート へのアクセスを許可するには

1. ホストのローカルコンソールにログインします。
   - VMware ESXi – 詳細については、「VMware ESXi でゲートウェイのローカルコンソールにアクセスする」を参照してください。
   - Microsoft Hyper-V – 詳細については、「Microsoft Hyper-V でゲートウェイのローカルコンソールにアクセスする」を参照してください。
2. プロンプトで、対応する番号を入力して [ゲートウェイコンソール] を選択します。
3. 「**h**」と入力して、利用可能なコマンドのリストを開きます。
4. 次のいずれかを行います：
   - ゲートウェイでパブリックエンドポイントを使用している場合は、[AVAILABLE COMMANDS] (利用可能なコマンド) ウィンドウに「**`open-support-channel`**」と入力して、Storage Gateway のカスタマーサポートに接続します。TCP ポート 22 を許可して、 AWSへのサポートチャネルを開くことができます。カスタマーサポートに接続する際、Storage Gateway はサポート番号を割り当てます。サポート番号を書き留めます。

- ゲートウェイが VPC エンドポイントを使用している場合は、[AVAILABLE COMMANDS (利用可能なコマンド)] ウィンドウで「**open-support-channel**」と入力します。ゲートウェイがアクティブ化されていない場合は、Storage Gateway のカスタマーサポートに接続する VPC エンドポイントまたは IP アドレスを指定します。TCP ポート 22 を許可して、 AWS へのサポートチャネルを開くことができます。カスタマーサポートに接続する際、Storage Gateway はサポート番号を割り当てます。サポート番号を書き留めます。

> **Note**
>
> チャネル番号は Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ポート番号ではありません。代わりに、ゲートウェイが Storage Gateway サーバーへの Secure Shell (SSH) (TCP 22) 接続を作成し接続のサポートチャネルを提供します。

5. サポートチャネルが確立されたら、 サポート がトラブルシューティングのサポートを提供 サポート できるように、サポートサービス番号を に提供します。
6. サポートセッションが完了したら、「**q**」と入力してセッションを終了します。サポートセッションが完了したことを Amazon Web Services サポートが通知するまでは、セッションを終了しないようにします。
7. ゲートウェイコンソールからログアウト**exit**するには、 を入力します。
8. プロンプトに従ってローカルコンソールを終了します。

Microsoft Hyper-V セットアップのトラブルシューティング

次の表は、Microsoft Hyper-V プラットフォームに Storage Gateway をデプロイする際に発生する可能性がある一般的な問題の一覧です。

問題	実行するアクション
ゲートウェイをインポートしようとすると、次のエラーメッセージが表示されます。 「仮想マシンのインポート中にサーバーエラーが発生しました。インポートに	このエラーは、次の原因で発生することがあります。 • 解凍されていないゲートウェイソースファイルのルートをポイントしている場合。[仮想マシンをインポート] ダイアログボックスで指定した場所の最後のパートは、`AWS-Storage-Gateway` となっている必要があります。以下に例を示します。

問題	実行するアクション
失敗しました。場所 [...] では、仮想マシンのインポートファイルが見つかりません。Hyper-V を使用して仮想マシンを作成してエクスポートする場合にのみ、仮想マシンをインポートできます。」	`C:\prod-gateway\unzippedSourceVM\AWS-Storage-Gateway\` . • ゲートウェイを既にデプロイしていて、[Import Virtual Machine] (仮想マシンのインポート) ダイアログボックスで、[Copy the virtual machine] (仮想マシンのコピー) オプションを選択していなかったか、[Duplicate all files] (すべてのファイルを複製する) オプションをオンにしていなかった場合、解凍したゲートウェイファイルがある場所に仮想マシンが作成されていて、この場所から再度インポートすることはできません。この問題を解決するには、未解凍のゲートウェイソースファイルの最新コピーを入手して、新しい場所にコピーします。インポートのソースとして新しい場所を使用します。 1 つの解凍されたソースファイルの場所から複数のゲートウェイを作成する場合は、[仮想マシンをコピー] を選択し、[仮想マシンをインポート] ダイアログボックスで、[すべてのファイルを複製] チェックボックスをオンにする必要があります。
ゲートウェイをインポートしようとすると、次のエラーメッセージが表示されます。 「仮想マシンのインポート中にサーバーエラーが発生しました。インポートに失敗しました。インポートタスクは [...] からファイルをコピーできませんでした。ファイルが存在しています。(0x80070050)」	既にゲートウェイをデプロイしていて、仮想ハードディスクファイルと仮想マシン構成ファイルを保存するデフォルトのフォルダを再利用しようとすると、このエラーが発生します。この問題を修正するには、[Hyper-V の設定] ダイアログボックスの左側にあるパネルで、[サーバー] の下に新しい場所を指定します。

問題	実行するアクション
ゲートウェイをインポートしようとすると、次のエラーメッセージが表示されます。 「仮想マシンのインポート中にサーバーエラーが発生しました。インポートに失敗しました。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、[仮想マシンをインポート] ダイアログボックスで、[仮想マシンをコピー] を選択し、[すべてのファイルを複製] ボックスをオンにしていることを確認して、VM の新しい一意の ID を作成します。
ゲートウェイ VM を起動しようとすると、次のエラーメッセージが表示されます。 「選択した仮想マシンを起動しようとしたときにエラーが発生しました。子パーティションのプロセッサの設定は、親パーティションと互換性がありません。「AWS-Storage-Gateway」を初期化できませんでした。(仮想マシン ID [...])」	このエラーは通常、ゲートウェイで必要とされる CPU と、ホストで使用可能な CPU の不一致が原因で発生します。VM の CPU 数が、基本ハイパーバイザーでサポートされていることを確認します。 Storage Gateway の要件の詳細については、「ボリュームゲートウェイのセットアップ要件」を参照してください。

問題	実行するアクション
ゲートウェイ VM を起動しようとすると、次のエラーメッセージが表示されます。 「選択した仮想マシンを起動しようとしたときにエラーが発生しました。「AWS-Storage-Gateway」を初期化できませんでした。(仮想マシン ID [...]) パーティションの作成に失敗しました。リクエストされたサービスを完了するためのシステムリソースが不足しています。(0x800705AA)」	このエラーは通常、ゲートウェイで必要とされる RAM と、ホストで使用可能な RAM の不一致が原因で発生します。 Storage Gateway の要件の詳細については、「ボリュームゲートウェイのセットアップ要件」を参照してください。
スナップショットとゲートウェイソフトウェアのアップデートが、予想とわずかに異なる時刻に発生します。	ゲートウェイの VM のクロックが実際の時刻からずれている可能性があります (クロックドリフトと呼ばれています)。ローカルゲートウェイコンソールの時刻同期オプションを使って、VM の時刻を確認して修正します。詳細については、「VM の時刻を Hyper-V または Linux KVM ホストの時刻と同期する」を参照してください。
解凍済みの Microsoft Hyper-V Storage Gateway ファイルを、ホストファイルシステムに保存する必要があります。	一般的な Microsoft Windows サーバーと同じようにホストにアクセスします。たとえば、ハイパーバイザーホストの名前が `hyperv-server` の場合、UNC パス `\\hyperv-server\c$` という UNC パスを使用できます。このパスは `hyperv-server` という名前が解決可能であるか、あるいはローカルホストファイルで定義されていることを前提としています。
ハイパーバイザーへの接続時に、認証情報の入力を求められます。	Sconfig.cmd ツールを使って、ハイパーバイザーホストのローカル管理者として、自分のユーザー認証情報を追加します。

問題	実行するアクション
Broadcom ネットワークアダプタを使用する Hyper-V ホストで仮想マシンキュー (VMQ) をオンにすると、ネットワークパフォーマンスが低下することがあります。	回避策については、Microsoft のドキュメントの「Poor network performance on virtual machines on a Windows Server 2012 Hyper-V host if VMQ is turned on」を参照してください。

Amazon EC2 ゲートウェイの問題のトラブルシューティング

以下のセクションでは、Amazon EC2 にデプロイされているゲートウェイを操作しているときに発生する可能性がある一般的な問題について説明します。オンプレミスのゲートウェイと Amazon EC2 にデプロイされているゲートウェイの違いに関する詳細については、「ボリュームゲートウェイ用にカスタマイズされた Amazon EC2 インスタンスをデプロイする」を参照してください。

トピック

- 少し時間が経ってもゲートウェイのアクティベーションが実行されない
- インスタンスリストに EC2 ゲートウェイインスタンスがない
- Amazon EBS ボリュームを作成したが、EC2 ゲートウェイインスタンスにアタッチできない
- EC2 ゲートウェイのボリュームターゲットにイニシエータをアタッチできない
- ストレージボリュームを追加するときに利用可能なディスクがないというメッセージが表示される
- アップロードバッファ領域を削減するために、アップロードバッファ領域として割り当てられたディスクを削除したい
- EC2 ゲートウェイとの間のスループットがゼロに低下する
- EC2 ゲートウェイ サポート のトラブルシューティングを支援したい
- Amazon EC2 シリアルコンソールを使用してゲートウェイインスタンスに接続したい

少し時間が経ってもゲートウェイのアクティベーションが実行されない

Amazon EC2 コンソールで以下を確認します。

- インスタンスに関連付けられているセキュリティグループでポート 80 が有効になっています。セキュリティグループのルールの追加に関する詳細については、「Amazon EC2 ユーザーガイド」の「セキュリティグループルールの追加」を参照してください。
- ゲートウェイインスタンスに実行中の印が付いています。Amazon EC2 コンソールで、インスタンスの [State] (状態) 値が RUNNING になっている必要があります。
- Amazon EC2 インスタンスタイプが「ストレージの要件」で説明する最低要件を満たしていることを確認します。

問題を修正したら、ゲートウェイを再度アクティ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、[Deploy a new Gateway on Amazon EC2] (Amazon EC2 に新しいゲートウェイをデプロイする) を選択し、インスタンスの IP アドレスを再入力します。

インスタンスリストに EC2 ゲートウェイインスタンスがない

インスタンスにリソースタグを指定せずに多くのインスタンスを実行中の場合は、起動したインスタンスの判断が困難になることがあります。この場合、ゲートウェイインスタンスを見つけるために、次のアクションを実行できます。

- インスタンスの [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、「**aws-storage-gateway-ami**」というテキストで始まります。
- Storage Gateway AMI を基礎とするインスタンスが複数ある場合、インスタンスの起動時間を確認してインスタンスを見分けます。

Amazon EBS ボリュームを作成したが、EC2 ゲートウェイインスタンスにアタッチできない

問題の Amazon EBS ボリュームがゲートウェイインスタンスと同じアベイラビリティーゾーンにあることを確認します。アベイラビリティーゾーンが異なる場合、インスタンスと同じアベイラビリティーゾーンで新しい Amazon EBS ボリュームを作成します。

EC2 ゲートウェイのボリュームターゲットにイニシエータをアタッチできない

iSCSI アクセスに使用しているポートを許可するルールが、インスタンスを起動したセキュリティグループに含まれていることを確認します。通常、ポートは 3260 に設定されています。ボリューム

への接続の詳細については、「Windows クライアントからボリュームへの接続」を参照してください。

ストレージボリュームを追加するときに利用可能なディスクがないというメッセージが表示される

新しくアクティベートしたゲートウェイには、ボリュームストレージが定義されていません。ボリュームストレージを定義するには、アップロードバッファおよびキャッシュストレージとして使用するために、先にゲートウェイにローカルディスクを割り当てる必要があります。Amazon EC2 にデプロイされているゲートウェイについては、ローカルディスクはインスタンスにアタッチされている Amazon EBS ボリュームになります。このエラーメッセージは、インスタンスに Amazon EBS ボリュームが定義されていないために発生する可能性が高いと考えらえます。

ゲートウェイを実行しているインスタンスに定義されているブロックデバイスを確認します。ブロックデバイスが 2 つだけ (AMI に付属するデフォルトデバイス) の場合、ストレージを追加してください。その設定方法の詳細については、「ボリュームゲートウェイ用にカスタマイズされた Amazon EC2 インスタンスをデプロイする」を参照してください。2 つ以上の Amazon EBS ボリュームを取り付けたら、ゲートウェイにボリュームストレージを作成してみます。

アップロードバッファ領域を削減するために、アップロードバッファ領域として割り当てられたディスクを削除したい

「割り当てるアップロードバッファのサイズの決定」のステップを実行してください。

EC2 ゲートウェイとの間のスループットがゼロに低下する

ゲートウェイインスタンスが実行中であることを確認します。たとえば、再起動に起因してインスタンスが起動中の場合、インスタンスが再開するのを待ちます。

また、ゲートウェイ IP が変更されていないことを確認します。インスタンスを停止し、再開した場合、インスタンスの IP アドレスが変わっている可能性があります。その場合、新しいゲートウェイをアクティブ化する必要があります。

Amazon CloudWatch コンソールにゲートウェイとの双方向のスループットを表示できます。ゲートウェイと との間のスループットの測定の詳細については AWS、「」を参照してくださいゲートウェイと AWSの間のパフォーマンスの測定。

EC2 ゲートウェイ サポート のトラブルシューティングを支援したい

Storage Gateway には、ゲートウェイの問題のトラブルシューティングに役立つゲートウェイへのアクセス サポート のアクティブ化など、いくつかのメンテナンスタスクを実行するために使用できるローカルコンソールが用意されています。デフォルトでは、ゲートウェイ サポート へのアクセスは無効になっています。このアクセスを有効にするには、Amazon EC2 ローカルコンソールを使用します。Amazon EC2 ローカルコンソールは、Secure Shell (SSH) を使用してログインします。SSH を使用して正常にログインするために、インスタンスのセキュリティグループには、TCP ポート 22 を開くルールが必要です。

> **Note**
>
> 既存のセキュリティグループに新しいルールを追加すると、新しいルールが、そのセキュリティグループを使用するすべてのインスタンスに適用されます。セキュリティグループと、セキュリティグループルールの追加方法については、Amazon EC2 ユーザーガイドの「Amazon EC2 とは」を参照してください。

ゲートウェイ サポート への接続を許可するには、まず Amazon EC2 インスタンスのローカルコンソールにログインし、Storage Gateway のコンソールに移動して、アクセスを提供します。

Amazon EC2 インスタンスにデプロイされたゲートウェイ サポート へのアクセスを有効にするには

1. Amazon EC2 インスタンスのローカルコンソールにログインします。手順については、Amazon EC2 ユーザーガイドの「Linux インスタンスへの接続」を参照してください。

   次のコマンドを使用して、EC2 インスタンスのローカルコンソールにログインできます。

   ```
   ssh -i PRIVATE-KEY admin@INSTANCE-PUBLIC-DNS-NAME
   ```

   > **Note**
   >
   > *PRIVATE-KEY* は、Amazon EC2 インスタンスを起動するために使用した EC2 キーペアのプライベート証明書を含む .pem ファイルです。詳細については、Amazon EC2 ユーザーガイドの「Amazon EC2 のキーペアと Linux インスタンス」を参照してください。
   > *INSTANCE-PUBLIC-DNS-NAME* は、ゲートウェイが実行中の Amazon EC2 インスタンスのパブリックドメインネームシステム (DNS) です。このパブリック DNS 名を取得す

るには、EC2 コンソールで Amazon EC2 インスタンスを選択して、[Description] (説明) タブをクリックします。

2. プロンプトで「**6 - Command Prompt**」と入力して、 サポート Channel コンソールを開きます。
3. 「**h**」と入力して [AVAILABLE COMMANDS (利用可能なコマンド)] ウィンドウを開きます。
4. 次のいずれかを行います：

   - ゲートウェイでパブリックエンドポイントを使用している場合は、[AVAILABLE COMMANDS] (利用可能なコマンド) ウィンドウに「**open-support-channel**」と入力して、Storage Gateway のカスタマーサポートに接続します。TCP ポート 22 を許可して、 AWSへのサポートチャネルを開くことができます。カスタマーサポートに接続する際、Storage Gateway はサポート番号を割り当てます。サポート番号を書き留めます。
   - ゲートウェイが VPC エンドポイントを使用している場合は、[AVAILABLE COMMANDS (利用可能なコマンド)] ウィンドウで「**open-support-channel**」と入力します。ゲートウェイがアクティブ化されていない場合は、Storage Gateway のカスタマーサポートに接続する VPC エンドポイントまたは IP アドレスを指定します。TCP ポート 22 を許可して、 AWS へのサポートチャネルを開くことができます。カスタマーサポートに接続する際、Storage Gateway はサポート番号を割り当てます。サポート番号を書き留めます。

   > **Note**
   >
   > チャネル番号は Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ポート番号ではありません。代わりに、ゲートウェイが Storage Gateway サーバーへの Secure Shell (SSH) (TCP 22) 接続を作成し接続のサポートチャネルを提供します。

5. サポートチャネルが確立されたら、 サポート がトラブルシューティングのサポートを提供 サポート できるように、サポートサービス番号を に提供します。
6. サポートセッションが完了したら、「**q**」と入力してセッションを終了します。サポートセッションが完了したことが サポート から通知されるまで、セッションを終了しないでください。
7. 「**exit**」と入力して、Storage Gateway コンソールを終了します。
8. コンソールメニューに従って Storage Gateway インスタンスからログアウトします。

Amazon EC2 シリアルコンソールを使用してゲートウェイインスタンスに接続したい

Amazon EC2 シリアルコンソールは、起動、ネットワーク設定、およびその他の問題のトラブルシューティングに使用できます。手順とトラブルシューティングのヒントについては、「Amazon Elastic Compute Cloud ユーザーガイド」の「Amazon EC2 シリアルコンソール」を参照してください。

ハードウェアアプライアンスの問題のトラブルシューティング

以下のトピックでは、Storage Gateway Hardware Appliance を使用する際に発生する可能性がある問題と、そのトラブルシューティング対策を示します。

サービスの IP アドレスを特定できない

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

ファクトリーリセットを実行するにはどうすればよいですか

アプライアンスでファクトリーリセットを実行する必要がある場合は、以下のサポートセクションの説明に従って、サポートについて Storage Gateway Hardware Appliance チームにお問い合わせください。

リモート再起動を実行するにはどうすればよいですか

アプライアンスをリモートで再起動する必要がある場合は、Dell iDRAC の管理インターフェイスを使用して実行できます。詳細については、Dell Technologies InfoHub ウェブサイトの「iDRAC9 Virtual Power Cycle: Remotely power cycle Dell EMC PowerEdge Servers」を参照してください。

Dell iDRAC のサポートを受けるにはどうすればよいですか

Dell PowerEdge サーバーには、Dell iDRAC 管理インターフェイスが搭載されています。次の構成を推奨します。

- iDRAC 管理インターフェイスを使用する場合は、デフォルトのパスワードを変更する必要があります。iDRAC 認証情報の詳細については、「Dell PowerEdge - What is the default sign-in credentials for iDRAC?」を参照してください。
- セキュリティ違反を防ぐため、ファームウェアが最新であることを確認します。
- iDRAC ネットワークインターフェイスを通常の (em) ポートに移動すると、パフォーマンスの問題が発生したり、アプライアンスの通常の機能を妨げたりする可能性があります。

ハードウェアアプライアンスのシリアル番号が見つからない

Storage Gateway コンソールを使用して、Storage Gateway ハードウェアアプライアンスのシリアル番号を確認できます。

ハードウェアアプライアンスのシリアル番号を確認するには:

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. ページの左側のナビゲーションメニューから [ハードウェア] を選択します。
3. リストからハードウェアアプライアンスを選択します。
4. アプライアンスの [詳細] タブで [シリアル番号] フィールドを見つけます。

ハードウェアアプライアンスのサポートの依頼先

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

サポート チームは、ゲートウェイの問題をリモートでトラブルシューティングするために、サポートチャネルをアクティブ化するよう求める場合があります。このポートは、ゲートウェイの通常のオペレーションでは開いておく必要はありませんが、トラブルシューティングでは必要です。以下の手順に示すように、ハードウェアコンソールからサポートチャネルをアクティブ化することができます。

のサポートチャネルを開くには AWS

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

ネットワーク接続やファイアウォールに問題がなければ、割り当てられたポート番号が 30 秒以内に表示されます。以下に例を示します。

[ステータス: ポート 19599 で開く]

3. ポート番号を書き留めて指定します サポート。

ボリュームの問題のトラブルシューティング

このセクションでは、ボリュームを使用しているときに発生する可能性のある最も一般的な問題と、これらを修正する際に推奨されるアクションについて説明します。

トピック

- ボリュームが設定されていないとコンソールに表示される
- ボリュームは復旧不可能であるとコンソールに表示される
- ゲートウェイキャッシュ型が到達不可能なためデータを復旧する場合
- ボリュームのステータスが PASS THROUGH であるとコンソールに表示される
- ボリュームの整合性を確認し、エラーがある場合は修正する
- ボリュームの iSCSI ターゲットが Windows のディスク管理コンソールに表示されない
- ボリュームの iSCSI ターゲット名を変更したい
- スケジュールしたボリュームのスナップショットが実行されなかった
- 障害が発生したディスクの取り外しまたは交換が必要な場合
- アプリケーションからボリュームへのスループットがゼロに低下した
- ゲートウェイのキャッシュディスクでエラーが発生する
- ボリュームのスナップショットのステータスが予想以上に長い時間にわたって PENDING のままである
- 高可用性のヘルス通知

ボリュームが設定されていないとコンソールに表示される

Storage Gateway コンソールで、ボリュームのステータスが「UPLOAD BUFFER NOT CONFIGURED (アップロードバッファが構成されていません)」と表示されている場合は、アップロードバッファ容量をゲートウェイに追加します。ゲートウェイのアップロードバッファが設定されていない場合、ゲートウェイを使用してアプリケーションデータを格納することはできません。詳細

については、「ゲートウェイ用のアップロードアップロードバッファまたはキャッシュストレージを追加して設定するには」を参照してください。

ボリュームは復旧不可能であるとコンソールに表示される

保管型ボリュームの場合、Storage Gateway コンソールにボリュームのステータスが「IRRECOVERABLE (回復不可能)」と表示されていたら、このボリュームはもう使用できません。Storage Gateway コンソールで、ボリュームの削除を試みることができます。ボリュームにデータがある場合は、新しいボリュームを作成するときに、最初にボリュームを作成するために使用された VM のローカルディスクに基づいて、データを復旧できます。新しいボリュームを作成するとき、[Preserve existing data] を選択します。ボリュームを作成する前に、必ずボリュームの保留スナップショットを削除してください。詳細については、「ストレージボリュームのスナップショットの削除」を参照してください。Storage Gateway コンソールでボリュームを削除できない場合は、ボリュームに割り当てられているディスクが VM から不適切に削除されたために、アプライアンスから削除できない可能性があります。

キャッシュ型ボリュームでは、Storage Gateway コンソールが示すボリュームのステータスが IRRECOVERABLE であれば、このボリュームはもう使用できません。ボリュームにデータがある場合、ボリュームのスナップショットを作成し、スナップショットからデータを回復したり、最後の復旧ポイントからボリュームをクローンしたりすることができます。データを復旧した後、こののボリュームは削除できます。詳細については、「ゲートウェイキャッシュ型が到達不可能なためデータを復旧する場合」を参照してください。

保存型ボリュームでは、回復不可能なボリュームの作成に使用されたディスクから新しいボリュームを作成できます。詳細については、「ストレージボリュームの作成」を参照してください。ボリュームステータスについては、「ボリュームステータスと移行について」を参照してください。

ゲートウェイキャッシュ型が到達不可能なためデータを復旧する場合

ゲートウェイが到達不可能になった時は (シャットダウン時など)、ボリューム復旧ポイントからスナップショットを作成し、そのスナップショットを使用するか、または既存ボリュームの最後の復旧ポイントから新しいボリュームをクローンすることができます。ボリューム復旧ポイントからのクローンは、スナップショットを作成するよりも素早く経済的です。ボリュームのクローン作成に関する詳細については、「復旧ポイントからキャッシュされたボリュームのクローン」を参照してください。

Storage Gateway には、キャッシュ型ボリュームゲートウェイアーキテクチャで各ボリュームの復旧ポイントが用意されています。ボリューム復旧ポイントとは、ボリュームのすべてのデータに整合性があり、そこからスナップショットを作成したり、ボリュームをクローンしたりできる時点です。

ボリュームのステータスが PASS THROUGH であるとコンソールに表示される

ボリュームのステータスが「PASSTHROUGH (パススルー)」であると Storage Gateway コンソールに表示されることがあります。ボリュームのステータスがパススルーとなる場合、複数の理由が考えられます。アクションが必要な理由と、そうでない理由があります。

