aws

開発者ガイド

AWS Backup

AWS Backup: 開発者ガイド

Table of Contents

とは AWS Backup

AWS Backup はフルマネージド型サービスで、 AWS サービス間、クラウド内、オンプレミスでのデータ保護の一元化と自動化を容易にします。このサービスを使用すると、バックアップポリシーを設定し、 AWS リソースのアクティビティを 1 か所でモニタリングできます。これにより、以前にで実行されたバックアップタスクを自動化および統合でき service-by-service、カスタムスクリプトや手動プロセスを作成する必要がなくなります。 AWS Backup コンソールでの数回のクリックで、データ保護ポリシーとスケジュールを自動化できます。

AWS Backup は、 以外の AWS 環境で実行するバックアップを管理しません AWS Backup。したがって、ビジネスおよび規制のコンプライアンス要件に対して一元化された end-to-end ソリューションが必要な場合は、 AWS Backup 今すぐ の使用を開始してください。

機能の概要

AWS Backup には、次のような多くの機能があります。

一元化されたバックアップ管理

AWS Backup には、一元化されたバックアップコンソール、一連のバックアップ APIsが用意されており、アプリケーションが使用する AWS サービス全体のバックアップを管理できます。 AWS Command Line Interface AWS CLIを使用すると AWS Backup、バックアップ要件を満たすバックアップポリシーを一元管理できます。その後、 AWS のサービス間で AWS リソースに適用して、アプリケーションデータを一貫性と準拠性のある方法でバックアップできます。 AWS Backup 一元化されたバックアップコンソールは、バックアップとバックアップアクティビティログの統合ビューを提供するため、バックアップの監査とコンプライアンスの確保が容易になります。

ポリシーベースのバックアップ

では AWS Backup、バックアッププラン と呼ばれるバックアップポリシーを作成できます。これらのバックアッププランを使用してバックアップ要件を定義し、使用する AWS サービス全体で保護するリソースに適用 AWS します。特定のビジネスおよび規制関連のコンプライアンス要件を満たす個別のバックアップ計画を作成できます。これにより、各 AWS リソースが要件に従ってバックアップされます。バックアップ計画を使用すると、スケーラブルな方法で、組織全体およびアプリケーション全体にバックアップ戦略を簡単に適用できます。

バックアッププランのすべての設定オプションについては、「バックアッププランのオプションと設定」を参照してください。

タグベースのバックアップポリシー

を使用して AWS Backup 、 AWS リソースにバックアッププランを適用するには、タグ付けなど、さまざまな方法を使用できます。タグ付けにより、すべてのアプリケーションにバックアップ戦略を簡単に実装し、すべての AWS リソースがバックアップおよび保護されるようにできます。 AWS タグは、 AWS リソースを整理および分類するための優れた方法です。 AWS タグとの統合により、リソースの AWS グループにバックアッププランをすばやく適用できるため、一貫性のある準拠した方法でバックアップされます。

リソースをバックアッププランに割り当てるすべての方法については、「バックアッププランへのリソースの割り当て」を参照してください。

ライフサイクル管理ポリシー

AWS Backup を使用すると、低コストのコールドストレージ階層にバックアップを保存することで、バックアップストレージコストを最小限に抑えながら、コンプライアンス要件を満たすことができます。また、定義したスケジュールに従ってウォームストレージからコールドストレージにバックアップを自動的に移行させる、ライフサイクルポリシーを設定できます。

コールドストレージに移行できるリソースのリストについては、「リソース別の機能の可用性」を参照してください。バックアッププランでコールドストレージを有効にする手順については、「ライフサイクルとストレージ階層」を参照してください。

リージョン間のバックアップ

を使用すると AWS Backup、バックアップを複数の異なる にオンデマンド AWS リージョン でコピーすることも、スケジュールされたバックアッププランの一部として自動的にコピーすることもできます。リージョン間のバックアップは、本番稼働用データから最小限の距離だけ離してバックアップを保存するビジネス継続性またはコンプライアンス要件がある場合に特に役立ちます。詳細については、「AWS リージョン間でのバックアップコピーの作成」を参照してください。

アカウント間管理およびアカウント間バックアップ

を使用して AWS Backup 、 AWS Organizations構造 AWS アカウント 内のすべてのバックアップを管理できます。アカウント間管理では、バックアップポリシーを自動的に使用して、組織内の AWS アカウント 全体にバックアッププランを適用できます。これにより、コンプライアンスとデータ保護が大規模に効率化され、運用上のオーバーヘッドが削減されます。また、個々のアカウント間でバックアッププランを手動で複製する必要がなくなります。詳細については、「複数の AWS アカウントにまたがる AWS Backup リソースの管理」を参照してください。

管理構造 AWS アカウント 内の複数の異なる AWS Organizations にバックアップをコピーすることもできます。この方法で、単一のリポジトリアカウントにバックアップを「ファンイン」し、復元力を高めるために「ファンアウト」バックアップを実行できます。「AWS アカウント間でのバックアップコピーの作成」を参照してください。

アカウント間管理とアカウント間バックアップ機能を使用する前に、 AWS Organizationsで既存の組織構造を設定しておく必要があります。組織単位 (OU) は、単一のエンティティとして管理できるアカウントのグループです。 AWS Organizations は、組織単位にグループ化して単一のエンティティとして管理できるアカウントのリストです。

Audit Manager による AWS Backup 監査とレポート

AWS Backup Audit Manager は、 全体のバックアップのデータガバナンスとコンプライアンス管理を簡素化するのに役立ちます AWS。 AWS Backup Audit Manager には、組織の要件に合わせてカスタマイズ可能なコントロールが組み込まれています。これらのコントロールを使用して、バックアップアクティビティとリソースを自動的に追跡することもできます。

AWS Backup Audit Manager は、定義したコントロールにまだ準拠していない特定のアクティビティやリソースを見つけるのに役立ちます。また、日次レポートが生成され、経時的にコントロールが遵守されている証拠を示すために使用できます。

バックアップコンプライアンスを全体的なコンプライアンス体制に含めるには、 AWS Backup Audit Manager の検出結果を に自動的にインポートします AWS Audit Manager。

増分バックアップ

AWS Backup は、定期的なバックアップを段階的に効率的に保存します。 AWS リソースの最初のバックアップは、データの完全なコピーをバックアップします。連続する増分バックアップごとに、AWS リソースへの変更のみがバックアップされます。増分バックアップにより、頻繁なバックアップのデータ保護とストレージコストを最小限に抑えることができます。

増分バックアップをサポートするリソースのリストについては、「リソース別の機能の可用性」を参照してください。。

フル AWS Backup 管理

一部のリソースタイプは、フル AWS Backup 管理をサポートしています。フル AWS Backup 管理には次のような利点があります。

- 独立した暗号化。ソースリソースと同じ暗号化キーを使用する代わりに、 AWS Backup ボールトの KMS キーを使用してバックアップ AWS Backup を自動的に暗号化します。これにより、防衛のレイヤーが増加します。詳細については、「でのバックアップの暗号化 AWS Backup」を参照してください。
- **awsbackup** Amazon リソースネーム (ARN) Backup ARN は `arn:aws:source-resource` の代わりに `arn:aws:backup` で始まります。これにより、送信元リソースではなく、バックアップに特に適用されるアクセスポリシーを作成できます。詳細については、「アクセスコントロール」を参照してください。
- 一元化されたバックアップ請求および Cost Explorer のコスト配分タグ。料金 AWS Backup （ストレージ、データ転送、復元、早期削除を含む) は、サポートされている各リソースの下ではなく、 Amazon Web Services 請求書の「バックアップ」の下に表示されます。Cost Explorer のコスト配分タグを使用して、バックアップコストを追跡および最適化することもできます。詳細については、「メータリング、コスト、および請求」を参照してください。

フル AWS Backup 管理の対象となるリソースタイプを確認するには、「」を参照してくださいリソース別の機能の可用性。

バックアップアクティビティモニタリング

AWS Backup は、 AWS サービス全体のバックアップおよび復元アクティビティの監査を簡素化するダッシュボードを提供します。 AWS Backup コンソールを数回クリックするだけで、最近のバックアップジョブのステータスを表示できます。 AWS サービス間でジョブを復元して、 AWS リソースが適切に保護されるようにすることもできます。

AWS Backup は、Amazon CloudWatch および Amazon と統合されています EventBridge。CloudWatch では、メトリクスを追跡し、アラームを作成できます。 EventBridge では、 AWS Backup イベントを表示およびモニタリングできます。詳細については、「 を使用したイベントのモニタリング AWS Backup EventBridge」および「 を使用した AWS Backup メトリクスのモニタリング CloudWatch」を参照してください。

AWS Backup は と統合されています AWS CloudTrail。 CloudTrail はバックアップアクティビティログの統合ビューであり、リソースのバックアップ方法を迅速かつ簡単に監査できます。 AWS Backup は Amazon Simple Notification Service (Amazon SNS) とも統合されているため、バックアップが成功したときや復元が開始されたときなどのバックアップアクティビティ通知が提供されます。詳細については、「 を使用した AWS Backup API コールのログ記録 CloudTrail」およびAmazon SNSを使用してイベントを追跡 AWS Backup する」を参照してください。

バックアップ保管庫のデータの保護

各 AWS Backup バックアップのコンテンツはイミュータブルです。つまり、誰もそのコンテンツを変更することはできません。 AWS Backup はバックアップボールトでバックアップを保護し、ソースインスタンスから安全に分離します。たとえば、ソースの Amazon EC2 インスタンスと Amazon EBS ボリュームを削除した場合でも、保管庫は、選択したライフサイクルポリシーに従って Amazon EC2 および Amazon EBS バックアップを保持します。

バックアップ保管庫にはリソースベースのアクセスポリシーが用意されており、誰がバックアップにアクセスできるかを定義します。バックアップ保管庫のアクセスポリシーを定義して、そのボールト内のバックアップに対してアクセス許可を持つユーザーと実行できるアクションを定義できます。これにより、 AWS サービス間のバックアップへのアクセスを簡単かつ安全に制御できます。の AWS およびカスタマー管理ポリシーを確認するには AWS Backup、「 の 管理ポリシー AWS Backup」を参照してください。

AWS Backup ボールトロックを使用すると、誰でも (自分を含む) がバックアップを削除したり、保持期間を変更したりしないようにできます。 AWS Backup ボールトロックはwrite-once-read-many、 (WORM) モデルを適用し、防御に別の防御レイヤーを深く追加するのに役立ちます。開始するには、「AWS Backup ボールトロック」を参照してください。

コンプライアンス義務のサポート

AWS Backup は、グローバルコンプライアンスの義務を満たすのに役立ちます。 AWS Backup は、以下の AWS コンプライアンスプログラムの範囲内にあります。

- フェドランプ高
- GDPR
- SOC 1、2、および 3
- PCI
- HIPAA
- そのほか多数

開始

の詳細については AWS Backup、「」から始めることをお勧めしますの開始方法 AWS Backup。

サポートされている AWS リソースとアプリケーション

以下は、 を使用してバックアップおよび復元できる AWS リソースとサードパーティーアプリケーションです AWS Backup。詳細については、「the section called “機能を利用できるリージョン”」を参照してください。

サービス	サポートされているリソースタイプ
Amazon Elastic Compute Cloud (Amazon EC2)	Amazon EC2 インスタンス (Instance Store-Backed AMI を除く)
Amazon Simple Storage Service (Amazon S3)	Amazon S3 データ
Amazon Elastic Block Store (Amazon EBS)	Amazon EBS ボリューム
Amazon DynamoDB	Amazon DynamoDB テーブル
Amazon Relational Database Service (Amazon RDS)	Amazon RDS データベースインスタンス (すべてのデータベースエンジンを含む)、マルチアベイラビリティゾーンクラスター
Amazon Aurora	Aurora クラスター
Amazon Elastic File System (Amazon EFS)	Amazon EFS ファイルシステム
FSx for Lustre	FSx for Lustre ファイルシステム
FSx for Windows File Server	FSx for Windows File Server ファイルシステム
Amazon FSx for NetApp ONTAP	FSx for ONTAP ファイルシステム
Amazon FSx for OpenZFS	FSx for OpenZFS ファイルシステム

サービス	サポートされているリソースタイプ
AWS Storage Gateway（ボリュームゲートウェイ）	AWS Storage Gateway ボリューム
Amazon DocumentDB	Amazon DocumentDB インスタンスベースのクラスター
Amazon Neptune	Amazon Neptune クラスター
Amazon Redshift	Amazon Redshift クラスター
Amazon Timestream	Amazon Timestream テーブル
上の VMware Cloud™ AWS	上の VMware Cloud™ 仮想マシン AWS
上の VMware Cloud™ AWS Outposts	上の VMware Cloud™ 仮想マシン AWS Outposts
AWS CloudFormation	AWS CloudFormation スタック
SAP HANA データベース	Amazon EC2 インスタンスでの SAP HANA データベース

料金

では AWS Backup、バックアップストレージ、復元されたデータ、復元テスト、クロスリージョンデータ転送、Audit Manager AWS Backup に対して料金が発生します。詳細については、「AWS Backup の料金」を参照してください。

AWS Backup 機能の可用性

AWS Backup 機能は、リソース および に従って提供されます AWS リージョン。次のセクションと表を使用して、機能の可用性を判断できます。

内容

- による機能の可用性 AWS リージョン
- がサポートするサービス AWS リージョン

すべてのサポートされているリソースで使用できる機能

AWS Backup では、サポートされている AWS サービスおよびサポートされているサードパーティーアプリケーションに対して、次の機能を提供しています。特に明記されていない限り、特定の機能やサービスのサポートを想定しないでください。

- バックアップスケジュールと保存管理の自動化
- バックアップモニタリングの一元化
- 暗号化バックアップ
- 増分バックアップ
- によるクロスアカウント管理 AWS Organizations
- AWS Backup Audit Manager による自動バックアップ監査とレポート
- AWS Backup ボールトロックを使用した Write-Once、Read-Many (WORM)

リソース別の機能の可用性

特定のリージョンでサポートされている AWS サービス AWS Backup で を使用するには、そのサービスがリージョンで利用可能である必要があります。リージョンでのサービスの可用性を確認するには、 のサービスエンドポイントを表示しますAWS 全般のリファレンス。

AWS Backup が をサポート	リージョン間のバックアップ	アカウント間のバックアップ	AWS Backup Audit Manager	増分バックアップ	継続的なバックアップと point-in-time 復元	フル管理	コールドストレージへのライフサイクル	項目レベルの復元 [1]	復元テスト
Amazon EC2	✓	✓	✓	✓					✓

AWS Backup が をサポート	リージョン間のバックアップ	アカウント間のバックアップ	AWS Backup Audit Manager	増分バックアップ	継続的なバックアップと point-in-time 復元	フル管理	コールドストレージへのライフサイクル	項目レベルの復元 [1]	復元テスト
Amazon S3	✓	✓	✓	✓	✓	✓		✓	✓
Amazon EBS	✓	✓	✓	✓			✓		✓
Amazon RDS 単一インスタンス	✓ [3]	✓ [3]	✓ [4]	✓	✓				✓
Amazon RDS クラスター	✓ [3]	✓ [3]	✓ [4]	✓					✓
Amazon Aurora	✓ [3]	✓ [3]	✓	✓ [6]	✓				✓
Amazon EFS	✓	✓	✓	✓		✓	✓	✓	✓
FSx for Lustre	✓	✓	✓	✓					✓

AWS Backup がをサポート	リージョン間のバックアップ	アカウント間のバックアップ	AWS Backup Audit Manager	増分バックアップ	継続的なバックアップと point-in-time 復元	フル管理	コールドストレージへのライフサイクル	項目レベルの復元 [1]	復元テスト
FSx for Windows File Server	✓	✓	✓	✓					✓
FSx for ONTAP			✓ [2]	✓					✓
FSx for OpenZFS	✓	✓	✓	✓					✓
AWS Storage Gateway	✓	✓	✓	✓					
Amazon DocumentDB	✓ [3]	✓ [3]	✓						✓
Amazon Neptune	✓ [3]	✓ [3]	✓						✓
Amazon Redshift								✓	
Timestream	✓	✓	✓	✓		✓	✓	✓	

AWS Backup がをサポート	リージョン間のバックアップ	アカウント間のバックアップ	AWS Backup Audit Manager	増分バックアップ	継続的なバックアップと point-in-time 復元	フル管理	コールドストレージへのライフサイクル	項目レベルの復元 [1]	復元テスト
Windows VSS	✓	✓	✓	✓					
仮想マシン	✓	✓	✓	✓		✓	✓	✓	
AWS CloudFormation テンプレート	✓	✓		✓ [5]		✓	✓ [5]		
Amazon Dynamo			✓						✓
AWS Backup 高度な機能ありの Dynamo	✓	✓	✓			✓	✓		✓

AWS Backup がをサポート	リージョン間のバックアップ	アカウント間のバックアップ	AWS Backup Audit Manager	増分バックアップ	継続的なバックアップと point-in-time 復元	フル管理	コールドストレージへのライフサイクル	項目レベルの復元 [1]	復元テスト
Amazon EC2 インスタンスでの SAP HANA データベース				✓	✓	✓	✓		

リソースタイプによっては、継続的バックアップ機能と、クロスリージョンおよびクロスアカウントコピーの両方が可能なリソースタイプがあります。継続的バックアップのクロスリージョンコピーまたはクロスアカウントコピーが作成されると、コピーされた復旧ポイント (バックアップ) はスナップショット (定期的) バックアップになります。Amazon RDS と Amazon S3 は増分スナップショットコピーをサポートします。Amazon Aurora はフルスナップショットコピーのみをサポートします。これらのコピーには PITR (ポイントインタイムリカバリ) は使用できません。

[1] 項目レベルの復元の「項目」は、サポートされているリソースによって異なります。例えば、ファイルシステム項目はファイルまたはディレクトリであり、S3 項目は S3 オブジェクトです。VMware 項目はディスクです。詳細については、サポートされているリソースの「バックアップの復元」セクションを参照してください。

[2] AWS Backup Audit Manager は、クロスアカウントコピー とクロスリージョンコピー を除くすべてのコントロールでこのリソースをサポートします。

[3] RDS、Aurora、DocumentDB、Neptune は、クロスリージョンバックアップとクロスアカウントバックアップの両方を実行する単一のコピーアクションをサポートしていません。どちらかを選択することができます。 AWS Lambda スクリプトを使用して、最初のコピーの完了をリッスンし、2 番目のコピーを実行してから、最初のコピーを削除することもできます。RDS マルチアベイラビリ

ティゾーン (マルチ AZ) データベースインスタンスはコピーできますが、マルチ AZ クラスターは現在、クロスリージョンコピーやクロスアカウントコピーをサポートしていません。詳細については、特定のリソースとのクロスリージョンコピーに関する考慮事項「」を参照してください。

[4] Backup Audit Manager がサポートされているリージョンについては、「RDS マルチアベイラビリティーゾーンのバックアップ」を参照してください。

[5] CloudFormation スタックバックアップ では、ネストされたリソースはソースリソースの機能を保持します。ただし、スタック内のリソースは、ポイントインタイム復元 (PITR) 機能 (Amazon S3 や Amazon RDS など) を保持しません。上記の行列内のプロパティは、スタック内のリソースではなく CloudFormation テンプレートにのみ適用されます。

[6] Aurora の場合、スナップショットはフルで、増分バックアップは PITR を通じて提供されます。

による機能の可用性 AWS リージョン

AWS Backup は、次のすべての で使用できます AWS リージョン。 AWS Backup 機能は、次の表に特に明記されていない限り、これらのすべてのリージョンで使用できます。

AWS Backup が をサポート	リージョン間のバックアップ	アカウント間管理	アカウント間バックアップ	AWS Backup Audit Manager とジョブダッシュボード	復元テスト
米国東部 (バージニア北部)	✓	✓	✓	✓	✓
米国東部 (オハイオ)	✓	✓	✓	✓	✓
米国西部 (北カリフォルニア)	✓	✓	✓	✓	✓
米国西部 (オレゴン)	✓	✓	✓	✓	✓

AWS Backup が をサポート	リージョン間のバックアップ	アカウント間管理	アカウント間バックアップ	AWS Backup Audit Manager とジョブダッシュボード	復元テスト
アフリカ (ケープタウン)	✓		✓	✓	✓
アジアパシフィック (香港)	✓		✓	✓	✓
アジアパシフィック (ハイデラバード)	✓		✓		✓
アジアパシフィック (ジャカルタ)	✓		✓		✓
アジアパシフィック (メルボルン)	✓		✓		✓
アジアパシフィック (ムンバイ)	✓	✓	✓	✓	✓
アジアパシフィック (大阪)	✓	✓	✓		✓
アジアパシフィック (ソウル)	✓	✓	✓	✓	✓

AWS Backup が をサポート	リージョン間のバックアップ	アカウント間管理	アカウント間バックアップ	AWS Backup Audit Manager とジョブダッシュボード	復元テスト
アジアパシフィック (シンガポール)	✓	✓	✓	✓	✓
アジアパシフィック (シドニー)	✓	✓	✓	✓	✓
アジアパシフィック (東京)	✓	✓	✓	✓	✓
カナダ (中部)	✓	✓	✓	✓	✓
カナダ西部 (カルガリー)	✓ (Amazon S3 を除く)		✓		
中国 (北京)	✓				
中国 (寧夏)	✓				
欧州 (フランクフルト)	✓	✓	✓	✓	✓
欧州 (アイルランド)	✓	✓	✓	✓	✓
欧州 (ロンドン)	✓	✓	✓	✓	✓
欧州 (ミラノ)	✓		✓	✓	✓
欧州 (パリ)	✓	✓	✓	✓	✓

AWS Backup が をサポート	リージョン間のバックアップ	アカウント間管理	アカウント間バックアップ	AWS Backup Audit Manager とジョブダッシュボード	復元テスト
欧州 (スペイン)	✓		✓		✓
欧州 (ストックホルム)	✓	✓	✓	✓	✓
欧州 (チューリッヒ)	✓		✓		✓
イスラエル (テルアビブ)	✓		✓		
中東 (バーレーン)	✓		✓	✓	✓
中東 (アラブ首長国連邦)	✓		✓		✓
南米 (サンパウロ)	✓	✓	✓	✓	✓
AWS GovCloud (米国東部)	✓	✓	✓	✓	
AWS GovCloud (米国西部)	✓	✓	✓	✓	

中国 (北京) および中国 (寧夏) は、両リージョン間のクロスリージョンコピーをサポートしています。これらの地域から他の地域への、または他の地域からこれらの地域へのクロスリージョンコピー

はサポートされていません。クロスアカウントコピーは、これらのリージョンではサポートされていません。

ジョブダッシュボードは、 AWS GovCloud （ 米国東部) および AWS GovCloud （ 米国西部) では使用できません。ジョブダッシュボードの集約は、クロスアカウント管理と AWS Backup Audit Manager をサポートするリージョンでのみ使用できます。

Amazon FSx for Windows File Server および Amazon Neptune は、オプトインリージョンでのクロスリージョンバックアップコピーをサポートしていません。

がサポートするサービス AWS リージョン

AWS Backup は、サポートされているすべてのリージョンで以下をサポートします。

- Aurora
- DynamoDB
- AWS Backup 高度な機能を備えた DynamoDB
- Amazon EBS
- Amazon EC2
- Amazon EFS
- Amazon Redshift
- Amazon RDS

次の表は、リージョン AWS のサービス 別の他の AWS Backup のサポートを示しています。

リージョンおよびサービス	Amazon FSx	EC2 インスタンス上の SAP HANA	Amazon S3	Storage Gateway	Amazon Timestream	VMware と Backup ゲートウェイ
米国東部 (バージニア北部)	✓	✓	✓	✓	✓	✓
米国東部 (オハイオ)	✓	✓	✓	✓	✓	✓

リージョンおよびサービス	Amazon FSx	EC2 インスタンス上の SAP HANA	Amazon S3	Storage Gateway	Amazon Timestream	VMware と Backup ゲートウェイ
米国西部（北カリフォルニア）	Windows、Lustre、ONTAP	✓	✓	✓		✓
米国西部（オレゴン）	Windows、Lustre、ONTAP	✓	✓	✓	✓	✓
アフリカ (ケープタウン)	Windows、Lustre、ONTAP	✓	✓ [1]	✓		✓
アジアパシフィック (香港)	✓	✓	✓ [1]	✓		✓
アジアパシフィック (ハイデラバード)	Windows、Lustre、ONTAP		✓ [1]	✓		
アジアパシフィック (ジャカルタ)	Windows、Lustre、ONTAP		✓	✓		
アジアパシフィック (メルボルン)	Windows、Lustre、ONTAP		✓ [1]	✓		

リージョンおよびサービス	Amazon FSx	EC2 インスタンス上の SAP HANA	Amazon S3	Storage Gateway	Amazon Timestream	VMware と Backup ゲートウェイ
アジアパシフィック (ムンバイ)	✓	✓	✓	✓		✓
アジアパシフィック (大阪)	Windows、Lustre	✓	✓ [1]	✓		✓
アジアパシフィック (ソウル)	✓	✓	✓	✓		✓
アジアパシフィック (シンガポール)	✓	✓	✓	✓		✓
アジアパシフィック (シドニー)	✓	✓	✓	✓	✓	✓
アジアパシフィック (東京)	✓	✓	✓	✓	✓	✓
カナダ (中部)	✓	✓	✓	✓		✓
カナダ西部 (カルガリー)						

リージョンおよびサービス	Amazon FSx	EC2 インスタンス上の SAP HANA	Amazon S3	Storage Gateway	Amazon Timestream	VMware と Backup ゲートウェイ
中国 (北京)	Windows; Lustre		✓ [1]	✓	✓	
中国 (寧夏)	Windows、Lustre		✓ [1]	✓	✓	
欧州 (フランクフルト)	✓	✓	✓	✓	✓	✓
欧州 (アイルランド)	✓	✓	✓	✓	✓	✓
欧州 (ロンドン)	✓	✓	✓	✓		✓
欧州 (ミラノ)	Windows、Lustre、ONTAP	✓	✓ [1]	✓		✓
欧州 (パリ)	Windows、Lustre、ONTAP	✓	✓	✓		✓
欧州 (スペイン)	Windows、Lustre、ONTAP		✓ [1]	✓		
欧州 (ストックホルム)	✓	✓	✓	✓		✓

リージョンおよびサービス	Amazon FSx	EC2 インスタンス上の SAP HANA	Amazon S3	Storage Gateway	Amazon Timestream	VMware と Backup ゲートウェイ
欧州 (チューリッヒ)	Windows、Lustre、ONTAP		✓ [1]	✓		
イスラエル (テルアビブ)	Windows、Lustre、ONTAP		✓ [1]	✓		
中東 (バーレーン)	Windows、Lustre、ONTAP	✓	✓ [1]	✓		✓
中東 (アラブ首長国連邦)			✓ [1]	✓		
南米 (サンパウロ)		✓	✓	✓		✓
AWS GovCloud (米国西部)	Windows、Lustre、ONTAP		✓ [1]	✓		✓
AWS GovCloud (米国東部)	Windows、Lustre、ONTAP		✓ [1]	✓		✓

Amazon FSx のチェックは、FSx for Windows File Server、FSx for Lustre、FSx for ONTAP、および FSx for OpenZFS がすべて によってそのリージョンでサポートされていることを示します AWS Backup。それ以外の場合は、サポートされている設定が一覧表示されます。

[1] クロスリージョンコピーとクロスアカウントコピーはサポートされていません。

AWS Backup: 仕組み

AWS Backup はフルマネージド型のバックアップサービスで、 AWS サービス間でデータのバックアップを簡単に一元化および自動化できます。では AWS Backup、バックアッププラン と呼ばれるバックアップポリシーを作成できます。これらのプランを使用して、データのバックアップ頻度やバックアップを保持する期間など、バックアップ要件を定義できます。

AWS Backup では、リソースにタグを付ける AWS だけでバックアッププランを適用できます。AWS Backup これにより、定義したバックアッププランに従って AWS リソースが自動的にバックアップされます。

以下のセクションでは、 の AWS Backup 仕組み、実装の詳細、セキュリティ上の考慮事項について説明します。

トピック

- がサポートされている AWS サービスと AWS Backup 連携する方法
- メータリング、コスト、および請求
- AWS Backup ブログ、動画、チュートリアル、その他のリソース

がサポートされている AWS サービスと AWS Backup 連携する方法

が AWS Backupサポートするサービスの中には、独自のスタンドアロンバックアップ機能 AWS を提供するものもあります。これらの機能は、 AWS Backupを使用するかどうかに関係なく利用できます。　ただし、他の AWS サービスが作成するバックアップは、 による中央ガバナンスには使用できません AWS Backup。

サポートされているすべての サービスのデータ保護を一元管理 AWS Backup するように を設定するには、 でそのサービスを管理することをオプトインし AWS Backup、オンデマンドバックアップを作成するか、バックアッププランを使用してバックアップをスケジュールし、バックアップをバックアップボールトに保存する必要があります。

トピック

- による サービスの管理にオプトインする AWS Backup
- Amazon S3 データの操作

- VMware 仮想マシンの操作
- Amazon DynamoDB の操作
- Amazon FSx ファイルシステムの操作
- Amazon EC2 の操作
- Amazon EFS の操作
- Amazon EBS の操作
- Amazon RDS と Aurora の操作
- の使用 AWS BackInt
- の使用 AWS Storage Gateway
- Amazon DocumentDB の操作
- Amazon Neptune の操作
- Amazon Timestream の使用
- の使用 AWS Organizations
- の使用 AWS CloudFormation
- SAP および SAP HANA AWS BackInt AWS Systems Manager での の使用
- AWS サービスが独自のリソースをバックアップする方法

による サービスの管理にオプトインする AWS Backup

新しい AWS サービスが利用可能になったら、 を有効に AWS Backup してそれらのサービスを使用する必要があります。有効になっていないサービスのリソースを使用して、オンデマンドバックアップまたはバックアッププランを作成しようとすると、エラーメッセージが表示され、プロセスを完了できません。

AWS Backup コンソールには、バックアッププランにリソースタイプを含める方法として、バックアッププランにリソースタイプを明示的に割り当てるか、すべてのリソースを含めるという 2 つの方法があります。これらの選択がサービスオプトインとどのように連携するかを理解するには、以下のポイントを参照してください。

- リソースの割り当てがタグのみに基づいている場合は、サービスオプトイン設定が適用されます。
- リソースタイプがバックアッププランに明示的に割り当てられている場合、その特定のサービスでオプトインが有効になっていなくても、バックアップに含まれます。これは、Aurora、Neptune、および Amazon DocumentDB には適用されません。これらのサービスを含めるには、オプトインを有効にする必要があります。

- リソース割り当てでリソースタイプとタグの両方が指定されている場合、指定されたリソースタイプが最初にフィルタリングされ、タグはそれらのリソースをさらにフィルタリングします。

  ほとんどのリソースタイプでは、サービスオプトイン設定は無視されます。ただし、Aurora、Neptune、Amazon DocumentDB にはサービスオプトインが必要です。
- Amazon FSx for NetApp ONTAP では、タグベースのリソース選択を使用する場合は、ファイルシステム全体ではなく個々のボリュームにタグを適用します。

サービスオプトイン設定は、リージョンに固有です。アカウントがリージョンで を使用する AWS Backup (バックアップボールトまたはバックアッププランを作成する) 場合、そのアカウントは、その時点でリージョン AWS Backup で によってサポートされているすべてのリソースタイプに自動的にオプトインされます。後日そのリージョンに追加されたサポート対象サービスは、バックアッププランに自動的に含まれません。サポートされたら、これらのリソースタイプをオプトインできます。

で使用するサービスを設定するには AWS Backup

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで [設定] を選択します。
3. [サービスのオプトイン] ページで、[リソースを設定] を選択します。
4. トグルスイッチを使用して、 で使用されるサービスを有効または無効にします AWS Backup。

   > **Important**
   >
   > RDS、Aurora、Neptune、および DocumentDB は同じ Amazon リソースネーム (ARN) を共有します。でこれらのリソースタイプの 1 つを管理するようにオプトインすると、バックアッププランに割り当てるときにすべてのリソースタイプに AWS Backup オプトインされます。いずれにしても、オプトイン状況を正確に表すために、すべてオプトインすることをおすすめします。

5. [確認] を選択します。

Amazon S3 データの操作

AWS Backup は、Amazon S3 バックアップのフルマネージドバックアップと復元を提供します。詳細については、「Amazon S3 バックアップ」を参照してください。

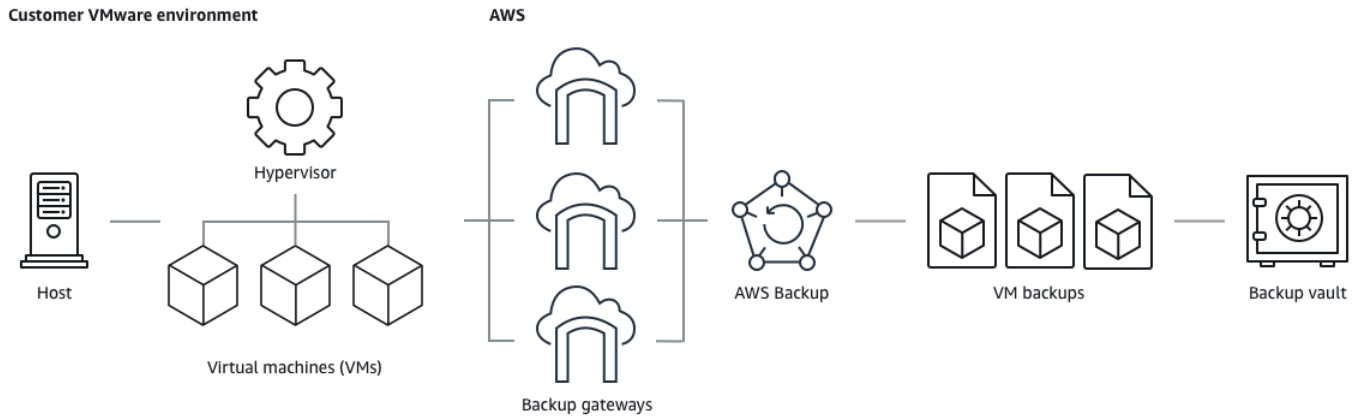
- リソースのバックアップ方法: の開始方法 AWS Backup
- を使用して Amazon S3 データを復元する方法 AWS Backup: S3 データの復元

S3 データの詳細については、「Amazon S3 ドキュメント」を参照してください。

VMware 仮想マシンの操作

AWS Backup は、オンプレミスの VMware 仮想マシン (VMs VMware Cloud™ (VMC) の VMs の一元化された自動データ保護をサポートします AWS。オンプレミスおよび VMC 仮想マシンから にバックアップできます AWS Backup。その後、 からオンプレミスまたは VMC AWS Backup のいずれかに復元できます。

Backup ゲートウェイは、VMware VMs にデプロイして に接続するためのダウンロード可能な AWS Backup ソフトウェアです AWS Backup。ゲートウェイは VM 管理サーバーに接続して VM を検出し、VM を検出し、データを暗号化し、効率的にデータを AWS Backupに転送します。次の図は、Backup ゲートウェイが VM に接続する方法を示しています。



- リソースのバックアップ方法: 仮想マシンのバックアップ
- VM リソースを復元する方法: を使用した仮想マシンの復元 AWS Backup

Amazon DynamoDB の操作

AWS Backup は、Amazon DynamoDB テーブルのバックアップと復元をサポートしています。DynamoDB は、高速で予測可能なパフォーマンスとシームレスな拡張性を特長とするフルマネージド NoSQL データベースサービスです。

の起動以降、 AWS Backup は常に DynamoDB をサポートしています。2021 年 11 月より、DynamoDB バックアップの高度な機能 AWS Backup も導入されました。これらの高度な機能には、 AWS リージョン アカウントと アカウント間でのバックアップのコピー、コールドストレージへのバックアップの階層化、アクセス許可とコスト管理のためのタグの使用などがあります。

2021 年 11 月以降にオンボーディングする新規 AWS Backup お客様は、高度な DynamoDB バックアップ機能がデフォルトで有効になります。

既存のすべての AWS Backup お客様が DynamoDB の高度な機能を有効にすることをお勧めします。高度な機能を有効にした後のウォームバックアップストレージに違いがないので、コールドストレージへのバックアップの階層化によりコストを節約したり、コスト配分タグを使用してコストを最適化できます。

高度な機能の完全な一覧と、その有効化の方法については、「アドバンスト DynamoDB バックアップ」を参照してください。

- リソースのバックアップ方法: の開始方法 AWS Backup
- DynamoDB リソースを復元する方法: Amazon DynamoDB テーブルの復元

DynamoDB の詳細については、Amazon DynamoDB 開発者ガイドの「Amazon DynamoDB とは」を参照してください。

Amazon FSx ファイルシステムの操作

AWS Backup は、Amazon FSx ファイルシステムのバックアップと復元をサポートしています。Amazon FSx は、ワークロードのネイティブ互換性と機能セットを備えたフルマネージド型のサードパーティーファイルシステムを提供します。 は、Amazon FSx の組み込みバックアップ機能 AWS Backup を使用します。したがって、 AWS Backup コンソールで取得されるバックアップには、Amazon FSx コンソールで取得されるバックアップと同じレベルのファイルシステムの一貫性およびパフォーマンス、復元オプションがあります。

AWS Backup を使用してこれらのバックアップを管理すると、無制限の保持オプションや、1 時間ごとにスケジュールされたバックアップを作成する機能などの追加機能を利用できます。さらに、ソースファイルシステムが削除された後でも、 はバックアップ AWS Backup を保持します。これにより、偶発的または悪意のある削除から保護されます。

バックアップポリシーを設定し、他の AWS サービスのサポートも拡張する中央バックアップコンソールからバックアップタスクをモニタリングする場合は、 AWS Backup を使用して Amazon FSx ファイルシステムを保護します。

- リソースのバックアップ方法: の開始方法 AWS Backup
- Amazon FSx リソースを復元する方法: FSx ファイルシステムの復元

Amazon FSx ファイルシステムの詳細については、「Amazon FSx ドキュメント」を参照してください。

Amazon EC2 の操作

AWS Backup は Amazon EC2 インスタンスをサポートします。

- リソースのバックアップ方法: の開始方法 AWS Backup
- Amazon EC2 リソースを復元する方法: Amazon EC2 インスタンスの復元

Amazon EBS ボリュームを含む EC2 インスタンス全体を含むオンデマンドバックアップジョブをスケジュールまたは実行できます。したがって、ルートボリューム、データボリューム、インスタンスタイプやキーペアなどの一部のインスタンス設定など、Amazon EC2 インスタンス全体を単一の復旧ポイントから復元できます。