たとえば、ゲートウェイのアップロードバッファ領域が完全に消費されているためボリュームのステータスが PASS THROUGH になっている場合には、アクションが必要です。アップロードバッファが過去に超過したかどうかを確認するには、Amazon CloudWatch コンソールで `UploadBufferPercentUsed` メトリクスを確認します。詳細については、「アップロードバッファのモニタリング」を参照してください。アップロードバッファ領域を使い切ったためゲートウェイのステータスが PASS THROUGH になっている場合、ゲートウェイに追加のアップロードバッファ領域を割り当てる必要があります。バッファ領域を追加すると、ボリュームのステータスが自動的に PASS THROUGH から BOOTSTRAPPING (ブートストラップ) に変わり、さらに AVAILABLE (使用可能) に変わります。ボリュームのステータスが BOOTSTRAPPING のとき、ゲートウェイはボリュームのディスクからデータを読み取り、このデータを Amazon S3 にアップロードして、必要に応じてキャッチアップします。ゲートウェイがキャッチアップを完了し、ボリュームデータを Amazon S3 に保存すると、ボリュームのステータスが AVAILABLE になり、スナップショットを再開できるようになります。ボリュームのステータスが PASS THROUGH または BOOTSTRAPPING になっても、ボリュームディスクとの間のデータの読み書きは続行できます。アップロードバッファ容量の追加に関する詳細については、割り当てるアップロードバッファのサイズの決定 を参照してください。

アップロードバッファを超過する前に、操作を行うには、ゲートウェイのアップロードバッファにしきい値アラームを設定できます。詳細については、「ゲートウェイのアップロードバッファの上限アラームを設定するには」を参照してください。

一方、たとえば、別のボリュームがブートストラップ中であるためブートストラップを待っているボリュームのステータスが PASS THROUGH である場合には、アクションは不要です。ゲートウェイはボリュームを 1 つずつ起動します。

まれに、PASS THROUGH ステータスにより、アップロードバッファに割り当てられているディスクに障害が発生したことが示されることがあります。その場合、ディスクを取り除く必要があります。詳細については、「ボリュームゲートウェイのストレージリソースの使用」を参照してください。ボリュームステータスについては、「ボリュームステータスと移行について」を参照してください。

ボリュームの整合性を確認し、エラーがある場合は修正する

ゲートウェイが Microsoft Windows イニシエータを使用してそのボリュームに接続している場合は、Windows CHKDSK ユーティリティを使用して、ボリュームの整合性を確認し、ボリュームにエラーがある場合はエラーを修正できます。Windows では、ボリュームの破損が検出されたときに自動的に CHKDSK ツールを実行できます。または、ユーザー自身がこのツールを実行することもできます。

ボリュームの iSCSI ターゲットが Windows のディスク管理コンソールに表示されない

ボリュームの iSCSI ターゲットが Windows のディスク管理コンソールに表示されない場合は、ゲートウェイのアップロードバッファが設定されていることを確認します。詳細については、「ゲートウェイ用のアップロードアップロードバッファまたはキャッシュストレージを追加して設定するには」を参照してください。

ボリュームの iSCSI ターゲット名を変更したい

ボリュームの iSCSI ターゲット名を変更するには、そのボリュームを削除し、新しいターゲット名で再度追加する必要があります。この操作を行うと、ボリューム上のデータを保持できます。

スケジュールしたボリュームのスナップショットが実行されなかった

スケジュールしたボリュームのスナップショットが実行されなかった場合は、ボリュームのステータスがパススルーであるかどうか、またはスケジュールしたスナップショットの実行時刻の直前にゲートウェイのアップロードバッファが完全に消費されていたかどうかを確認します。Amazon CloudWatch コンソールで、ゲートウェイの `UploadBufferPercentUsed` メトリクスを確認し、そのメトリクスに対してアラームを作成できます。詳細については、アップロードバッファのモニタリングおよびゲートウェイのアップロードバッファの上限アラームを設定するにはを参照してください。

障害が発生したディスクの取り外しまたは交換が必要な場合

障害が発生したボリュームディスクや、不要なボリュームを交換する必要がある場合は、まず Storage Gateway コンソールを使用してボリュームを削除する必要があります。詳細については、「ボリュームを削除するには」を参照してください。次に、ハイパーバイザークライアントを使用して、バックアップストレージを削除します。

- VMware ESXi の場合、ストレージボリュームの削除 の説明に基づき、バックアップストレージを削除します。
- Microsoft Hyper-V の場合、バックアップストレージを削除します。

アプリケーションからボリュームへのスループットがゼロに低下した

アプリケーションからボリュームへのスループットがゼロに低下した場合は、以下を試してください。

- VMware vSphere クライアントを使用している場合は、ボリュームの [Host IP] アドレスが、vSphere クライアントの [Summary] タブに表示されるアドレスの 1 つと一致していることを確認します。ストレージボリュームの [Host IP] (ホスト IP) アドレスは、Storage Gateway コンソールのボリュームの [Details] (詳細) タブで確認できます。ゲートウェイに新しい静的 IP アドレスを割り当てたときなどは、IP アドレスに不一致が発生することがあります。不一致がある場合、「ゲートウェイ VM のシャットダウン」に示されているように、Storage Gateway コンソールからゲートウェイを再起動します。再起動後、[ISCSI Target Info] (ISCSI ターゲット情報) タブのストレージボリュームの [Host IP] (ホスト IP) アドレスは、ゲートウェイの [Summary] (概要) タブの vSphere クライアントに表示される IP アドレスと一致するはずです。
- ボリュームの [ホスト IP] ボックスに IP アドレスがなく、ゲートウェイがオンラインである場合。たとえば、2 つ以上のネットワークアダプタを備えたゲートウェイのネットワークアダプタの IP アドレスに関連付けられたボリュームを作成するときにこの状態が発生することがあります。ボリュームに関連付けられているネットワークアダプタを取り外すか無効にすると、IP アドレスが [ホスト IP] に表示されなくなる場合があります。この問題に対処するには、ボリュームを削除し、その既存のデータを保持したまま再度作成します。
- アプリケーションで使用する iSCSI イニシエータが現在、ストレージボリュームの iSCSI ターゲットにマッピングされていることを確認します。ストレージボリュームへの接続の詳細については、Windows クライアントからボリュームへの接続 を参照してください。

ボリュームのスループットを表示し、Amazon CloudWatch コンソールからアラームを作成できます。アプリケーションからボリュームへのスループットの測定に関する詳細については、「アプリケーションとゲートウェイの間のパフォーマンスの測定」を参照してください。

ゲートウェイのキャッシュディスクでエラーが発生する

ゲートウェイの 1 つ以上のキャッシュディスクに障害が発生した場合、仮想テープとボリュームに対する読み取りおよび書き込みオペレーションがゲートウェイによって禁止されます。通常の機能を再開するには、次の手順に従ってゲートウェイを再設定します。

- キャッシュディスクにアクセスできない、または使用できない場合は、ゲートウェイ構成からディスクを削除します。
- キャッシュディスクがまだアクセス可能で使用可能な場合は、ゲートウェイに再接続します。

> **Note**
>
> キャッシュディスクを削除した場合、ゲートウェイが通常の機能を再開したとき、クリーンデータがあるテープまたはボリューム (キャッシュディスクと Amazon S3 とのデータが同期している場合) は引き続き使用できます。例えば、ゲートウェイに 3 つのキャッシュディスクがあり、2 つを削除した場合、クリーンであるテープまたはボリュームは AVAILABLE ステータスになります。他のテープおよびボリュームは、IRRECOVERABLE ステータスになります。
>
> ゲートウェイのキャッシュディスクとして工フェメラルディスクを使用したり、キャッシュディスクを工フェメラルドライブにマウントしたりすると、ゲートウェイのシャットダウン時にキャッシュディスクが失われます。キャッシュディスクと Amazon S3 が同期していないときにゲートウェイをシャットダウンすると、データが失われる可能性があります。そのため、工フェメラルドライブやディスクを使用することは推奨されていません。

ボリュームのスナップショットのステータスが予想以上に長い時間にわたって PENDING のままである

ボリュームのスナップショットが予想以上に長い時間にわたって保留中状態のままである場合は、ゲートウェイ VM が予期せずクラッシュしたか、ボリュームのステータスがパススルーまたは回復不能に変わった可能性があります。これらのいずれかの場合、スナップショットのステータスは PENDING のままになり、スナップショットは正常に完了しません。この場合は、スナップショットを削除することをお勧めします。詳細については、「ストレージボリュームのスナップショットの削除」を参照してください。

ボリュームのステータスが使用可能に戻ったら、ボリュームの新しいスナップショットを作成します。ボリュームステータスについては、「ボリュームステータスと移行について」を参照してください。

高可用性のヘルス通知

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

高可用性に関する問題のトラブルシューティング

可用性の問題が発生した場合の対処方法については、以下を参照してください。

トピック

- ヘルス通知
- メトリクス

ヘルス通知

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

トピック

- 通知: Reboot
- 通知: HardReboot
- 通知: HealthCheckFailure
- 通知: AvailabilityMonitorTest

通知: Reboot

ゲートウェイ VM の再起動時に、再起動通知が表示される場合があります。VM ハイパーバイザーの管理コンソールまたは Storage Gateway コンソールを使用して、ゲートウェイ VM を再起動できます。また、ゲートウェイのメンテナンスサイクル中にゲートウェイソフトウェアを使用して再起動することもできます。

実行するアクション

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

通知: HardReboot

ゲートウェイ VM が予期せず再起動された場合、HardReboot 通知が表示されることがあります。このような再起動の原因としては、電源の喪失、ハードウェア障害、またはその他のイベントが考えられます。VMware ゲートウェイの場合、vSphere High Availability のアプリケーションの監視によるリセットにより、このイベントがトリガーされることがあります。

実行するアクション

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

通知: HealthCheckFailure

VMware vSphere HA のゲートウェイでは、ヘルスチェックが不合格になり、VM の再起動が要求されたときに HealthCheckFailure 通知が表示される場合があります。このイベントは、AvailabilityMonitorTest 通知によって示される可用性をモニタリングするためのテスト中にも発生します。この場合、HealthCheckFailure 通知の発生が想定されます。

> **Note**
>
> この通知は VMware ゲートウェイ専用です。

実行するアクション

AvailabilityMonitorTest 通知が表示されることなくこのイベントが繰り返し発生する場合は、VM インフラストラクチャに問題 (ストレージ、メモリなど) がないか確認してください。さらにサポートが必要な場合は、 にお問い合わせください サポート。

通知: AvailabilityMonitorTest

VMware vSphere HA のゲートウェイでは、VMware で可用性とアプリケーションのモニタリングシステムのテストを実行すると、AvailabilityMonitorTest 通知が表示されます。

メトリクス

AvailabilityNotifications メトリクスはすべてのゲートウェイで使用できます。このメトリクスは、ゲートウェイによって生成された可用性関連のヘルス通知の数です。Sum 統計情報を使用して、ゲートウェイで可用性関連のイベントが発生しているかどうかを調べます。イベントの詳細については、設定した CloudWatch ロググループを参照してください。

ボリュームゲートウェイのベストプラクティス

このセクションは、ゲートウェイ、ローカルディスク、スナップショット、およびデータを操作するためのベストプラクティスに関する情報を提供する以下のトピックで構成されます。このセクションで説明されている情報を理解し、 AWS Storage Gatewayの問題を避けるためにこれらのガイドラインに従うことをお勧めします。デプロイで発生する可能性がある一般的な問題の診断と解決に関する追加のガイダンスについては、「ゲートウェイのトラブルシューティング」を参照してください。

トピック

- ベストプラクティス: データの復旧
- 不要なリソースのクリーンアップ
- ボリュームで課金されるストレージ量を削減する

ベストプラクティス: データの復旧

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

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

トピック

- 予期しない仮想マシンのシャットダウンからの復旧
- 正しく機能していないゲートウェイまたは VM からのデータの復旧
- 回復不可能なボリュームからのデータの復旧
- 正しく機能していないキャッシュディスクからのデータの復旧
- 破損したファイルシステムからのデータの復旧
- アクセス不能なデータセンターからのデータの復旧

予期しない仮想マシンのシャットダウンからの復旧

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

- 停止によりネットワーク接続の問題が発生した場合、問題をトラブルシューティングできます。ネットワーク接続をテストする方法については、「ゲートウェイのインターネット接続のテスト」を参照してください。
- キャッシュ型ボリュームの設定の場合、ゲートウェイが到達可能になると、ボリュームが BOOTSTRAPPING ステータスになります。この機能により、ローカルに保存されたデータが引き続き同期されます AWS。このステータスの詳細については、「ボリュームステータスと移行について」を参照してください。
- ゲートウェイが正しく機能せず、予期しないシャットダウンの結果としてボリュームまたはテープに問題が発生した場合、データを回復できます。データの復旧方法については、シナリオに当てはまる以下のクションを参照してください。

正しく機能していないゲートウェイまたは VM からのデータの復旧

ゲートウェイまたは仮想マシンが誤動作した場合、Amazon S3 のボリュームにアップロード AWS されて保存されたデータを復元できます。キャッシュボリュームゲートウェイの場合、復旧スナップショットからデータを復旧します。保管型ボリュームゲートウェイの場合、ボリュームの最新の Amazon EBS スナップショットからデータを復元できます。テープゲートウェイの場合、復旧ポイントから新しいテープゲートウェイに 1 つ以上のテープを復旧します。

キャッシュ型ボリュームゲートウェイが到達不可能になった場合、以下のステップを使用して復旧スナップショットからデータを復旧できます。

1. で AWS Management Console、正常に機能していないゲートウェイを選択し、復旧するボリュームを選択し、そこから復旧スナップショットを作成します。
2. 新しいボリュームゲートウェイをデプロイしてアクティブ化します。または、正常に機能する既存のボリュームゲートウェイがある場合、そのゲートウェイを使用してボリュームデータを復旧できます。
3. 作成したスナップショットを見つけ、機能しているゲートウェイの新しいボリュームにスナップショットを復旧します。
4. オンプレミスのアプリケーションサーバーで、新しいボリュームを iSCSI デバイスとしてマウントします。

復旧スナップショットからキャッシュ型ボリュームデータを復旧する方法の詳細については、「ゲートウェイキャッシュ型が到達不可能なためデータを復旧する場合」を参照してください。

回復不可能なボリュームからのデータの復旧

ボリュームのステータスが IRRECOVERABLE の場合、このボリュームを使用することはできません。

保管型ボリュームでは、以下のステップを使用して、回復不可能なボリュームから新しいボリュームにデータを取得できます。

1. 回復不可能なボリュームの作成に使用されたディスクから新しいボリュームを作成します。
2. 新しいボリュームを作成するとき、既存のデータを保持します。
3. 回復不可能なボリュームの保留中のスナップショットジョブをすべて削除します。
4. ゲートウェイから回復不可能なボリュームを削除します。

キャッシュ型ボリュームについては、新しいボリュームのクローンには最後の復旧ポイントを使用することをお勧めします。

回復不可能なボリュームから新しいボリュームにデータを取得する方法の詳細については、「ボリュームは復旧不可能であるとコンソールに表示される」を参照してください。

正しく機能していないキャッシュディスクからのデータの復旧

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

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

破損したファイルシステムからのデータの復旧

ファイルシステムが破損した場合、**fsck** コマンドを使用してファイルシステムにエラーがないかチェックし、修復できます。ファイルシステムを修復できる場合、以下で説明するようにファイルシステムのそのボリュームからデータを復旧できます。

1. 仮想マシンをシャットダウンし、Storage Gateway マネジメントコンソールを使用して復旧スナップショットを作成します。このスナップショットは、 に保存されている最新のデータを表します AWS。

   > **Note**
   >
   > ファイルシステムを修復できない場合、またはスナップショットの作成プロセスが正常に完了しない場合は、フォールバックとしてこのスナップショットを使用します。

   復旧スナップショットの作成方法については、「ゲートウェイキャッシュ型が到達不可能なためデータを復旧する場合」を参照してください。
2. **fsck** コマンドを使用してファイルシステムにエラーがないかチェックし、修復を試みます。
3. ゲートウェイ VM を再起動します。
4. ハイパーバイザーホストが起動を開始したら、シフトキーを押したままにして grub ブートメニューを表示します。
5. メニューで、編集する [**e**] を押します。
6. カーネル行 (2 行目) を選択し、**e** を押して編集します。
7. カーネルコマンドラインに **init=/bin/bash** オプションを追加します。スペースを使用して、ここで追加したオプションと前のオプションを区切ります。
8. console= 行を両方とも削除し、= 記号に続く値をすべて (カンマで区切られた値も含めて) 削除します。
9. **Return** を押して変更を保存します。
10. **b** を押して、変更したカーネルオプションでコンピューターを起動します。コンピューターが起動して bash# プロンプトが表示されます。
11. 「**/sbin/fsck -f *dev/sda1***」と入力してプロンプトからこのコマンドを手動で実行し、ファイルシステムをチェックして修理します。/dev/sda1 パスに対してコマンドが機能しない場合は、**lsblk** を使用して / のルートファイルシステムデバイスを特定し、代わりにそのパスを使用できます。
12. ファイルシステムチェックと修復が完了したら、インスタンスを再起動します。grub の設定が元の値に戻り、ゲートウェアが通常どおり起動します。
13. 元のゲートウェイから作成されているスナップショットが完成するまで待ち、スナップショットデータを検証します。

元のボリュームをそのまま使い続けることも、復旧スナップショットまたは完成したスナップショットに基づく新しいボリュームを使用して新しいゲートウェイを作成することもできます。または、このボリュームから完成したスナップショットから新しいボリュームを作成することもできます。

アクセス不能なデータセンターからのデータの復旧

ゲートウェイまたはデータセンターが何らかの理由でアクセス不能である場合は、異なるデータセンターにある別のゲートウェイにデータを復元するか、Amazon EC2 インスタンスにホストされているゲートウェイに復元することができます。別のデータセンターへのアクセス権がない場合は、Amazon EC2 インスタンスにゲートウェイを作成することをお勧めします。手順は、データ復旧元のゲートウェイの種類によって異なります。

アクセス無効なデータセンターのボリュームゲートウェイからデータを復旧するには

1. Amazon EC2 ホストで新しいボリュームゲートウェイを作成してアクティブ化します。詳細については、「ボリュームゲートウェイ用にカスタマイズされた Amazon EC2 インスタンスをデプロイする」を参照してください。

   > **Note**
   >
   > ゲートウェイ保管型ボリュームは Amazon EC2 インスタンスにホストすることはできません。

2. 新しいボリュームを作成し、ターゲットゲートウェイとして EC2 ゲートウェイを選択します。詳細については、「ストレージボリュームの作成」を参照してください。

   復旧するボリュームの最新の復旧ポイントからの Amazon EBS スナップショットまたはクローンに基づいて新しいボリュームを作成します。

   ボリュームがスナップショットに基づいている場合、そのスナップショット ID を指定します。

   復旧ポイントからボリュームのクローンを作成する場合は、ソースボリュームを選択します。

不要なリソースのクリーンアップ

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

不要なリソースをクリーンアップする

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

ボリュームで課金されるストレージ量を削減する

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

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

Storage Gateway に関するその他のリソース

このセクションでは、ゲートウェイのセットアップや管理に役立つ AWS とサードパーティーのソフトウェア、ツール、リソース、および Storage Gateway のクォータについて説明します。

トピック

- ゲートウェイ VM ホストのデプロイと設定 - ゲートウェイの仮想マシンホストをデプロイして設定する方法について説明します。
- ボリュームゲートウェイのストレージリソースの使用 - ローカルディスクの削除やゲートウェイ Amazon EC2 インスタンスでの Amazon EBS ボリュームの管理など、ボリュームゲートウェイのストレージリソースに関連する手順について説明します。
- ゲートウェイのアクティベーションキーを取得する - 新しいゲートウェイをデプロイするときに提供する必要があるアクティベーションキーの確認場所について説明します。
- iSCSI イニシエータの接続 - Internet Small Computer System Interface (iSCSI) ターゲットとして公開されているボリュームまたは仮想テープライブラリ (VTL) デバイスを操作する方法を説明します。
- Storage Gateway AWS Direct Connect での の使用 - オンプレミスゲートウェイと AWS クラウドの間に専用ネットワーク接続を作成する方法について説明します。
- ゲートウェイアプライアンスの IP アドレスの取得 - 新しいゲートウェイをデプロイするときに指定する必要があるゲートウェイの仮想マシンホスト IP アドレスの確認場所について説明します。
- Storage Gateway のリソースとリソース ID の説明 - Storage Gateway によって作成されたリソースとサブリソース AWS を識別する方法について説明します。
- Storage Gateway リソースのタグ付け - メタデータタグを使用してリソースを分類し、管理を容易にする方法について説明します。
- Storage Gateway のオープンソースコンポーネントの使用 - Storage Gateway 機能の配信に使用されるサードパーティーのツールとライセンスについて説明します。
- AWS Storage Gateway クォータ - ボリュームサイズと数量の最大制限、ローカルディスクサイズの推奨事項など、ボリュームゲートウェイの制限とクォータについて説明します。

ゲートウェイ VM ホストのデプロイと設定

このセクションのトピックでは、VMware、Hyper-V、または Linux KVM で実行されているオンプレミスアプライアンス、および AWS クラウドの Amazon EC2 インスタンスで実行されているアプラ

イアンスなど、Storage Gateway アプライアンスの仮想マシンホストをセットアップして管理する方法について説明します。

トピック

- ボリュームゲートウェイ用のデフォルトの Amazon EC2 ホストをデプロイする - デフォルトの仕様を使用して、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにボリュームゲートウェイをデプロイおよびアクティブ化する方法について説明します。
- ボリュームゲートウェイ用にカスタマイズされた Amazon EC2 インスタンスをデプロイする - カスタマイズされた設定を使用して、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにボリュームゲートウェイをデプロイおよびアクティブ化する方法について説明します。
- Amazon EC2 インスタンスメタデータオプションの変更 - IMDS バージョン 1 (IMDSv1) を使用する受信メタデータリクエストを受け入れるか、すべてのメタデータリクエストが IMDS バージョン 2 (IMDSv2) を使用するように Amazon EC2 ゲートウェイインスタンスを設定する方法について説明します。
- VM の時刻を Hyper-V または Linux KVM ホストの時刻と同期する - オンプレミスの Hyper-V または Linux KVM ゲートウェイ仮想マシンの時刻を表示して、Network Time Protocol (NTP) サーバーに同期する方法について説明します。
- VM の時刻と VMware ホストの時刻を同期する - VMware ゲートウェイ仮想マシンのホスト時刻をチェックし、必要に応じて時刻を設定し、その時刻を Network Time Protocol (NTP) サーバーに自動的に同期するようにホストを設定する方法について説明します。
- VMware ホストでの準仮想化の設定 - Storage Gateway アプライアンスの VMware ホストプラットフォームを設定して、準仮想 Internet Small Computer System Interface Protocol (iSCSI) コントローラーを使用する方法について説明します。
- ゲートウェイのネットワークアダプタの設定 - 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する方法、または複数の IP アドレスからアクセスできるように複数のネットワークアダプタを使用する方法について説明します。
- Storage Gateway での VMware vSphere High Availability の使用 - VMware vSphere High Availability で動作するように Storage Gateway を設定することで、ストレージワークロードをハードウェア、ハイパーバイザー、またはネットワーク障害から保護する方法について説明します。

ボリュームゲートウェイ用のデフォルトの Amazon EC2 ホストをデプロイする

このトピックでは、Amazon EC2 ホストをデフォルト設定でデプロイする手順を説明します。

Amazon Elastic Compute Cloud (Amazon EC2) インスタンスでボリュームゲートウェイをデプロイしてアクティブ化できます。 AWS Storage Gateway Amazon マシンイメージ (AMI) は、コミュニティ AMI として利用できます。

> **Note**
>
> Storage Gateway コミュニティ AMI は公開されており、 AWSがフルサポートを提供しています。パブリッシャーが検証 AWS済みプロバイダーであることがわかります。

1. Amazon EC2 インスタンスをセットアップするには、ワークフローの [プラットフォームオプション] セクションで [ホストプラットフォーム] として [Amazon EC2] を選択します。Amazon EC2 インスタンスの設定手順については、「Amazon EC2 インスタンスをデプロイしてボリュームゲートウェイをホストする」を参照してください。
2. インスタンスを起動を選択して、Amazon EC2 コンソールで AWS Storage Gateway AMI テンプレートを開き、インスタンスタイプ、ネットワーク設定、ストレージの設定などの追加設定をカスタマイズします。
3. オプションで、Storage Gateway コンソールで [デフォルト設定を使用] を選択し、デフォルト設定で Amazon EC2 インスタンスをデプロイできます。

   [デフォルト設定を使用] を選択した場合、Amazon EC2 インスタンスには、以下のデフォルト設定が適用されます。

   - インスタンスタイプ — m5.xlarge
   - ネットワーク設定
     - [VPC] で、EC2 インスタンスを実行する VPC を選択します。
     - [サブネット] で、EC2 インスタンスを起動するサブネットを指定します。

     > **Note**
     >
     > VPC サブネットは、VPC 管理コンソールでパブリック IPv4 アドレスの自動割り当て設定が有効になっている場合にのみ、ドロップダウンに表示されます。

- 自動割り当てパブリック IP — 有効

EC2 セキュリティグループが作成され、EC2 インスタンスに関連付けられます。このセキュリティグループには、次のインバウンドポートルールが適用されます。

> **Note**
>
> ゲートウェイをアクティブ化する間は、ポート 80 を開く必要があります。このポートはアクティブ化の直後に閉じます。それ以降、EC2 インスタンスには、選択した VPC の他のポートでのみアクセスできます。
> ゲートウェイの iSCSI ターゲットには、ゲートウェイと同じ VPC 内のホストからのみアクセスできます。iSCSI ターゲットに VPC 外部のホストからアクセスする必要がある場合は、適切なセキュリティグループルールを更新する必要があります。
> セキュリティグループはいつでも編集できます。Amazon EC2 インスタンスの詳細ページに移動し、[セキュリティ] を選択します。[セキュリティグループの詳細] に移動し、セキュリティグループ ID を選択してください。

[ポート]	[プロトコル]	ファイルシステムプロトコル
80	TCP	アクティブ化のための HTTP アクセス
3260	TCP	iSCSI

- ストレージを設定

デフォルト設定	AMI ルートボリューム	ボリューム 2 キャッシュ	ボリューム 3 キャッシュ			
デバイス名		'/dev/sdb'	'/dev/sdc'			
サイズ	80 GiB	165 GiB	150 GiB			
ボリュームタイプ	gp3	gp3	gp3			
IOPS	3000	3000	3000			
終了時に削除	あり	あり	あり			
暗号化された	いいえ	いいえ	いいえ			
スループット	125	125	125			

ボリュームゲートウェイ用にカスタマイズされた Amazon EC2 インスタンスをデプロイする

Amazon Elastic Compute Cloud (Amazon EC2) インスタンスでボリュームゲートウェイをデプロイしてアクティブ化できます。 AWS Storage Gateway Amazon Machine Image (AMI) は、コミュニティ AMI として利用できます。

> **Note**
>
> Storage Gateway コミュニティ AMI は公開されており、 AWSがフルサポートを提供しています。パブリッシャーが検証 AWS済みのプロバイダーであることがわかります。
> ボリュームゲートウェイ AMI では、次の命名規則を使用します。AMI 名に追加されるバージョン番号は、バージョンリリースごとに変更されます。

```
aws-storage-gateway-CLASSIC-2.9.0
```

Amazon EC2 インスタンスをデプロイしてボリュームゲートウェイをホストするには

1. Storage Gateway コンソールを使用して、新しいゲートウェイのセットアップを開始します。手順については、「ボリュームゲートウェイをセットアップする」を参照してください。[プラットフォームオプション] セクションが表示されたら、[ホストプラットフォーム] として [Amazon EC2] を選択し、次の手順に従って、ボリュームゲートウェイをホストする Amazon EC2 インスタンスを起動します。

   > **Note**
   >
   > Amazon EC2 ホストプラットフォームは、キャッシュ型ボリュームのみに対応しています。保管型ボリュームゲートウェイは EC2 インスタンスにはデプロイできません。

2. インスタンスを起動を選択してAmazon EC2 AWS Storage Gateway コンソールで AMI テンプレートを開き、追加の設定を構成できます。

   Quicklaunch を使用して、Amazon EC2 インスタンスをデフォルト設定で起動します。Amazon EC2 Quicklaunch のデフォルト仕様の詳細については、「 Amazon EC2 の Quicklaunch 設定の仕様」を参照してください。

3. [名前] に、Amazon EC2 インスタンスの名前を入力します。インスタンスがデプロイされたら、この名前を検索して、Amazon EC2 コンソールのリストページでインスタンスを見つけることができます。

4. [インスタンスタイプ] セクションの [インスタンスタイプ] で、インスタンスのハードウェア構成を選択します。ハードウェア構成は、ゲートウェイをサポートするための所定の最小要件を満たしている必要があります。m5.xlarge インスタンスタイプから使い始めてみることを推奨します。このインスタンスタイプは、ゲートウェイが正しく機能するための最小要件を満たしています。詳細については、「Amazon EC2 インスタンスタイプでの要件」を参照してください。

   必要に応じて、起動後のインスタンスのサイズ変更を行うことができます。詳細については、「Amazon EC2 ユーザーガイド」の「Amazon EC2 インスタンスタイプの変更」を参照してください。

> **Note**
>
> 特定のインスタンスタイプ (特に i3 EC2) では、NVMe SSD ディスクを使用します。このことが原因で、ボリュームゲートウェイの起動時または停止時に問題が起きる場合があります。例えば、キャッシュからデータが失われる可能性があります。Amazon CloudWatch メトリクス `CachePercentDirty` をモニタリングし、システムを起動または停止するのは、このパラメータが `0` の場合のみにします。ゲートウェイのメトリクスのモニタリングに関する詳細については、CloudWatch ドキュメントの「Storage Gateway Metrics and Dimensions」を参照してください。

5. [キーペア (ログイン)] セクションの [キーペア名 - 必須] で、インスタンスに安全に接続するために使用するキーペアを選択します。必要に応じて新しいキーペアを作成できます。詳細については、「Amazon Elastic Compute Cloud Linux インスタンス用ユーザーガイド」の「キーペアを作成する」を参照してください。
6. [ネットワーク設定] セクションで、事前設定された設定内容を確認し、[編集] を選択して以下のフィールドを変更します。

   a. [VPC - 必須] で、Amazon EC2 インスタンスを起動する VPC を選択します。詳細については、「Amazon Virtual Private Cloud ユーザーガイド」の「Amazon VPC の仕組み」を参照してください。

   b. (オプション) [サブネット] で、Amazon EC2 インスタンスを起動するサブネットを選択します。

   c. [Auto-assign Public IP] (パブリック IP の自動割当て) で、[Enable] (有効化) を選択します。
7. [ファイアウォール (セキュリティグループ)] サブセクションで、事前設定された設定内容を確認します。Amazon EC2 インスタンス用に作成される新しいセキュリティグループのデフォルトの名前と説明を必要に応じて変更するか、代わりに既存のセキュリティグループのファイアウォールルールを適用することができます。
8. [インバウンドセキュリティグループのルール] サブセクションで、クライアントがインスタンスへの接続に使用するポートを開くファイアウォールルールを追加します。ボリュームゲートウェイに必要なポートの詳細については、「ポート要件」を参照してください。ファイアウォールルールの追加の詳細については、「Amazon Elastic Compute Cloud Linux インスタンス用ユーザーガイド」の「セキュリティグループのルール」を参照してください。

> **Note**
>
> ボリュームゲートウェイでは、インバウンドトラフィックと、ゲートウェイのアクティブ化中の 1 回限りの HTTP アクセス用に、TCP ポート 80 を開く必要があります。このポートは、アクティブ化の後で閉じることができます。
> また、iSCSI アクセス用に TCP ポート 3260 を開く必要があります。

9. [高度なネットワーク設定] サブセクションで、事前設定された設定内容を確認し、適宜変更します。
10. [ストレージを設定] ページで [新しいボリュームの追加] を選択して、ゲートウェイインスタンスにストレージを追加します。

> **Important**
>
> 事前設定されたルートボリュームに加えて、キャッシュストレージ用に 165 GiB 以上の容量がある Amazon EBS ボリュームを少なくとも 1 つ、アップロードバッファ用に 150 GiB 以上の容量がある Amazon EBS ボリュームを少なくとも 1 つ追加する必要があります。パフォーマンスを向上させるため、それぞれ 150 GiB 以上の容量がある複数の EBS ボリュームをキャッシュストレージ用に割り当てることをお勧めします。

11. [高度な詳細] セクションで、事前設定された設定内容を確認し、適宜変更します。
12. [インスタンスを起動] を選択し、指定した設定内容で新しい Amazon EC2 ゲートウェイインスタンスを起動します。
13. 新しいインスタンスが正常に起動したことを確認するには、Amazon EC2 コンソールの [インスタンス] ページに移動し、新しいインスタンスを名前で検索します。[インスタンスの状態] に [実行中] と緑のチェックマークが表示されていること、また、ステータスチェックが完了し、緑色のチェックマークが表示されていることを確認します。
14. 詳細ページからインスタンスを選択します。[インスタンスの概要] セクションからパブリック IPv4 アドレスをコピーし、Storage Gateway コンソールの [ゲートウェイのセットアップ] ページに戻って、ボリュームゲートウェイのセットアップを再開します。

Storage ゲートウェイボリュームStorage Gatewayの起動に使用する AMI ID を決定できます。 AWS Systems Manager

AMI ID を確認するには、以下のいずれかを実行します。

- Storage Gateway コンソールを使用して、新しいゲートウェイのセットアップを開始します。手順については、「ボリュームゲートウェイをセットアップする」を参照してください。プラットフォームオプションセクションに移動したら、ホストプラットフォームとして Amazon EC2 を選択し、インスタンスを起動を選択して Amazon EC2 コンソールで AWS Storage Gateway AMI テンプレートを開きます。

  EC2 コミュニティ AMI ページにリダイレクトされ、URL に AWS リージョンの AMI ID が表示されます。

- Systems Manager パラメータストアにクエリを実行します。 AWS CLI または Storage Gateway API を使用して、`/aws/service/storagegateway/ami/CACHED/latest`キャッシュ型ボリュームゲートウェイまたはストアドボリュームゲートウェイの名前空間で Systems Manager パブリックパラメータ`/aws/service/storagegateway/ami/STORED/latest`をクエリできます。たとえば、次の CLI コマンドを使用すると、指定した で現在の AMI の ID が返され AWS リージョン ます。

  ```
  aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/
  STORED/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/
  STORED/latest",
          "Name": "/aws/service/storagegateway/ami/STORED/latest",
          "Value": "ami-123c45dd67d891000"
      }
  }
  ```

Amazon EC2 インスタンスメタデータオプションの変更

インスタンスメタデータサービス (IMDS) は、Amazon EC2 インスタンスメタデータに安全にアクセスするために提供されるインスタンス上のコンポーネントです。インスタンスは、IMDS バージョン 1 (IMDSv1) を使用する受信メタデータリクエストを受け入れるように設定することも、すべてのメタデータリクエストで IMDS バージョン 2 (IMDSv2) の使用をリクエストするように設定するこ

ともできます。IMDSv2 はセッション指向のリクエストを使用し、IMDS へのアクセス試行に利用される可能性があるいくつかのタイプの脆弱性を軽減します。IMDSv2 の詳細については、「Amazon Elastic Compute Cloud ユーザーガイド」の「インスタンスメタデータサービスバージョン 2 の仕組み」を参照してください。

Storage Gateway をホストするすべての Amazon EC2 インスタンスに IMDSv2 をリクエストすることをお勧めします。新しく起動されたすべてのゲートウェイインスタンスでは、デフォルトで IMDSv2 が必要です。IMDSv1 メタデータリクエストを受け入れるようにまだ設定されている既存のインスタンスがある場合、IMDSv2 の使用を要求するようにインスタンスメタデータオプションを変更する手順については、「Amazon Elastic Compute Cloud ユーザーガイド」の「IMDSv2 の使用を要求する」を参照してください。この変更を適用するために、インスタンスを再起動する必要はありません。

VM の時刻を Hyper-V または Linux KVM ホストの時刻と同期する

VMware ESXi にデプロイされたゲートウェイの場合、時刻のずれを防ぐには、ハイパーバイザーホストの時刻を設定して、仮想マシンの時刻をホストと同期するだけで十分です。詳細については、「VM の時刻と VMware ホストの時刻を同期する」を参照してください。Microsoft Hyper-V または Linux KVM にデプロイされたゲートウェイの場合、次に説明する手順を使用して、定期的に仮想マシンの時刻を確認することをお勧めします。

ハイパーバイザーゲートウェイ仮想マシンの時刻を表示してネットワークタイムプロトコル (NTP) サーバーと同期するには

1. ゲートウェイのローカルコンソールにログインします。

   - Microsoft Hyper-V ローカルコンソールへのログインの詳細については、「Microsoft Hyper-V でゲートウェイのローカルコンソールにアクセスする」を参照してください。
   - Linux のカーネルベース仮想マシン (KVM) のローカルコンソールへのログインの詳細については、「Linux KVM でゲートウェイのローカルコンソールにアクセスする」を参照してください。

2. [Storage Gateway の設定] メインメニュー画面で、対応する数字を入力して、[システム時刻の管理] を選択します。
3. [システム時刻の管理] メニュー画面で、対応する数字を入力して、[システム時刻の表示と同期] を選択します。

   ゲートウェイローカルコンソールは、現在のシステム時刻を表示し、NTP サーバーによって報告された時刻と比較して、2 つの時刻の正確な差異を秒単位で報告します。

4. 時刻の差異が 60 秒を超える場合は、**y** を入力してシステム時刻を NTP 時刻と同期します。それ以外の場合は、「**n**」と入力します。

   時刻の同期には数分かかる場合があります。

VM の時刻と VMware ホストの時刻を同期する

ゲートウェイを正常にアクティブ化するには、VM の時刻をホストの時刻と同期し、ホストの時刻を正しく設定する必要があります。このセクションでは、最初に VM の時刻をホストの時刻に同期します。続いて、ホストの時刻を確認し、必要であればホストの時刻を設定して、ホストの時刻がネットワークタイムプロトコル (NTP) サーバーに自動的に同期するように設定します。

> **Important**
>
> ゲートウェイを正常にアクティブ化するには、VM の時刻とホストの時刻を同期する必要があります。

VM の時刻とホストの時刻を同期するには

1. VM の時刻を構成します。

   a. vSphere クライアントで、アプリケーションウィンドウの左側にあるパネルでゲートウェイ VM の名前を右クリックして VM のコンテキストメニューを開き、[設定の編集] を選択します。

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

   b. [オプション] タブを選択し、オプションリストで [VMware ツール] を選択します。

   c. [仮想マシンのプロパティ] ダイアログボックスの右側にある [アドバンスト] セクションで、[ゲスト時刻をホストと同期する] オプションをチェックし、[OK] を選択します。

      VM の時刻がホストと同期されます。

2. ホストの時刻を構成します。

   ホストの時計が正しい時刻に設定されてかを確認するのは重要です。ホストの時計の設定が済んでいない場合は、次の手順に従って、時計を設定して NTP サーバーと同期します。

   a. VMware vSphere クライアントで、左側のパネル vSphere ホストノードを選択し、[設定] タブを選択します。

b. [Software] (ソフトウェア) パネルで [Time Configuration] (時刻設定) を選択してから、[Properties] (プロパティ) リンクを選択します。

   [Time Configuration] ダイアログボックスが表示されます。

c. [日付と時刻] で、vSphere ホストの日付と時刻を設定します。

d. 時刻を NTP サーバーに自動的に同期するように、ホストを設定します。

   i. [時刻設定] ダイアログボックスで [オプション] を選択してから、[NTP デーモン (ntpd) オプション] ダイアログボックスで、左パネルの [NTP 設定] を選択します。

   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。

   ドメイン名として `pool.ntp.org` を使用できます。

   iv. [NTP デーモン (ntpd) オプション] ダイアログボックスで、左側のパネルの [全般] を選択します。

   v. [サービスコマンド] で、[開始] を選択してサービスを開始します。

   後でこの NTP サーバー参照を変更したり他の参照を追加した場合、新しいサーバーを使用するには、サービスを再起動する必要があります。

e. [OK] を選択して、[NTP 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 ホストでの準仮想化の設定

次の手順では、Storage Gateway アプライアンスの VMware ホストプラットフォームを設定して、準仮想 Internet Small Computer System Interface Protocol (iSCSI) コントローラーを使用する方法について説明します。準仮想 iSCSI コントローラーは、スループットを高め、CPU 使用率を低下させることができる高性能ストレージコントローラーです。これらのコントローラーは、高性能ストレージ環境に最適です。このように iSCSI コントローラーを設定すると、Storage Gateway 仮想マシンはホストオペレーティングシステムと連携して、ゲートウェイコンソールが仮想マシンに追加する仮想ディスクを識別できるようにします。

> **Note**
>
> ゲートウェイコンソールでこれらのディスクを設定するときに、ディスクの識別の問題を防ぐために、このステップを完了する必要があります。

準仮想化コントローラーを使用するように VMware ホストプラットフォームを設定するには

1. VMware vSphere クライアントで、アプリケーションウィンドウの左側のナビゲーションペインでゲートウェイ仮想マシンの名前を右クリックしてコンテキストメニューを開き、[設定の編集] を選択します。
2. [仮想マシンのプロパティ] ダイアログボックスで、[ハードウェア] タブを選択します。
3. [ハードウェア] タブで、[SCSI コントローラー 0] を選択し、[変更タイプ] を選択します。
4. [SCSI コントローラータイプの変更] ダイアログボックスで、SCSI コントローラータイプとして [VMware 準仮想化] を選択し、[OK] を選択します。

ゲートウェイのネットワークアダプタの設定

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

トピック

- ゲートウェイによる VMXNET3 ネットワークアダプタの使用の設定
- 複数の NIC に対するゲートウェイの設定

ゲートウェイによる VMXNET3 ネットワークアダプタの使用の設定

Storage Gateway は、VMware ESXi ホストと Microsoft Hyper-V ハーパーバイザーホストの両方で E1000 ネットワークアダプタタイプをサポートしています。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。これらのアダプタの詳細については、Broadcom (VMware) ウェブサイトの「Choosing a network adapter for your virtual machine」を参照してください。

> **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] 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. ネットワークタイプウィザードで、[Adapter Type] (アダプタタイプ) に **VMXNET3** を選択してから、[Next] (次へ) をクリックします。

8. Virtual Machine Properties ウィザードの [Adapter Type] セクションで [Current Adapter] 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。デフォルト認証情報を使用してログインする方法については、「デフォルトの認証情報を使用したローカルコンソールへのログイン」を参照してください。
2. プロンプトで、対応する番号を入力して [Network Configuration] を選択します。
3. プロンプトで、対応する番号を入力して [Reset all to DHCP] 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。

   ゲートウェイが既にアクティブになっている場合は、ゲートウェイをシャットダウンし、Storage Gateway マネジメントコンソールから再起動する必要があります。ゲートウェイが再起動したら、インターネットへのネットワーク接続をテストする必要があります。ネットワーク接続をテストする方法については、「ゲートウェイのインターネット接続のテスト」を参照してください。

複数の NIC に対するゲートウェイの設定

複数のネットワークアダプタ (NIC) を使用するようにゲートウェイを設定すると、複数の IP アドレスからアクセスできます。このようにするのは、次のような場合です。

- スループットの最大化 – ネットワークアダプタがボトルネックになっている場合に、ゲートウェイへのスループットを最大にしたい場合があります。
- アプリケーションの分離 – アプリケーションがゲートウェイのボリュームに書き込む方法を分離することが必要な場合があります。たとえば、重要なストレージアプリケーションで、ゲートウェイ用に定義されている特定のアダプタが排他的に使用されるように設定することがあります。

- ネットワークの制約 – アプリケーション環境によっては、iSCSI ターゲットとそれに接続するイニシエータを、ゲートウェイが AWSとの通信に使用するネットワークとは異なるネットワークに分離しておくことが必要な場合があります。

一般的な複数アダプタのユースケースでは、ゲートウェイが通信するルートとして 1 つのアダプタが設定されています AWS (つまり、デフォルトゲートウェイとして)。この 1 つのアダプタを除き、イニシエータは接続先の iSCSI ターゲットを含むアダプタと同じサブネット内に存在する必要があります。そうでない場合は、意図したターゲットと通信できない可能性があります。ターゲットが との通信に使用されるのと同じアダプターで設定されている場合 AWS、そのターゲットとトラフィックの iSCSI AWS トラフィックは同じアダプターを通過します。

1 つのアダプタを Storage Gateway コンソールに接続するように設定し、その後 2 つ目のアダプタを追加した場合、Storage Gateway は 2 番目のアダプタを優先ルートとして使用するように自動的にルートテーブルを設定します。複数のアダプタを設定する手順については、以下のセクションを参照してください。

- VMware ESXi ホストでの複数のネットワークアダプタの設定
- Microsoft Hyper-V ホストでの複数のネットワークアダプタの設定

VMware ESXi ホストでの複数のネットワークアダプタの設定

次の手順では、ゲートウェイ VM で 1 つのネットワークアダプタが定義済みであることを前提に、VMware ESXi でアダプタを設定する方法を説明します。

VMware ESXi ホストで追加のネットワークアダプタを使用するようにゲートウェイを設定するには

1. ゲートウェイをシャットダウンします。
2. VMware vSphere クライアントで、ゲートウェイの VM を選択します。

   この手順では、VM の電源は入れたままにしてかまいません。
3. クライアントでゲートウェイ VM のコンテキスト (右クリック) メニューを開き、[Edit Settings] を選択します。
4. [Virtual Machine Properties] (仮想マシンのプロパティ) ダイアログボックスの [Hardware] (ハードウェア) タブで、[Add] (追加) を選択してデバイスを追加します。
5. [Add Hardware] ウィザードに従って、ネットワークアダプタを追加します。

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

b. [Network Type] (ネットワークタイプ) ペインで、[Type] (タイプ) に [Connect at power on] (電源投入時に接続) が選択されていることを確認してから、[Next] (次へ) をクリックします。

   Storage Gateway では VMXNET3 ネットワークアダプタを使用することをお勧めします。アダプタのリストに表示されるアダプタタイプの詳細については、ESXi and vCenter Server Documentation の Network Adapter Types を参照してください。

c. [Ready to Complete] ペインで情報を確認し、[Finish] を選択します。

6. VM の [Summary] タブを選択し、[IP Address] ボックスの横にある [View All] を選択します。[Virtual Machine IP Addresses] ウィンドウに、ゲートウェイへのアクセスに使用できるすべての IP アドレスが表示されます。2 番目の IP アドレスがゲートウェイに対して表示されることを確認します。

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

7. Storage Gateway コンソールでゲートウェイをオンにします。

8. Storage Gateway コンソールの [Navigation] (ナビゲーション) ペインで、[Gateways] (ゲートウェイ) を選択し、アダプタを追加したゲートウェイを選択します。2 番目の IP アドレスが [詳細] タブに表示されることを確認します。

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でのタスクの実行」を参照してください。

Microsoft Hyper-V ホストでの複数のネットワークアダプタの設定

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、[仮想マシン] パネルからゲートウェイ VM を選択します。
3. ゲートウェイ VM がオフになっていない場合は、VM 名を右クリックしてコンテキストメニューを開き、[オフにする] を選択します。
4. ゲートウェイ VM 名を右クリックしてコンテキストメニューを開き、[設定] を選択します。
5. [設定] ダイアログボックスの [ハードウェア] で、[ハードウェアの追加] を選択します。
6. [設定] ダイアログボックスの右側にある [ハードウェアの追加] パネルで、[ネットワークアダプタ] を選択し、[追加] を選択してデバイスを追加します。
7. ネットワークアダプタを設定し、[適用する] を選択して設定を適用します。
8. [設定] ダイアログボックスの [ハードウェア] で、新しいネットワークアダプタがハードウェアリストに追加されたことを確認し、[OK] を選択します。
9. Storage Gateway コンソールを使用してゲートウェイをオンにします。
10. Storage Gateway コンソールの [ナビゲーション] パネルで、[ゲートウェイ] を選択し、アダプタを追加したゲートウェイを選択します。2 番目の IP アドレスが [詳細] タブに表示されることを確認します。

VMware、Hyper-V、KVM ホストに共通するローカルコンソールタスクについては、「VM ローカルコンソールでのタスクの実行」を参照してください。

Storage Gateway での VMware vSphere High Availability の使用

Storage Gateway は、VMware vSphere High Availability (VMware HA) と統合された一連のアプリケーションレベルのヘルスチェックを通じて VMware の高可用性を提供します。このアプローチは、ハードウェア、ハイパーバイザー、またはネットワーク障害からストレージのワークロードを保護するのに役立ちます。また、接続タイムアウトや、ファイル共有またはボリュームを使用できないなどのソフトウェアエラーからの保護にも役立ちます。

vSphere HA は、冗長性を確保するために仮想マシンとそれらが存在するホストをクラスターにプールすることによって機能します。クラスター内のホストはモニタリングされ、障害が発生した場合は、障害が発生したホスト上の仮想マシンが代替ホストで再起動されます。通常、この復旧はデータ損失なしで迅速に行われます。vSphere HA の詳細については、VMware ドキュメントの「How vSphere HA Works」を参照してください。

> **Note**
>
> 障害が発生した仮想マシンを再起動し、新しいホストで iSCSI 接続を再確立するために必要な時間は、ホストオペレーティングシステムとリソースの負荷、ディスク速度、ネットワー

ク接続、SAN/ストレージインフラストラクチャなど、多くの要因によって異なります。フェイルオーバーのダウンタイムを最小限に抑えるには、「ゲートウェイパフォーマンスの最適化」で説明されている推奨事項を実装します。
Storage Gateway を VMware HA とともに使用するには、次のことの実行をお勧めします。