VSS 対応の Microsoft Windows アプリケーションをバックアップおよび復元することもできます。オンデマンドバックアップまたはスケジュールバックアップ計画の一部として、アプリケーション整合性バックアップのスケジュール設定、ライフサイクルポリシーの定義、整合性のとれたリストアを実行できます。詳細については、「Windows VSS バックアップの作成」を参照してください。

AWS Backup はEC2 インスタンスをいつでも再起動しません。

イメージとスナップショット

Amazon EC2 インスタンスをバックアップすると、 はルート Amazon EBS ストレージボリューム、起動設定、および関連するすべての EBS ボリュームのスナップショット AWS Backup を取得します。 は、インスタンスタイプ、セキュリティグループ、Amazon VPC、モニタリング設定、タグなど、EC2 インスタンスの特定の設定パラメータ AWS Backup を保存します。バックアップデータは、Amazon EBS ボリュームバックアップされた Amazon マシンイメージ (AMI) として保存されます。

を使用して管理 AWS Backup されている Amazon マシンイメージ (AMI) または Amazon EBS スナップショットを削除 AWS Backup し、Amazon EC2 ごみ箱を設定している場合、Amazon EC2 ごみ箱ポリシーに従ってイメージまたはスナップショットに料金が発生する可能性があります。Amazon EC2 ごみ箱のスナップショットとイメージは、ごみ箱から復元した場合 AWS Backup 、 によって管理されなくなり、 AWS Backup ポリシーによって管理されなくなります。

AWS Backup Amazon EBS スナップショットロックが適用されている AWS Backup マネージド Amazon EC2 AMI に関連付けられた マネージド Amazon EBS スナップショットおよびスナップショットは、スナップショットロック期間がバックアップライフサイクルを超える場合、リカバリポイントライフサイクルの一部として削除できない場合があります。この場合、復旧ポイントのステータスは EXPIRED になります。これらの復旧ポイントは、最初に Amazon EBS Snapshot Lock の解除を選択すると、手動で削除できます。

AWS Backup は、Amazon EC2 バックアップに関連付けられた EBS スナップショットを暗号化できます。これは、Amazon EC2 AMI のスナップショットを作成するときに、基盤となる EBS ボリュームに適用されるのと同じ暗号化を が AWS Backup 使用するのと似ており、元のインスタンスの設定パラメータは復元メタデータに保持されます。

スナップショットはボリュームから暗号化を取得し、対応するスナップショットにも同じ暗号化が適用されます。コピーされた AMI の EBS スナップショットは常に暗号化されます。コピー中に KMS キーを指定すると、指定されたキーが適用されます。KMS キーを指定しない場合、デフォルトの KMS キーが適用されます。

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」および「Amazon EBS ユーザーガイド」の「Amazon EBS 暗号化」を参照してください。 Amazon EC2

Amazon EFS の操作

AWS Backup は Amazon Elastic File System (Amazon EFS) をサポートしています。

- リソースのバックアップ方法: の開始方法 AWS Backup
- Amazon EFS リソースを復元する方法: Amazon EFS ファイルシステムの復元

Amazon EFS ファイルシステムの詳細については、Amazon Elastic File System ユーザーガイド」の「Amazon Elastic File System とは」を参照してください。

Amazon EBS の操作

AWS Backup は、Amazon Elastic Block Store (Amazon EBS) ボリュームをサポートします。

AWS Backup Amazon EBS スナップショットロックが適用されている AWS Backup マネージド Amazon EC2 AMI に関連付けられた マネージド Amazon EBS スナップショットおよびスナップショットは、スナップショットロック期間がバックアップライフサイクルを超える場合、リカバリポイントライフサイクルの一部として削除できない場合があります。この場合、復旧ポイントのステー

タスは EXPIRED になります。これらの復旧ポイントは、最初に Amazon EBS Snapshot Lock の解除を選択すると、手動で削除できます。

- リソースのバックアップ方法: の開始方法 AWS Backup
- Amazon EBS ボリュームを復元する方法: Amazon EBS ボリュームの復元

詳細については、「Amazon EBS ユーザーガイド」の「Amazon EBS ボリューム」を参照してください。

Amazon RDS と Aurora の操作

AWS Backup は、Amazon RDS データベースエンジンと Aurora クラスターをサポートします。

- リソースのバックアップ方法: の開始方法 AWS Backup
- Amazon RDS リソースを復元する方法: RDS データベースの復元
- Aurora クラスターを復元する方法: Amazon Aurora クラスターの復元

Amazon RDS の詳細については、Amazon RDS ユーザーガイドの「Amazon Relational Database Service とは」を参照してください。

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

> **Note**
>
> Amazon RDS コンソールからバックアップジョブを開始すると、Aurora クラスターのバックアップジョブと競合し、Backup ジョブが完了する前に期限切れになるエラーが発生する可能性があります。この問題が発生した場合は、 AWS Backupで長いバックアップウィンドウを構成します。

> **Note**
>
> RDS Custom for SQL Server および RDS Custom for Oracle は、現在、 AWS Backupによってサポートされていません。

> **Note**
>
> AWS は、Aurora で自動バックアップが有効になっており、Aurora 自動バックアップの保持期間が Aurora スナップショットの保持期間を超えている限り、バックアップボールト内に保存されている Aurora スナップショットには課金されません。バックアップボールト内のスナップショットは、スナップショットのデータベースが削除された場合に課金されます (誤って削除したり、Blue/Green デプロイ中に削除したりする場合があります)。
> 削除されたデータベースから大量のスナップショットや頻繁なバックアップを行うと、多額のストレージ料金が発生する可能性があります。AWS Backup 見積りツールにアクセスして、発生する可能性のある AWS Backup 料金を見積もります。

の使用 AWS BackInt

AWS Backup は AWS Backint と連携して、Amazon EC2 インスタンスでの SAP HANA データベースのバックアップと復元をサポートします。

- SAP HANA リソースのバックアップと復元の手順: SAP HANA Amazon EC2 インスタンスのバックアップと復元
- AWS Backint Agent をセットアップする: AWS Backint Agent for SAP HANA

の使用 AWS Storage Gateway

AWS Backup は Storage Gateway ボリュームゲートウェイをサポートします。Amazon EBS スナップショットを Storage Gateway ボリュームとして復元することもできます。

- リソースのバックアップ方法: の開始方法 AWS Backup
- Storage Gateway のリソースを復元する方法: Storage Gateway ボリュームの復元

Amazon DocumentDB の操作

AWS Backup は Amazon DocumentDB クラスターをサポートします。

- リソースのバックアップ方法: の開始方法 AWS Backup
- Amazon DocumentDB リソースを復元する方法: DocumentDB クラスターの復元。

Amazon Neptune の操作

AWS Backup は Amazon Neptune クラスターをサポートします。

- リソースのバックアップ方法: の開始方法 AWS Backup
- Amazon Neptune クラスターを復元する方法: Neptune クラスターの復元

Amazon Timestream の使用

AWS Backup は Amazon Timestream テーブルをサポートします。

- Timestream テーブルをバックアップする方法。
- Timestream テーブルを復元するする方法。

の使用 AWS Organizations

AWS Backup は と連携して AWS Organizations 、クロスアカウントのモニタリングと管理を簡素化します。

- Organizations での管理アカウントを作成する。
- クロスアカウント管理を有効にする。
- 委任された管理者のアカウントを指定し、ポリシーを委任する。

の使用 AWS CloudFormation

AWS Backup サポート AWS CloudFormation テンプレートとアプリケーションスタック

- AWS CloudFormation スタックバックアップ

SAP および SAP HANA AWS BackInt AWS Systems Manager での の使用

AWS Backup は AWS BackInt 、SAP HANA のバックアップおよび復元機能をサポートするために、SSM for SAP と連携します。

- Amazon EC2 インスタンス上の SAP HANA データベースのバックアップ
- AWS Systems Manager for SAP の使用を開始する

- AWS SAP HANA 用 Backint Agent

AWS サービスが独自のリソースをバックアップする方法

特定のサービスのバックアップおよび復元プロセス、特に復元中にその AWS サービスの新しいインスタンスを設定する必要がある場合は、技術ドキュメントを参照してください AWS 。以下は、ドキュメントのリストです。

- Amazon EC2 関連サービス
- Amazon EFS AWS Backup での の使用
- DynamoDB のオンデマンドバックアップと復元
- Amazon EBS スナップショット
- Amazon RDS DB インスタンスのバックアップと復元
  - DB クラスターのバックアップと復元の概要
- FSx for Windows File Server AWS Backup での の使用
- AWS Backup FSx for Lustre での の使用
- でのボリュームのバックアップ AWS Storage Gateway
- Amazon DocumentDB でのバックアップと復元
- Amazon Neptune クラスターのバックアップと復元

メータリング、コスト、および請求

AWS Backup 料金

現在の AWS Backup 料金は、 AWS Backup の料金で利用できます。

> **Important**
>
> 追加料金を回避するには、ウォームストレージ期間を「少なくとも 1 週間」に設定して、リテンションポリシーを構成します。
> たとえば、毎日のバックアップを取って 1 日保持するとします。さらに、保護されたリソースが非常に大きいため、バックアップが完了するまでに 1 日かかると仮定します。 は保持期間を 1 日に AWS Backup 実装し、バックアップジョブが完了するとバックアップをウォームストレージから削除します。翌日、ウォームストレージにバックアップがないため、 は増

分バックアップを作成 AWS Backup できません。この保存期間はベストプラクティスに従わなかったため、毎日フルバックアップを作成するリスクとコストがかかります。
詳細については AWS Support 、 にお問い合わせください。

AWS Backup 請求

リソースタイプがフル AWS Backup 管理をサポートしている場合、 AWS Backup アクティビティ (ストレージ、データ転送、復元、早期削除を含む) の料金は、 Amazon Web Services 請求書の「バックアップ」セクションに表示されます。フル AWS Backup 管理をサポートするサービスのリストについては、リソース別の機能の可用性表の「フル AWS Backup 管理」セクションを参照してください。

リソースタイプがフル AWS Backup 管理をサポートしていない場合、バックアップの AWS Backup ストレージコストなどのアクティビティの一部に、それぞれの AWS サービスによって請求が反映されます。

コピージョブの失敗

課金されるのは、コピー先のボールトに復旧ポイントが作成された後のみです。コピージョブが失敗し、復旧ポイントが作成されない場合は課金されません。

コスト配分タグ

コスト配分タグを使用して、詳細なレベルで AWS Backup コストを追跡および最適化し、 を使用してそれらのタグを表示およびフィルタリングできます AWS Cost Explorer。

コスト配分タグを使用するには、「AWS Backupを使用した Amazon EFS のコストの自動バックアップとバックアップコストの最適化」、および「コスト配分タグの使用」を参照してください。

AWS Backup Audit Manager の料金

AWS Backup Audit Manager は、コントロール評価の数に基づいて使用料を請求します。制御評価は、1 つのコントロールに対する 1 つのリソースの評価です。コントロール評価料金は AWS Backup 請求書に表示されます。現在の管理評価料金については、「AWS Backup 料金」を参照してください。

AWS Backup Audit Manager コントロールを使用するには、バックアップアクティビティを追跡するために AWS Config 記録を有効にする必要があります。記録された設定項目ごとに AWS Config 料金

が課金され、これらの料金は AWS Config 請求書に表示されます。現在の構成項目の記録された価格については、AWS Config 料金を参照してください。

Amazon Aurora の料金

Aurora の継続的バックアップに設定された保持期間 (最大 35 日間) の間、スナップショットにはストレージ料金は発生しません。この期間を過ぎて保持されたスナップショットは、フルバックアップとして課金されます。

AWS Backup ブログ、動画、チュートリアル、その他のリソース

の詳細については AWS Backup、以下を参照してください。

- を使用してオンプレミスの VMware 仮想マシンをバックアップおよび復元します AWS Backup。 オルムイワ・コヤとエゼキエル・オエリンデと (2022 年 6 月)。
- AWS Backup を使用して Amazon Aurora データベースを保護します。 クリス・ヘンドン、ブランドン・ルバドゥ、トーマス・リドルと (2022 年 5 月)。
- クロスアカウントとクロスリージョンバックアップによる、暗号化された Amazon RDS インスタンスの保護 エバン・ペックとサビス・ベンキタチャラパシーと (2022 年 5 月)。
- と を使用して、セキュリティ体制を自動化 AWS Backup および改善します AWS PrivateLink。ビラル・アラムと (2022 年 4 月)。
- 集約された毎日のクロスアカウントマルチリージョン AWS Backup レポートを取得します。ワリ・アクバリとサビス・ベンキタチャラパシー (2022 年 2 月) と。
- AWS Backup および を使用して、バックアップ結果の可視性を自動化します AWS Security Hub。カニシュク・マハジャンと (2022 年 1 月) 。
- でバックアップを保護するためのセキュリティのベストプラクティスの上位 10 件 AWS。オオユミ・イブクンと (2022 年 1 月) と。
- FSx for Lustre AWS を使用した での SAS グリッドの最適化 (および を使用したディザスタリカバリの最適化 AWS Backup) 。マット・セーガーとシェイ・ラットンと (2022 年 1 月)。
- Amazon Neptune のデータ保護とコンプライアンスを で一元化 AWS Backupします。ブライアン・オキーフと (2021 年 11 月)。
- AWS Backupで (MongoDB 互換で) Amazon DocumentDB のバックアップと復元を管理する。カルティク・ヴィジェイラガバンと (2021 年 11 月)。
- AWS Backup Audit Manager を使用してデータ保護ポリシーの監査を簡素化します。ジョーダン・ビョークマン、ハルシサ・プッタと (2021 年 11 月)。

- AWS Backup ボールトロック を使用してバックアップのセキュリティ体制を強化します。ロランド・ミラーと (2021 年 10 月)。
- AWS Backup 復元ジョブ でリソースタグを保持する方法。イブクン・オエウミ、アミー・シャー、サビス・Venkitachalapathy と (2021 年 9 月)。
- でサービスコントロールポリシーを使用してバックアップへのアクセスを管理する AWS Backup。サビス・ Venkitachalapathy、イブクン・オエウミと (2021 年 8 月)。
- を使用して、 AWS のサービス全体で大規模な集中バックアップを自動化します AWS Backup。イブクン・オエウミ、サビス・ Venkitachalapathyと (2021 年 7 月)。
- ブログ: AWS Backup と VSS を使用して Microsoft SQL Server のバックアップを簡素化する方法。シアーヴァシュ・イラニ、セファー・サミエイと (2021 年 7 月)。
- を使用してデータ復旧の検証を自動化します AWS Backup。マハンス・ジャヤデヴァと (2021 年 6 月)。
- AWS Backup ジョブ をモニタリングするための通知の設定。ヴァージル・エンネスと (2021 年 6 月)。
- AWS Backupを使用して Amazon EFS のバックアップを自動化し、バックアップコストを最適化する。プラチ・グプタ、ロヒット・ヴェルマと (2021 年 6 月)。
- Amazon EFS バックアップコストの管理 : コスト配分タグ AWS Backup のサポート。アディティヤ・マルヴァーダと (2021 年 5 月)。
- を使用して、アカウントとリージョン間で暗号化されたバックアップを作成して共有します AWS Backup。プラチ・グプタと (2021 年 5 月)。
- AWS Backup は、コンプライアンスとデータ保護のニーズに対して FedRAMP High が承認されました。アンディ・グライムズと (2021 年 5 月)。
- ZS Associates は、 を使用してバックアップ効率を向上させます AWS Backup。ミテシュ・ナイク、ヒラナンド・ムルチャンダニ、スシャント・ジャドハブと (2021 年 5 月)。
- チュートリアル: を使用した Amazon EBS のバックアップと復元 AWS Backup。ファティマ・カマルと (2021 年 4 月)。
- ビデオチュートリアル: バックアップのクロスリージョンコピーの管理。David と DeLuca (4 月 2021 年) 。
- AWS Tools for を使用して複数の AWS Backup 復旧ポイントを削除します PowerShell。シェリフ・タラートと (2021 年 4 月)。
- を使用した Amazon FSx のクロスリージョンおよびクロスアカウントバックアップ AWS Backup。アダム・ハンター、ファティマ・カマルと (2021 年 4 月)。

- の Amazon CloudWatch イベントとメトリクス AWS Backup。ロランド・ミラーと (2021 年 3 月)。
- チュートリアル: を使用した Amazon Relational Database Service (RDS) のバックアップと復元 AWS Backup。ファティマ・カマルと (2021 年 3 月)。
- を使用した Amazon RDS の P oint-in-time リカバリと継続的バックアップ AWS Backup。ケリー・グリフィンと (2021 年 3 月)。
- AWS Service Catalog AWS Backup を使用して を自動化します。John Husemorler を使用して (2021 年 1 月) 。
- AWS Backupを使用したクロスアカウントバックアップとクロスリージョンコピーでデータリカバリを保護する。シェール・サイモンと (2021 年 1 月)。
- AWS re:Invent recap: データ保護と への準拠 AWS Backup。ナンシー・ワンと (2020 年 12 月)。
- AWS Backup は、 AWS リソース全体で一元化されたデータ保護を提供します。ナンシー・ワンと (2020 年 11 月)。
- Tech Talk: AWS Backupでの大規模なデータ保護。カリーム・ビヘイリーと (2020 年 9 月)。
- を使用したクロスリージョンコピーによるクロスアカウント管理の一元化 AWS Backup。シェール・サイモンと (2020 年 9 月)。
- ビデオチュートリアル: AWS Organizations を使用して で大規模なバックアップを管理する AWS Backup。イルダル・シャラフェエフと (2020 年 7 月)。
- AWS Organizations を使用して、 でバックアップを大規模に管理します AWS Backup。ナンシー・ワン、アビ・ドラブキン、ガネーシュ・スンダレサン、ヴィカス・シャーと (2020 年 6 月)。
- を使用して Amazon EFS ファイルとフォルダを復旧します AWS Backup。エイブラール・フセイン、グルダス・パイと (2020 年 5 月)。
- Amazon EFS と AWS Backupを使用して自動バックアップをスケジュールする。ロブ・バーンズと (2019 年 12 月)。
- re:Invent Recording: AWS re:Invent 2019: Deep dive on AWS Backup ft. ラックスペース 。ナンシー・ワン、ジェイソン・パバオと (2019 年 12 月)。
- によるデータの保護 AWS Backup。アンソニー・フィオーレと (2019 年 7 月)。
- マーケティングビデオ: AWS Backupの紹介。2019 年 1 月。
- ビデオ: AWS Backupの概要 AWS トレーニングと認定。

を初めてセットアップ AWS する

AWS Backup を初めて使用する場合は、事前に以下のタスクを完了してください。

1. にサインアップする AWS
2. IAM ユーザーの作成
3. IAM ロールを作成する

にサインアップする AWS

Amazon Web Services (AWS) にサインアップすると AWS、 を含む のすべてのサービスに が自動的にサインアップ AWS アカウント されます AWS Backup。料金は、使用するサービスの料金のみが請求されます。

AWS Backup 使用料の詳細については、AWS Backup 「 の料金」ページを参照してください。

を AWS アカウント すでにお持ちの場合は、次のタスクに進んでください。 AWS アカウントをお持ちでない場合は、以下の手順に従ってアカウントを作成してください。

を作成するには 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、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

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

次のタスクで必要になるため、 AWS アカウント 番号を書き留めます。

IAM ユーザーの作成

などの のサービスでは AWS Backup、リソースへのアクセス許可があるかどうかをサービスが判断できるように、アクセス時に認証情報を指定する必要があります。 AWS では AWS、 AWS アカウント ルートユーザーを使用してリクエストを行わないことをお勧めします。代わりに、IAM ユーザーを作成し、そのユーザーにフルアクセスを許可します。このようなユーザーを管理者ユーザーと呼びます。 AWS アカウント ルートユーザー認証情報の代わりに管理者ユーザー認証情報を使用して、 AWS を操作し、バケットの作成、ユーザーの作成、アクセス許可の付与などのタスクを実行できます。詳細については、AWS 全般のリファレンスの「AWS アカウント ルートユーザーの認証情報と IAM ユーザーの認証情報」、および IAM ユーザーガイドの「IAM でのベストプラクティス」を参照してください。

にサインアップした AWS が、自分で IAM ユーザーを作成していない場合は、IAM コンソールを使用して作成できます。

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。	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。 AWS Command Line Interface

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 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「最初の IAM 管理者のユーザーおよびグループの作成」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の管理」に従って、プログラムによるアクセスを設定します。

この新しい IAM ユーザーとしてサインインするには、 からサインアウトします AWS Management Console。次に、次の URL を使用します。your_aws_account_id はハイフンのない AWS アカウント数字です (例えば、 AWS アカウント 数字が の場合1234-5678-9012、 AWS アカウント ID は です123456789012) 。

```
https://your_aws_account_id.signin.aws.amazon.com/console/
```

作成した IAM ユーザー名とパスワードを入力します。サインインすると、ナビゲーションバーに your_user_name@your_aws_account_id と表示されます。

サインインページの URL に AWS アカウント ID を含めない場合は、アカウントエイリアスを作成できます。IAM ダッシュボードで [アカウントの別名を作成] をクリックし、エイリアス (会社名など) を入力します。アカウントエイリアスを作成した後、サインインするには、次の URL を使用します。

```
https://your_account_alias.signin.aws.amazon.com/console/
```

アカウントの IAM ユーザーのためのサインイン用リンクを確認するには、IAM コンソールを開き、ダッシュボードの [AWS アカウント エイリアス] を確認します。

IAM ロールを作成する

IAM コンソールを使用して、サポートされているリソースへのアクセス AWS Backup 許可を付与する IAM ロールを作成できます。IAM ロールを作成したら、ポリシーを作成して、このロールにアタッチします。

コンソールで IAM ロールを作成するには

1. AWS マネジメントコンソール にサインインし、IAM コンソール を開きます。
2. IAM コンソールで、[Roles] ナビゲーションペイン、[Create Role (ロールを作成)] の順に選択します。
3. [AWS サービスロール] を選択し、次に [AWS Backup] 用の [選択] をクリックします。[次のステップ: アクセス許可] を選択します。
4. [許可ポリシーをアタッチ] ページで [AWSBackupServiceRolePolicyForBackup] と [AWSBackupServiceRolePolicyForRestores] の両方にチェックを入れます。これらの AWS 管理ポリシーは、サポートされているすべての AWS リソースをバックアップおよび復元する AWS Backup アクセス許可を付与します。管理ポリシーの詳細と例については、「管理ポリシー」を参照してください。

   その後 [次へ: タグ] を選択します。
5. [次へ: レビュー] を選択します。
6. [Role Name] (ロール名) に、ロールの目的がわかるような名前を入力します。ロール名は 内で一意である必要があります AWS アカウント。ロールは多くのエンティティにより参照されるため、作成後にロール名を変更することはできません。

   [ロールの作成] を選択します。
7. [Roles] (ロール) ページで、作成したロールを選択し、詳細ページを開きます。

の開始方法 AWS Backup

このチュートリアルでは、 AWS Backup の機能を使用するための一般的な手順を示します。この技術ドキュメントの他の部分と同様に、他のウィンドウの AWS マネジメントコンソール も参照してください。

また、以下のチュートリアルを読むことで、特定のサービス AWS Backup で を使用する方法を学ぶこともできます。

- を使用した Amazon Relational Database Service (Amazon RDS) のバックアップと復元 AWS Backup
- チュートリアル: を使用した Amazon EBS のバックアップと復元 AWS Backup

トピック

前提条件

作業を開始する前に、次の項目が揃っていることを確認してください。

- AWS アカウント。詳細については、「を初めてセットアップ AWS する」を参照してください。
- でサポートされているリソースが少なくとも 1 つあります AWS Backup。
- バックアップする AWS サービスとリソースに精通している必要があります。「サポートされている AWS リソースとサードパーティーアプリケーションのリスト」を参照してください。

新しい AWS サービスが利用可能になったら、 を有効に AWS Backup してそれらのサービスを使用します。

で使用する AWS サービスを設定するには AWS Backup

1. にサインインし AWS Management Console、https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで [設定] を選択します。
3. [サービスのオプトイン] ページで、[リソースを設定] を選択します。
4. 「リソースの設定」ページで、トグルスイッチを使用して、 で使用されるサービスを有効または無効にします AWS Backup。サービスを設定したら、[確認] を選択します。オプトインしている AWS サービスが で利用できることを確認します AWS リージョン。

詳細については、バックアッププランへのリソースの割り当て「」を参照してください。 AWS Backup コンソールでは、ユーザーはバックアッププランにリソースタイプを割り当てることができます。これは、その特定のサービスでオプトインが有効になっていない場合でも含まれます。

- バックアップするリソースがすべて同じ AWS リージョンにあることを確認します。

このチュートリアルを完了するには、 AWS アカウント ルートユーザーを使用して にサインインします AWS Management Console。ただし、 AWS Identity and Access Management (IAM) では、AWS アカウント ルートユーザーを使用しないことをお勧めします。代わりに、アカウントに管理者を作成し、それらの認証情報を使用してアカウントのリソースを管理します。詳細については、「を初めてセットアップ AWS する」を参照してください。

AWS Backup コンソールには、 リソースをバックアップするためのさまざまなオプションが用意されています。オンデマンドでバックアップを作成したり、リソースのバックアップ方法をスケジュールして設定したり、リソースの作成時に自動的にバックアップするようにリソースを設定したりできます。

開始方法 1: サービスオプトイン

AWS Backup コンソールには、バックアッププランにリソースタイプを含めるには、バックアッププランにリソースタイプを明示的に割り当てるか、すべてのリソースを含めるという 2 つの方法があります。これらの選択がサービスオプトインとどのように連携するかを理解するには、以下のポイントを参照してください。

- リソースの割り当てがタグのみに基づいている場合は、サービスオプトイン設定が適用されます。
- リソースタイプがバックアッププランに明示的に割り当てられている場合、その特定のサービスでオプトインが有効になっていなくても、バックアップに含まれます。これは、Aurora、Neptune、および Amazon DocumentDB には適用されません。これらのサービスを含めるには、オプトインを有効にする必要があります。
- リソース割り当てでリソースタイプとタグの両方が指定されている場合、指定されたリソースタイプが最初にフィルタリングされ、タグはそれらのリソースをさらにフィルタリングします。

  ほとんどのリソースタイプでは、サービスオプトイン設定は無視されます。ただし、Aurora、Neptune、および Amazon DocumentDB にはサービスオプトインが必要です。
- Amazon FSx for NetApp ONTAP では、タグベースのリソース選択を使用する場合は、ファイルシステム全体ではなく個々のボリュームにタグを適用します。

オプトインの選択は、特定のアカウントと に適用されます AWS リージョン。アカウントがリージョンで を使用する AWS Backup (バックアップボールトまたはバックアッププランを作成する) 場合、そのアカウントは、その時点でリージョン AWS Backup で によってサポートされているすべてのリソースタイプに自動的にオプトインされます。後日そのリージョンに追加されたサポート対象サービスは、バックアッププランに自動的に含まれません。サポートされたら、これらのリソースタイプをオプトインできます。

AWS Backup は、ますます多くの AWS サービスやサードパーティーアプリケーションをサポートするため、新しくサポートされるリソースにオプトインするには、このステップを再確認する必要がある場合があります。

AWS Backup は、 以外の AWS 環境で作成されたバックアップを管理または管理しません AWS Backup。

を使用してサポートされているすべてのリソースタイプ AWS Backup を保護するようにオプトインするには

1. にサインインし AWS Management Console、https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. 左側のナビゲーションペインで [設定] を選択します。
3. サービスオプトインで、[リソースの設定] を選択します。
4. すべてのトグルを右側に移動して、 AWS Backupがサポートするすべてのリソースにオプトインします。
5. [確認] を選択します。

次のステップ

を使用してオンデマンドバックアップを作成するには AWS Backup、「」に進みます開始方法 2: オンデマンドバックアップの作成。

開始方法 2: オンデマンドバックアップの作成

AWS Backup コンソールの「保護されたリソース」ページには、 AWS Backup 少なくとも 1 回バックアップされたリソースが一覧表示されます。 AWS Backup を初めて使用する場合、このページには Amazon EBS ボリュームや Amazon RDS データベースなどのリソースはリストされていません。リソースがバックアッププランに割り当てられていても、バックアップがスケジュールされたバックアップジョブを 1 回も実行したことがない場合も同様です。

この最初のステップでは、リソースのいずれかのオンデマンドバックアップを作成します。そうすることで、そのリソースが [Protected resources (保護されたリソース)] ページにリストされます。

オンデマンドバックアップを作成するには

1. にサインインし AWS Management Console、https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインを使用して、[保護されたリソース]、[オンデマンドバックアップの作成] の順に選択します。
3. [オンデマンドバックアップを作成] ページで、バックアップするリソースタイプを選択します。たとえば、Amazon DynamoDB テーブルの [DynamoDB] を選択します。
4. 保護するリソースの名前または ID を選択します。選択したリソースが、必要なリソースであることを確認します。

   > **Note**
   >
   > Amazon FSx for Lustre で、Persistent と Persistent_2 という 2 つのデプロイタイプがサポートされています。

5. [今すぐバックアップを作成] が選択されていることを確認します。これにより、すぐにバックアップが開始され、保存されたリソースがより早く [保護されたリソース] ページに表示されます。
6. コールドストレージへの移行の値 (該当する場合) および有効期限の値を指定します。

> **Note**
>
> - コールドストレージに移行できるリソースの一覧については、リソース別の機能の可用性 表の「コールドストレージへのライフサイクル」セクションを参照してください。他のすべてのリソースタイプはウォームストレージに保存され、コールドストレージへの移行式は無視されます。[Expire (有効期限)] 値はすべてのリソースタイプに対して有効です。
> - バックアップの有効期限が切れ、ライフサイクルポリシーの一部として削除対象としてマークされると、 はランダムに選択された時点で次の 8 時間にわたってバックアップ AWS Backup を削除します。このウィンドウは、一貫したパフォーマンスを確保するのに役立ちます。

7. 既存のバックアップボールトを選択します。[Create new backup vault (新しいバックアップボールトを作成)] を選択すると、ボールトを作成する新しいページが開きます。完了すると、[Create on-demand backup (オンデマンドバックアップを作成)] ページに戻ります。
8. [IAM role (IAM ロール)] では、[Default role (デフォルトロール)] を選択します。

> **Note**
>
> アカウントに AWS Backup デフォルトのロールが存在しない場合、正しいアクセス許可を持つロールが作成されます。

9. オンデマンドバックアップに 1 つ以上のタグを割り当てる場合は、[キー] とオプションの [値]] を入力して、[タグを追加] を選択します。

> **Note**
>
> - Amazon EC2 リソースの場合、このバックアップに追加するタグに加えて、 は既存のグループタグと個々のリソースタグ AWS Backup を自動的にコピーします。詳細については、「バックアップへのタグのコピー」を参照してください。
> - タグベースのバックアッププランを作成するときに、デフォルトロール 以外のロールを選択する場合は、タグ付けされたすべてのリソースをバックアップするために必要なアクセス許可があることを確認してください。 は、選択したタグを持つすべてのリソースを処理し AWS Backup ようとします。アクセス権限のないリソースが検出されると、バックアッププランは失敗します。

10. [オンデマンドバックアップを作成] を選択します。[ジョブ] ページに移動し、ジョブのリストが表示されます。
11. リソースタイプが EC2 の場合、[バックアップの詳細設定] セクションが表示されます。EC2 インスタンスが Microsoft Windows を実行している場合は、[Windows VSS] を選択します。これにより、アプリケーション整合性のある Windows VSS バックアップを取ることができます。

> **Note**
>
> AWS Backup は現在、Amazon EC2 でのみ実行されているリソースのアプリケーション整合性のあるバックアップをサポートしています。Windows VSS バックアップでは、すべてのインスタンスタイプまたはアプリケーションがサポートされているわけではありません。詳細については、「Windows VSS バックアップの作成」を参照してください。

12. バックアップするリソースの [バックアップジョブ ID] を選択すると、そのジョブの詳細が表示されます。

次のステップ

バックアップアクティビティを自動化するには、開始方法 3: スケジュールされたバックアップの作成 に進みます。

開始方法 3: スケジュールされたバックアップの作成

AWS Backup チュートリアルのこのステップでは、バックアッププランを作成し、それにリソースを割り当て、バックアップボールトを作成します。

作業を開始する前に、前提条件が揃っていることを確認してください。詳細については、「の開始方法 AWS Backup」を参照してください。

トピック

ステップ 1: バックアッププランを既存のものから作成する

バックアッププランは、Amazon DynamoDB テーブルや Amazon Elastic File System (Amazon EFS) ファイルシステムなどの AWS リソースをいつどのようにバックアップするかを定義するポリシー式です。バックアッププランにリソースを割り当て AWS Backup 、バックアッププランに従ってそれらのリソースのバックアップを自動的にバックアップして保持します。詳細については、「バックアッププランを使用したバックアップの管理」を参照してください。

新しいバックアップ計画を作成するには、2 つの方法があります。1 つを最初から作成することも、既存のバックアップ計画に基づいて作成することもできます。この例では、 AWS Backup コンソールを使用して、既存のバックアッププランを変更してバックアッププランを作成します。

既存のものからバックアッププランを作成するには

1. にサインインし AWS Management Console、https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ダッシュボードから、[バックアッププランを管理] を選択します。または、ナビゲーションペインを使用して、[バックアッププラン] を選択してから、[バックアッププランの作成] を選択します。
3. [テンプレートから開始] を選択し、リストからプラン (例えば、`Daily-Monthly-1yr-Retention` など) を選択して、[バックアッププラン名] ボックスに名前を入力します。

   > **Note**
   >
   > 既存のプランと同じバックアッププランを作成しようとすると、`AlreadyExistsException` エラーが発生します。

4. プランの概要ページで、必要なバックアップルールを選択し、[編集] を選択します。
5. ルールに使用する値を見直して選択します (ルールのオプションについては「バックアッププランのオプションと設定」を参照)。
6. バックアップボールトでは、[デフォルト] または [新しいバックアップボールトの作成] を選択して新しいボールトを作成します。
7. (オプション) - 送信先リージョンのリストから を選択して、バックアップを別のリージョンにコピー AWS リージョン します。さらにリージョンを追加するには、[コピーを追加] を選択します。
8. ルールの編集が完了したら、[バックアップルールの保存] を選択します。

[概要] ページで、[リソースを割り当てる] を選択して、次のセクションの準備をします。

ステップ 2: バックアッププランにリソースを割り当てる

バックアッププランを作成したら、そのバックアッププランに AWS リソースを割り当てる必要があります。リソース割り当ての詳細については、「バックアッププランへのリソースの割り当て」を参照してください。

バックアッププランに割り当てる既存の AWS リソースがまだない場合は、この演習で使用する新しいリソースをいくつか作成します。サポートされている AWS リソースとサードパーティーアプリケーションを使用して 1 つまたは 2 つのリソースを作成します。

バックアッププランにリソースを割り当てるには

1. 前のステップで、[リソースの割り当て] ページに移動するはずです。
2. [リソースの割り当て名] を入力します。
3. [IAM ロール] で、[デフォルトロール] を選択します。別のロールを選択する場合は、割り当てるすべてのリソースをバックアップするアクセス権限が必要です。
4. [リソースの割り当て] セクションで、[すべてのリソースタイプを含める] を選択します。リソースタイプは、 AWS Backupがサポートする AWS サービスまたはサードパーティーのアプリケーションです。このバックアッププランは、 を使用して保護するためにオプトインしたすべてのリソースタイプを保護するようになりました。 AWS Backup
5. [リソースを割り当てる] を選択します。

バックアッププランの [要約] ページに戻ります。[バックアッププランを作成] を選択して、最初のバックアッププランをデプロイします。

ステップ 3: バックアップボールトの作成

AWS Backup コンソールで自動的に作成されるデフォルトのバックアップボールトを使用する代わりに、特定のバックアップボールトを作成して、同じボールト内のバックアップのグループを保存および整理できます。

バックアップボールトの詳細については、「バックアップボールト」を参照してください。

バックアップボールトを作成するには

1. AWS Backup コンソールのナビゲーションペインで、バックアップボールト を選択します。

> **Note**
>
> ナビゲーションペインが左側に表示されない場合は、 AWS Backup コンソールの左上隅にあるメニューアイコンを選択してナビゲーションペインを開くことができます。

2. [Create backup vault (バックアップボールトを作成)] を選択します。
3. バックアップボールトの名前を入力します。保存するものがわかるような名前や、必要なバックアップを検索しやすい名前を付けることができます。例えば、**`FinancialBackups`** のような名前を付けます。
4. AWS Key Management Service （ AWS KMS) キーを選択します。既に作成したキーを使用するか、デフォルトの AWS Backup KMS キーを選択できます。

> **Note**
>
> ここで指定する AWS KMS キーは、 AWS Backup 独立した暗号化をサポートするサービスのバックアップにのみ適用されます。 AWS Backup 独立した暗号化をサポートするリソースタイプのリストを確認するには、リソース別の機能の可用性表の「フル AWS Backup 管理」セクションを参照してください。

5. 必要に応じて、バックアップボールトを検索および識別するタグを追加します。例えば、**`BackupType:Financial`** というタグを追加できます。
6. バックアップ保管庫を作成 を選択します。
7. ナビゲーションペインで [Backup vaults (バックアップボールト)] を選択して、バックアップボールトが追加されていることを確認します。

> **Note**
>
> バックアッププランの 1 つでバックアップルールを編集して、そのルールによって作成されたバックアップを、作成したバックアップボールトに保存できるようになりました。

次のステップ

Amazon EFS ファイルシステムを具体的にバックアップするには、開始方法 4: Amazon EFS 自動バックアップの作成 に進みます。

開始方法 4: Amazon EFS 自動バックアップの作成

Amazon EFS コンソールを使用して Amazon Elastic File System (Amazon EFS) ファイルシステムを作成すると、デフォルトで自動バックアップがオンになります。既存の Amazon EFS ファイルシステムを自動的にバックアップする場合は、Amazon EFS コンソール、API、または CLI を使用してバックアップできます。

コンソールを使用して既存の Amazon EFS ファイルシステムを自動的にバックアップするには

1. https://console.aws.amazon.com/efs で Amazon EFS コンソールを開きます。
2. [ファイルシステム] ページで、自動バックアップをオンにするファイルシステムを選択します。
3. 一般設定パネルの [編集] を選択します。
4. 自動バックアップを有効にするには、[自動バックアップの有効化] を選択します。