- Storage Gateway VM を含む VMware ESX の .ova ダウンロード可能なパッケージをデプロイするのは、クラスター内の 1 つのホストだけにします。
- .ova パッケージをデプロイする場合は、1 つのホストだけにローカルではないデータストアを選択してください。代わりに、クラスターのすべてのホストにアクセスできるデータストアを使用します。1 つのホストだけにローカルなデータストアを選択し、そのホストに障害が発生した場合、データソースはクラスター内の他のホストからアクセスできない可能性があります。また、他のホストへのフェイルオーバーが成功しない可能性があります。
- フェイルオーバー中にストレージボリュームのターゲットとイニシエータの接続が切れないように、オペレーティングシステム用の、推奨される iSCSI 設定に従ってください。フェイルオーバーが発生した場合、ゲートウェイ VM がフェイルオーバークラスター内の新しいホストで開始するまで、数秒から数分かかることがあります。Windows クライアントと Linux クライアントに推奨される iSCSI タイムアウトは、フェイルオーバーの発生にかかる一般的な時間より長くなっています。Windows クライアントのタイムアウト設定のカスタマイズに関する詳細については、「Windows iSCSI 設定のカスタマイズ」を参照してください。Linux クライアントのタイムアウト設定のカスタマイズに関する詳細については、「Linux iSCSI 設定のカスタマイズ」を参照してください。
- クラスタリングを利用して .ova パッケージをクラスターにデプロイした場合、プロンプトが表示されたら、ホストを選択します。その他の方法として、クラスター内のホストに直接デプロイすることもできます。

次のトピックでは、Storage Gateway を VMware HA クラスターにデプロイする方法について説明します。

トピック

- vSphere の VMware HA クラスターの設定
- Storage Gateway コンソールから .ova イメージをダウンロードする
- ゲートウェイのデプロイ
- (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、オプションごとに次の値を設定します。

   - [Host Failure Response]: [Restart VMs]
   - [Response for Host Isolation]: [Shut down and restart VMs]
   - [Datastore with PDL]: [Disabled]
   - [Datastore with APD]: [Disabled]
   - [VM Monitoring]: [VM and Application Monitoring]
2. 次の値を調整して、クラスターの感度を微調整します。

   - [Failure interval] – この期間の後、VM ハートビートが受信されない場合、VM は再起動されます。
   - [Minimum uptime] – クラスターは、VM が VM ツールのハートビートのモニタリングを開始した後でこの時間待機します。
   - [Maximum per-VM resets] – クラスターは、最大リセット時間枠内で最大この回数 VM を再起動します。
   - [Maximum resets time window] – VM ごとの最大リセット回数をカウントする時間枠。

   設定する値がわからない場合は、次の設定例を使用します。

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

クラスターで他の 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。

Storage Gateway コンソールから .ova イメージをダウンロードする

ゲートウェイタイプの .ova イメージをダウンロードするには

- Storage Gateway コンソールの [ゲートウェイのセットアップ] ページで、ゲートウェイタイプとホストプラットフォームを選択し、コンソールに表示されるリンクを使用して .ova をダウンロードします。詳細については、「ボリュームゲートウェイをセットアップする」を参照してください。

ゲートウェイのデプロイ

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

ゲートウェイの .ova イメージをデプロイするには

1. .ova イメージをクラスター内のホストの 1 つにデプロイします。
2. ルートディスクとキャッシュ用に選択したデータストアが、クラスター内のすべてのホストで使用可能であることを確認します。Storage Gateway の .ova ファイルを VMware 環境またはオンプレミス環境にデプロイする場合、ディスクは準仮想化 SCSI ディスクと呼ばれます。準仮想化は、ゲートウェイ VM がホストオペレーティングシステムと共同して、VM に追加される仮想ディスクをコンソールが識別できるようにするモードです。

   準仮想化コントローラーを使用するように VM を構成するには

   1. VMware vSphere クライアントでゲートウェイ VM のコンテキスト (右クリック) メニューを開き、[Edit Settings] を選択します。
   2. [Virtual Machine Properties] ダイアログボックスで [Hardware] タブを選択し、[SCSI controller 0] を選択して [Change Type] を選択します。
   3. [Change SCSI Controller Type] ダイアログボックスで、SCSI コントローラータイプとして [VMware Paravirtual] を選択し、[OK] を選択します。

(オプション) クラスター上の他の VM に対する上書きオプションの追加

クラスターで他の VM が実行されている場合は、各 VM 専用にクラスター値を設定することもできます。手順については、「VMware vSphere オンラインドキュメント」の「Customize an Individual Virtual Machine」を参照してください。

クラスター上の他の VM のオーバーライドオプションを追加するには

1. VMware vSphere の [Summary] ページで、クラスターを選択してクラスターページを開き、[Configure] を選択します。
2. [Configuration] タブを選択し、[VM Overrides] を選択します。
3. 新しい VM オーバーライドオプションを追加して、各値を変更します。

   [vSphere HA - VM モニタリング] の各オプションに次の値を設定します。

   - [VM モニタリング]: [上書きが有効] - [VM およびアプリケーションのモニタリング]
   - [VM モニタリングの機密性]: [上書きが有効] - [VM とアプリケーションのモニタリング]
   - [VM モニタリング]: [カスタム]
   - [失敗の間隔]: **30** 秒
   - [最小稼働時間]: **120** 秒
   - [Maximum per-VM resets]: **5**
   - [最大リセット時間枠]: **1** 時間以内

ゲートウェイのアクティブ化

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

ゲートウェイをアクティブ化するには

- 以下のトピックで概説されている手順に従ってください。

  a. ボリュームゲートウェイを に接続する AWS

  b. 設定を確認してボリュームゲートウェイをアクティブ化する

  c. ボリュームゲートウェイを設定する

VMware High Availability 設定のテスト

ゲートウェイをアクティブ化したら、設定をテストします。

VMware HA 設定をテストするには

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. ナビゲーションペインで [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。

VMware HA イベントに関する情報は、Amazon CloudWatch ロググループで確認できます。詳細については、「CloudWatch Log Group を使用したボリュームゲートウェイヘルスログの取得」を参照してください。

ボリュームゲートウェイのストレージリソースの使用

このセクションのトピックでは、ボリュームゲートウェイアプライアンスとその仮想ホストプラットフォームに関連付けられているストレージリソースを管理する方法について説明します。これには、ゲートウェイのハイパーバイザーホストプラットフォームにアタッチされた物理ディスクなどのリソースが含まれ、VMware vSphere ESXi、Microsoft Hyper-V、または Linux のカーネルベース仮想マシン (KVM) 仮想化ホストからディスクを削除する特定の手順が含まれます。これには、 AWS クラウドの Amazon EC2 でホストされているゲートウェイのゲートウェイの Amazon EC2 インスタンスにアタッチされた Amazon EC2ボリュームの管理も含まれます。

トピック

- ゲートウェイからのディスクの削除 - 物理ディスクに障害が発生した場合など、ゲートウェイの VMware vSphere ESXi、Microsoft Hyper-V、または Linux のカーネルベース仮想マシン (KVM) 仮想化ホストプラットフォームからディスクを削除する必要がある場合の対処方法について説明します。
- Amazon EC2 ゲートウェイでの Amazon EBS ボリュームの管理 - Amazon EC2 インスタンスでホストされているゲートウェイのアップロードバッファまたはキャッシュストレージとして使用するために割り当てられた Amazon EBS ボリュームの数量を増減する方法について説明します。例えば、アプリケーションストレージが時間の経過とともに増減する必要がある場合などです。

ゲートウェイからのディスクの削除

基になるディスクをゲートウェイから削除することはお勧めしませんが、障害が発生したディスクがあるときなどは、ディスクをゲートウェイから削除することが必要になる場合があります。

VMware ESXi でホストされているゲートウェイからのディスクの削除

VMware ハイパーバイザーでホストされているゲートウェイからディスクを削除するには、次の手順に従います。

アップロードバッファ (VMware ESXi) 用に割り当てられているディスクを削除するには

1. vSphere クライアントでコンテキスト (右クリック) メニューを開き、ゲートウェイ VM の名前を選択して、[Edit Settings] を選択します。
2. [Virtual Machine Properties] ダイアログボックスの [Hardware] タブで、アップロードバッファ領域として割り当てられているディスクを選択し、[Remove] を選択します。

   [Virtual Machine Properties] (仮想マシンのプロパティ) ダイアログボックスの [Virtual Device Node] (仮想デバイスノード) の値が、前に書き留めた値と同じであることを確認します。そうすることで、正しいディスクを削除することができます。
3. [Removal Options] パネルでオプションを選択し、[OK] を選択して、ディスクを削除するプロセスを完了します。

Microsoft Hyper-V でホストされているゲートウェイからのディスクの削除

Microsoft Hyper-V ハイパーバイザーでホストされているゲートウェイからディスクを削除するには、次の手順に従います。

アップロードバッファ (Microsoft Hyper-V) として割り当てられた基盤となるディスクを削除するには

1. Microsoft Hyper-V Manager でコンテキスト (右クリック) メニューを開き、ゲートウェイ VM の名前を選択して、[Settings] を選択します。
2. [Settings] ダイアログボックスの [Hardware] リストで、削除するディスクを選択し、[Remove] を選択します。

   ゲートウェイに追加したディスクは、[Hardware] (ハードウェア) リストの [SCSI Controller] (SCSI コントローラー) エントリに表示されます。[Controller] 値と [Location] 値が、前に書き留めた値と同じであることを確認します。そうすることで、正しいディスクを削除することができます。

   Microsoft Hyper-V Manager に表示される最初の SCSI コントローラはコントローラ 0 です。
3. [OK] を選択して変更を適用します。

Linux KVM でホストされているゲートウェイからのディスクの削除

Linux カーネルベースの仮想マシン (KVM) ハイパーバイザーでホストされているゲートウェイからディスクをデタッチするには、次のような `virsh` コマンドを使用します。

```
$ virsh detach-disk domain_name /device/path
```

KVM ディスクの管理の詳細については、ご使用の Linux ディストリビューションのドキュメントを参照してください。

Amazon EC2 ゲートウェイでの Amazon EBS ボリュームの管理

最初にゲートウェイを Amazon EC2 インスタンスとして実行するように設定したとき、アップロードバッファおよびキャッシュストレージとして使用するために Amazon EBS ボリュームを割り当てました。時間の経過と共にアプリケーションのニーズが変化した場合、この用途のために追加の Amazon EBS ボリュームを割り当てることができます。前に割り当てた Amazon EBS ボリュームを削除して、割り当てたストレージを減らすこともできます。Amazon EBS の詳細については、「Amazon EC2 ユーザーガイド」の「Amazon Elastic Block Store (Amazon EBS)」を参照してください。

ゲートウェイにストレージを追加する前に、ゲートウェイのアプリケーションニーズに基づいて、アップロードバッファとキャッシュストレージのサイズを設定する方法を確認してください。これを

行うには、「割り当てるアップロードバッファのサイズの決定」と「割り当てるキャッシュストレージのサイズの決定」を参照してください。

アップロードバッファおよびキャッシュストレージとして割り当てることができる最大ストレージにはクォータがあります。インスタンスにはいくらでも Amazon EBS ボリュームをアタッチすることができますが、アップロードバッファおよびキャッシュストレージとしてのボリュームの領域は、ストレージのクォータまでしか設定できません。詳細については、「AWS Storage Gateway クォータ」を参照してください。

Amazon EBS ボリュームを追加してゲートウェイ用に設定するには

1. Amazon EBS ボリュームを作成します。手順については、「Amazon EC2 ユーザーガイド」の「Amazon EBS ボリュームの作成」を参照してください。
2. Amazon EC2 インスタンスに Amazon EBS ボリュームをアタッチします。手順については、「Amazon EC2 ユーザーガイド」の「Amazon EBS ボリュームを Amazon EC2 インスタンスにアタッチ」を参照してください。
3. アップロードバッファまたはキャッシュストレージとして追加した Amazon EBS ボリュームを設定します。手順については、Storage Gateway のローカルディスクの管理 を参照してください。

アップロードバッファに割り当てた量のストレージが不要になることがあります。

Amazon EBS ボリュームを作成するには

> ⚠ Warning
>
> 以下の手順は、キャッシュに割り当てられたボリュームではなく、アップロードバッファ領域として割り当てられた Amazon EBS ボリュームにのみ適用されます。

1. 「ゲートウェイ VM のシャットダウン」セクションで説明されているアプローチに従ってゲートウェイをシャットダウンします。
2. Amazon EC2 インスタンスから Amazon EBS ボリュームをデタッチします。手順については、「Amazon EC2 ユーザーガイド」の「Amazon EC2 インスタンスから Amazon EBS ボリュームをデタッチ」を参照してください。
3. Amazon EBS ボリュームを削除します。手順については、「Amazon EC2 ユーザーガイド」の「Amazon EBS ボリュームの削除」を参照してください。

4. 「ゲートウェイ VM のシャットダウン」セクションで説明されているアプローチに従ってゲートウェイを起動します。

ゲートウェイのアクティベーションキーを取得する

ゲートウェイのアクティベーションキーを受け取るには、ゲートウェイ仮想マシン (VM) にウェブリクエストを行います。VM はアクティベーションキーを含むリダイレクトを返します。アクティベーションキーは、ゲートウェイの設定を指定するための `ActivateGateway` API アクションのパラメータの 1 つとして渡されます。詳細については、「Storage Gateway API リファレンス」の「ActivateGateway」を参照してください。

> **Note**
>
> ゲートウェイのアクティベーションキーは、未使用の場合 30 分で有効期限が切れます。

ゲートウェイ VM に対して行うリクエストには、アクティベーションが発生する AWS リージョンが含まれます。応答のリダイレクトで返される URL には、`activationkey` と呼ばれるクエリ文字列パラメータが含まれています。このクエリ文字列パラメータが、アクティベーションキーです。クエリ文字列の形式は次のようになります。`http://`*`gateway_ip_address`*`/?activationRegion=`*`activation_region`*このクエリの出力で、アクティベーションリージョンとキーの両方が返されます。

URL には、`vpcEndpoint`、VPC エンドポイントタイプを使用して接続するゲートウェイの VPC エンドポイント ID も含まれています。

> **Note**
>
> Storage Gateway ハードウェアアプライアンス、VM イメージテンプレート、Amazon EC2 Amazon マシンイメージ (AMI) には、このページで説明するウェブリクエストを受信して応答するために必要な HTTP サービスが事前設定されています。ゲートウェイに追加のサービスをインストールすることは必須ではなく、推奨もされていません。

トピック

- Linux (curl)
- Linux (bash/zsh)

- Microsoft Windows PowerShell
- ローカルコンソールを使用する

Linux (curl)

次の例では、Linux (curl) を使用してアクティベーションキーを取得する方法を示しています。

> **Note**
>
> 強調表示された変数を、ゲートウェイの実際の値に置き換えてください。指定できる値は次のとおりです。
>
> - *gateway_ip_address* - ゲートウェイの IPv4 アドレス。例: 172.31.29.201
> - *gateway_type* - STORED、CACHED、VTL、FILE_S3、または FILE_FSX_SMB など、アクティブ化するゲートウェイのタイプ。
> - *region_code* - ゲートウェイをアクティブ化するリージョン。「AWS 全般のリファレンス」の「リージョンエンドポイント」を参照してください。このパラメータが指定されていない場合、または指定された値がスペルミスであるか、有効なリージョンと一致しない場合、コマンドはデフォルトで us-east-1 リージョンになります。
> - *vpc_endpoint* - ゲートウェイのVPC エンドポイント名。例: vpce-050f90485f28f2fd0-iep0e8vq.storagegateway.us-west-2.vpce.amazonaws.com

パブリックエンドポイントのアクティベーションキーを取得するには:

```
curl "http://gateway_ip_address/?activationRegion=region_code&no_redirect"
```

VPC エンドポイントのアクティベーションキーを取得するには:

```
curl "http://gateway_ip_address/?
activationRegion=region_code&vpcEndpoint=vpc_endpoint&no_redirect"
```

Linux (bash/zsh)

次の例では、Linux (bash/zsh) を使用して HTTP レスポンスを取得し、HTTP ヘッダーを解析してアクティベーションキーを取得する方法を示します。

```
function get-activation-key() {
  local ip_address=$1
  local activation_region=$2
  if [[ -z "$ip_address" || -z "$activation_region" || -z "$gateway_type" ]]; then
    echo "Usage: get-activation-key ip_address activation_region gateway_type"
    return 1
  fi

  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region&gatewayType=$gateway_type"); then
    activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')
    echo "$activation_key_param" | cut -f2 -d=
  else
    return 1
  fi
}
```

Microsoft Windows PowerShell

次の例では、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,
    [parameter(Mandatory=$true)][string]$GatewayType
  )
  PROCESS {
    $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion&gatewayType=$GatewayType" -MaximumRedirection 0 -
ErrorAction SilentlyContinue
    if ($request) {
      $activationKeyParam = $request.Headers.Location | Select-String -Pattern
 "activationKey=([A-Z0-9-]+)"
      $activationKeyParam.Matches.Value.Split("=")[1]
    }
  }
}
```

ローカルコンソールを使用する

次の例では、ローカルコンソールを使用してアクティベーションキーを生成し、表示する方法を示しています。

ローカルコンソールからゲートウェイのアクティベーションキーを取得するには

1. ローカルコンソールにログインします。Windows コンピュータから Amazon EC2 インスタンスに接続する場合は、admin としてログインします。
2. ログイン後に [AWS Appliance Activation - Configuration] メインメニューが表示されたら、`0` を選択して [Get activation key] を選択します。
3. [Storage Gateway for gateway family] オプションを選択します。
4. プロンプトが表示されたら、ゲートウェイをアクティブ化する AWS リージョンを入力します。
5. ネットワークタイプとして 1 [Public] または 2 [VPC endpoint] を入力します。
6. エンドポイントタイプとして 1 [Standard] または 2 [Federal Information Processing Standard (FIPS)] を入力します。

iSCSI イニシエータの接続

ゲートウェイを管理するには、Internet Small Computer System Interface (iSCSI) ターゲットとして公開されているボリュームまたは仮想テープライブラリ (VTL) デバイスを使用します。ボリュームゲートウェイの場合、iSCSI ターゲットはボリュームです。テープゲートウェイの場合、ターゲットは VTL デバイスです。この作業の一部として、これらのターゲットへの接続、iSCSI 設定のカスタマイズ、Red Hat Linux クライアントからの接続、チャレンジハンドシェイク認証プロトコル (CHAP) の設定などのタスクを行います。

トピック

- Windows クライアントからボリュームへの接続
- ボリュームから Linux クライアントへの接続
- iSCSI 設定のカスタマイズ
- iSCSI ターゲットの CHAP 認証の設定

iSCSI 標準は、インターネットプロトコル (IP) ベースのストレージデバイスとクライアントとの間の接続を開始および管理するための IP ベースのストレージネットワーク標準です。iSCSI 接続と関連コンポーネントの説明に使用される用語の定義を以下に示します。

iSCSI イニシエータ

iSCSI ネットワークのクライアントコンポーネント。イニシエータは iSCSI ターゲットにリクエストを送信します。イニシエータはソフトウェアまたはハードウェアで実装できます。Storage Gateway は、ソフトウェアイニシエータのみをサポートします。

iSCSI ターゲット

イニシエータからリクエストを受け取って応答する iSCSI ネットワークのサーバーコンポーネント。各ボリュームは、iSCSI ターゲットとして公開されます。各 iSCSI ターゲットに接続される iSCSI イニシエータは 1 つだけです。

Microsoft iSCSI イニシエータ

クライアントコンピュータ (ゲートウェイに書き込むデータがあるアプリケーションを実行しているコンピュータ) を外部の iSCSI ベースのアレイ (ゲートウェイ) に接続できるようにする、Microsoft Windows コンピュータ上のソフトウェアプログラム。接続は、ホストコンピュータのイーサネットネットワークアダプタカードを使用して行われます。Microsoft iSCSI イニシエータは、Windows Server 2022 の Storage Gateway で検証されています。イニシエータはオペレーティングシステムに組み込まれています。

Red Hat iSCSI イニシエータ

`iscsi-initiator-utils` Resource Package Manager (RPM) パッケージでは、Red Hat Linux 用にソフトウェアで実装されている iSCSI イニシエータを提供されています。このパッケージには、iSCSI プロトコル用のサーバーデーモンが含まれます。

各タイプのゲートウェイを iSCSI デバイスに接続でき、これらの接続は、次に説明するように、カスタマイズできます。

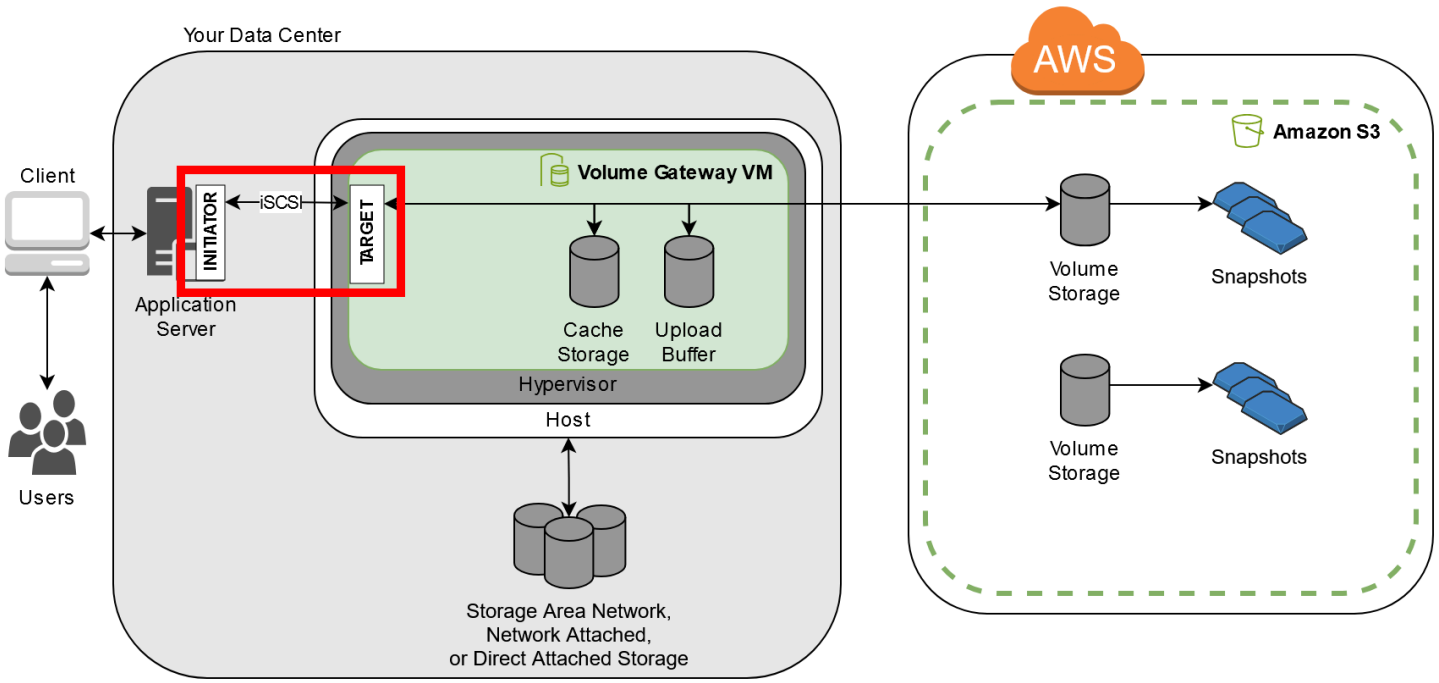
Windows クライアントからボリュームへの接続

ボリュームゲートウェイは、ユーザーがゲートウェイ用に作成したボリュームを iSCSI ターゲットとして公開します。詳細については、「クライアントへのボリュームの接続」を参照してください。

> **Note**
>
> ボリュームターゲットに接続するには、ゲートウェイにアップロードバッファが設定されている必要があります。ゲートウェイにアップロードバッファが設定されていない場合、ボリュームのステータスは UPLOAD BUFFER NOT CONFIGURED と表示されます。保管型ボリュームセットアップでゲートウェイのアップロードバッファを設定するには、「ゲー

トウェイ用のアップロードアップロードバッファまたはキャッシュストレージを追加して設定するには」を参照してください。キャッシュ型ボリュームセットアップでゲートウェイのアップロードバッファを設定するには、「ゲートウェイ用のアップロードアップロードバッファまたはキャッシュストレージを追加して設定するには」を参照してください。

次の図は、Storage Gateway アーキテクチャ全体を示しており、特に iSCSI ターゲットを強調表示しています。詳細については、「ボリュームゲートウェイの仕組み」を参照してください。



ボリュームには、Windows クライアントまたは Red Hat Linux クライアントから接続できます。必要に応じて、どちらかのクライアントタイプに対して CHAP を設定することもできます。

ゲートウェイは、各ボリュームを iSCSI ターゲットとして公開します。指定した名前の先頭には、`iqn.1997-05.com.amazon:` が付けられます。例えば、ターゲット名に `myvolume` を指定した場合、このボリュームとの接続に使用する iSCSI ターゲットは `iqn.1997-05.com.amazon:myvolume` になります。iSCSI 経由でボリュームをマウントするためのアプリケーションの設定方法の詳細については、「Windows クライアントからボリュームへの接続」を参照してください。

To	参照先
Windows からボリュームに接続します。	Microsoft Windows クライアントへの接続

To	参照先
Red Hat Linux からボリュームに接続します。	Red Hat Enterprise Linux クライアントへの接続
Windows および Red Hat Linux 用に CHAP 認証を設定します。	iSCSI ターゲットの CHAP 認証の設定

Windows クライアントをストレージボリュームに接続するには

1. Windows クライアントコンピュータの [Start] (スタート) メニューで、[Search Programs and files] (プログラムとファイルの検索) ボックスに **`iscsicpl.exe`** と入力し、iSCSI イニシエータプログラムを見つけて実行します。

   > **Note**
   >
   > iSCSI イニシエータを実行するには、クライアントコンピュータに対する管理者権限が必要です。

2. プロンプトが表示されたら、[Yes] を選択して、Microsoft iSCSI イニシエータサービスを開始します。
3. [iSCSI Initiator Properties] (iSCSI イニシエータのプロパティ) ダイアログボックスで、[Discovery] (検出) タブを選択して、[Discover Portal] (ポータルの検出) を選択します。
4. [Discover Target Portal] (ターゲットポータルの検索) ダイアログボックスで、[IP address or DNS name]] (IP アドレスまたは DNS 名) に iSCSI ターゲットの IP アドレスを入力し、[OK] をクリックします。ゲートウェイの IP アドレスを取得するには、Storage Gateway コンソールの [Gateway] (ゲートウェイ) タブを確認します。Amazon EC2 インスタンスにゲートウェイをデプロイした場合、パブリック IP アドレスまたは DNS アドレスは、Amazon EC2 コンソールの [Description] (説明) タブに表示されます。

   これで IP アドレスは、[Discovery] タブの [Target portals] のリストに表示されます。

> **Warning**
>
> ゲートウェイが Amazon EC2 インスタンスにデプロイされている場合、パブリックインターネット接続経由でゲートウェイにアクセスすることはできません。Amazon EC2 インスタンスの Elastic IP アドレスは、ターゲットアドレスとして使用できません。

5. ゲートウェイのストレージボリュームターゲットに新しいターゲットポータルを接続します。

   a. [Targets] タブを選択します。

      新しいターゲットポータルが非アクティブのステータスで表示されます。表示されるターゲット名は、ステップ 1 でストレージボリュームに指定した名前と同じになるはずです。

   b. ターゲットを選択し、[Connect] を選択します。

      ターゲット名がまだ入力されていない場合は、ステップ 1 に示すように、ターゲットの名前を入力します。[Connect to Target] (ターゲットに接続) ダイアログボックスで、[Add this connection to the list of Favorite Targets] (この接続をターゲットの「お気に入り」リストに追加) を選択してから、[OK] をクリックします。

   c. [Target] (ターゲット) タブで、ターゲットの [Status] (ステータス) が、ターゲットが接続されていることを示す値 [Connected] (接続済) であることを確認し、[OK] をクリックします。

これで、このストレージボリュームにデータを保存できるように Windows 用に初期化して、フォーマットを実行する準備が整いました。そのためには、Windows Disk Management ツールを使用します。

> **Note**
>
> この演習には必須ではありませんが、「Windows iSCSI 設定のカスタマイズ」トピックで説明しているように、実際のアプリケーション用に iSCSI 設定をカスタマイズすることを強くお勧めします。

ボリュームから Linux クライアントへの接続

Red Hat Enterprise Linux (RHEL) を使用している場合は、`iscsi-initiator-utils` RPM パッケージを使用して、ゲートウェイの iSCSI ターゲット (ボリュームまたは VTL デバイス) に接続します。

Linux クライアントを iSCSI ターゲットに接続するには

1. `iscsi-initiator-utils` RPM パッケージがクライアントにまだインストールされていない場合はインストールします。

   パッケージをインストールするには、以下のコマンドを使用できます。

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

2. iSCSI デーモンが実行していることを確認します。

   a. 次のいずれかのコマンドを使用して、iSCSI デーモンが実行されていることを確認します。

      RHEL 8 または 9 の場合は、次のコマンドを使用します。

      ```
      sudo service iscsid status
      ```

   b. ステータスコマンドが running ステータスを返さない場合は、次のいずれかのコマンドを使用してデーモンを起動します。

      RHEL 8 または 9 の場合は、次のコマンドを使用します。通常、`iscsid`サービスを明示的に開始する必要はありません。

      ```
      sudo service iscsid start
      ```

3. ゲートウェイに対して定義されているボリュームまたは VTL デバイスターゲットを検出するには、次の discovery コマンドを使用します。

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

   前のコマンドの *[GATEWAY_IP]* 変数の値を、実際のゲートウェイの IP アドレスに置き換えます。ゲートウェイ IP は、Storage Gateway コンソール上のボリュームの [iSCSI Target Info] (iSCSI ターゲット情報) プロパティに表示されます。

discovery コマンドの出力は、次の出力例のようになります。

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

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

iSCSI 修飾名 (IQN) は組織ごとに固有であるため、実際の IQN の値は上で示されているものとは異なります。ターゲットの名前は、ボリュームを作成したときに指定した名前です。このターゲット名も、Storage Gateway コンソールでボリュームを選択したときに、[iSCSI Target Info] (iSCSI ターゲット情報) プロパティのペインに表示されます。

4. ターゲットに接続するには、以下のコマンドを使用します。

connect コマンドでは正しい *[GATEWAY_IP]* と IQN を指定する必要があります。

> **Warning**
>
> ゲートウェイが Amazon EC2 インスタンスにデプロイされている場合、パブリックインターネット接続経由でゲートウェイにアクセスすることはできません。Amazon EC2 インスタンスの Elastic IP アドレスは、ターゲットアドレスとして使用できません。

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

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

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

コマンドの出力は、次の出力例のようになります。

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

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

iSCSI 設定のカスタマイズ

イニシエータを設定した後は、イニシエータがターゲットから切断されないように iSCSI の設定をカスタマイズすることを強くお勧めします。

次の手順で示すように、iSCSI タイムアウトの値を増やすと、アプリケーションが、長時間を要する書き込みオペレーションやネットワークの中断などの一時的な問題に適切に対処できるようになります。

> **Note**
>
> レジストリを変更する前に、レジストリのバックアップコピーを作成する必要があります。バックアップコピーの作成と、レジストリの操作時に従うべきその他のベストプラクティスについては、Microsoft TechNet Library の「Registry best practices」を参照してください。

トピック

- Windows iSCSI 設定のカスタマイズ
- Linux iSCSI 設定のカスタマイズ
- ボリュームゲートウェイの Linux ディスクタイムアウト設定のカスタマイズ

Windows iSCSI 設定のカスタマイズ

Windows クライアントを使用するときは、Microsoft iSCSI イニシエータを使用して、ゲートウェイボリュームに接続します。ボリュームに接続する方法については、「クライアントへのボリュームの接続」を参照してください。

Windows iSCSI の設定をカスタマイズするには

1. リクエストをキューに保持する最大時間を長くします。

   a. レジストリエディタ (`Regedit.exe`) を起動します。

   b. 以下で示されている iSCSI コントローラの設定を含むデバイスクラスのグローバル一意識別子 (GUID) に移動します。

> **Warning**
>
> [ControlSet001] や [ControlSet002] などの他のコントロールセットではなく、[CurrentControlSet] サブキーで作業していることを確認します。

```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}
```

c. 以下で [*<Instance Number>*] として示されている Microsoft iSCSI イニシエータのサブキーを 探します。

キーは、`0000` などの 4 桁の数字で表されます。

```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\[<Instance Number]
```

コンピュータにインストールされているものによっては、Microsoft iSCSI イニシエータのサブキーが `0000` ではない場合があります。`DriverDesc` という文字列の値が `Microsoft iSCSI Initiator` であることを確認することによって、正しいサブキーを選択したことを確認できます。

d. [Parameters] サブキーを選択して iSCSI 設定を表示します。

e. [MaxRequestHoldTime] DWORD (32 ビット) 値のコンテキスト (右クリック) メニューを開き、[Modify] (変更) を選択して、値を **`600`** に変更します。

[MaxRequestHoldTime] は、Microsoft iSCSI イニシエータが `Device Removal` イベントの上部レイヤーに通知する前に、未処理のコマンドを保持して再試行する秒数を指定します。この値は、保持時間が 600 秒であることを表します。

2. 以下のパラメータを変更して、iSCSI パケットで送信できるデータの最大量を増やすことができます。

- [FirstBurstLength] は、未承諾書き込みリクエストで送信できるデータの最大量を制御します。この値を **262144**、または Windows OS のデフォルト値のいずれか大きい方に設定します。

- MaxBurstLength は FirstBurstLength に似ていますが、承諾書き込みシーケンスで送信できるデータの最大量を設定します。この値を **1048576**、または Windows OS のデフォルト値のいずれか大きい方に設定します。
- [MaxRecvDataSegmentLength] は、1 つのプロトコルデータユニット (PDU) に関連付けられている最大データセグメントサイズを制御します。この値を **262144**、または Windows OS のデフォルト値のいずれか大きい方に設定します。

> **Note**
>
> さまざまなバックアップソフトウェアをさまざまな iSCSI 設定を使用して最適化できます。これらのパラメータのどの値により最高のパフォーマンスが得られるかを確認するには、バックアップソフトウェアのドキュメントを参照してください。

3. 次に示すように、ディスクタイムアウトの値を大きくします。

   a. レジストリエディタ (`Regedit.exe`) をまだ起動していない場合は、起動します。

   b. 以下に示すように、[CurrentControlSet] の [Services] (サービス) サブキーの中の [Disk] (ディスク) サブキーに移動します。

   ```
   HKEY_Local_Machine\SYSTEM\CurrentControlSet\Services\Disk
   ```

   c. [TimeOutValue] DWORD (32 ビット) 値のコンテキスト (右クリック) メニューを開き、[Modify] (変更) を選択して、値を **600** に変更します。

   [TimeOutValue] は、iSCSI イニシエータが接続を切断して再確立することでセッション回復を試みる前に、ターゲットからの応答を待機する秒数を指定します。この値は、タイムアウト値が 600 秒の期間であることを表します。

4. 新しい設定値を有効にするために、システムを再起動します。

   再起動する前に、ボリュームへのすべての書き込みオペレーションの結果がフラッシュされていることを確認する必要があります。そのためには、再起動の前に、マッピングされたすべてのストレージボリュームのディスクをオフラインにします。

Linux iSCSI 設定のカスタマイズ

イニシエータを設定した後は、イニシエータがターゲットから切断されないように iSCSI の設定をカスタマイズすることを強くお勧めします。次に示すように、iSCSI タイムアウトの値を増やすと、

アプリケーションが、長時間を要する書き込みオペレーションやネットワークの中断などの一時的な問題に適切に対処できるようになります。

> **Note**
>
> コマンドは、Linux のタイプごとにわずかに異なる場合があります。次の例は、Red Hat Linux に基づいています。

Linux iSCSI の設定をカスタマイズするには

1. リクエストをキューに保持する最大時間を長くします。

   a. /etc/iscsi/iscsid.conf ファイルを開き、次の行を探します。

   ```
   node.session.timeo.replacement_timeout = [replacement_timeout_value]
   node.conn[0].timeo.noop_out_interval = [noop_out_interval_value]
   node.conn[0].timeo.noop_out_timeout = [noop_out_timeout_value]
   ```

   b. *[replacement_timeout_value]* の値を **600** に設定します。

   [noop_out_interval_value] の値を **60** に設定します。

   [noop_out_timeout_value] の値を **600** に設定します。

   これら 3 つの値の単位はすべて秒です。

   > **Note**
   >
   > ゲートウェイを検出する前に、iscsid.conf を設定する必要があります。既にゲートウェイを検出している場合や、ターゲットにログインしている場合、またはその両方が該当する場合は、次のコマンドを使用して検出データベースからエントリを削除できます。その後、再検出または再ログインを行って、新しい設定を取得できます。
   >
   > ```
   > iscsiadm -m discoverydb -t sendtargets -p [GATEWAY_IP]:3260 -o delete
   > ```

2. 各レスポンスで送信できるデータ量の最大値を増やします。

a. /etc/iscsi/iscsid.conf ファイルを開き、次の行を探します。

```
node.session.iscsi.FirstBurstLength = [replacement_first_burst_length_value]
node.session.iscsi.MaxBurstLength = [replacement_max_burst_length_value]
node.conn[0].iscsi.MaxRecvDataSegmentLength
 = [replacement_segment_length_value]
```

b. パフォーマンスを向上させるには、以下の値をお勧めします。バックアップソフトウェアは異なる値を使用するように最適化されている場合もあるため、最良の結果を得るにはバックアップソフトウェアのドキュメントを参照してください。

[replacement_first_burst_length_value] の値を **262144**、または Linux OS のデフォルト値のいずれか大きい方に設定します。

[replacement_max_burst_length_value] の値を **1048576**、または Linux OS のデフォルトのいずれか大きい方に設定します。

[replacement_segment_length_value] の値を **262144**、または Linux OS のデフォルト値のいずれか大きい方に設定します。

> **Note**
>
> さまざまなバックアップソフトウェアをさまざまな iSCSI 設定を使用して最適化できます。これらのパラメータのどの値により最高のパフォーマンスが得られるかを確認するには、バックアップソフトウェアのドキュメントを参照してください。

3. システムを再起動して、新しい設定値を有効にします。

再起動する前に、テープへのすべての書き込みオペレーションの結果がフラッシュされていることを確認します。これを行うには、再起動の前に、テープをアンマウントします。

ボリュームゲートウェイの Linux ディスクタイムアウト設定のカスタマイズ

ボリュームゲートウェイを使用している場合は、前のセクションで説明した iSCSI 設定に加えて、次の Linux ディスクタイムアウト設定をカスタマイズできます。

Linux ディスクタイムアウト設定をカスタマイズするには

1. ルールファイルのディスクタイムアウトの値を大きくします。

a. RHEL 5 イニシエータを使用している場合は、/etc/udev/rules.d/50-udev.rules ファイルを開き、次の行を見つけます。

```
ACTION=="add", SUBSYSTEM=="scsi" , SYSFS{type}=="0|7|14", \
RUN+="/bin/sh -c 'echo [timeout] > /sys$$DEVPATH/timeout'"
```

このルールファイルは、RHEL 6 または 7 イニシエータにはないので、次のルールに従って作成する必要があります。

```
ACTION=="add", SUBSYSTEMS=="scsi" , ATTRS{model}=="Storage Gateway",
RUN+="/bin/sh -c 'echo [timeout] > /sys$$DEVPATH/timeout'"
```

RHEL 6 でタイムアウトの値を変更するには、次のコマンドを使用して、上記のコード行を追加します。

```
sudo vim /etc/udev/rules.d/50-udev.rules
```

RHEL 7 でタイムアウトの値を変更するには、次のコマンドを使用して、上記のコード行を追加します。

```
sudo su -c "echo 600 > /sys/block/[device name]/device/timeout"
```

b. *[timeout]* (タイムアウト) の値を **600** に設定します。

この値は、タイムアウト値が 600 秒であることを表します。

2. システムを再起動して、新しい設定値を有効にします。

再起動する前に、ボリュームへのすべての書き込みオペレーションの結果がフラッシュされていることを確認します。そのためには、再起動の前に、ストレージボリュームをアンマウントします。

3. 次のコマンドを使用して設定をテストできます。

```
udevadm test [PATH_TO_ISCSI_DEVICE]
```

このコマンドは、iSCSI デバイスに適用される udev ルールを表示します。

iSCSI ターゲットの CHAP 認証の設定

Storage Gateway は、Challenge-Handshake Authentication Protocol (CHAP) を使用して、ゲートウェイと iSCSI イニシエータの間の認証を行うことができます。CHAP は、ボリュームと VTL デバイスターゲットへのアクセスの認証時に、iSCSI イニシエータのアイデンティティを定期的に確認することにより、プレイバック攻撃から保護します。

> **Note**
>
> CHAP 設定はオプションですが、強くお勧めします。

CHAP を設定するには、Storage Gateway コンソールと、ターゲットへの接続に使用される iSCSI イニシエータソフトウェアの両方で、設定を行う必要があります。Storage Gateway では相互 CHAP が使用され、イニシエータがターゲットを認証するときに、ターゲットもイニシエータを認証します。

ターゲットの相互 CHAP をセットアップするには

1. 「Storage Gateway コンソールでボリュームターゲットに CHAP を設定するには」の説明に従って、Storage Gateway コンソールで CHAP を設定します。
2. クライアントイニシエータソフトウェアで、CHAP の設定を完了します。

   - Windows クライアントで相互 CHAP を設定するには、「Windows クライアントで相互 CHAP を設定するには」を参照してください。
   - Red Hat Linux クライアントで相互 CHAP を設定するには、「Red Hat Linux クライアントで相互 CHAP を設定するには」を参照してください。

Storage Gateway コンソールでボリュームターゲットに CHAP を設定するには

この手順では、ボリュームの読み書きに使用される 2 つのシークレットキーを指定します。同じキーを、クライアントのイニシエータを設定する手順でも使用します。

1. Storage Gateway コンソールのナビゲーションペインで、[Volumes] (ボリューム) を選択します。
2. [Actions (アクション)] メニューで、[Configure CHAP Authentication (CHAP 認証の設定)] を選択します。

3. [Configure CHAP Authentication] (CHAP 認証の設定) ダイアログボックスで要求された情報を入力します。

   a. [Initiator Name] (イニシエータ名) に iSCSI イニシエータの名前を入力します。この名前は Amazon iSCSI 修飾名 (IQN) で、`iqn.1997-05.com.amazon:` が先頭に付加され、ターゲット名が続きます。以下に例を示します。

      `iqn.1997-05.com.amazon:`*`your-volume-name`*

      イニシエータの名前は、iSCSI イニシエータソフトウェアを使用して確認できます。たとえば、Windows クライアントの場合、名前は iSCSI イニシエータの [Configuration] タブの値です。詳細については、「Windows クライアントで相互 CHAP を設定するには」を参照してください。

      > **Note**
      >
      > イニシエータの名前を変更するには、最初に CHAP を無効にし、iSCSI イニシエータソフトウェアでイニシエータの名前を変更した後、新しい名前で CHAP を有効にします。

   b. [Secret used to Authenticate Initiator] (イニシエータ認証に使用するシークレットキー) に、要求されるシークレットキーを入力します。

      このシークレットキーは、12 文字以上、16 文字以下である必要があります。この値は、ターゲットとの CHAP に参加するためにイニシエータ (つまり、Windows クライアント) が知っている必要があるシークレットキーです。

   c. [Secret used to Authenticate Target (Mutual CHAP)] (ターゲット認証に使用するシークレットキー (相互 CHAP)) に、要求されるシークレットキーを入力します。

      このシークレットキーは、12 文字以上、16 文字以下である必要があります。この値は、イニシエータとの CHAP に参加するためにターゲットが認識している必要のあるシークレットキーです。

      > **Note**
      >
      > ターゲットを認証するために使用されるシークレットキーは、イニシエータを認証するためのシークレットキーとは異なるものである必要があります。

   d. [Save] を選択します。

4. [Details] タブを選択し、[iSCSI CHAP Authentication] が [true] に設定されていることを確認します。

Windows クライアントで相互 CHAP を設定するには

この手順では、コンソールでボリュームの CHAP を設定するために使用したキーを使用して、Microsoft iSCSI イニシエータで CHAP を設定します。

1. iSCSI イニシエータがまだ起動されていない場合は、Windows クライアントコンピュータの [Start] (スタート) メニューで [Run] (実行) に「**`iscsicpl.exe`**」と入力し、[OK] をクリックして、プログラムを実行します。
2. イニシエータ (つまり、Windows クライアント) の相互 CHAP を設定します。

   a. [設定] タブを選択します。

   > **Note**
   >
   > [Initiator Name] の値は、イニシエータおよび会社に固有の値です。前に示した名前は、Storage Gateway コンソールの [Configure CHAP Authentication] (CHAP 認証の設定) ダイアログボックスで使用した値です。
   > 例の画像で表示されている名前は、デモンストレーション用です。

   b. [CHAP] を選択します。

   c. [iSCSI Initiator Mutual Chap Secret] (iSCSI イニシエータ相互 CHAP シークレットキー) ダイアログボックスで、相互 CHAP のシークレットキー値を入力します。

      このダイアログボックスには、イニシエータ (Windows クライアント) がターゲット (ストレージボリューム) を認証するために使用するシークレットキーを入力します。このシークレットキーを使用すると、ターゲットはイニシエータに対する読み書きを実行できます。このシークレットキーは、[Configure CHAP Authentication] (CHAP 認証の設定) ダイアログボックス内の [Secret used to Authenticate Target (Mutual CHAP)] (ターゲット認証に使用するシークレットキー (相互 CHAP)) に入力したシークレットキーと同じです。詳細については、「iSCSI ターゲットの CHAP 認証の設定」を参照してください。

   d. 入力したキーが 12 文字に達していない場合、または 16 文字を超えている場合、[Initiator CHAP secret] (イニシエータ CHAP シークレットキー) エラーダイアログボックスが表示されます。

[OK] をクリックし、もう一度キーを入力します。

3. イニシエータのシークレットでターゲットを設定して、相互 CHAP の構成を完了します。

   a. [Targets] タブを選択します。

   b. CHAP の対象として設定するターゲットが現在接続されている場合は、ターゲットを選択してから [Disconnect] をクリックして、ターゲットを切断します。

   c. CHAP の対象として設定するターゲットを選択し、[Connect] を選択します。

   d. [Connect to Target] ダイアログボックスで [Advanced] を選択します。

   e. [Advanced Settings] ダイアログボックスで CHAP を設定します。

      i. [CHAP ログオンを有効にする] を選択します。

      ii. イニシエータを認証するために必要なシークレットキーを入力します。このシークレットキーは、[Configure CHAP Authentication] (CHAP 認証の設定) ダイアログボックス内の [Secret used to Authenticate Initiator] (イニシエータ認証に使用するシークレットキー) に入力したシークレットキーと同じです。詳細については、「iSCSI ターゲットの CHAP 認証の設定」を参照してください。

      iii. [Perform mutual authentication] を選択します。

      iv. [OK] を選択して変更を適用します。

   f. [Connect to Target] ダイアログボックスで [OK] を選択します。

4. 正しいシークレットキーを指定した場合、ターゲットのステータスが [Connected] と表示されます。

Red Hat Linux クライアントで相互 CHAP を設定するには

この手順では、Storage Gateway コンソールでボリュームの CHAP を設定するために使用したものと同じキーを使用して、Linux iSCSI イニシエータで CHAP を設定します。

1. iSCSI デーモンが実行されていて、ターゲットに既に接続されていることを確認してください。これら 2 つのタスクを完了していない場合は、「Red Hat Enterprise Linux クライアントへの接続」を参照してください。

2. CHAP を設定するターゲットを切断し、既存の設定を削除します。

   a. ターゲット名を検索し、定義済みの設定であることを確認するには、次のコマンドを使用して、保存されている設定の一覧を表示します。

```
sudo /sbin/iscsiadm --mode node
```

b. ターゲットから切断します。

次のコマンドは、Amazon iSCSI 修飾名 (IQN) で定義されている **myvolume** という名前のターゲットから切断します。必要に応じて、ターゲットの名前と IQN を変更します。

```
sudo /sbin/iscsiadm --mode node --logout GATEWAY_IP:3260,1
 iqn.1997-05.com.amazon:myvolume
```

c. ターゲットの設定を削除します。

次のコマンドは、**myvolume** ターゲットに対する設定を削除します。

```
sudo /sbin/iscsiadm --mode node --op delete --targetname
 iqn.1997-05.com.amazon:myvolume
```

3. iSCSI 設定ファイルを編集して、CHAP を有効にします。

a. イニシエータ (つまり、使用しているクライアント) の名前を取得します。

次のコマンドは、/etc/iscsi/initiatorname.iscsi ファイルからイニシエータの名前を取得します。

```
sudo cat /etc/iscsi/initiatorname.iscsi
```

このコマンドの出力は次のようになります。

```
InitiatorName=iqn.1994-05.com.redhat:8e89b27b5b8
```

b. /etc/iscsi/iscsid.conf ファイルを開きます。

c. ファイルで以下の行のコメントを解除し、*username*、*password*、*username_in*、および *password_in* の正しい値を指定します。