デフォルトのバックアッププラン設定は `daily backups, 35-day retention` です。デフォルトのバックアップウィンドウ (バックアップが実行される時間枠) は、午前 5 時 (協定世界時) に開始に設定され、8 時間続きます。

> **Note**
>
> Amazon EFS 自動バックアップボールト `aws/efs/automatic-backup-vault` は、それらの自動バックアップのみで予約されています。
> このボールトは、クロスアカウントコピーの作成や、他の自動化されていないバックアッププランによって作成されたバックアップの送信先として使用しないでください。他のバックアッププランの宛先として使用すると、「権限が不十分です」というエラーが表示されます。

AWS Backup は、ユーザーに代わって アカウントでサービスにリンクされたロールを作成します。このロールには、Amazon EFS バックアップを実行するために必要なアクセス権限が付与されています。サービスにリンクされたロールの詳細情報については、「AWS Backupのサービスにリンクされたロールの使用」を参照してください。

Amazon EFS コンソール、API、または CLI を使用して自動バックアップを有効または無効にする step-by-step 方法については、Amazon Elastic File System ユーザーガイド」の「自動バックアップ」を参照してください。

次のステップ

作成したバックアップを表示するには、開始方法 5: バックアップジョブと復旧ポイントの表示 に進みます。

開始方法 5: バックアップジョブと復旧ポイントの表示

を使用すると AWS Backup、使用する AWS サービス全体のバックアップおよび復元アクティビティのステータスやその他の詳細を表示できます。

AWS Backup ダッシュボードでは、バックアッププランの管理、オンデマンドバックアップの作成、バックアップの復元、バックアップジョブと復元ジョブのステータスの表示を行うことができます。

トピック

バックアップジョブのステータスを表示する

AWS Backup ダッシュボードを使用して、バックアップおよび復元アクティビティのステータスをすばやく表示します。

バックアップジョブのステータスを表示するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、ダッシュボード を選択します。
3. バックアップジョブのステータスを表示するには、[Backup jobs details (バックアップジョブの詳細)] を選択します。これにより [バックアップジョブ] ページに移動します。ここでバックアップジョブと復元ジョブを含むテーブルを確認できます。
4. 時系列で表示されるジョブをフィルタリングできます。たとえば、過去 24 時間、過去 1 週間、過去 30 日間に作成されたジョブなどです。また、歯車アイコンを選択して、各ページに表示するジョブ数を設定することもできます。

ボールト内のすべてのバックアップの表示

AWS Backupの指定されたボールト内に作成されたバックアップを表示するには、次のステップに従います。

ボールト内のすべてのバックアップを表示するには

1. AWS Backup コンソールのナビゲーションペインで、バックアップボールト を選択します。
2. オンデマンドまたはスケジュールされたバックアップを作成するときに使用したボールトを選択して、このボールト内に作成されたすべてのバックアップを表示します。

> **Note**
>
> 各バックアップにはステータスがあり、通常は完了です。何らかの理由でライフサイクル設定に従ってバックアップを削除できない場合、このバックアップ AWS Backup は期限切れとしてマークされます。期限切れのバックアップが消費するストレージに対して課金されるため、削除する必要があります。

保護されたリソースの詳細の表示

[Protected resources (保護されたリソース)] ページで、 AWS Backupでバックアップされたリソースの詳細を詳しく見ることができます。

保護されたリソースを表示するには

1. AWS Backup コンソールのナビゲーションペインで、保護されたリソース を選択します。
2. バックアップされている AWS リソースを表示します。リストでリソースを選択し、そのリソースのバックアップを調べます。

次のステップ

表示した復旧ポイントを復元するには、開始方法 6: バックアップの復元 に進みます。

開始方法 6: バックアップの復元

リソースが少なくとも 1 回バックアップされると、保護されていると見なされ、 を使用して復元できます AWS Backup。 AWS Backup コンソールを使用してリソースを復元するには、次のステップに従います。

特定のサービスのパラメータの復元、または AWS CLI または AWS Backup API を使用したバックアップの復元については、「バックアップの復元」を参照してください。

リソースを復元するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[保護されたリソース] を選択し、復元するリソース ID を選択します。
3. リソースタイプを含む復旧ポイントのリストが、[リソース ID] に表示されます。リソースを選択して、[リソースの詳細] ページを開きます。
4. リソースを復元するには、[バックアップ] ペインで、リソースの復旧ポイント ID の横にあるラジオボタンをクリックします。ペインの右上隅にある [復元] を選択します。
5. 復元パラメータを指定します。表示される復元パラメータは、選択したリソースタイプに固有です。

   > **Note**
   >
   > バックアップを 1 つだけ保持している場合、復元できるのは、そのバックアップを実行した時点のファイルシステムの状態に限られます。以前の増分バックアップに復元することはできません。

   特定のリソースを復元する方法については、「バックアップの復元」を参照してください。
6. [ロールを復元] で [デフォルトのロール] を選択します。

   > **Note**
   >
   > アカウントに AWS Backup デフォルトのロールが存在しない場合、正しいアクセス許可を持つロールが作成されます。
7. [バックアップを復元] を選択します。

[復元ジョブ] ペインが表示されます。ページ上部のメッセージには、復元ジョブに関する情報が表示されます。

> **Note**
>
> Amazon EFS インスタンス内の特定の項目を復元するために復元を実行すると、それらの項目を新規または既存のファイルシステムに復元できます。項目を既存のファイルシステムに復元する場合、 はルートディレクトリから新しい Amazon EFS ディレクトリ AWS Backup を作成し、項目を含めます。復元ディレクトリには、指定した項目の完全な階層構造が保持されます。例えば、ディレクトリ A にサブディレクトリ B、C、D が含まれている場合、A、B、C、D が復元されると、 は階層構造 AWS Backup を保持します。
> Amazon EFS の部分的な復元を既存のファイルシステムに、または新しいファイルシステムに対して実行するかに関係なく、復元の試行ごとにルートディレクトリから復元されたファイルが含まれる新しい復旧ディレクトリが作成されます。同じパスで複数の復元を試みると、復元先のディレクトリが複数になる場合があります。

Amazon EFS インスタンスを復元するには

Amazon EFS インスタンスを復元する場合、[完全な復元] でファイルシステム全体の復元を実行できます。または、[項目レベルの復元] を使用して特定のファイルやディレクトリを復元できます (項目レベルの復元には制限があります)。詳細については、「EFS ファイルシステムの復元」を参照してください)。他のタイプでのリソース復元の詳細については、「バックアップの復元」を参照してください。

> **Note**
>
> Amazon EFS インスタンスを復元するには、`backup:startrestorejob` を「許可」する必要があります。

バックアップの復元の詳細については、「バックアップの復元」を参照してください。

次のステップ

AWS Backup Audit Manager を使用すると、バックアップアクティビティとリソースを監査できます。また、バックアップ、復元、およびコピージョブの証拠として使用できるレポートを作成する

こともできます。レポートを作成するには、「開始方法 7: 監査レポートの作成」を参照してください。

開始方法 7: 監査レポートの作成

では開始方法 5: バックアップジョブと復旧ポイントの表示、 AWS Backup Dashboard 、Backup ボールト 、および Protected Resources ビューでバックアップアクティビティを確認しました。ただし、これらのビューは動的であり、いつアクセスしたかに応じて更新されます。これらのビューは、組織のデータ保護要件と統制を長期間にわたって継続的に遵守していることを示す最良の証拠であるとは限りません。

このステップでは、 AWS Backup Audit Manager を使用してオンデマンドバックアップジョブレポートを作成します。

AWS Backup Audit Manager は、さまざまな監査レポートを CSV、JSON、またはその両方の形式で毎日およびオンデマンドで Amazon S3 バケットに配信します。多くのカスタマイズ可能なコントロールに対して、バックアップアクティビティとリソースのコンプライアンスを監査できます。バックアップ、コピー、および復元ジョブに関するレポートを受け取ることができます。バックアップジョブレポートは、バックアップジョブが実行されたことを示す証拠です。

以下は、バックアップ計画の例です。


```
{
  "reportItems": [
    {
      "reportTimePeriod": "2021-07-14T00:00:00Z - 2021-07-15T00:00:00Z",
      "accountId": "112233445566",
      "region": "us-west-2",
      "backupJobId": "FCCB040A-9426-2A49-2EA9-5EAFFAC00000",
      "jobStatus": "COMPLETED",
      "resourceType": "EC2",
      "resourceArn": "arn:aws:ec2:us-west-2:112233445566:instance/i-0bc877aee77800000",
      "backupPlanArn": "arn:aws:backup:us-west-2:112233445566:backup-plan:349f2247-
b489-4301-83ac-4b7dd7200000",
      "backupRuleId": "ab88bbf8-ff4e-4f1b-92e7-e13d3e6abcde",
      "creationDate": "2021-07-14T23:53:47.229Z",
      "completionDate": "2021-07-15T00:16:07.282Z",
      "recoveryPointArn": "arn:aws:ec2:us-west-2::image/ami-030cafb98e5aabcde",
      "jobRunTime": "00:22:20",
      "backupSizeInBytes": 8589934592,
      "backupVaultName": "Default",
```

```
      "backupVaultArn": "arn:aws:backup:us-west-2:112233445566:backup-vault:Default",
      "iamRoleArn": "arn:aws:iam::112233445566:role/service-role/
AWSBackupDefaultServiceRole"
    }
  ]
}
```

バックアップレポート (オンデマンドバックアップレポートを含む) を作成するには、まずレポートを自動化して Amazon S3 バケットに配信するレポートプランを作成します。

レポートプランでは、レポートを受け取る Amazon S3 バケットが必要です。新しい S3 バケットを設定する手順については、Amazon Simple Storage Service ユーザーガイドの「ステップ 1: 最初の S3 バケットの作成」を参照してください。

レポートプランを作成するには

1. にサインインし AWS Management Console、https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. 左のナビゲーションペインの [レポート] を選択します。
3. [レポートプランの作成] を選択します。
4. ドロップダウンリストから、[バックアップジョブレポート] を選択します。
5. [レポートプラン名] に **`TestBackupJobReport`** を入力します。
6. [ファイル形式] では、[CSV] と [JSON] の両方を選択します。
7. [S3 バケット名] で、ドロップダウンリストからレポートの送信先を選択します。
8. [レポートプランの作成] を選択します。

次に、S3 バケットが からレポートを受信することを許可する必要があります AWS Backup。 AWS Backup Audit Manager は自動的に S3 アクセスポリシーを生成します。

このアクセスポリシーを表示して適用するには

1. 左のナビゲーションペインの [レポート] を選択します。
2. [レポートプラン名] で、レポートプランの名前を選択します (`TestBackupJobReport`)。
3. [編集] を選択します。
4. [S3 バケットのアクセスポリシーの表示] を選択します。
5. [アクセス権限のコピー] を選択します。

6. [バケットポリシーの編集] を選択して送信先 S3 バケットのポリシーを編集し、バックアップジョブレポートを受信できるようにします。
7. 送信先 S3 バケットポリシーにアクセス権限をコピーまたは追加します。

次に、最初のバックアップジョブレポートを作成します。

オンデマンドバックアップレポートを作成するには

1. 左のナビゲーションペインの [レポート] を選択します。
2. [レポートプラン名] で、レポートプランの名前を選択します (`TestBackupJobReport`)。
3. [オンデマンドレポートの作成] を選択します。

最後に、レポートを表示します。

レポートを表示するには

1. 左のナビゲーションペインの [レポート] を選択します。
2. [レポートプラン名] で、レポートプランの名前を選択します (`TestBackupJobReport`)。
3. [レポートジョブ] セクションで、[S3 リンク] を選択します。これにより、送信先 S3 バケットに移動します。
4. [ダウンロード] を選択します。
5. CSV ファイルまたは JSON ファイルの操作に使用するプログラムを使用してレポートを開きます。

次のステップ

はじめにリソースをクリーンアップし、不要な課金を回避するには 開始方法 8: リソースのクリーンアップ に進みます。

開始方法 8: リソースのクリーンアップ

「の開始方法 AWS Backup」のすべてのタスクを実行した後は、作成した内容をクリーンアップして、不要な課金が発生しないようにします。

トピック

ステップ 1: 復元された AWS リソースを削除する

Amazon Elastic Block Store (Amazon EBS) ボリュームや Amazon DynamoDB テーブルなど、復旧ポイントから復元した AWS リソースを削除するには、そのサービスの コンソールを使用します。たとえば、Amazon Elastic File System (Amazon EFS) ファイルシステムを削除するには、[Amazon EFS コンソール] を使用します。

> **Note**
>
> この情報は、バックアップボールトに保存されている復旧ポイントではなく、復元されたリソースを指します。

ステップ 2: バックアッププランの削除

スケジュールされたバックアップを作成しない場合は、バックアッププランを削除する必要があります。バックアッププランを削除する前に、そのバックアッププランに対するリソース割り当てをすべて削除する必要があります。

バックアッププランを削除するには、以下のステップを実行します。

バックアッププランを削除するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[バックアッププラン] を選択します。
3. [Backup plans (バックアッププラン)] ページで、削除するバックアッププランを選択します。そのバックアップの詳細ページが表示されます。
4. プランのリソース割り当てを削除するには、割り当て名の横にあるラジオボタンを選択し、[Delete (削除)] を選択します。

5. バックアッププランを削除するには、ページの右上隅にある [Delete (削除)] を選択します。
6. 確認ページで、プラン名を入力して [Delete (削除)] を選択します。

ステップ 3: 復旧ポイントの削除

次に、バックアップボールトにあるバックアップ復旧ポイントを削除できます。

復旧ポイントの削除

1. AWS Backup コンソールのナビゲーションペインで、バックアップボールト を選択します。
2. [バックアップボールト] ページで、バックアップを保存したバックアップボールトを選択します。
3. 復旧ポイントを確認し、[削除] を選択します。
4. 複数の復旧ポイントを削除する場合、次の手順を実行します。

    a. リストに連続バックアップが含まれている場合は、継続バックアップデータを保持するか削除するかを選択します。

    b. リストされているすべての復旧ポイントを削除するには、**delete** を入力してから、[復旧ポイントの削除] を選択します。

    ページの上部に、緑色の成功バナーが表示されるまで、ブラウザのタブを開いたままにします。このタブを早期に閉じると、削除プロセスが終了して削除したい復旧ポイントの一部が残ることがあります。詳細については、「バックアップの削除」を参照してください。

ステップ 4: バックアップボールトの削除

デフォルトのバックアップボールトは、一般に削除できません。ただし、特定のリージョンにほかのボールトが 1 つ以上のある場合は、 AWS CLIを使用してそのリージョンのデフォルトバックアップボールトを削除できます。

その中のバックアップ (復旧ポイント) がすべて削除されたら、デフォルトでない他のボールトも削除できます。削除するには、空のボールトで [削除] を選択します。

ステップ 5: レポートプランの削除

レポートプランでは、毎日新しいレポートが自動的に送信されます。これを防ぐには、レポートプランを削除します。

レポートプランを削除するには

1. AWS Backup コンソールのナビゲーションペインで、レポート を選択します。
2. [レポートプラン名] で、レポートプランの名前を選択します。
3. [削除] を選択します。
4. レポートプラン名を入力し、[レポートプランの削除] を選択します。

ステップ 6: レポートの削除

レポートごとに、[単一オブジェクトの削除] の手順に従ってレポートを削除できます。送信先 S3 バケットが不要になった場合は、バケットからすべてのオブジェクトを削除した後、[バケットの削除] の手順に従ってバケットを削除できます。

バックアッププランを使用したバックアップの管理

では AWS Backup、バックアッププランは、Amazon DynamoDB テーブルや Amazon Elastic File System (Amazon EFS) ファイルシステムなどの AWS リソースをバックアップするタイミングと方法を定義するポリシー式です。バックアッププランにリソースを割り当てると、 はバックアッププランに従ってそれらのリソースのバックアップ AWS Backup を自動的にバックアップおよび保持します。さまざまなバックアップ要件を持つワークロードがある場合は、複数のバックアッププランを作成できます。デフォルトでは、バックアップウィンドウは AWS Backupによって最適化されます。バックアップウィンドウは、コンソールを使用しても、プログラムでも、カスタマイズできます。

AWS Backup は、定期的なバックアップを段階的に効率的に保存します。 AWS リソースの最初のバックアップは、データの完全なコピーをバックアップします。連続する増分バックアップごとに、AWS リソースへの変更のみがバックアップされます。増分バックアップにより、頻繁なバックアップのデータ保護とストレージコストを最小限に抑えることができます。

AWS Backup また、 は保持設定に基づいてバックアッププランのライフサイクルをシームレスに管理するため、必要に応じて復元できます。

以下のセクションでは、 でのバックアップ戦略の管理の基本について説明します AWS Backup。

トピック

- バックアッププランの作成
- バックアッププランへのリソースの割り当て
- バックアッププランの削除
- バックアッププランの更新

バックアッププランの作成

コンソール、API AWS Backup 、CLI、SDK、または AWS CloudFormation テンプレートを使用してバックアッププランを作成できます。

トピック

- AWS Backup コンソールを使用したバックアッププランの作成
- を使用したバックアッププランの作成 AWS CLI

- バックアッププランのオプションと設定
- AWS CloudFormation バックアッププランの テンプレート

AWS Backup コンソールを使用したバックアッププランの作成

https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。ダッシュボードから、[バックアッププランを管理] を選択します。または、ナビゲーションペインを使用して、[バックアッププラン] を選択してから、[バックアッププランの作成] を選択します。

開始オプション

新しいバックアッププランの開始には 3 つの選択肢があります。

- ステップ 1: バックアッププランを既存のものから作成する
- 新しいプランを立てる
- を使用したバックアッププランの作成 AWS CLI

このチュートリアルでは、[新しいプランを立てる] を選択します。設定の各項目には、ページ内の拡張セクションへのリンクがあり、該当セクションに移動して詳細を確認できます。

1. にプラン名を入力しますバックアッププラン名。作成後にプランの名前を変更することはできません。

   既存のプランと同じバックアッププランを作成しようとすると、`AlreadyExistsException`エラーが発生します。
2. 必要に応じて、バックアッププランにタグを追加できます。
3. バックアップルールの設定 : [バックアップルールの設定] セクションでは、バックアップのスケジュール、期間、およびライフサイクルを設定します。
4. スケジュール:

   a. テキストフィールドにバックアップルール名を入力します。

   b. バックアップボールトのドロップダウンメニューで、[デフォルト] を選択するか、[新しいバックアップボールトを作成] を選択して新しいボールトを作成します。

   c. バックアップ頻度のドロップダウンメニューで、このプランでバックアップを作成する頻度を選択します。
5. バックアップ期間:

a. 開始時刻は、システムのローカルタイムゾーンでデフォルトで午前 12:30 (24 時間で 00:30) に設定されます。

b. [次の時間以内に開始] のデフォルトは、8 時間です。これを変更して、バックアップを開始する時間帯を指定できます。

c. [次の時間以内に完了] のデフォルトは、7 日です。

6. 継続的バックアップと point-in-time 復元 (PITR)： point-in-time 継続的バックアップのリカバリ (PITR) を有効にする を選択できます。このタイプのバックアップでサポートされているリソースを確認するには、「リソース別の機能の可用性 の表」を参照してください。