```
node.session.auth.authmethod = CHAP
node.session.auth.username = username
node.session.auth.password = password
node.session.auth.username_in = username_in
node.session.auth.password_in = password_in
```

指定する値の説明については、次の表を参照してください。

構成設定	値
username	この手順の前のステップで検出したイニシエータ名です。この値は、iqn で始まります。たとえば、**iqn.1994-05.com.redhat:8e89b27b5b8** は有効な *username* 値です。
password	イニシエータ (使用しているクライアント) がボリュームと通信するときにイニシエータを認証するために使用されるシークレットキー。
username_in	ターゲットボリュームの IQN。この値は、iqn で始まり、ターゲット名で終わります。たとえば、**iqn.1997-05.com.amazon:myvolume** は有効な *username_in* 値です。
password_in	ターゲット (ボリューム) がイニシエータと通信するときにターゲットを認証するために使用されるシークレットキー。

d. 設定ファイルの変更を保存して、ファイルを閉じます。

4. ターゲットを検出して、ログインします。そのためには、「Red Hat Enterprise Linux クライアントへの接続」の手順に従ってください。

Storage Gateway AWS Direct Connect での の使用

AWS Direct Connect は、内部ネットワークを Amazon Web Services クラウドにリンクします。Storage Gateway AWS Direct Connect で を使用すると、高スループットのワークロードのニーズに合わせた接続を作成し、オンプレミスゲートウェイと 間の専用ネットワーク接続を提供できます AWS。

Storage Gateway ではパブリックエンドポイントを使用します。 AWS Direct Connect 接続を使用すると、パブリック仮想インターフェイスを作成して、トラフィックを Storage Gateway エンドポイントにルーティングできます。パブリック仮想インターフェイスは、お客様のネットワークパスの中でインターネットサービスプロバイダーをバイパスします。Storage Gateway サービスのパブリッ

クエンドポイントは、場所と同じ AWS リージョン AWS Direct Connect にあることも、別の AWS リージョンにあることもできます。

次の図は、 が Storage Gateway と AWS Direct Connect 連携する方法の例を示しています。
AWS 直接接続を使用してクラウドに接続された Storage Gateway を示すネットワークアーキテクチャ。

次の手順では、機能するゲートウェイを作成済みであることを前提としています。

Storage Gateway AWS Direct Connect で を使用するには

1. オンプレミスデータセンターと Storage Gateway エンドポイント間の AWS Direct Connect 接続を作成して確立します。接続の作成方法の詳細については、AWS Direct Connect ユーザーガイドの「使用の開始 AWS Direct Connect」を参照してください。
2. オンプレミスの Storage Gateway アプライアンスを AWS Direct Connect ルーターに接続します。
3. パブリック仮想インターフェイスを作成し、それに応じてオンプレミスのルーターを設定します。Direct Connect を使用する場合でも、VPC エンドポイントは HAProxy で作成する必要があります。詳細については、AWS Direct Connect ユーザーガイドの「仮想インターフェイスを作成する」を参照してください。

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

ゲートウェイアプライアンスの IP アドレスの取得

ホストを選択してゲートウェイ VM をデプロイしたら、ゲートウェイを接続してアクティブ化します。これを行うには、ゲートウェイ VM の IP アドレスが必要です。ゲートウェイのローカルコンソールから IP アドレスを取得します。ローカルコンソールにログインし、コンソールページの先頭から IP アドレスを取得します。

オンプレミスでデプロイされているゲートウェイでは、ハイパーバイザーでも IP アドレスを取得できます。Amazon EC2 ゲートウェイでは、Amazon EC2 マネジメントコンソールから Amazon EC2 インスタンスの IP アドレスを取得することもできます。ゲートウェイの IP アドレスを見つける方法については、次の 1 つを参照してください。

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

- Linux カーネルベースの仮想マシン (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 のホストから IP アドレスを取得する

IP アドレスが見つかったら、それを書き留めます。Storage Gateway コンソールに戻り、コンソールで IP アドレスを入力します。

Amazon EC2 のホストから IP アドレスを取得する

ゲートウェイをデプロイする Amazon EC2 インスタンスの IP アドレスを取得するには、EC2 インスタンスのローカルコンソールにログインします。コンソールページの先頭から IP アドレスを取得します。手順については、Amazon EC2 ゲートウェイのローカルコンソールへのログイン を参照してください。

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 のリソースとリソース ID の説明

Storage Gateway では、プライマリリソースはゲートウェイですが、他の種類のリソースとして、ボリューム、仮想テープ、iSCSI ターゲット、vtl デバイスなどもあります。これらは、サブリソースと呼ばれ、ゲートウェイに関連付けられている場合にのみ存在します。

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`*
ボリューム ARN	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`* `/volume/`*`volume-id`*
ターゲット ARN (iSCSI ターゲット)	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`* `/target/`*`iSCSItarget`*

また、Storage Gateway は EC2 インスタンスと EBS ボリュームの使用とスナップショットをサポートしています。これらのリソースは Storage Gateway で使用される Amazon EC2 リソースです。

リソース 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 のリソース ID は大文字です。ただし、Amazon EC2 API でこれらのリソース ID を使用する場合、Amazon EC2 には小文字のリソース ID が必要です。リソース ID を EC2 API で使用するには、小文字に変更する必要があります。たとえば、ボリュームの ID が Storage Gateway では `vol-1122AABB` であるとします。この ID を EC2 API で使用するには、`vol-1122aabb` に変更する必要があります。これを行わなければ、EC2 API が正常に動作しない場合があります。

Storage Gateway リソースのタグ付け

Storage Gateway では、タグを使用してリソースを管理できます。タグを付けることにより、メタデータをリソースに追加し、リソースを簡単に管理できるように分類できます。タグはそれぞれ、ユーザー定義の 1 つのキーと 1 つの値で構成されています。タグはゲートウェイ、ボリューム、および仮想テープに追加できます。追加したタグに基づいて、これらのリソースを検索したりフィルタリングしたりできます。

例えば、組織内の各部門が使用する Storage Gateway リソースを識別するためにタグを使用できます。経理部が使用するゲートウェイとボリュームには、`key=department`、`value=accounting` のようにタグを付けます。このタグでフィルタリングを実行して、経理部が使用するすべてのゲートウェイとボリュームを特定し、この情報を使用してコストを確認できます。詳細については、「コスト配分タグの使用」と「Tag Editor の使用」を参照してください。

タグが付いている仮想テープをアーカイブしても、そのテープのタグはアーカイブで維持されます。同様に、そのテープをアーカイブから別のゲートウェイで取得しても、そのタグは新しいゲートウェイで維持されます。

タグには意味論的意味はなく、タグは文字列として解釈されます。

タグには以下の制限があります。

- タグのキーと値は大文字と小文字が区別されます。
- 1 つのリソースに付けることができるタグの最大数は 50 です。
- タグキーを aws: で始めることはできません。このプレフィックスは AWS 専用として予約されています。
- キープロパティに使用できる文字は、UTF-8 文字および数字、スペース、特殊文字 +、-、=、.、:、/、@ です。

タグの操作

Storage Gateway コンソール、Storage Gateway API、または Storage Gateway コマンドラインインターフェイス (CLI) を使用して、タグを使用した作業ができます。以下の手順は、コンソールでタグを追加する方法、編集する方法、および削除する方法を示しています。

タグを追加するには

1. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. ナビゲーションペインで、タグを付けるリソースを選択します。

   たとえば、ゲートウェイにタグを付ける場合は、[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. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. タグを編集するリソースを選択します。
3. [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. Storage Gateway コンソール (https://console.aws.amazon.com/storagegateway/home) を開きます。
2. タグを削除するリソースを選択します。
3. [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。

Storage Gateway のオープンソースコンポーネントの使用

このセクションでは、Storage Gateway の機能を提供するために活用しているサードパーティ製のツールとライセンスについて説明します。

AWS Storage Gateway ソフトウェアに含まれている、特定のオープンソースソフトウェアコンポーネントのソースコードは、以下の場所からダウンロードできます。

- VMware ESXi にデプロイされたゲートウェイの場合は、sources.tar をダウンロードします。
- Microsoft Hyper-V にデプロイされたゲートウェイの場合は、sources_hyperv.tar をダウンロードします。
- Linux Kernel ベースの仮想マシン (KVM) にデプロイされたゲートウェイの場合は、sources_KVM.tar をダウンロードします。

この製品には、OpenSSL ツールキット (http://www.openssl.org/) での使用を前提に OpenSSL プロジェクトにより開発されたソフトウェアが含まれています。依存するすべてのサードパーティー製ツールの関連ライセンスについては、サードパーティーのライセンスを参照してください。

AWS Storage Gateway クォータ

このトピックでは、Storage Gateway のボリュームとテープのクォータ、設定、およびパフォーマンスの制限について説明します。

トピック

- ボリュームのクォータ
- ゲートウェイのローカルディスクの推奨サイズ

ボリュームのクォータ

次の表は、ボリュームのクォータの一覧です。

説明	キャッシュボリューム	保管型ボリューム
ボリュームの最大サイズ **Note** サイズが 16 TiB より大きいキャッシュ型ボリュームからスナップショットを作成する場合、それを Storage Gateway ボリュームに復元することはできますが、Amazon Elastic Block Store (Amazon EBS) ボリュームに復元することはできません。	32 TiB	16 TiB
ゲートウェイあたりの最大ボリューム数	32	32
ゲートウェイのすべてのボリュームの合計サイズ	1,024 TiB	512 TiB

ゲートウェイのローカルディスクの推奨サイズ

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

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

> **Note**
>
> キャッシュおよびアップロードバッファ用として、1 つ以上のローカルドライブを、最大容量まで構成することができます。
> 既存のゲートウェイにキャッシュやアップロードバッファを追加する場合、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やアップロードバッファとして割り当て済みである場合は、既存のディスクサイズを変更しないでください。

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ムで設定および管理できます。このセクションでは、 AWS Storage Gateway オペレーション、認証のリクエスト署名、エラー処理について説明します。Storage Gateway で利用できるリージョンとエンドポイントの詳細については、「AWS 全般のリファレンス」の「AWS Storage Gateway エンドポイントとクォータ」を参照してください。

> **Note**
>
> でアプリケーションを開発するときに、 AWS SDKs を使用することもできます AWS Storage Gateway。 AWS SDKs for Java、.NET、および PHP は、基盤となる AWS Storage Gateway API をラップし、プログラミングタスクを簡素化します。SDK ライブラリのダウンロードについては、「サンプルコードライブラリ」を参照してください。

トピック

- Storage Gateway の必須リクエストヘッダー
- リクエストへの署名
- エラーレスポンス
- アクション

Storage Gateway の必須リクエストヘッダー

このセクションでは、Storage Gateway に対するすべての 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。HTTP ヘッダーでは、呼び出すオペレーション、リクエストの日付、リクエストの送信者として認可されていることを示す情報など、リクエストに関する重要な情報を特定します。ヘッダーは大文字と小文字を区別されず、ヘッダーの順序は重要ではありません。

次の例では、ActivateGateway オペレーションで使用されるヘッダーを示します。

```
POST / HTTP/1.1
```

```
Host: storagegateway.us-east-2.amazonaws.com
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120425/us-east-2/
storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target,
 Signature=9cd5a3584d1d67d57e61f120f35102d6b3649066abdd4bf4bbcf05bd9f2f8fe2
x-amz-date: 20120912T120000Z
x-amz-target: StorageGateway_20120630.ActivateGateway
```

以下に、Storage Gateway への POST リクエストに含めることが必須の各ヘッダーを示します。以下に示す「x-amz」で始まるヘッダーは AWS、固有のヘッダーです。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`	Authorization ヘッダーには、リクエストがリクエスタに対して有効なアクションかどうかを Storage Gateway が判別するための、リクエストに関するいくつかの情報が含まれています。このヘッダーの形式は次のとおりです (改行は読みやすくするために追加されています)。 `Authorization: AWS4-HMAC_SHA456 Credentials= YourAccessKey /yyymmdd/region/storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target, Signature= CalculatedSignature` この構文では、YourAccessKey、年、月、日 (yyyymmdd)、リージョン、および CalculatedSignature が指定されています。認可ヘッダーの形式は、 AWS V4 署名プロセスの要件によって指定されています。署名の詳細については、トピック リクエストへの署名 を参照してください。
`Content-Type`	Storage Gateway に対するすべてのリクエストでは、コンテンツタイプとして `application/x-amz-json-1.1` を使用します。 `Content-Type: application/x-amz-json-1.1`

ヘッダー	説明
Host	ホストヘッダーは、リクエストを送信する Storage Gateway エンドポイントを指定するために使用します。例えば storagegateway.us-east-2.amazonaws.com は、米国東部 (オハイオ) リージョンのエンドポイントを表します。Storage Gateway で利用できるエンドポイントの詳細については、「AWS 全般のリファレンス」の「AWS Storage Gateway エンドポイントとクォータ」を参照してください。 `Host: storagegateway. region.amazonaws.com`
x-amz-date	タイムスタンプは HTTP Dateヘッダーまたは AWS x-amz-date ヘッダーで指定する必要があります。(一部の HTTP クライアントライブラリでは、Date ヘッダーを設定することができません)。x-amz-date ヘッダーがある場合には、そのリクエストの認証時に Storage Gateway により Date ヘッダーが無視されます。x-amz-date の形式は、ISO8601 Basic の YYYYMMDD'T'HHMMSS'Z' 形式でなければなりません。Date ヘッダーと x-amz-date ヘッダーの両方を使用する場合は、Date ヘッダーの形式は ISO8601 でなくてもかまいません。 `x-amz-date: YYYYMMDD'T'HHMMSS'Z'`
x-amz-target	このヘッダーでは、API のバージョンおよびリクエストするオペレーションを指定します。ターゲットヘッダーの値を作成するには、API のバージョンと API の名前を次のような形式で連結します。 `x-amz-target: StorageGateway_ APIversion .operationName` operationName 値 (例: ActivateGateway) は、API リスト (Storage Gateway の API リファレンス) で確認できます。

リクエストへの署名

Storage Gateway では、リクエストに署名することで、送信するすべてのリクエストを認証する必要があります。リクエストに署名するには、暗号化ハッシュ関数を使用してデジタル署名を計算します。暗号化ハッシュは、入力データから一意のハッシュ値生成して返す関数です。ハッシュ関数に渡される入力データとしては、リクエストのテキスト、およびシークレットアクセスキーが該当します。ハッシュ関数から返されるハッシュ値をリクエストに署名として含めます。署名は、リクエストの `Authorization` ヘッダーの一部です。

Storage Gateway は、受け取ったリクエストに対して、その署名に使用されたものと同じハッシュ関数と入力を使用して署名を再計算します。再計算された署名とリクエスト内の署名が一致した場合、Storage Gateway はそのリクエストを処理します。それ以外の場合、リクエストは拒否されます。

Storage Gateway は、AWS 署名バージョン 4 を使用した認証をサポートしています。署名の計算プロセスは 3 つのタスクに分けることができます。

- タスク 1: 正規リクエストを作成する

  HTTP リクエストを正規形式に変換します。Storage Gateway は、送信された署名と比較するための再計算に正規化形式を使用するので、署名には正規化形式の使用が必須です。

- タスク 2: 署名対象の文字列を作成する

  暗号化ハッシュ関数への入力値の 1 つとして使用する文字列を作成します。署名文字列と呼ばれる文字列は、ハッシュアルゴリズムの名前、要求日付、認証情報スコープの文字列、および前のタスクで正規化されたリクエストを結合したものです。認証情報スコープの文字列自体は、日付、リージョン、およびサービス情報を結合したものです。

- タスク 3: 署名を作成する

  2 つの入力文字列 (署名文字列と派生キー) を受け付ける暗号化ハッシュ関数を使用して、リクエストの署名を作成します。シークレットアクセスキーから開始し、認証情報スコープの文字列を使用して一連のハッシュベースのメッセージ認証コード (HMAC) を作成することで、派生キーが計算されます。

署名の計算例

次の例で、ListGateways の署名を作成する詳細な手順を示します。実際の署名計算方法を確認するときに、この例を参考にしてください。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 (あるいは任意の Storage Gateway API)に、クエリパラメータがないためです。

タスク 2: 署名対象の文字列を作成する のための 署名用の文字列は次のとおりです。

```
AWS4-HMAC-SHA256
20120910T000000Z
20120910/us-east-2/storagegateway/aws4_request
92c0effa6f9224ac752ca179a04cecbede3038b0959666a8160ab452c9e51b3e
```

署名する文字列の最初の行はアルゴリズム、2 行目はタイムスタンプ、3 行目は認証情報スコープ、最後の行はタスク 1 で作成した正規リクエストのハッシュです。

タスク 3: 署名を作成する の場合、派生キーは、次のように表すことができます。

```
derived key = HMAC(HMAC(HMAC(HMAC("AWS4" + YourSecretAccessKey,"20120910"),"us-
east-2"),"storagegateway"),"aws4_request")
```

シークレットアクセスキー wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY を使用する場合、計算された署名は次のようになります。

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

最後のステップは、Authorization ヘッダーの構築です。デモンストレーションのアクセスキー AKIAIOSFODNN7EXAMPLE の場合、ヘッダーは次のとおりです (読みやすいように改行しています)。

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120910/us-east-2/
storagegateway/aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

エラーレスポンス

トピック

- 例外
- オペレーションエラーコード
- エラーレスポンス

このセクションでは、 AWS Storage Gateway エラーに関するリファレンス情報を提供します。これらのエラーは、エラー例外とオペレーションエラーコードを表しています。例えば、エラー

例外 InvalidSignatureException は、リクエスト署名に問題がある場合に、API レスポンスによって返されます。ただし、オペレーションエラーコード ActivationKeyInvalid は、ActivateGateway API に対してのみ返されます。

エラーの種類に応じて、Storage Gateway は例外だけを返すことも、例外とオペレーションエラーコードの両方を返すこともあります。エラーレスポンスの例を エラーレスポンス に示します。

例外

次の表に、 AWS Storage Gateway API の例外を示します。 AWS Storage Gateway オペレーションがエラーレスポンスを返すと、レスポンス本文にはこれらの例外のいずれかが含まれます。InternalServerError と InvalidGatewayRequestException は、特定のオペレーションエラーコードを表示するオペレーションエラーコード オペレーションエラーコード メッセージの 1 つを返します。

Exception	メッセージ	HTTP ステータスコード
IncompleteSignatureException	指定された署名は不完全です。	400 Bad Request
InternalFailure	リクエストの処理は、不明なエラー、例外、または失敗により実行できませんでした。	500 Internal Server Error
InternalServerError	オペレーションエラーコード のオペレーションエラーコードメッセージの 1 つ。	500 Internal Server Error
InvalidAction	要求されたアクション、またはオペレーションは無効です。	400 Bad Request
InvalidClientTokenId	指定された X.509 証明書または AWS アクセスキー ID がレコードに存在しません。	403 Forbidden
InvalidGatewayRequestException	オペレーションエラーコード のオペレーションエラーコードメッセージの 1 つ。	400 Bad Request

Exception	メッセージ	HTTP ステータスコード
InvalidSignatureException	計算したリクエスト署名が、指定された署名と一致しません。 AWS アクセスキーと署名方法を確認します。	400 Bad Request
MissingAction	リクエストに、アクションまたはオペレーションのパラメータが含まれていません。	400 Bad Request
MissingAuthenticationToken	リクエストには、有効な (登録された) AWS アクセスキー ID または X.509 証明書が含まれている必要があります。	403 Forbidden
RequestExpired	リクエストの有効時間、またはリクエスト時間が過ぎています (どちらも 15 分間のパディング)。もしくは、リクエスト時間の発生が 15 分以上先です。	400 Bad Request
SerializationException	シリアル化の実行中にエラーが発生しました。JSON ペイロードが正しく形成されていることを確認してください。	400 Bad Request
ServiceUnavailable	サーバーの一時的な障害により、リクエストは失敗しました。	503 Service Unavailable
SubscriptionRequiredException	AWS アクセスキー ID には、サービスのサブスクリプションが必要です。	400 Bad Request
ThrottlingException	速度を超過しました。	400 Bad Request
TooManyRequests	Too many requests。	429 Too Many Requests

Exception	メッセージ	HTTP ステータスコード
`UnknownOperationException`	不明のオペレーションが指定されました。有効なオペレーションの一覧を Storage Gateway のオペレーション に示します。	400 Bad Request
`UnrecognizedClientException`	リクエストに含まれているセキュリティトークンが無効です。	400 Bad Request
`ValidationException`	入力パラメータの値が正しくないか、範囲外です。	400 Bad Request

オペレーションエラーコード

次の表は、 AWS Storage Gateway オペレーションエラーコードとAPIs 間のマッピングを示しています。すべてのオペレーションエラーコードは、例外 で説明しているとおりに、2 つの一般的な例外 (`InternalServerError` もしくは `InvalidGatewayRequestException`) のいずれかと同時に返されます。

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
`ActivationKeyExpired`	指定されたアクティベーションキーの有効期限が切れました。	ActivateGateway
`ActivationKeyInvalid`	指定されたアクティベーションキーは無効です。	ActivateGateway
`ActivationKeyNotFound`	指定されたアクティベーションキーは見つかりませんでした。	ActivateGateway

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
BandwidthThrottleScheduleNotFound	指定された帯域幅スロットルは見つかりませんでした。	DeleteBandwidthRateLimit
CannotExportSnapshot	指定されたスナップショットはエクスポートできません。	CreateCachediSCSIVolume CreateStorediSCSIVolume
InitiatorNotFound	指定されたイニシエータは見つかりませんでした。	DeleteChapCredentials
DiskAlreadyAllocated	指定されたディスクは、既に割り当てられています。	AddCache AddUploadBuffer AddWorkingStorage 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

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
DiskSizeLessThanVolumeSize	指定されたディスクサイズは、ボリュームサイズ未満です。	CreateStorediSCSIVolume
DuplicateCertificateInfo	指定された証明書情報が重複しています。	ActivateGateway

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
GatewayInternalError	ゲートウェイ内部エラーが発生しました。	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
GatewayNotConnected	指定されたゲートウェイは、接続されていません。	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
GatewayNotFound	指定されたゲートウェイは、見つかりませんでした。	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
		ListLocalDisks ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
GatewayProxyNetworkConnectionBusy	指定されたゲートウェイプロキシネットワーク接続はビジーです。	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
InternalError	内部エラーが発生しました。	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
InvalidParameters	指定されたリクエストに不正なパラメータが含まれています。	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
LocalStorageLimitExceeded	ローカルストレージの上限を超えました。	AddCache AddUploadBuffer AddWorkingStorage
LunInvalid	指定された LUN が正しくありません。	CreateStorediSCSIVolume

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
MaximumVolumeCountExceeded	最大ボリューム数を超えました。	CreateCachediSCSIVolume CreateStorediSCSIVolume DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes
NetworkConfigurationChanged	ゲートウェイのネットワーク構成が変更されました。	CreateCachediSCSIVolume CreateStorediSCSIVolume

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
NotSupported	指定されたオペレーションは、サポートされていません。	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
OutdatedGateway	指定されたゲートウェイは、最新のものではありません。	ActivateGateway
SnapshotInProgressException	指定されたスナップショットは処理中です。	DeleteVolume
SnapshotIdInvalid	指定されたスナップショットは無効です。	CreateCachediSCSIVolume CreateStorediSCSIVolume

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
StagingAreaFull	ステージングエリアが満杯です。	CreateCachediSCSIVolume CreateStorediSCSIVolume
TargetAlreadyExists	指定されたターゲットは、既に存在しています。	CreateCachediSCSIVolume CreateStorediSCSIVolume
TargetInvalid	指定されたターゲットは無効です。	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials UpdateChapCredentials
TargetNotFound	指定されたターゲットは、見つかりませんでした。	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials DeleteVolume UpdateChapCredentials

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
UnsupportedOperationForGatewayType	指定されたオペレーションは、ゲートウェイタイプに対して有効ではありません。	AddCache AddWorkingStorage CreateCachediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteSnapshotSchedule DescribeCache DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes DescribeUploadBuffer DescribeWorkingStorage ListVolumeRecoveryPoints
VolumeAlreadyExists	指定されたボリュームは、既に存在しています。	CreateCachediSCSIVolume CreateStorediSCSIVolume
VolumeIdInvalid	指定されたボリュームは無効です。	DeleteVolume
VolumeInUse	指定されたボリュームは、既に使われています。	DeleteVolume

オペレーションエラーコード	メッセージ	このエラーコードを返すオペレーション
VolumeNotFound	指定されたボリュームは、見つかりませんでした。	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint DeleteVolume DescribeCachediSCSIVolumes DescribeSnapshotSchedule DescribeStorediSCSIVolumes UpdateSnapshotSchedule
VolumeNotReady	指定されたボリュームは、準備できていません。	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint

エラーレスポンス

エラーが発生した場合、レスポンスヘッダー情報には、以下の項目が含まれています。

- 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。

型: 文字列

error

API 固有のエラー詳細が含まれています。特定の API に固有ではない一般的なエラーの場合、このようなエラー情報は表示されません。

タイプ: コレクション

errorCode

オペレーションエラーコードの 1 つ。

型: 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。

型: 文字列

メッセージ

オペレーションエラーコードメッセージの 1 つ 。

型: 文字列

エラーレスポンスの例

DescribeStorediSCSIVolumes API を使用して、存在しないゲートウェイ ARN リクエスト入力を指定した場合、次の JSON 本文が返されます。

```
{
  "__type": "InvalidGatewayRequestException",
  "message": "The specified volume was not found.",
  "error": {
```