7. ライフサイクル

a. コールドストレージ : このボックスを選択すると、合計保持期間で指定したスケジュールに従って、対象となるリソースタイプをコールドストレージに移行できます。コールドストレージを使用するには、合計保持期間が 90 日以上である必要があります。

b. Amazon EBS のコールドストレージは Amazon EBS Snapshots Archive です。アーカイブのストレージ階層に移行されたスナップショットは、コンソールにコールド階層として表示されます。コールドストレージを有効にしてバックアップ頻度を毎月以下にした場合は、バックアッププランで EBS スナップショットを移行できます。

c. [合計保持期間]は、リソースを AWS Backupに保持する日数です。ウォームストレージとコールドストレージを合計した日数となります。

8. (オプション) バックアップのコピーを別の AWS リージョンに保存したい場合は、[コピー先にコピー] を使用して対象リソースのクロスリージョンコピーを作成します。

9. (オプション) 復旧ポイントにタグを追加します。

10. すべてのセクションを仕様に従って設定したら、[バックアップルールを保存] を選択します。

を使用したバックアッププランの作成 AWS CLI

JSON ドキュメントでバックアッププランを定義して、 AWS Backup コンソールまたは AWS CLI を使用して提供することもできます。次の JSON ドキュメントには、太平洋標準時 1:00 に日次バックアップを作成するサンプルバックアッププランが含まれています (該当する場合、現地時刻は夏時間、標準時間、夏時間の条件に調整されます) 。1 年後にバックアップが自動的に削除されます。

```
{
  "BackupPlan":{
    "BackupPlanName":"test-plan",
    "Rules":[
```

```
      {
        "RuleName":"test-rule",
        "TargetBackupVaultName":"test-vault",
        "ScheduleExpression":"cron(0 1 ? * * *)",
        "ScheduleExpressionTimezone":"America/Los_Angeles",
        "StartWindowMinutes":integer, // Value is in minutes
        "CompletionWindowMinutes":integer, // Value is in minutes
        "Lifecycle":{
          "DeleteAfterDays":integer, // Value is in days
        }
      }
    ]
  }
}
```

JSON ドキュメントは任意の名前で保存できます。次の CLI コマンドは、test-backup-plan.json という名前の JSON がある create-backup-plan を表示します。

```
aws backup create-backup-plan --cli-input-json file://PATH-TO-FILE/test-backup-plan.json
```

一部のシステムでは曜日に 0 から 6 までの番号が付けられますが、1 から 7 までの番号が付けられます。詳細については、「Cron 式」を参照してください。タイムゾーンの詳細については、Amazon Location Service API リファレンスTimeZoneの「」を参照してください。

バックアッププランのオプションと設定

AWS Backup コンソールでバックアッププランを定義するときは、次のオプションを設定します。

バックアッププラン名

一意のバックアッププラン名を指定する必要があります。

既存のプラン名と同じ名前を選択すると、エラーメッセージが返されます。

バックアップルール

バックアッププランは、1 つ以上のバックアップルールで構成されます。バックアッププランにバックアップルールを追加するか、バックアッププラン内の既存ルールを編集するには、次の手順を実行します。

1. AWS Backup コンソールの左側のナビゲーションペインで、バックアッププラン を選択します。
2. [バックアッププラン名] で、バックアッププランを選択します。
3. [バックアップルール] セクションで、
   - バックアップルールを追加するには、[バックアップルールの追加] を選択します。
   - 既存のバックアップルールを編集するには、ルールを選択し [編集] を選択します。

> **Note**
>
> 複数のルールを含むバックアッププランがあり、2 つのルールの時間枠が重複している場合、 はバックアップ AWS Backup を最適化し、保持時間が長いルールのバックアップを作成します。最適化では、毎日のバックアップが行われるときだけでなく、フルスタートウィンドウも考慮されます。

各バックアップルールは以下の要素で構成されています。

バックアップルール名

バックアップルール名では大文字と小文字が区別されます。1 ~ 50 文字の英数字またはハイフンを含める必要があります。

Backup frequency

バックアップ頻度によって、スナップショットバックアップ AWS Backup を作成する頻度が決まります。頻度はコンソールを使用して、12 時間、毎日、毎週または毎月から選択できます。また、スナップショットのバックアップを 1 時間ごとに作成する cron 式を作成することもできます。 AWS Backup CLI を使用すると、スナップショットのバックアップを 1 時間ごとにスケジュールできます。

毎週を選択する場合は、バックアップする曜日を指定できます。毎月を選択する場合は、月の特定の日を選択できます。

サポートされているリソースの継続的バックアップを有効にするチェックボックスをオンにして、point-in-time 復元 (PITR) 対応の継続的バックアップルールを作成することもできます。スナップショットバックアップとは異なり、継続的バックアップでは point-in-time 復元を実行できます。継続バックアップの詳細については、「ポイントインタイムリカバリ」を参照してください。

バックアップウィンドウ

バックアップウィンドウは、そのバックアップウィンドウの開始時刻と、ウィンドウの期間 (時間単位) で構成されます。バックアップジョブは、このウィンドウ内で開始されます。コンソールのデフォルト設定は以下のとおりです。

- システムのタイムゾーン (24 時間システムでは 0:30) の現地時間午前 12:30
- 8 時間以内に開始
- 7 日以内に完了

  ([以内に完了] パラメータは Amazon FSx リソースには適用されません)

cron 式を使用して、バックアップ頻度とバックアップウィンドウの開始時刻をカスタマイズできます。 AWS cron 式の 6 つのフィールドを確認するには、「Amazon CloudWatch Events ユーザーガイド」の「Cron 式」を参照してください。 AWS cron 式の 2 つの例は、 `15 * ? * * *` (1 時間ごとに 15 分後にバックアップを取る) と `0 12 * * ? *` (毎日正午 UTC にバックアップを取る) です。例の表については、前のリンクをクリックしてページを下にスクロールします。

AWS Backup は 00:00 から 23:59 までの cron 式を評価します。「12 時間ごと」のバックアップルールを作成し、11:59 より後の開始時刻を指定すると、1 日に 1 回のみ実行されます。

継続的バックアップおよび point-in-time 復元 (PITR) は、一定期間に記録された変更を参照するため、時間式または cron 式でスケジュールすることはできません。

> **Note**
>
> 一般に、 AWS データベースサービスはメンテナンスウィンドウの 1 時間前または間にバックアップを開始できず、Amazon FSx はメンテナンスウィンドウまたは自動バックアップウィンドウの 4 時間前または間にバックアップを開始できません (Amazon Aurora は、このメンテナンスウィンドウの制限から除外されます) 。その間にスケジュールされたスナップショットバックアップは失敗します。
> AWS Backup を使用して、サポートされているサービスのスナップショットバックアップと継続的バックアップの両方にオプトインする場合、例外が発生します。 AWS Backup では、競合を避けるため、バックアップウィンドウを自動的にスケジュールします。サポートされている サービスのリストと、 AWS Backup を使用して継続的なバックアップを作成する方法については、「ポイントインタイムリカバリ」を参照してください。

バックアップルールの重複

場合によっては、バックアッププランに複数の重複するルールが含まれている場合があります。異なるルールの開始ウィンドウが重複すると、 AWS Backup は保持期間が長いルールでバックアップを保持します。たとえば、次の 2 つのルールを持つバックアッププランを考えてみましょう。

1. 1 時間のスタートウィンドウを使用して、毎時バックアップし、1 日保持します。
2. 8 時間のスタートウィンドウを使用して、12 時間ごとにバックアップし、1 週間保持します。

24 時間後、2 番目のルールでは 2 つのバックアップを作成します (保持期間が長いため)。最初のルールでは 8 つのバックアップを作成します (2 番目のルールの 8 時間のスタートウィンドウでは、時間単位のバックアップの実行が妨げられるため)。具体的には次のとおりです。

このスタートウィンドウ中	このルールではバックアップを 1 つ作成します。
午前 0 時 ~ 午前 8 時	12 時間ごと
8 ~ 9	毎時
9 ~ 10	毎時
10 ~ 11	毎時
11 ~ 正午	毎時
正午 ~ 午後8時	12 時間ごと
8 ~ 9	毎時
9 ~ 10	毎時
10 ~ 11	毎時
11 ~ 午前 0 時	毎時

開始ウィンドウ中、バックアップジョブのステータスは、正常に開始されるか、開始ウィンドウの時間がなくなるまで CREATED ステータスのままになります。開始ウィンドウ時間内にジョブの再試行を許可するエラー AWS Backup を受け取った場合、 AWS Backup は、バックアップが正常

に開始 (ジョブステータスが に変わるRUNNING) されるまで、またはジョブステータスが に変わるEXPIRED (開始ウィンドウ時間が終了すると発生することが予想される) まで、少なくとも 10 分ごとにジョブの開始を自動的に再試行します。

ライフサイクルとストレージ階層

バックアップが保持される指定された期間のことを、バックアップの「ライフサイクル」と呼びます。バックアップはライフサイクルの終了時まで復元できます。

これは、 AWS Backup コンソールのバックアップルール設定のライフサイクルセクションで、合計保持期間として設定されます。

を使用する場合 AWS CLI、これはパラメータ を使用して設定されますDeleteAfterDays。スナップショットの保持期間は 1 日から 100 年 (入力しない場合は無期限) で、継続的バックアップの保持期間は 1 日から 35 日間です。バックアップの作成日は、バックアップジョブが開始された日付であり、完了した日付ではありません。バックアップジョブが開始されたのと同じ日付に完了しない場合は、バックアップジョブが開始された日付を使用して保持期間を計算します。

バックアップはストレージ階層で保持されます。「AWS Backup の料金」で説明されているように、ストレージと復元にかかるコストは階層ごとに異なります。作成されたバックアップはすべて、ウォームストレージに保存されます。バックアップの保持期間によっては、コールドストレージと呼ばれる低コストの階層にバックアップを移行した方がよい場合もあります。このオプション機能を利用できるリソースについては「リソース別の機能の可用性」を参照してください。

Console

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. バックアッププランを作成または編集します。
3. バックアップルール設定のライフサイクルセクションで、[バックアップをウォームストレージからコールドストレージに移動] チェックボックスをオンにします。
4. (オプション) Amazon EBS がバックアップ対象のリソースの 1 つで、バックアップ頻度が毎月以下の場合は、EBS Snapshots Archive を使用してそれらをコールド階層に移行できます。
5. バックアップをウォームストレージに保持する値 (日数) を入力します。 AWS Backup は、少なくとも 8 日間を推奨します。
6. 合計保持期間の値 (日数) を入力します。合計保持期間とウォームストレージでの保持時間の差は、バックアップがコールドストレージに保持される日数になります。

AWS CLI

1. create-backup-plan または update-backup-plan を使用します。
2.
3. EBS リソースにはブール値パラメータ OptInToArchiveForSupportedResources を指定します。
4. MoveToColdStorageAfterdays パラメータを指定します。
5. DeleteAfterDays パラメータを使用します。この値は、MoveToColdStorageAfterDays に指定した値に 90 (日) を加えた値にする必要があります。

コールドストレージは現在、以下のリソースタイプで利用できます。

リソースタイプ	コールドストレージでの増分バックアップまたはフルバックアップ
AWS CloudFormation	増分
高度な機能ありの DynamoDB	フル。どの階層でも増分バックアップは不可
Amazon EBS (EBS Snapshots Archive を使用)	フル。移行後、増分バックアップはフルバックアップになります。
Amazon EFS	増分
Amazon EC2 インスタンスで実行される SAP HANA データベース	増分
Amazon Timestream	増分
VMware 仮想マシン	増分

コンソールまたはコマンドラインでコールドストレージへの移行を有効にすると、コールドストレージ (またはアーカイブ) のバックアップには以下の条件が適用されます。

- 移行するバックアップは、ウォームストレージの時間に加えて、コールドストレージに最低 90 日間保存する必要があります。 AWS Backup では、保持期間を「数日後にコールドに移行」設定よ

りも 90 日間長く設定する必要があります。バックアップがコールドに移行された後に、「コールドへの移行 (日数)」設定を変更することはできません。

- 増分バックアップをサポートするサービスもあります。増分バックアップの場合、少なくとも 1 つのウォームフルバックアップが必要です。 AWS Backup 少なくとも 8 日後までバックアップをコールドストレージに移動しないようにライフサイクル設定を設定することをお勧めします。フルバックアップがコールドストレージに移行されすぎる場合 (例えば、1 日後にコールドストレージに移行した場合) 、 AWS Backup は別のウォームフルバックアップを作成します。
- 増分バックアップをサポートするリソースタイプでは、移行されたデータがウォームバックアップによって参照されなくなった場合、 はデータをウォームストレージからコールドストレージ AWS Backup に転送します。コールドストレージで保持されているバックアップ内のデータで、他のコールドストレージによってのみ参照されるデータには、コールドストレージ階層の料金が課金されます。それ以外のバックアップには、引き続きウォームストレージ階層の料金が適用されます。

バックアップボールト

バックアップボールトは、バックアップを整理するコンテナです。バックアップルールによって作成されたバックアップは、バックアップルールで指定されたバックアップボールトに整理されます。バックアップボールトを使用して、バックアップボールト内のバックアップを暗号化するために使用される AWS Key Management Service （ AWS KMS) 暗号化キーを設定し、バックアップボールト内のバックアップへのアクセスを制御できます。バックアップボールトを整理しやすいように、バックアップボールトにタグを追加することもできます。デフォルトのボールトを使用しない場合は、独自のものを作成できます。バックアップボールトを作成する step-by-step 手順については、「」を参照してくださいステップ 3: バックアップボールトの作成。

リージョンにコピー

バックアッププランの一部として、オプションで別の AWS リージョンにバックアップコピーを作成できます。詳細については、「AWS リージョン全体でのバックアップのコピーの作成」を参照してください。

バックアップコピーを定義するときは、次のオプションを構成します。

送信先リージョン

バックアップコピーの送信先リージョン。

(詳細設定) バックアップボールト

コピーの送信先バックアップボールト。

(詳細設定) IAM ロール

コピーの作成時に が AWS Backup 使用する IAM ロール。ロールは、 がロールを AWS Backup 引き受けることができる信頼されたエンティティとして AWS Backup リストされている必要もあります。デフォルト を選択し、 AWS Backup デフォルトのロールがアカウントに存在しない場合、正しいアクセス許可を持つロールが作成されます。

(詳細設定) ライフサイクル

バックアップコピーをコールドストレージに移行するタイミングと、コピーの有効期限 (削除) を指定します。コールドストレージに移行されたバックアップは、そこに最低 90 日保存される必要があります。コピーがコールドストレージに移行された後には、この値を変更できません。

[有効期限切れ] で、コピーが作成されてから削除されるまでの日数を指定します。これは、[コールドストレージへの移行] の値より 90 日以上大きい数値にする必要があります。

復旧ポイントに追加されるタグ

ここにリストするタグは、バックアップ作成時に自動的に追加されます。

バックアッププランに追加されるタグ

これらのタグは、バックアッププラン自体に関連付けられます。バックアッププランの整理と追跡に便利です。

バックアップの詳細設定

Amazon EC2 インスタンスで、実行中のサードパーティアプリケーションのアプリケーション整合性のあるバックアップを有効にします。現在、 は Windows VSS backups AWS Backup AWS Backup をサポートしています。Windows VSS バックアップから特定の Amazon EC2 インスタンスタイプを除外します。詳細については、「Windows VSS バックアップの作成」を参照してください。

AWS CloudFormation バックアッププランの テンプレート

リファレンス用に 2 つのサンプル AWS CloudFormation テンプレートが用意されています。最初のテンプレートでは、シンプルなバックアッププランを作成します。2 番目のテンプレートでは、バックアッププランで VSS バックアップが有効になります。

> **Note**
>
> デフォルトのサービスロールを使用している場合は、#######を AWSBackupServiceRolePolicyForBackup に置き換えます。

```
Description: backup plan template to back up all resources daily at 5am UTC, and tag
 all recovery points with backup:daily.

Resources:
  KMSKey:
    Type: AWS::KMS::Key
    Properties:
      Description: "Encryption key for daily"
      EnableKeyRotation: True
      Enabled: True
      KeyPolicy:
        Version: "2012-10-17"
        Statement:
          - Effect: Allow
            Principal:
              "AWS": { "Fn::Sub": "arn:${AWS::Partition}:iam::${AWS::AccountId}:root" }
            Action:
              - kms:*
            Resource: "*"

  BackupVaultWithDailyBackups:
    Type: "AWS::Backup::BackupVault"
    Properties:
      BackupVaultName: "BackupVaultWithDailyBackups"
      EncryptionKeyArn: !GetAtt KMSKey.Arn

  BackupPlanWithDailyBackups:
    Type: "AWS::Backup::BackupPlan"
    Properties:
      BackupPlan:
        BackupPlanName: "BackupPlanWithDailyBackups"
        BackupPlanRule:
          - RuleName: "RuleForDailyBackups"
            TargetBackupVault: !Ref BackupVaultWithDailyBackups
            ScheduleExpression: "cron(0 5 ? * * *)"
    DependsOn: BackupVaultWithDailyBackups
```

```
DDBTableWithDailyBackupTag:
  Type: "AWS::DynamoDB::Table"
  Properties:
    TableName: "TestTable"
    AttributeDefinitions:
      - AttributeName: "Album"
        AttributeType: "S"
    KeySchema:
      - AttributeName: "Album"
        KeyType: "HASH"
    ProvisionedThroughput:
      ReadCapacityUnits: "5"
      WriteCapacityUnits: "5"
    Tags:
      - Key: "backup"
        Value: "daily"

BackupRole:
  Type: "AWS::IAM::Role"
  Properties:
    AssumeRolePolicyDocument:
      Version: "2012-10-17"
      Statement:
        - Effect: "Allow"
          Principal:
            Service:
              - "backup.amazonaws.com"
          Action:
            - "sts:AssumeRole"
    ManagedPolicyArns:
      - "arn:aws:iam::aws:policy/service-role/service-role"

TagBasedBackupSelection:
  Type: "AWS::Backup::BackupSelection"
  Properties:
    BackupSelection:
      SelectionName: "TagBasedBackupSelection"
      IamRoleArn: !GetAtt BackupRole.Arn
      ListOfTags:
        - ConditionType: "STRINGEQUALS"
          ConditionKey: "backup"
          ConditionValue: "daily"
    BackupPlanId: !Ref BackupPlanWithDailyBackups
```

```
    DependsOn: BackupPlanWithDailyBackups
```

```
Description: backup plan template to enable Windows VSS and add backup rule to take
 backup of assigned resources daily at 5am UTC.

Resources:
  KMSKey:
    Type: AWS::KMS::Key
    Properties:
      Description: "Encryption key for daily"
      EnableKeyRotation: True
      Enabled: True
      KeyPolicy:
        Version: "2012-10-17"
        Statement:
          - Effect: Allow
            Principal:
              "AWS": { "Fn::Sub": "arn:${AWS::Partition}:iam::${AWS::AccountId}:root" }
            Action:
              - kms:*
            Resource: "*"

  BackupVaultWithDailyBackups:
    Type: "AWS::Backup::BackupVault"
    Properties:
      BackupVaultName: "BackupVaultWithDailyBackups"
      EncryptionKeyArn: !GetAtt KMSKey.Arn

  BackupPlanWithDailyBackups:
    Type: "AWS::Backup::BackupPlan"
    Properties:
      BackupPlan:
        BackupPlanName: "BackupPlanWithDailyBackups"
        AdvancedBackupSettings:
          - ResourceType: EC2
            BackupOptions:
              WindowsVSS: enabled
        BackupPlanRule:
          - RuleName: "RuleForDailyBackups"
            TargetBackupVault: !Ref BackupVaultWithDailyBackups
            ScheduleExpression: "cron(0 5 ? * * *)"

    DependsOn: BackupVaultWithDailyBackups
```