```
    "errorCode": "VolumeNotFound"
  }
}
```

Storage Gateway が計算した署名が、リクエストと一緒に送信された署名と一致しない場合、次の JSON 本文が返されます。

```
{
  "__type": "InvalidSignatureException",
  "message": "The request signature we calculated does not match the signature you
 provided."
}
```

Storage Gateway のオペレーション

Storage Gateway オペレーションのリストについては、 AWS Storage Gateway API リファレンスの「Actions」を参照してください。

「ボリュームゲートウェイユーザーガイド」のドキュメント履歴

- API バージョン: 2013-06-30
- ドキュメントの最新更新日: 2020 年 11 月 24 日

次の表に、2018 年 4 月以降の AWS Storage Gateway ユーザーガイドの各リリースにおける重要な変更点を示します。このドキュメントの更新に関する通知を受け取るには、RSS フィードにサブスクライブできます。

変更	説明	日付
FSx File Gateway の可用性変更の通知	新規のお客様への Amazon FSx File Gateway の提供は終了しました。FSx File Gateway の既存のお客様は、通常どおりサービスを引き続き使用できます。FSx File Gateway に似た機能については、このブログ記事を参照してください。	2024 年 10 月 28 日
FSx File Gateway の可用性変更の通知	AWS Storage Gatewayの FSx File Gateway は、2024 年 10 月 28日以降、新しいお客様は利用できなくなります。サービスを使用するには、その日より前にサインアップする必要があります。FSx File Gateway の既存のお客様は、通常どおりサービスを引き続き使用できます。FSx File Gateway に似た機能については、このブログ記事を参照してください。	2024 年 9 月 26 日

メンテナンスの更新をオンまたはオフにするオプションを追加	Storage Gateway は、オペレーティングシステムとソフトウェアのアップグレード、安定性、パフォーマンス、セキュリティに対処するための修正、新機能へのアクセスなどを含む定期的なメンテナンスの更新を受け取ります。デプロイ内の個々のゲートウェイごとにこれらの更新をオンまたはオフにするように設定を構成できるようになりました。詳細については、「AWS Storage Gateway コンソールを使用したゲートウェイの更新の管理」を参照してください。	2024 年 6 月 6 日
Snowball Edge でのテープゲートウェイのサポートを廃止	Snowball Edge デバイスでテープゲートウェイをホストすることはできなくなりました。	2024 年 3 月 14 日
サードパーティ製アプリケーションを使用してゲートウェイの設定をテストする手順を更新	サードパーティ製アプリケーションを使用してゲートウェイの設定をテストする手順で、バックアップジョブの進行中にゲートウェイが再起動した場合に想定される動作についての説明が追記されました。詳細については、「」を参照してください。	2023 年 10 月 24 日

CloudWatch の推奨アラームを更新	CloudWatch HealthNotifications アラームが、すべてのゲートウェイタイプとホストプラットフォームに適用されるようになり、これらすべてに対して推奨されるようになりました。HealthNotifications および AvailabilityNotifications の推奨構成設定も更新されました。詳細については、「CloudWatch アラームの説明」を参照してください。	2023 年 10 月 2 日
テープゲートウェイとボリュームゲートウェイのユーザーガイドを分離	以前は「Storage Gateway ユーザーガイド」にテープゲートウェイとボリュームゲートウェイの両方のタイプの情報を記載していましたが、「テープゲートウェイユーザーガイド」と「ボリュームゲートウェイユーザーガイド」に分割し、それぞれに該当タイプのゲートウェイに関する情報のみを記載するようにしました。詳細については、「テープゲートウェイユーザーガイド」と「ボリュームゲートウェイユーザーガイド」を参照してください。	2022 年 3 月 23 日

ゲートウェイの作成手順を更新	Storage Gateway コンソールを使用してゲートウェイを作成する手順が、すべてのゲートウェイタイプについて更新されました。詳細については、「ゲートウェイを作成する」を参照してください。	2022 年 1 月 18 日
テープのインターフェイスが新しくなりました	AWS Storage Gateway コンソールのテープの概要ページが、新しい検索およびフィルタリング機能で更新されました。新機能について説明するため、このガイドに記載されている関連するすべての手順が更新されました。詳細については、「Managing Your Tape Gateway」を参照してください。	2021 年 9 月 23 日
テープゲートウェイによる Quest NetVault Backup 13 のサポート	テープゲートウェイが、Microsoft Windows Server 2012 R2 または Microsoft Windows Server 2016 で実行されている Quest NetVault Backup 13 をサポートするようになりました。詳細については、「Quest NetVault Backup を使用したセットアップのテスト」を参照してください。	2021 年 8 月 22 日

テープゲートウェイおよびボリュームゲートウェイのガイドから S3 ファイルゲートウェイのトピックが削除されました	テープゲートウェイおよびボリュームゲートウェイのユーザーガイドでは、ゲートウェイの種類を個別に設定するお客様にとってわかりやすくなるよう、不要なトピックがいくつか削除されました。	2021 年 7 月 21 日
テープゲートウェイによる Windows および Linux での IBM Spectrum Protect 8.1.10 のサポート	テープゲートウェイが、Microsoft Windows Server および Linux で実行されている IBM Spectrum Protect バージョン 8.1.10 をサポートするようになりました。詳細については、「Testing Your Setup by Using IBM Spectrum Protect」を参照してください。	2020 年 11 月 24 日
FedRAMP コンプライアンス	Storage Gateway が FedRAMP に準拠するようになりました。詳細については、「Compliance validation for Storage Gateway」を参照してください。	2020 年 11 月 24 日
スケジュールベースの帯域幅のスロットリング	Storage Gateway のテープゲートウェイとボリュームゲートウェイで、スケジュールベースの帯域幅のスロットリングがサポートされるようになりました。詳細については、「Storage Gateway コンソールを使用した帯域幅スロットリングのスケジューリング」を参照してください。	2020 年 11 月 9 日

キャッシュ型ボリュームおよびテープゲートウェイのローカルキャッシュストレージが 4 倍増加	Storage Gateway のキャッシュ型ボリュームおよびテープゲートウェイで、最大 64 TB のローカルキャッシュがサポートされるようになりました。より大きな作業データセットへの低レイテンシーアクセスが実現するため、オンプレミスアプリケーションのパフォーマンスが向上します。詳細については、「ゲートウェイのローカルディスクの推奨サイズ」を参照してください。	2020 年 11 月 9 日
ゲートウェイの移行	Storage Gateway で、キャッシュ型のボリュームゲートウェイを新しい仮想マシンに移行できるようになりました。詳細については、「Moving Cached Volumes to a New Cached Volume Gateway Virtual Machine」を参照してください。	2020 年 9 月 10 日

テープ保持ロックと Write-Once-Read-Many (WORM) のテープ保護のサポート	Storage Gateway で、仮想テープでのテープ保持ロックおよび write once read many (WORM) がサポートされるようになりました。テープ保持ロックを使用すると、アーカイブされた仮想テープの保持モードと期間を指定できます。これにより、一定期間 (最大 100 年間)、削除されるのを防ぐことができます。これには、テープの削除や保存設定の変更が可能なユーザーに関するアクセス許可のコントロールが含まれます。詳細については、「Using Tape Retention Lock」を参照してください。WORM を有効にした仮想テープでは、仮想テープライブラリ内のアクティブなテープのデータに対する上書きや消去を防止できます。詳細については、「Write Once, Read Many (WORM) Tape Protection」を参照してください。	2020 年 8 月 19 日
コンソールを使用したハードウェアアプライアンスの注文	AWS Storage Gateway コンソールからハードウェアアプライアンスを注文できるようになりました。詳細については、「Storage Gateway ハードウェアアプライアンスの使用」を参照してください。	2020 年 8 月 12 日

新しい AWS リージョンでの連邦情報処理規格 (FIPS) エンドポイントのサポート	米国東部 (オハイオ)、米国西部 (バージニア北部)、米国西部 (北カリフォルニア)、米国西部 (オレゴン)、およびカナダ (中部) の各リージョンで FIPS エンドポイントを使用してゲートウェイをアクティブ化できるようになりました。詳細については、「AWS 全般のリファレンス」の「AWS Storage Gateway エンドポイントとクォータ」を参照してください。	2020 年 7 月 31 日
ゲートウェイの移行	Storage Gateway で、テープおよび保管型のボリュームゲートウェイを新しい仮想マシンに移行できるようになりました。詳細については、「新しいゲートウェイへのデータの移動」を参照してください。	2020 年 7 月 31 日
Storage Gateway コンソールでの Amazon CloudWatch アラームの表示	Storage Gateway コンソールで CloudWatch アラームを表示できるようになりました。詳細については、「CloudWatch アラームの説明」を参照してください。	2020 年 5 月 29 日

連邦情報処理規格 (FIPS) エンドポイントのサポート	AWS GovCloud (US) リージョンで FIPS エンドポイントを持つゲートウェイをアクティブ化できるようになりました。ボリュームゲートウェイの FIPS エンドポイントを選択するには、「サービスエンドポイントの選択」を参照してください。テープゲートウェイの FIPS エンドポイントを選択するには、「テープゲートウェイを AWSに接続する」を参照してください。	2020 年 5 月 22 日
新しい AWS リージョン	Storage Gateway がアフリカ (ケープタウン) および欧州 (ミラノ) リージョンで利用できるようになりました。詳細については、「AWS 全般のリファレンス」の「AWS Storage Gateway エンドポイントとクォータ」を参照してください。	2020 年 5 月 7 日

S3 Intelligent-Tiering ストレージクラスのサポート	Storage Gateway で S3 Intelligent-Tiering ストレージクラスがサポートされるようになりました。S3 Intelligent-Tiering ストレージクラスは、パフォーマンスの低下や、オペレーション上のオーバーヘッドを発生させることなく、最もコスト効率の高いストレージアクセス階層に自動的にデータを移動することで、ストレージコストを最小限に抑えます。詳細については、Amazon Simple Storage Service ユーザーガイドで「アクセスパターンが変化する、またはアクセスパターンが不明なデータを、自動的に最適化するためのストレージクラス」を参照してください。	2020 年 4 月 30 日
テープゲートウェイの書き込みおよび読み取りパフォーマンスが 2 倍に向上	Storage Gateway のテープゲートウェイの仮想テープ間で、書き込みおよび読み取りパフォーマンスが 2 倍向上しました。バックアップや復元に要する時間が短縮されます。詳細については、Storage Gateway ユーザーガイドの「Performance Guidance for Tape Gateways」を参照してください。	2020 年 4 月 23 日

自動テープ作成のサポート	Storage Gateway で、新しい仮想テープを自動的に作成できるようになりました。テープゲートウェイは、設定された最小数のテープを利用可能な状態に維持するために、自動的に新しい仮想テープを作成し、これらの新しいテープをバックアップアプリケーションでインポートできるようにします。このため、バックアップジョブを中断なく実行できるようになります。詳細については、Storage Gateway ユーザーガイドの「Creating Tapes Automatically」を参照してください。	2020 年 4 月 23 日
新しい AWS リージョン	Storage Gateway が、 AWS GovCloud (米国東部) リージョンで利用可能になりました。詳細については、「AWS 全般のリファレンス」の「AWS Storage Gateway エンドポイントとクォータ」を参照してください。	2020 年 3 月 12 日

Linux カーネルベース仮想マシン (KVM) ハイパーバイザーのサポート	Storage Gateway で、KVM 仮想プラットフォームにオンプレミスゲートウェイをデプロイできるようになりました。KVM にデプロイされたゲートウェイは、既存のオンプレミスのゲートウェイと同じ機能と特徴をすべて備えています。詳細については、Storage Gateway ユーザーガイドの「Supported Hypervisors and Host Requirements」を参照してください。	2020 年 2 月 4 日
VMware vSphere High Availability のサポート	Storage Gateway で、VMware 上での高可用性がサポートされるようになりました。これは、ハードウェア、ハイパーバイザー、またはネットワーク障害からストレージワークロードを保護するのに役立ちます。詳細については、Storage Gateway ユーザーガイドの「Using VMware vSphere High Availability with Storage Gateway」を参照してください。このリリースでは、パフォーマンス向上も行われています。詳細については、Storage Gateway ユーザーガイドの「Performance」を参照してください。	2019 年 11 月 20 日

テープゲートウェイの新しい AWS リージョン	テープゲートウェイが南米 (サンパウロ) リージョンで利用可能になりました。詳細については、「AWS 全般のリファレンス」の「AWS Storage Gateway エンドポイントとクォータ」を参照してください。	2019 年 9 月 24 日
Linux が IBM Spectrum Protect バージョン 7.1.9 をサポート、テープゲートウェイの最大テープ容量が 5 TiB に増加	テープゲートウェイが Microsoft Windows 用だけでなく Linux 用の IBM Spectrum Protect (Tivoli Storage Manager) バージョン 7.1.9 もサポートするようになりました。詳細については、Storage Gateway ユーザーガイドの「Testing Your Setup by Using IBM Spectrum Protect」を参照してください。また、テープゲートウェイで仮想テープの最大容量が 2.5 TiB から 5 TiB に増加しました。詳細については、Storage Gateway ユーザーガイドの「Quotas for Tapes」を参照してください。	2019 年 9 月 10 日

Amazon CloudWatch Logs のサポート	ファイルゲートウェイで Amazon CloudWatch ロググループを設定して、ゲートウェイとそのリソースのエラーと状態について通知を受け取ることができるようになりました。詳細については、Storage Gateway ユーザーガイドの「Getting Notified About Gateway Health and Errors With Amazon CloudWatch Log Groups」を参照してください。	2019 年 9 月 4 日
新しい AWS リージョン	Storage Gateway が、アジアパシフィック (香港) リージョンで利用できるようになりました。詳細については、「AWS 全般のリファレンス」の「AWS Storage Gateway エンドポイントとクォータ」を参照してください。	2019 年 8 月 14 日
新しい AWS リージョン	Storage Gateway が、中東 (バーレーン) リージョンで利用できるようになりました。詳細については、「AWS 全般のリファレンス」の「AWS Storage Gateway エンドポイントとクォータ」を参照してください。	2019 年 7 月 29 日

仮想プライベートクラウド (VPC) でゲートウェイをアクティブ化するためのサポート	VPC でゲートウェイをアクティベートできるようになりました。オンプレミスのソフトウェアアプライアンスとクラウドベースのストレージインフラストラクチャの間にプライベート接続を作成することができます。詳細については、「仮想プライベートクラウドでゲートウェイをアクティブ化する」を参照してください。	2019 年 6 月 20 日
S3 Glacier Flexible Retrieval から S3 Glacier Deep Archive への仮想テープの移行に対応	コストの効率化と長期間のデータ保管用に、S3 Glacier Flexible Retrieval ストレージクラスにアーカイブされている仮想テープを S3 Glacier Deep Archive ストレージクラスに移動できるようになりました。詳細については、「S3 Glacier Flexible Retrieval から S3 Glacier Deep Archive へのテープの移動」を参照してください。	2019 年 5 月 28 日

SMB ファイル共有の Microsoft Windows ACL SMB サポート	ファイルゲートウェイの場合、Microsoft Windows アクセスコントロールリスト (ACL) を使用して、サーバーメッセージブロック (SMB) ファイル共有へのアクセスを制御できるようになりました。詳細については、「Microsoft Windows ACL を使用して、SMB ファイル共有へのアクセスを制御する」を参照してください。	2019 年 5 月 8 日
S3 Glacier Deep Archive との統合	テープゲートウェイは S3 Glacier Deep Archive と統合できます。S3 Glacier Deep Archive で仮想テープを長期データ保持用にアーカイブできるようになりました。詳細については、「仮想テープのアーカイブ」を参照してください。	2019 年 3 月 27 日

欧州での Storage Gateway ハードウェアアプライアンスの可用性	Storage Gateway ハードウェアアプライアンスが、欧州で利用できるようになりました。詳細については、「AWS 全般のリファレンス」の「AWS Storage Gateway ハードウェアアプライアンスリージョン」を参照してください。さらに、Storage Gateway ハードウェアアプライアンスで利用可能なストレージを 5 TB から 12 TB に増やし、取り付けられている銅線ネットワークカードを 10 ギガビットの光ファイバーネットワークカードに交換できます。詳細については、「ハードウェアアプライアンスの設定」を参照してください。	2019 年 2 月 25 日
との統合 AWS Backup	Storage Gateway は と統合されます AWS Backup。を使用して AWS Backup 、Cloud-Backed ストレージに Storage Gateway ボリュームを使用するオンプレミスのビジネスアプリケーションをバックアップできるようになりました。詳細については、「ボリュームのバックアップ」を参照してください。	2019 年 1 月 16 日

Bacula Enterprise および IBM Spectrum Protect のサポート	テープゲートウェイで、Bacula Enterprise および IBM Spectrum Protect がサポートされるようになりました。また、Storage Gateway で Veritas NetBackup、Veritas Backup Exec および Quest NetVault Backup の新しいバージョンもサポートされるようになりました。これらのバックアップアプリケーションを使用してデータを Amazon S3 にバックアップし、オフラインストレージ (S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive) に直接アーカイブできるようになりました。詳細については、「バックアップソフトウェアを使用してゲートウェイのセットアップをテストする」を参照してください。	2018 年 11 月 13 日

Storage Gateway ハードウェアアプライアンスのサポート	Storage Gateway ハードウェアアプライアンスには、サードパーティーのサーバーにプリインストールされた Storage Gateway ソフトウェアが含まれています。 AWS Management Consoleからアプライアンスを管理できます。アプライアンスは、ファイルゲートウェイ、テープゲートウェイ、およびボリュームゲートウェイをホストできます。詳細については、「Using the Storage Gateway Hardware Appliance」を参照してください。	2018 年 9 月 18 日
Microsoft System Center 2016 Data Protection Manager (DPM) との互換性	テープゲートウェイが Microsoft System Center 2016 Data Protection Manager (DPM) に対応しました。Microsoft DPM を使用してデータを Amazon S3 にバックアップし、オフラインストレージ (S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive) に直接アーカイブできるようになりました。詳細については、「Microsoft System Center Data Protection Manager を使用したセットアップのテスト」を参照してください。	2018 年 7 月 18 日

サーバーメッセージブロック (SMB) プロトコルのサポート	ファイルゲートウェイで、ファイル共有にサーバーメッセージブロック (SMB) プロトコルを使用できるようになりました。詳細については、「ファイル共有の作成」を参照してください。	2018 年 6 月 20 日
ファイル共有、キャッシュ型ボリューム、および仮想テープの暗号化のサポート	AWS Key Management Service （ AWS KMS) を使用して、ファイル共有、キャッシュ型ボリューム、または仮想テープに書き込まれたデータを暗号化できるようになりました。現在、この暗号化には AWS Storage Gateway API を使用できます。詳細については、「Data encryption using AWS KMS」を参照してください。	2018 年 12 月 6 日

NovaStor DataCenter/Network のサポート	テープゲートウェイが NovaStor DataCenter/Network に対応しました。NovaStor DataCenter/Network バージョン 6.4 または 7.1 を使用して、データを Amazon S3 にバックアップし、オフラインストレージ (S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive) に直接アーカイブできるようになりました。詳細については、「NovaStor DataCenter/Network を使用したセットアップのテスト」を参照してください。	2018 年 5 月 24 日

以前の更新

以下の表に、2018 年 5 月より前の 『AWS Storage Gateway ユーザーガイド』の各リリースにおける重要な変更点を示します。

変更	説明	変更日
S3 1 ゾーン_IA ストレージクラスのサポート	ファイルゲートウェイで、S3 1 ゾーン_IA をファイル共有のデフォルトのストレージクラスとして選択できるようになりました。このストレージクラスを使用すると、Amazon S3 の単一のアベイラビリティーゾーンにオブジェクトデータを保存できます。詳細については、「Create a file share」を参照してください。	2018 年 4 月 4 日
新しいリージョン	テープゲートウェイがアジアパシフィック (シンガポール) リージョンで利用できるようになりました。詳細については、「AWS リージョン Storage Gateway をサポートする」を参照してください。	2018 年 4 月 3 日

変更	説明	変更日
キャッシュの更新通知、リクエスタ支払いおよび Amazon S3 バケットの固定 ACL のサポート。	ファイルゲートウェイで、ゲートウェイによる Amazon S3 バケットのキャッシュの更新が完了したときに、通知を受けることができるようになりました。詳細については、Storage Gateway API リファレンスの「RefreshCache.html」を参照してください。 ファイルゲートウェイを使用して、バケット所有者ではなくリクエスタまたはリーダーがアクセス料金を支払うことができるようになりました。 ファイルゲートウェイを使用して、NFS ファイル共有にマッピングする S3 バケットの所有者に完全なコントロールを付与できるようになりました。 詳細については、「Create a file share」を参照してください。	2018 年 3 月 1 日
Dell EMC NetWorker V9.x のサポート	テープゲートウェイは、Dell EMC NetWorker V9.x をサポートするようになりました。Dell EMC NetWorker V9.x を使用して、データを Amazon S3 にバックアップし、オフラインストレージ (S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive) に直接アーカイブできるようになりました。詳細については、「Dell EMC NetWorker を使用したセットアップのテスト」を参照してください。	2018 年 2 月 27 日
新しいリージョン	Storage Gateway が欧州 (パリ) リージョンで利用可能になりました。詳細については、「AWS リージョン Storage Gateway をサポートする」を参照してください。	2017 年 12 月 18 日

変更	説明	変更日
ファイルのアップロード通知および MIME タイプの推測のサポート	ファイルゲートウェイで、NFS ファイル共有に書き込まれたすべてのファイルが Amazon S3 にアップロードされたときに通知を受信できるようになりました。詳細については、Storage Gateway API リファレンスの「NotifyWhenUploaded」を参照してください。 ファイルゲートウェイを使用して、アップロードされたオブジェクトの MIME タイプをファイルの拡張子に基づいて推測できるようになりました。詳細については、「Create a file share」を参照してください。	2017 年 11 月 21 日
VMware ESXi Hypervisor バージョン 6.5 のサポート	AWS Storage Gateway で VMware ESXi Hypervisor バージョン 6.5 がサポートされるようになりました。これは、バージョン 4.1、5.0、5.1、5.5、および 6.0 に加えてサポートされます。詳細については、「サポートされているハイパーバイザーとホストの要件」を参照してください。	2017 年 9 月 13 日
Commvault 11 との互換性	テープゲートウェイが Commvault 11 に対応しました。Commvault を使用してデータを Amazon S3 にバックアップし、オフラインストレージ (S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive) に直接アーカイブできるようになりました。詳細については、「Commvault を使用したセットアップのテスト」を参照してください。	2017 年 9 月 12 日
Microsoft Hyper-V ハイパーバイザーのファイルゲートウェイサポート	Microsoft Hyper-V ハイパーバイザーにファイルゲートウェイをデプロイできるようになりました。詳細については、サポートされているハイパーバイザーとホストの要件 を参照してください。	2017 年 6 月 22 日

変更	説明	変更日
3 ~ 5 時間のテープをアーカイブから取得するサポート	テープゲートウェイでは、3 ~ 5 時間でテープをアーカイブから取得できるようになりました。バックアッププアプリケーションまたは仮想テープライブラリ (VTL) によってテープに書き込まれるデータ量を判断することもできます。詳細については、「テープの使用状況の表示」を参照してください。	2017 年 5 月 23 日
新しいリージョン	Storage Gateway がアジアパシフィック (ムンバイ) リージョンで利用可能になりました。詳細については、「AWS リージョン Storage Gateway をサポートする」を参照してください。	2017 年 5 月 02 日
ファイル共有の設定に更新します ファイル共有のためのキャッシュ更新のサポート	ファイルゲートウェイで、ファイル共有の設定にマウントオプションが追加されました。ファイル共有に squash と読み取り専用オプションを設定できるようになりました。詳細については、「Create a file share」を参照してください。 ファイルゲートウェイで、最後にバケットのコンテンツのリストが取得され、その結果がキャッシュに保存された時点以降に Amazon S3 バケットに追加または削除されたオブジェクトを、検出できるようになりました。詳細については、API リファレンスの「RefreshCache」を参照してください。	2017 年 3 月 28 日
ボリュームのクローンをサポート	キャッシュ型ボリュームゲートウェイの場合、 は既存のボリュームからボリュームのクローンを作成する機能をサポートする AWS Storage Gateway ようになりました。詳細については、「ボリュームをクローンする」を参照してください。	2017 年 3 月 16 日

変更	説明	変更日
Amazon EC2 のファイルゲートウェイのサポート	AWS Storage Gateway では、Amazon EC2 にファイルゲートウェイをデプロイできるようになりました。Storage Gateway Amazon マシンイメージ (AMI) をコミュニティ AMI として利用できるようになりました。この AMI を使用して、Amazon EC2 でファイルゲートウェイを起動できます。ファイルゲートウェイを作成して EC2 インスタンスにデプロイする方法については、「Create and activate an Amazon S3 File Gateway」または「Create and activate an Amazon FSx File Gateway」を参照してください。ファイルゲートウェイ AMI を起動する方法については、「Deploying an S3 File Gateway on an Amazon EC2 host」または「Deploying FSx File Gateway on an Amazon EC2 host」を参照してください。	2017 年 2 月 08 日