バックアッププランへのリソースの割り当て

リソース割り当ては AWS Backup 、バックアッププランを使用して保護するリソースを指定します。 AWS Backup では、シンプルなデフォルト設定と、バックアッププランにリソースを割り当てるためのきめ細かなコントロールの両方が提供されます。バックアッププランを実行するたびに、リソース割り当て基準に一致するすべてのリソース AWS アカウント について をスキャンします。このレベルの自動化により、バックアッププランとリソース割り当てを 1 回だけ定義できます。 AWS Backup は、以前に定義したリソース割り当てに適した新しいリソースを検索してバックアップする作業を省くことができます。

が管理することをオプトインした AWS Backupがサポートするリソースタイプ AWS Backup を割り当てることができます。よりサポートされるリソースタイプにオプトインする方法については、AWS Backup「開始方法 1: サービスオプトイン」を参照してください。

AWS Backup コンソールには、バックアッププランにリソースタイプを含める方法として、バックアッププランにリソースタイプを明示的に割り当てるか、すべてのリソースを含めるという 2 つの方法があります。これらの選択がサービスオプトインとどのように連携するかを理解するには、以下のポイントを参照してください。

- リソースの割り当てがタグのみに基づいている場合は、サービスオプトイン設定が適用されます。
- リソースタイプがバックアッププランに明示的に割り当てられている場合、その特定のサービスでオプトインが有効になっていなくても、バックアップに含まれます。これは、Aurora、Neptune、および Amazon DocumentDB には適用されません。これらのサービスを含めるには、オプトインを有効にする必要があります。
- リソース割り当てでリソースタイプとタグの両方が指定されている場合、指定されたリソースタイプが最初にフィルタリングされ、タグはそれらのリソースをさらにフィルタリングします。

  ほとんどのリソースタイプでは、サービスオプトイン設定は無視されます。ただし、Aurora、Neptune、Amazon DocumentDB にはサービスオプトインが必要です。
- アカウントがリージョンで を使用する AWS Backup （ バックアップボールトまたはバックアッププランを作成する) 場合、そのアカウントは、その時点でリージョン AWS Backup で によってサポートされているすべてのリソースタイプに自動的にオプトインされます。後日そのリージョンに追加されたサポート対象サービスは、バックアッププランに自動的に含まれません。サポートされたら、これらのリソースタイプをオプトインできます。
- Amazon FSx for NetApp ONTAP では、タグベースのリソース選択を使用する場合は、ファイルシステム全体ではなく個々のボリュームにタグを適用します。

リソースの割り当てには、リソースタイプとリソースを含める (または除外する) ことができます。

- リソースタイプには、 AWS Backupがサポートする AWS サービスまたはサードパーティーアプリケーションのすべてのインスタンスまたはリソースが含まれます。たとえば、DynamoDB リソースタイプはすべての DynamoDB テーブルを指します。
- リソースは、DynamoDB テーブルの 1 つなど、リソースタイプの単一のインスタンスです。一意のリソース ID を使用してリソースを指定できます。

タグと条件演算子を使用して、リソースの割り当てをさらに絞り込むことができます。

トピック

コンソールを使用したリソースの割り当て

[リソースの割り当て] ページに移動するには:

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. [バックアッププラン] を選択します。
3. [バックアッププランを作成)] を選択します。
4. [テンプレートの選択] のドロップダウンリストで、任意のテンプレートを選択してから、[プランの作成] を選択します。
5. バックアッププラン名を入力します。
6. [プランの作成] を選択します。
7. [リソースを割り当てる] を選択します。

リソースの割り当てを開始するには、[一般] セクションに追加します。

1. リソースの割り当て名を入力します。
2. [既定のロール] または [IAM ロールを選択] を選択します。

> **Note**
>
> IAM ロールを選択した場合は、割り当てるすべてのリソースをバックアップする権限があることを確認します。ロールがバックアップ権限のないリソースに遭遇すると、バックアッププランは失敗します。

リソースを割り当てるには、リソースの割り当てセクションの [リソース選択の定義] で 2 つのオプションのいずれかを選択します。

- すべてのリソースタイプを含める。このオプションは、バックアッププランに割り当てられた現在および将来の AWS Backupでサポートされるすべてのリソースを保護するようにバックアッププランを設定します。このオプションを使用すると、データ資産をすばやく簡単に保護できます。

  このオプションを選択すると、オプションで次のステップとしてタグを使用して選択範囲を絞り込むことができます。
- 特定のリソースタイプを含める。このオプションを選択する場合は、次のステップで特定のリソースタイプを選択する必要があります。

  1. [リソースタイプの選択] ドロップダウンメニューを使用して、1 つ以上のリソースタイプを割り当てます。

     > **Important**
     >
     > RDS、Aurora、Neptune、および DocumentDB は同じ Amazon リソースネーム (ARN) を共有します。 AWS Backup を使用してこれらのリソースタイプの 1 つを管理するようにオプトインすると、バックアッププランに割り当てる際にすべてのリソースタイプがオプトインされます。選択を絞り込むには、タグと条件演算子を使用します。

     完了すると、 は選択したリソースタイプのリストとそのデフォルト設定 AWS Backup を表示します。これは、選択したリソースタイプごとにすべてのリソースを保護するためのものです。
  2. 必要に応じて、選択したリソースタイプから特定のリソースを除外する場合は、次の手順を実行します。

     1. [リソースの選択] ドロップダウンメニューを使用して、デフォルトオプションの選択を解除します。

2. バックアッププランに割り当てる特定のリソースを選択します。

3. オプションで、選択したリソースタイプから特定のリソース ID を除外することができます。このオプションは、前のステップで多くのリソースを選択するよりも高速になる可能性があるため、多数のリソースのうち 1 つまたは少数のリソースを除外する場合に使用します。リソースタイプからリソースを除外する前に、リソースタイプを含める必要があります。次のステップを使用して、リソース ID を除外します。

   1. [選択したリソースタイプから特定のリソース ID を除外する] で、リソースタイプの選択を使用して含めたリソースタイプを 1 つ以上選択します。
   2. リソースタイプごとに、リソースの選択メニューを使用して、除外するリソースを 1 つ以上選択します。

以前の選択肢に加えて、オプションのタグを使用して選択範囲を絞り込む機能を使用して、さらに詳細な選択を行うことができます。この機能を使用すると、タグを使用してリソースのサブセットを含めるように現在の選択を絞り込むことができます。

タグは、リソースの特定、整理、およびフィルタリングに役立つ特定のリソースに割り当てることができるキーと値のペアです。タグでは、大文字と小文字が区別されます。詳細については、AWS 全般リファレンスの「AWS リソースのタグ付け」を参照してください。

2 つ以上のタグを使用して選択範囲を絞り込むと、効果は AND 条件になります。たとえば、2 つのタグを使用して選択範囲を絞り込むと、`env: prod` および `role: application` では、両方のタグを持つリソースのみをバックアッププランに割り当てます。

タグを使用して選択を絞り込むには:

1. [タグを使用して選択範囲を絞り込む] で、ドロップダウンリストから [キー] を選択します。
2. ドロップダウンリストから [値の条件] を選択します。

   - 値は、次の入力、つまりキーと値のペア値を指します。
   - 条件は `Equals`、`Contains`、`Begins with` または `Ends with`、またその逆は `Does not equal`、`Does not contain`、`Does not begin with` または `Does not end with` です。

3. ドロップダウンリストから [値] を選択します。
4. 別のタグを使用してさらに絞り込むには、[タグの追加] を選択します。

プログラムによるリソースの割り当て

JSON ドキュメントでリソースの割り当てを定義できます。このサンプルリソース割り当ては、すべての Amazon EC2 インスタンスをバックアッププラン *BACKUP-PLAN-ID* に割り当てます。

```
{
  "BackupPlanId":"BACKUP-PLAN-ID",
  "BackupSelection":{
    "SelectionName":"resources-list-selection",
    "IamRoleArn":"arn:aws:iam::ACCOUNT-ID:role/IAM-ROLE-ARN",
    "Resources":[
      "arn:aws:ec2:*:*:instance/*"
    ]
  }
}
```

この JSON が backup-selection.json として保存されていると仮定すると、次の CLI コマンドを使用して、これらのリソースをバックアッププランに割り当てることができます。

```
aws backup create-backup-selection --cli-input-json file://PATH-TO-FILE/backup-selection.json
```

以下は、対応する JSON ドキュメントとともにリソース割り当ての例です。このテーブルを読みやすくするために、例ではフィールド "BackupPlanId"、"SelectionName"、および "IamRoleArn" を省略しています。ワイルドカード * は 0 個以上の空白でない文字を表します。

Example 例: アカウント内のすべてのリソースを選択する

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ]
  }
}
```

Example 例: アカウント内のすべてのリソースを選択するが、EBS ボリュームを除外する

```
{
  "BackupSelection":{
    "Resources":[
```

```
      "*"
    ],
    "NotResources":[
      "arn:aws:ec2:*:*:volume/*"
    ]
  }
}
```

Example 例: でタグ付けされたすべてのリソースを選択するが"backup":"true"、EBS ボリュームを除外する

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "NotResources":[
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ]
    }
  }
}
```

Example 例: すべての EBS ボリュームと、 と の両方のタグが付いた RDS DB インスタンスを選択する "backup":"true""stage":"prod"

ブール値の算術は IAM ポリシーの場合と同様であり、"Resources" はブール値 OR を使用して組み合わせ、"Conditions" はブール値 AND を使用して組み合わせます。

対応する Aurora、Neptune、または DocumentDB リソースがないため、"Resources" 式 "arn:aws:rds:*:*:db:*" では RDS DB インスタンスのみが選択されます。

```
{
  "BackupSelection":{
    "Resources":[
```

```
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:rds:*:*:db:*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        },
        {
          "ConditionKey":"aws:ResourceTag/stage",
          "ConditionValue":"prod"
        }
      ]
    }
  }
}
```

Example 例: タグ付けされている"backup":"true"がタグ付けされていないすべての EBS ボリュームと RDS インスタンスを選択する "stage":"test"

```
{
  "BackupSelection":{
    "Resources":[
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:rds:*:*:db:*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ],
      "StringNotEquals":[
        {
          "ConditionKey":"aws:ResourceTag/stage",
          "ConditionValue":"test"
        }
      ]
    }
  }
}
```

Example 例: でタグ付けされたすべてのリソース"key1"と、 で始まる"include"が で始まる値"key2"、および という単語を含む値ではない値を選択します。 "exclude"

ワイルドカード文字は文字列の先頭、最後、および途中で使用できます。上記の例の `include*` および `*exclude*` でワイルドカード文字 (*) を使用することに注意してください。前の例 `arn:aws:rds:*:*:db:*` のように、文字列の途中にワイルドカード文字を使用することもできます。

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "Conditions":{
      "StringLike":[
        {
          "ConditionKey":"aws:ResourceTag/key1",
          "ConditionValue":"include*"
        }
      ],
      "StringNotLike":[
        {
          "ConditionKey":"aws:ResourceTag/key2",
          "ConditionValue":"*exclude*"
        }
      ]
    }
  }
}
```

Example 例: FSx ファイルシステムと RDS、Aurora、Neptune、DocumentDB リソース"backup":"true"を除く、 でタグ付けされたすべてのリソースを選択する

`NotResources` の項目は、ブール値 OR を使用して結合されます。

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "NotResources":[
      "arn:aws:fsx:*",
```

```
      "arn:aws:rds:*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ]
    }
  }
}
```

Example 例: タグ"backup"と任意の値でタグ付けされたすべてのリソースを選択する

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "Conditions":{
      "StringLike":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"*"
        }
      ]
    }
  }
}
```

Example 例: でタグ付けされたリソースを除く、すべての FSx ファイルシステム"my-aurora-cluster"、Aurora クラスター "backup":"true"、および でタグ付けされたすべてのリソースを選択します。 "stage":"test"

```
{
  "BackupSelection":{
    "Resources":[
      "arn:aws:fsx:*",
      "arn:aws:rds:*:*:cluster:my-aurora-cluster"
    ],
    "ListOfTags":[
```

```
      {
        "ConditionType":"StringEquals",
        "ConditionKey":"backup",
        "ConditionValue":"true"
      }
    ],
    "Conditions":{
      "StringNotEquals":[
        {
          "ConditionKey":"aws:ResourceTag/stage",
          "ConditionValue":"test"
        }
      ]
    }
  }
}
```

Example 例: でタグ付けされた EBS ボリューム**"backup":"true"**を除く、 タグでタグ付けされたすべてのリソースを選択する **"stage":"test"**

2 つの CLI コマンドを使用して、このリソースグループを選択するための 2 つの選択項目を作成します。最初の選択は、EBS ボリュームを除くすべてのリソースに適用されます。2 番目の選択は EBS ボリュームに適用されます。

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "NotResources":[
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ]
    }
  }
}
```

```
{
  "BackupSelection":{
    "Resources":[
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ],
      "StringNotEquals":[
        {
          "ConditionKey":"aws:ResourceTag/stage",
          "ConditionValue":"test"
        }
      ]
    }
  }
}
```

を使用したリソースの割り当て AWS CloudFormation

この end-to-end AWS CloudFormation テンプレートは、リソース割り当て、バックアッププラン、および宛先バックアップボールトを作成します。

- という名前のバックアップボールト*CloudFormationTestBackupVault*。
- という名前のバックアッププラン*CloudFormationTestBackupPlan*。このプランでは 2 つのバックアップルールが含まれており、どちらも毎日正午 12 時 (UTC) にバックアップを行い、それらを 210 日間保持します。
- という名前のリソース選択*BackupSelectionName*。
- • リソース割り当ては、次のリソースをバックアップします。
  - キーバリューのペア backupplan:dsi-sandbox-daily でタグ付けされた任意のリソース。
  - prod または prod/ で始まる値でタグ付けされたリソース。
- リソースの割り当てでは、次のリソースはバックアップされません。
  - RDS、Aurora、Neptune、または DocumentDB クラスターのどれでもかまいません。

- test または test/ で始まる値でタグ付けされたリソース。

```
Description: "Template that creates Backup Selection and its dependencies"
Parameters:
  BackupVaultName:
    Type: String
    Default: "CloudFormationTestBackupVault"
  BackupPlanName:
    Type: String
    Default: "CloudFormationTestBackupPlan"
  BackupSelectionName:
    Type: String
    Default: "CloudFormationTestBackupSelection"
  BackupPlanTagValue:
    Type: String
    Default: "test-value-1"
  RuleName1:
    Type: String
    Default: "TestRule1"
  RuleName2:
    Type: String
    Default: "TestRule2"
  ScheduleExpression:
    Type: String
    Default: "cron(0 12 * * ? *)"
  StartWindowMinutes:
    Type: Number
    Default: 60
  CompletionWindowMinutes:
    Type: Number
    Default: 120
  RecoveryPointTagValue:
    Type: String
    Default: "test-recovery-point-value"
  MoveToColdStorageAfterDays:
    Type: Number
    Default: 120
  DeleteAfterDays:
    Type: Number
    Default: 210
Resources:
  CloudFormationTestBackupVault:
```

```
    Type: "AWS::Backup::BackupVault"
    Properties:
      BackupVaultName: !Ref BackupVaultName
  BasicBackupPlan:
    Type: "AWS::Backup::BackupPlan"
    Properties:
      BackupPlan:
        BackupPlanName: !Ref BackupPlanName
        BackupPlanRule:
          - RuleName: !Ref RuleName1
            TargetBackupVault: !Ref BackupVaultName
            ScheduleExpression: !Ref ScheduleExpression
            StartWindowMinutes: !Ref StartWindowMinutes
            CompletionWindowMinutes: !Ref CompletionWindowMinutes
            RecoveryPointTags:
              test-recovery-point-key-1: !Ref RecoveryPointTagValue
            Lifecycle:
              MoveToColdStorageAfterDays: !Ref MoveToColdStorageAfterDays
              DeleteAfterDays: !Ref DeleteAfterDays
          - RuleName: !Ref RuleName2
            TargetBackupVault: !Ref BackupVaultName
            ScheduleExpression: !Ref ScheduleExpression
            StartWindowMinutes: !Ref StartWindowMinutes
            CompletionWindowMinutes: !Ref CompletionWindowMinutes
            RecoveryPointTags:
              test-recovery-point-key-1: !Ref RecoveryPointTagValue
            Lifecycle:
              MoveToColdStorageAfterDays: !Ref MoveToColdStorageAfterDays
              DeleteAfterDays: !Ref DeleteAfterDays
      BackupPlanTags:
        test-key-1: !Ref BackupPlanTagValue
    DependsOn: CloudFormationTestBackupVault

  TestRole:
    Type: "AWS::IAM::Role"
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: "Allow"
            Principal:
              Service:
                - "backup.amazonaws.com"
            Action:
```

```
              - "sts:AssumeRole"
      ManagedPolicyArns:
        - !Sub "arn:${AWS::Partition}:iam::aws:policy/service-
role/AWSBackupServiceRolePolicyForBackup"
  BasicBackupSelection:
    Type: 'AWS::Backup::BackupSelection'
    Properties:
      BackupPlanId: !Ref BasicBackupPlan
      BackupSelection:
        SelectionName: !Ref BackupSelectionName
        IamRoleArn: !GetAtt TestRole.Arn
        ListOfTags:
          - ConditionType: STRINGEQUALS
            ConditionKey: backupplan
            ConditionValue: dsi-sandbox-daily
        NotResources:
          - 'arn:aws:rds:*:*:cluster:*'
        Conditions:
          StringEquals:
            - ConditionKey: 'aws:ResourceTag/path'
              ConditionValue: prod
          StringNotEquals:
            - ConditionKey: 'aws:ResourceTag/path'
              ConditionValue: test
          StringLike:
            - ConditionKey: 'aws:ResourceTag/path'
              ConditionValue: prod/*
          StringNotLike:
            - ConditionKey: 'aws:ResourceTag/path'
              ConditionValue: test/*
```

リソースの割り当てクォータ

次のクォータは、単一のリソースの割り当てに適用されます。

- ワイルドカードを含まない 500 Amazon リソースネーム (ARN)
- ワイルドカード表現の 30 ARN
- 30 条件
- リソース割り当てごとに 30 タグ (タグあたりのリソース数に制限はありません)

バックアッププランの削除

バックアッププランは、関連付けられた選択リソースがすべて削除された後に削除できます。これらの選択は、リソース割り当て とも呼ばれます。バックアッププランの削除前にこれらが削除されていない場合、コンソールに「関連するバックアッププランの選択はバックアッププランの削除前に削除する必要があります」というエラーが表示されます。コンソールを使用するか、 を使用しますDeleteBackupSelection。

バックアッププランを削除すると、そのプランの現在のバージョンが削除されます。現在のバージョンと以前のバージョン (存在する場合) はまだ存在しますが、それらはコンソールの [Backup plans (バックアッププラン)] に表示されなくなります。

> **Note**
>
> バックアッププランを削除しても、既存のバックアップは削除されません。既存のバックアップを削除するには、バックアップの削除のステップを使用してバックアップボールトから削除します。