Arcserve 17 との互換性	テープゲートウェイが Arcserve 17 に対応しました。Arcserve を使用してデータを Amazon S3 にバックアップし、S3 Glacier Flexible Retrieval に直接アーカイブできるようになりました。詳細については、「Arcserve Backup r17.0 を使用したセットアップのテスト」を参照してください。	2017 年 1 月 17 日
新しいリージョン	Storage Gateway は、欧州 (ロンドン) リージョンで利用可能になりました。詳細については、「AWS リージョン Storage Gateway をサポートする」を参照してください。	2016 年 12 月 13 日
新しいリージョン	Storage Gateway は、カナダ (中部) リージョンで利用可能になりました。詳細については、「AWS リージョン Storage Gateway をサポートする」を参照してください。	2016 年 12 月 08 日

変更	説明	変更日
ファイルゲートウェイのサポート	Storage Gateway で、ボリュームゲートウェイとテープゲートウェイに加えてファイルゲートウェイも利用できるようになりました。ファイルゲートウェイでは、サービスおよび仮想ソフトウェアアプライアンスを組み合わせ、ネットワークファイルシステム (NFS) のような業界標準のファイルプロトコルを使用することで、Amazon S3 でオブジェクトを保存し、取得することができます。ゲートウェイでは、NFS マウントポイントのファイルとして、Amazon S3 のオブジェクトへのアクセスが提供されます。	2016 年 11 月 29 日
Backup Exec 16	テープゲートウェイが Backup Exec 16 に対応しました。Backup Exec 16 を使用してデータを Amazon S3 にバックアップし、オフラインストレージ (S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive) に直接アーカイブできるようになりました。詳細については、「Veritas Backup Exec を使用したセットアップのテスト」を参照してください。	2016 年 11 月 7 日
Micro Focus (HPE) Data Protector 9.x との互換性	テープゲートウェイが Micro Focus (HPE) Data Protector 9.x に対応しました。HPE Data Protector を使用してデータを Amazon S3 にバックアップし、S3 Glacier Flexible Retrieval に直接アーカイブできるようになりました。詳細については、「Micro Focus (HPE) Data Protector を使用したセットアップのテスト」を参照してください。	2016 年 11 月 2 日
新しいリージョン	Storage Gateway が米国東部 (オハイオ) リージョンで利用可能になりました。詳細については、「AWS リージョン Storage Gateway をサポートする」を参照してください。	2016 年 10 月 17 日

変更	説明	変更日
Storage Gateway コンソールの再設計	ゲートウェイ、ボリューム、仮想テープを簡単に設定、管理、モニタリングできるよう、Storage Gateway マネジメントコンソールが再設計されました。ユーザーインターフェイスは、フィルタリングできるビューを提供し、CloudWatch や Amazon EBS などの統合 AWS サービスへの直接リンクを提供するようになりました。詳細については、「にサインアップする AWS Storage Gateway」を参照してください。	2016 年 8 月 30 日
Veeam Backup & Replication V9 アップデート 2 以降のバージョンとの互換性	テープゲートウェイが Veeam Backup & Replication V9 アップデート 2 以降のバージョン (バージョン 9.0.0.1715 以降) に対応しました。Veeam Backup Replication V9 Update 2 以降を使用して、データを Amazon S3 にバックアップし、オフラインストレージ (S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive) に直接アーカイブできるようになりました。詳細については、「Veeam Backup & Replication を使用したセットアップのテスト」を参照してください。	2016 年 8 月 15 日
より長いボリューム ID とスナップショット ID	Storage Gateway で、ボリュームとスナップショットにより長い ID を使用できるようになりました。ボリューム、スナップショット、その他のサポートされている AWS リソースに対して、長い ID 形式をアクティブ化できます。詳細については、「Storage Gateway のリソースとリソース ID の説明」を参照してください。	2016 年 4 月 25 日

変更	説明	変更日
新しいリージョン ストレージ容量が最大 512 TiB の保存型ボリュームのサポート Storage Gateway ローカルコンソールに対して行われたゲートウェイのその他の更新と機能の強化	テープゲートウェイが、アジアパシフィック (ソウル) リージョンで使用できるようになりました。詳細については、「AWS リージョン Storage Gateway をサポートする」を参照してください。 保存型ボリュームの場合、ストレージ容量が最大 512 TiB のストレージボリュームを最大 32 個 (各ボリュームのサイズは最大 16 TiB) 作成できるようになりました。詳細については、「保管型ボリュームのアーキテクチャ」および「AWS Storage Gateway クォータ」を参照してください。 仮想テープライブラリ内のすべてのテープの合計サイズは 1 PiB に増加します。詳細については、「AWS Storage Gateway クォータ」を参照してください。 Storage Gateway コンソールで VM ローカルコンソールのパスワードを設定できるようになりました。詳細については、Storage Gateway コンソールからのローカルコンソールパスワードの設定 を参照してください。	2016 年 3 月 21 日
Dell EMC NetWorker 8.x との互換性	テープゲートウェイが Dell EMC NetWorker 8.x に対応しました。Dell EMC NetWorker を使用してデータを Amazon S3 にバックアップし、オフラインストレージ (S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive) に直接アーカイブできるようになりました。詳細については、「Dell EMC NetWorker を使用したセットアップのテスト」を参照してください。	2016 年 2 月 29 日

変更	説明	変更日
VMware ESXi Hypervisor バージョン 6.0 および Red Hat Enterprise Linux 7 iSCSI イニシエータのサポート	AWS Storage Gateway は、VMware ESXi Hypervisor バージョン 6.0 と Red Hat Enterprise Linux 7 iSCSI イニシエータをサポートするようになりました。詳細については、サポートされているハイパーバイザーとホストの要件およびサポートされている iSCSI イニシエータを参照してください。	2015 年 10 月 20 日
コンテンツの再編成	このリリースでは、ドキュメントが改善されており、新たに含められた「アクティブ化したゲートウェイの管理」セクションに、すべてのゲートウェイソリューションに共通の管理タスクがまとめられています。次に、デプロイしてアクティベートした後のゲートウェイを管理する方法が記載されています。詳細については、「ボリュームゲートウェイの管理」を参照してください。	

変更	説明	変更日
ストレージ容量が最大 1,024 TiB のキャッシュ型ボリュームのサポート VMware ESXi ハイパーバイザーでの VMXNET3 (10 GbE) ネットワークアダプタタイプのサポート パフォーマンスの拡張 Storage Gateway のローカルコンソールの拡張と更新	キャッシュ型ボリュームの場合、ストレージ容量が最大 1,024 TiB のストレージボリュームを最大 32 個作成できるようになりました。詳細については、「キャッシュ型ボリュームのアーキテクチャ」および「AWS Storage Gateway クォータ」を参照してください。 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 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。詳細については、「ゲートウェイのネットワークアダプタの設定」を参照してください。 Storage Gateway の最大アップロード速度が 120 MB/秒に向上し、最大ダウンロード速度が 20 MB/秒に向上しました。 Storage Gateway ローカルコンソールが更新および強化され、メンテナンスタスクを実行するための機能が追加されました。詳細については、「ゲートウェイのネットワークの設定」を参照してください。	2015 年 9 月 16 日
タグ指定のサポート	Storage Gateway でリソースのタグ付けがサポートされるようになりました。ゲートウェイ、ボリューム、および仮想テープにタグを追加して、簡単に管理できるようになりました。詳細については、「Storage Gateway リソースのタグ付け」を参照してください。	2015 年 9 月 2 日
Quest (旧 Dell) NetVault Backup 10.0 との互換性	テープゲートウェイが Quest NetVault Backup 10.0 に対応しました。Quest NetVault Backup 10.0 を使用してデータを Amazon S3 にバックアップし、オフラインのストレージ (S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive) に直接アーカイブできるようになりました。詳細については、「Quest NetVault Backup を使用したセットアップのテスト」を参照してください。	2015 年 6 月 22 日

変更	説明	変更日
保管型ボリュームゲートウェイのセットアップ用 16 TiB ストレージボリュームのサポート	Storage Gateway で、保管型ボリュームのゲートウェイの設定用に 16 TiB ストレージボリュームがサポートされるようになりました。16 TiB ストレージボリュームを 12 個作成できるようになりました (ストレージは最大 192 TiB)。詳細については、「保管型ボリュームのアーキテクチャ」を参照してください。	2015 年 6 月 3 日
Storage Gateway ローカルコンソールでのシステムリソースチェックのサポート	ゲートウェイが適切に機能するには、システムリソース (仮想 CPU コア、ルートボリュームサイズ、および RAM) が十分であるかどうかを確認できるようになりました。詳細については、ゲートウェイシステムリソースのステータスの表示 または ゲートウェイシステムリソースのステータスの表示 を参照してください。	
Red Hat Enterprise Linux 6 iSCSI イニシエータのサポート	Storage Gateway で Red Hat Enterprise Linux 6 iSCSI イニシエータがサポートされるようになりました。詳細については、「ボリュームゲートウェイのセットアップ要件」を参照してください。	
	このリリースでは、次のように Storage Gateway が改良および更新されています。 • Storage Gateway コンソールから、最後にソフトウェア更新が正常にゲートウェイに適用された日時を確認できるようになりました。詳細については、「ゲートウェイアップデートの管理」を参照してください。 • Storage Gateway で、API を使用して、ストレージボリュームに接続されている iSCSI イニシエータをリストできるようになりました。詳細について	

変更	説明	変更日
	は、API リファレンスの「ListVolumeInitiators」を参照してください。	
Microsoft Hyper-V hypervisor バージョン 2012 および 2012 R2 のサポート	Storage Gateway で、Microsoft Hyper-V hypervisor バージョン 2012 および 2012 R2 がサポートされるようになりました。これは、Microsoft Hyper-V hypervisor バージョン 2008 R2 に加えてサポートされます。詳細については、「サポートされているハイパーバイザーとホストの要件」を参照してください。	2015 年 4 月 30 日
Symantec Backup Exec 15 との互換性	テープゲートウェイが Symantec Backup Exec 15 に対応しました。Symantec Backup Exec 15 を使用してデータを Amazon S3 にバックアップし、オフラインストレージ (S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive) に直接アーカイブできるようになりました。詳細については、「Veritas Backup Exec を使用したセットアップのテスト」を参照してください。	2015 年 4 月 6 日
ストレージボリュームに対する CHAP 認証サポート	Storage Gateway で、ストレージボリュームに対する CHAP 認証の設定がサポートされるようになりました。詳細については、「ボリューム用の CHAP 認証の設定」を参照してください。	2015 年 4 月 2 日
VMware ESXi Hypervisor バージョン 5.1 および 5.5 のサポート	Storage Gateway で、VMware ESXi Hypervisor バージョン 5.1 および 5.5 がサポートされるようになりました。これは、VMware ESXi Hypervisor バージョン 4.1 および 5.0 に加えてサポートされます。詳細については、「サポートされているハイパーバイザーとホストの要件」を参照してください。	2015 年 30 月 3 日

変更	説明	変更日
Windows CHKDSK ユーティリティのサポート	Storage Gateway で、Windows CHKDSK ユーティリティがサポートされるようになりました。このユーティリティを使用すると、ボリュームの整合性を確認し、ボリューム上のエラーを修正することができます。詳細については、「ボリュームの問題のトラブルシューティング」を参照してください。	2015 年 3 月 04 日
との統合 AWS CloudTrail による API コールのキャプチャ	Storage Gateway は AWS CloudTrail、Amazon Web Services アカウントで Storage Gateway によって、または Storage Gateway に代わって行われた API コール AWS CloudTrail をキャプチャし、指定した Amazon S3 バケットにログファイルを配信するようになりました。詳細については、「での ログ記録とモニタリング AWS Storage Gateway」を参照してください。 このリリースで、Storage Gateway は次の点で改良および更新されました。 • キャッシュストレージにダーティデータがある仮想テープ (AWSにアップロードされていないコンテンツを含むテープ) は、ゲートウェイのキャッシュ型ドライブの変更時に復旧されるようになりました。詳細については、「回復不可能なゲートウェイからの仮想テープの復旧」を参照してください。	2014 年 12 月 16 日

変更	説明	変更日
追加のバックアップソフトウェアやメディアチェンジャーとの互換性	テープゲートウェイが、次のバックアップソフトウェアに対応しました。 • Symantec Backup Exec 2014 • Microsoft System Center 2012 R2 Data Protection Manager • Veeam Backup & Replication V7 • Veeam Backup & Replication V8 これらの 4 つのバックアップソフトウェア製品と Storage Gateway 仮想テープライブラリ (VTL) を使用して、データを Amazon S3 にバックアップし、オフラインストレージ (S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive) に直接アーカイブできるようになりました。詳細については、「バックアップソフトウェアを使用してゲートウェイのセットアップをテストする」を参照してください。 Storage Gateway で、新しいバックアップソフトウェアと連携する追加のメディアチェンジャーが提供されるようになりました。 このリリースには、さまざまな AWS Storage Gateway 改善と更新が含まれています。	2014 年 11 月 3 日
欧州 (フランクフルト) リージョン	Storage Gateway は、欧州 (フランクフルト) リージョンで利用可能になりました。詳細については、「AWS リージョン Storage Gateway をサポートする」を参照してください。	2014 年 10 月 23 日

変更	説明	変更日
コンテンツの再編成	すべてのゲートウェイソリューションに共通の「はじめに」セクションを作成しました。次に、ゲートウェイをダウンロード、デプロイ、およびアクティブ化するための手順を説明します。ゲートウェイをデプロイおよびアクティブ化した後は、保管型ボリューム、キャッシュ型ボリューム、テープゲートウェイを設定する個別の手順に進むことができます。詳細については、「テープゲートウェイの作成」を参照してください。	2014 年 5 月 19 日
Symantec Backup Exec 2012 との互換性	テープゲートウェイが Symantec Backup Exec 2012 に対応しました。Symantec Backup Exec 2012 を使用してデータを Amazon S3 にバックアップし、オフラインストレージ (S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive) に直接アーカイブできるようになりました。詳細については、「Veritas Backup Exec を使用したセットアップのテスト」を参照してください。	2014 年 4 月 28 日

変更	説明	変更日
Windows Server Failover Clustering のサポート VMware ESX イニシエータのサポート Storage Gateway ローカルコンソールでの設定タスクの実行のサポート	• Storage Gateway では、ホストが Windows Server Failover Clustering (WSFC) を使用してアクセスを調整する場合に、同じボリュームで複数のホストに接続できるようになりました。ただし、ESFC を使用せずに同じボリュームで複数のホストに接続することはできません。 • Storage Gateway では、ESX ホストを通じてストレージ接続を直接管理できるようになりました。これによって、VM のゲスト OS にあるイニシエータを使用する方法の代替手段が提供されます。 • Storage Gateway では、Storage Gateway ローカルコンソールでの設定タスクの実行を行えるようになりました。オンプレミスにデプロイされたゲートウェイでの設定タスクの実行については、「VM ローカルコンソールでのタスクの実行」または「VM ローカルコンソールでのタスクの実行」を参照してください。EC2 インスタンスにデプロイされたゲートウェイでの設定タスクの実行については、「Amazon EC2 ローカルコンソールでのタスクの実行または「Amazon EC2 ローカルコンソールでのタスクの実行」を参照してください。	2014 年 1 月 31 日

変更	説明	変更日
仮想テープライブラリ (VTL) のサポートと、API バージョン (2013 年 6 月 30 日) の導入	Storage Gateway は、オンプレミスのソフトウェアアプライアンスをクラウドベースのストレージに接続して、オンプレミスの IT 環境を AWS ストレージインフラストラクチャと統合します。Storage Gateway で、ボリュームゲートウェイ (キャッシュ型ボリュームと保管型ボリューム) に加え、ゲートウェイ — 仮想テープライブラリ (VTL) がサポートされるようになりました。ゲートウェイごとに最大 10 個の仮想テープドライブを使用して、テープゲートウェイを構成できます。各仮想テープドライブは SCSI コマンドセットに応答するため、既存のオンプレミスバックアップアプリケーションを修正する必要はありません。詳細については、AWS Storage Gateway ユーザーガイドの次のトピックを参照してください。 • アーキテクチャの概要については、「テープゲートウェイの仕組み (アーキテクチャ)」を参照してください。 • テープゲートウェイを使い始めるには、「テープゲートウェイの作成」を参照してください。	2013 年 11 月 5 日
Microsoft Hyper-V のサポート	Storage Gateway で、Microsoft Hyper-V 仮想プラットフォームにオンプレミスゲートウェイをデプロイできるようになりました。Microsoft Hyper-V にデプロイされたゲートウェイには、既存のオンプレミスストレージゲートウェイと同じ機能と特徴がすべてあります。Microsoft Hyper-V を使ってゲートウェイのデプロイを開始するには、サポートされているハイパーバイザーとホストの要件 を参照してください。	2013 年 4 月 10 日

変更	説明	変更日
Amazon EC2 でのゲートウェイのデプロイのサポート	Storage Gateway で、Amazon Elastic Compute Cloud (Amazon EC2) にゲートウェイをデプロイする機能を利用できるようになりました。AWS Marketplace で利用可能な Storage Gateway AMI を使用して、Amazon EC2 でゲートウェイのインスタンスを起動できます。Storage Gateway AMI を使用してゲートウェイのデプロイを開始するには、「ボリュームゲートウェイ用にカスタマイズされた Amazon EC2 インスタンスをデプロイする」を参照してください。	2013 年 1 月 15 日

変更	説明	変更日
キャッシュ型ボリュームのサポートと、API バージョン (2012 年 6 月 30 日) の導入	このリリースでは、Storage Gateway でキャッシュ型ボリュームのサポートが導入されました。キャッシュ型ボリュームは、オンプレミスストレージを拡張する必要性を最小限に抑えます。同時に、アプリケーションからは引き続き、アクティブデータへの低レイテンシーなアクセスが可能になります。最大容量 32 TiB のストレージボリュームを作成し、オンプレミスのアプリケーションサーバーから iSCSI デバイスとしてマウントすることが可能です。キャッシュ型ボリュームに書き込まれたデータは Amazon Simple Storage Service (Amazon S3) に保管され、オンプレミスのストレージハードウェアには、最近読み書きされたキャッシュのみがローカルに保存されます。キャッシュ型ボリュームでは、古くてあまり頻繁にアクセスされないデータなど、取得時に高レイテンシーが許容されるデータには Amazon S3 を使用し、低レイテンシーアクセスが必要なデータにはオンプレミスストレージを使用できます。 このリリースでは、Storage Gateway での現在のオペレーションに加え、新しい API バージョンも導入されました。これにより、キャッシュ型ボリュームをサポートする新しいオペレーションが利用可能になります。 これら 2 つの Storage Gateway ソリューションの詳細については、ボリュームゲートウェイの仕組み を参照してください。 また、テストのセットアップもお試しください。手順については、「テープゲートウェイの作成」を参照してください。	2012 年 10 月 29 日

変更	説明	変更日
API と IAM のサポート	このリリースでは、Storage Gateway に API サポートと AWS Identity and Access Management(IAM) のサポートが導入されました。 • API のサポート — Storage Gateway リソースを、プログラムで設定および管理できるようになりました。API の詳細については、AWS Storage Gateway ユーザーガイドの「Storage Gateway の API リファレンス」を参照してください。 • IAM のサポート — AWS Identity and Access Management (IAM) を使用すると、ユーザーを作成し、Storage Gateway リソースへのユーザーアクセスを IAM ポリシーで管理できます。IAM ポリシーの例については、「AWS Storage Gatewayの Identity and Access Management」を参照してください。IAM の詳細については、AWS Identity and Access Management (IAM) の詳細ページを参照してください。	2012 年 5 月 9 日
静的 IP のサポート	ローカルゲートウェイに対して、静的 IP を指定できるようになりました。詳細については、「ゲートウェイのネットワークの設定」を参照してください。	2012 年 3 月 5 日
新規ガイド	これは『AWS Storage Gateway ユーザーガイド』の最初のリリースです。	2012 年 1 月 24 日

ボリュームゲートウェイアプライアンスソフトウェアのリリースノート

これらのリリースノートでは、ボリュームゲートウェイアプライアンスの各バージョンに含まれる新機能と更新された機能、改善点、修正点について説明します。各ソフトウェアバージョンは、リリース日と一意のバージョン番号によって識別されます。

Storage Gateway コンソールで詳細ページを確認するか、次のような AWS CLI コマンドを使用して DescribeGatewayInformation API アクションを呼び出すことで、ゲートウェイのソフトウェアバージョン番号を確認できます。

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

バージョン番号は API レスポンスの `SoftwareVersion` フィールドで返されます。

> **Note**
>
> 次の状況では、ゲートウェイはソフトウェアバージョン情報を報告しません。
>
> - ゲートウェイはオフラインです。
> - ゲートウェイは、バージョンレポートをサポートしていない古いソフトウェアを実行しています。
> - ゲートウェイタイプは FSx File Gateway です。

ゲートウェイのデフォルトの自動メンテナンスと更新スケジュールを変更する方法など、ボリュームゲートウェイの更新の詳細については、「コンソールを使用した AWS Storage Gateway更新の管理」を参照してください。

リリース日	ソフトウェアのバージョン	リリースノート
2025-07-01	2.12.11	• オペレーティングシステムとソフトウェア要素を更新して、新規および既存のゲ

リリース日	ソフトウェアのバージョン	リリースノート
		ートウェイのセキュリティとパフォーマンスを改善
2025-06-02	2.12.10	• オペレーティングシステムとソフトウェア要素を更新して、新規および既存のゲートウェイのセキュリティとパフォーマンスを改善
2025-05-01	2.12.9	• オペレーティングシステムとソフトウェア要素を更新して、新規および既存のゲートウェイのセキュリティとパフォーマンスを改善
2025-05-01	2.12.8	• オペレーティングシステムとソフトウェア要素を更新して、新規および既存のゲートウェイのセキュリティとパフォーマンスを改善
2025-04-01	2.12.7	• オペレーティングシステムとソフトウェア要素を更新して、新規および既存のゲートウェイのセキュリティとパフォーマンスを改善
2025-03-04	2.12.6	• オペレーティングシステムとソフトウェア要素を更新して、新規および既存のゲートウェイのセキュリティとパフォーマンスを改善

リリース日	ソフトウェアのバージョン	リリースノート
2025-02-04	2.12.5	• オペレーティングシステムとソフトウェア要素を更新して、新規および既存のゲートウェイのセキュリティとパフォーマンスを改善 • ソフトウェアの更新後にゲートウェイがシャットダウン状態のままになる可能性がある問題に対処しました
2025-01-07	2.12.3	• オペレーティングシステムとソフトウェア要素を更新して、新規および既存のゲートウェイのセキュリティとパフォーマンスを改善
2024-12-06	2.12.2	• オペレーティングシステムとソフトウェア要素を更新して、新規および既存のゲートウェイのセキュリティとパフォーマンスを改善
2024-11-06	2.12.1	• オペレーティングシステムとソフトウェア要素を更新して、新規および既存のゲートウェイのセキュリティとパフォーマンスを改善

リリース日	ソフトウェアのバージョン	リリースノート
2024-10-03	2.12.0	• ゲートウェイの再起動またはゲートウェイのソフトウェア更新後に iSCSI イニシエータがボリュームに自動的に再接続しない問題を修正 • オペレーティングシステムとソフトウェア要素を更新して、新規および既存のゲートウェイのセキュリティとパフォーマンスを改善
2024-08-30	2.11.0	• オペレーティングシステムとソフトウェア要素を更新して、新規および既存のゲートウェイのセキュリティとパフォーマンスを改善
2024-07-29	2.10.0	• オペレーティングシステムとソフトウェア要素を更新して、新規および既存のゲートウェイのセキュリティとパフォーマンスを改善 • その他のバグ修正と機能強化
2024-06-17	2.9.2	• オペレーティングシステムとソフトウェア要素を更新して、新規および既存のゲートウェイのセキュリティとパフォーマンスを改善

リリース日	ソフトウェアのバージョン	リリースノート
2024-05-28	2.9.0	• ソフトウェア更新中のゲートウェイの再起動時間を短縮 • ネットワーク帯域幅を推定するために転送されるデータ量を削減
2024-05-08	2.8.3	• SOCKS5 プロキシ使用時のクラウド接続の問題に対応
2024-04-10	2.8.1	• 2.8.0 で導入されたメモリ使用量の問題に対処 • セキュリティパッチの更新 • ソフトウェア更新プロセスの改善 • 新しいゲートウェイの Network Time Protocol (NTP) コンポーネントの欠落に対処
2024-03-06	2.8.0	• 新しいゲートウェイのセキュリティとパフォーマンスを向上させるためにオペレーティングシステムとソフトウェア要素を更新 • セキュリティパッチの更新
2023-12-19	2.7.0	• 新しいゲートウェイのセキュリティとパフォーマンスを向上させるためにオペレーティングシステムとソフトウェア要素を更新
2023-12-14	2.6.6	• メンテナンスリリース

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。