AWS Backup コンソールを使用してバックアッププランを削除するには

1. にサインインし AWS Management Console、https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. 左側にあるナビゲーションペインで、[Backup plans (バックアッププラン)] を選択します。
3. リストで、バックアッププランを選択します。
4. そのバックアッププランに関連付けられているリソース割り当てがあればそれを選択します。
5. [削除] を選択します。

バックアッププランの更新

バックアップ計画の作成後に、プランを編集できます。たとえば、タグを追加したり、バックアップルールを追加、編集、削除したりできます。バックアッププランに対する変更は、そのバックアッププランによって作成された既存のバックアップには影響しません。変更後に作成されるバックアップのみに適用されます。

たとえば、バックアップルールでバックアップの保持期間を更新しても、更新前に作成されたバックアップの保持期間は変わりません。今後そのルールによって作成されたバックアップには、更新された保持期間が反映されます。

作成後にプランの名前を変更することはできません。

AWS Backup コンソールを使用してバックアッププランを編集するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[バックアッププラン] を選択します。
3. 2 番目のペインの Backup プラン の下に、既存のバックプランが表示されます。Backup プラン名の列にある下線付きリンクを選択すると、選択したバックアッププランの詳細が表示されます。
4. バックアップルールの編集、リソース割り当ての表示、バックアップジョブの表示、タグの管理、Windows VSS 設定の変更を行うことができます。
5. バックアップルールを更新するには、バックアップルールの名前を選択します。

   タグを追加または削除するには、タグの管理を選択します。

   Windows VSS のオンとオフを切り替えるには、高度なバックアップ設定の横にある編集を選択します。
6. 希望する設定を変更し、 の保存 を選択します (複数可) 。

バックアップボールト

> **Note**
>
> 2023 年 8 月 9 日以降、 AWS Backup は論理エアギャップボールト を使用するためのプレビューを提供しています。このプレビューに登録するには、<aws-backup-vault-preview@amazon.com> にメールでリクエストを送信します。プレビュー期間中、およびプレビュー期間後に、機能が変更または調整される場合があります。サービスの一般提供 (GA) が開始されると、プレビュー中に提供されたデータや構成は利用できなくなります。 AWS として、プレビューでは、実稼働データではなくテストデータを使用することをおすすめします。

では AWS Backup、バックアップボールトはバックアップを保存および整理するコンテナです。

バックアップボールトを作成するときは、このボールトに配置されたバックアップの一部を暗号化する AWS Key Management Service （ AWS KMS) 暗号化キーを指定する必要があります。他のバックアップの暗号化は、ソース AWS サービスによって管理されます。暗号化の詳細については、「AWSでのバックアップの暗号化」チャートを参照してください。

アカウントには、常にデフォルトのバックアップボールトがあります。バックアップグループ別に異なる暗号化キーやアクセスポリシーが必要な場合は、複数のバックアップボールトを作成できます。

このセクションでは、 AWS Backupでバックアップボールトを管理する方法の概要を示します。

トピック

- 論理エアギャップボールト (プレビュー)
- バックアップボールトの作成
- バックアップボールトでのアクセスポリシーの設定
- AWS Backup ボールトロック
- バックアップボールトを削除する

論理エアギャップボールト (プレビュー)

> **Note**
>
> 2023 年 8 月 9 日以降、 AWS Backup は論理エアギャップボールト を使用するためのプレビューを提供しています。このプレビューに登録するには、<aws-backup-vault-preview@amazon.com> にメールでリクエストを送信します。プレビュー期間中、およびプレビュー期間後に、機能が変更または調整される場合があります。サービスの一般提供 (GA) が開始されると、プレビュー中に提供されたデータや構成は利用できなくなります。 AWS として、プレビューでは、実稼働データではなくテストデータを使用することをおすすめします。

概要

AWS Backup は、バックアップのコピーを他のボールトに保存できるセカンダリタイプのボールトをプレビューしています。論理エアギャップボールトは、特別なボールトとして、バックアップボールトの機能に加えてセキュリティ機能が強化されているほか、他のアカウントや組織とボールトへのアクセスを共有できるため、リソースの迅速な復旧が必要なインシデントが発生した場合に、復旧時間 (RTO) を速く、柔軟に行えるようになります。

論理エアギャップボールトには追加の保護機能が備わっています。これらのボールトはそれぞれ AWS 所有キーで暗号化され、各ボールトにはコンプライアンスモードでボールトロックが設定されています。

論理エアギャップボールトを組織やアカウント間で共有して、必要に応じてボールとを共有しているアカウントからその中に保存されているバックアップを復元できるようにすることもできます。

プレビュー期間中は、論理エアギャップボールトのストレージに追加料金はかかりません。論理エアギャップボールトにあるバックアップのコピーには課金されませんが、標準のバックアップボールトとクロスリージョンコピーのバックアップは、引き続き公表された料金 (「料金」を参照) で課金されます。

ユースケース

論理エアギャップボールトは、データ保護戦略の一環として機能するセカンダリボールトです。このボールトは、次のようなバックアップ用ボールトを希望する場合に、組織的な保持と復元を強化するのに役立ちます。

- コンプライアンスモードで自動的にボールトロックが設定されるもの
- バックアップを作成したアカウントとは別のアカウントと共有したり復元したりできるバックアップが含まれているもの
- AWS 所有キーで暗号化されている

論理エアギャップボールトでは、以下のリソースがサポートされます。

- Amazon EC2
- Amazon EBS
- Amazon S3
- Amazon EFS
- Amazon RDS

論理エアギャップボールトの、このプレビューは、米国東部 (バージニア北部) リージョンでのみ利用できます。この機能は現在 1 つのリージョンでのみ利用できるため、このプレビュー期間中はクロスリージョンコピーはサポートされていません。

標準のバックアップボールトとの比較対照

バックアップボールトは、 で使用されるボールトのプライマリタイプおよび標準タイプです AWS Backup。バックアップが作成されると、各バックアップはバックアップボールトに保存されます。リソースベースのポリシーを割り当てて、ボールト内に保存されているバックアップのライフサイクルなど、ボールトに保存されているバックアップを管理できます。

論理エアギャップボールトは、セキュリティが強化され、復旧時間 (RTO) を短縮するための柔軟な共有機能を備えた特別なボールトです。このボールトには、最初に作成されて標準のバックアップボールトに保存されたバックアップのコピーが保管されます。

バックアップボールトはキーで暗号化できます。これは、アクセスを、意図されているユーザーに制限するセキュリティメカニズムです。これらのキーは、カスタマー管理でも AWS 管理でもかまいません。さらに、バックアップボールトはボールトロックによってさらに保護できます。論理エアギャップボールトには、コンプライアンスモードのボールトロックが装備されています。

初期リソースの作成時に AWS KMS キーを手動で変更またはカスタマーマネージドキー (CMK) として設定しなかった場合、バックアップを論理エアギャップボールトにコピーすることはできません。

機能	バックアップボールト	論理エアギャップボールト (プレビュー)
バックアップの作成	バックアップが作成されると、復旧ポイントとして保存されます	作成時にはバックアップはこのボールトには保存されません
バックアップストレージ	リソースの初期バックアップとバックアップのコピーを保存できます	他のボールトからのバックアップのコピーを保存できます
セキュリティ	オプションでキーで暗号化可能 (カスタマー管理または AWS 管理) オプションでボールトロックでロック可能です	AWS 所有キーで暗号化されている コンプライアンスモードでは常にボールトロックでロックされます
共有性	アクセスはポリシーと AWS Organizations によって管理できます と互換性がありません AWS Resource Access Manager	オプションとして、AWS RAM を用いてアカウント間で共有できます
復元	バックアップが、ボールトを所有しているのと同じアカウントで復元できます	バックアップを所有しているアカウントとは別のアカウントでボールトが共有されている場合、その別のアカウントでバックアップを復元できます
リージョナリティー	AWS Backup が動作するすべてのリージョンで使用可能	プレビュー中に米国東部 (バージニア北部) リージョンで使用できます
リソースhttps://docs.aws.amazon.com/aws-backup/lat	AWS Backup サポートされているすべてのリソースを含むバックアップを保存できます	Amazon EC2、Amazon EBS、Amazon EFS、Amazon S3、または Amazon RDS

機能	バックアップボールト	論理エアギャップボールト (プレビュー)
est/devguide/whatisbackup.html#supported-resources		データを含むバックアップを保存できます

論理エアギャップボールトをコンソールから作成する

> **Important**
>
> ボールトが作成されると、ボールト名、ボールトタイプ、最小保持期間と最大保持期間を変更することはできません。また、ボールトロックを削除することもできません。
> サービスが一般利用可能になると、プレビュー中に提供されるデータと設定は利用できなくなります。 AWS プレビューでは、本番データの代わりにテストデータを使用することをお勧めします。

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[ボールト] を選択します。
3. どちらのタイプのボールトも表示されます。[新しいボールトを作成] を選択します。
4. バックアップボールトの名前を入力します。保存するものがわかるような名前や、必要なバックアップを検索しやすい名前を付けることができます。例えば、`FinancialBackups` のような名前を付けます。
5. [論理エアギャップボールト] ラジオボタンを選択します。
6. [最小保持期間] を設定します。

   この値 (日単位、月単位、年単位) は、バックアップをこのボールトに保持できる最短期間です。保持期間がこの値より短いバックアップは、このボールトにコピーできません。
7. [最大保持期間] を設定します。

   この値 (日単位、月単位、年単位) は、バックアップをこのボールトに保持できる最長期間です。保持期間がこの値を超えるバックアップは、このボールトにコピーできません。
8. (オプション) 論理エアギャップボールトを検索して識別するのに役立つタグを追加します。例えば、`BackupType:Financial` というタグを追加できます。
9. [ボールトを作成] を選択します。

10. 設定を確認します。すべての設定が意図したとおりに表示されたら、[論理的に工アギャップのあるボールトを作成] を選択します。
11. コンソールに新しいボールトの詳細ページが表示されます。ボールトの詳細が想定どおりであることを確認します。

論理工アギャップボールトの詳細をコンソールに表示

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. 左側のナビゲーションペインで、[ボールト] を選択します。
3. ボールトの説明の下には、「このアカウントが所有するボールト」と「このアカウントと共有されるボールト」の 2 つのリストが表示されます。ボールトを表示するには、目的のタブを選択します。
4. [ボールト名] で、ボールトの名前をクリックして詳細ページを開きます。概要、復旧ポイント、保護対象リソース、アカウント共有、アクセスポリシー、タグの詳細を表示できます。

コンソールで、標準のバックアップボールトから、論理工アギャップボールトにコピーします。

論理工アギャップボールトは、バックアッププランではコピージョブのコピー先ターゲット、またはオンデマンドコピージョブのターゲットにしかなれません。

コピージョブを開始するには、次のものが必要です

- バックアップボールト
- 論理工アギャップボールト
- Amazon EC2、Amazon EBS、Amazon RDS、Amazon S3、または Amazon EFS データを含むバックアップ
- コピーの作成に使用されているロールのアクセス許可 `kms:CreateGrant`。
- 論理工アギャップボールトへのコピージョブの一部として AWS マネージドキーで暗号化されたバックアップはありません

上記を確認したら、

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

2. 左側のナビゲーションペインで、[ボールト] を選択します。
3. ボールトの詳細ページには、そのボールト内のすべての復旧ポイントが表示されます。コピーする復旧ポイントの横にチェックマークを付けます。
4. 次に [アクション] を選択し、ドロップダウンメニューから [編集] を選択します。
5. 次の画面で、コピー先の詳細を入力します。

    a. リージョンを米国東部 (バージニア北部) に設定する必要があります
    b. コピー先バックアップボールトドロップダウンメニューに、対象となるコピー先ボールトが表示されます。そのうちの一つを選択し、「`logically air-gapped vault`」と入力します。
6. すべての詳細設定を完了したら、[コピー] を選択します。

コンソールの [ジョブ] ページで [コピー] ジョブを選択すると、現在のコピージョブを表示できます。

詳細については、「バックアップのコピー」、「クロスリージョンバックアップ」、「クロスアカウントバックアップ」を参照してください。

論理エアギャップボールトをコンソールから共有する

> **Note**
>
> アカウントの共有や共有管理ができるのは、特定の IAM 権限を持つアカウントだけです。

AWS RAM を使用して、指定した他のアカウントと論理エアギャップボールトを共有できます。を使用して共有するには AWS RAM、以下があることを確認します。

- にアクセスできる 2 つ以上のアカウント AWS Backup
- 共有するアカウントには、必要な RAM アクセス許可があります。この手順にはアクセス許可 `ram:CreateResourceShare` が必要です。ポリシー `AWSResourceAccessManagerFullAccess` には、必要な RAM 関連のアクセス許可がすべて含まれています。
- 少なくとも 1 つの論理エアギャップボールト

論理エアギャップボールトを共有するには、

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. 左側のナビゲーションペインで、[ボールト] を選択します。
3. ボールトの説明の下には、「このアカウントが所有するボールト」と、「このアカウントと共有されるボールト」の 2 つのリストが表示されます。目的のリストを選択すると、ボールトが表示されます。
4. [ボールト名]で、論理エアギャップボールトの名前を選択し、詳細ページを開きます。
5. [アカウント共有] ペインには、ボールトがどのアカウントと共有されているかが表示されます。
6. 別のアカウントとの共有を開始したり、すでに共有されているアカウントを編集したりするには、[共有の管理] を選択します。

AWS RAM 共有の管理が選択されると、コンソールが開きます。 AWS RAM を使用してリソースを共有する手順については、AWS 「RAM でのリソース共有の作成」を参照してください。

適切なアクセス許可があることを確認します。Backup Administrator IAM ポリシー [AWSBackupFullAccess] と Backup Operator IAM ポリシー [AWSBackupOperatorAccess] には、共有アカウントを表示するために必要なアクセス許可が含まれていますが、共有に使用するロールには、 などの RAM からアカウントを共有するための Resource Access Manager の書き込みアクセス許可が必要です`ram:CreateResourceShare`。

共有を受信する招待を承諾するよう招待されたアカウントは、12 時間以内にその招待を受け入れる必要があります。「AWS RAM ユーザーガイド」の「リソース共有の招待の承諾と拒否」を参照してください。

共有手順が完了して承諾されると、ボールトの概要ページが [アカウント共有] = [共有 - 下記のアカウント共有表をご覧ください] の下に表示されます。

コンソールを使用して、論理エアギャップボールトからバックアップを復元する

論理エアギャップボールトに保存されているバックアップは、そのボールトを所有しているアカウントから、またはそのボールトを共有している任意のアカウントから復元できます。

復旧ポイントを復元する方法については、「バックアップの復元」を参照してください。

コンソールを使用して、論理エアギャップボールトを削除

> **Important**
>
> サービスが一般利用可能になると、プレビュー中に提供されるデータと設定は利用できなくなります。 AWS プレビューでは、本番データの代わりにテストデータを使用することをお勧めします。

ボールトを削除するには、「バックアップボールトの削除」を参照してください。バックアップ (復旧ポイント) がまだ保存されているボールとは削除できません。削除操作を開始する前に、ボールトにバックアップがないことを確認してください。

CLI/API による論理エアギャップボールト

を使用して AWS CLI 、論理エアギャップボールトのオペレーションをプログラムで実行できます。各 CLI は、その CLI が発信される AWS サービスに固有です。共有に関連するコマンドには `aws ram` が付加されています。他のすべてのコマンドには `aws backup` が付加される必要があります。

作成

以下のサンプル CLI コマンド `CreateLogicallyAirGappedBackupVault` を変更して、論理的にエアギャップのあるバックアップボールトを作成できます。

```
aws backup create-logically-air-gapped-backup-vault \
--region us-east-1 \
--backup-vault-name sampleName \
--min-retention-days 7 \
--max-retention-days 35 \
--creator-request-id 123456789012-34567-8901 // optional
```

詳細を表示

以下のサンプル CLI コマンド `DescribeBackupVault` を変更して、ボールトに関する詳細を取得できます。

```
aws backup describe-backup-vault \
--region us-east-1  \
```

```
--backup-vault-name testvaultname
```

共有

> **Note**
>
> アカウントを共有および共有管理できるのは、十分な IAM アクセス許可を持つアカウントだけです。

ユーザーがリソースを共有できるようにするサービスである AWS Resource Access Manager (RAM) を通じて、論理エアギャップボールトを共有できます。

AWS RAM は CLI コマンド を使用しますcreate-resource-share。このコマンドにアクセスできるのは、十分な許可を持つ管理者アカウントだけです。CLI の手順については、「AWS RAMでのリソース共有の作成」を参照してください。

ステップ 1~4 は、論理エアギャップボールトを所有するアカウントで行います。ステップ 5~8 は、論理エアギャップボールトを共有するアカウントで行います。

1. 所有しているアカウントにログインするか、ソースアカウントにアクセスするための十分な認証情報を組織のユーザーに要求すると、次の手順は完了します。
   - リソース共有が以前に作成されており、それにリソースを追加する場合は、代わりに新しいボールトの ARN とともに CLI associate-resource-share を使用してください。
2. RAM 経由で共有するのに十分な許可を持つロールの認証情報を取得します。これらを CLI に入力します。
   - この手順にはアクセス許可 ram:CreateResourceShare が必要です。ポリシーAWSResourceAccessManagerFullAccessには、RAM 関連のアクセス許可がすべて含まれています。
3. を使用しますcreate-resource-share。
   a. 論理エアギャップボールトの ARN を含めます。
   b. 入力例:

```
aws ram create-resource-share \
--name MyLogicallyAirGappedVault \
```

```
--resource-arns arn:aws:backup:us-east-1:123456789012:backup-vault:test-vault-1
 \
--principals 123456789012 \
--region us-east-1
```

出力例:

```
{
   "resourceShare":{
      "resourceShareArn":"arn:aws:ram:us-east-1:123456789012:resource-
share/12345678-abcd-09876543",
      "name":"MyLogicallyAirGappedVault",
      "owningAccountId":"123456789012",
      "allowExternalPrincipals":true,
      "status":"ACTIVE",
      "creationTime":"2021-09-14T20:42:40.266000-07:00",
      "lastUpdatedTime":"2021-09-14T20:42:40.266000-07:00"
   }
}
```

4. 出力内のリソース共有 ARN をコピーします (これは以降のステップで必要です)。共有の受け取りを招待するアカウントのオペレーターに ARN を渡します。
5. リソース共有 ARN を取得します

   a. ステップ 1～4 を実行しなかった場合は、実行した resourceShareArn を取得します。

   b. 例: arn:aws:ram:us-east-1:*123456789012*:resource-share/*12345678-abcd-09876543*
6. CLI では、受取人のアカウントの認証情報を想定します。
7. 「get-resource-share-invitations」を使ってリソース共有の招待を取得します。詳細については、「AWS RAM ユーザーガイド」の「招待の承諾と拒否」を参照してください。
8. コピー先 (リカバリ) アカウントで招待を承諾します。

   - 「accept-resource-share-invitation」を使用します (「reject-resource-share-invitation」も可能です)。

リスト

CLI コマンド「ListBackupVaults」を変更して、アカウントが所有し、アカウント内に存在するすべてのボールトを一覧表示できます。

```
aws backup list-backup-vaults \
--region us-east-1
```

論理エアギャップボールトのみを一覧表示するには、以下のパラメーターを追加します

```
--by-vault-type LOGICALLY_AIR_GAPPED_BACKUP_VAULT
```

アカウントと共有されているボールトを一覧表示するには、お以下を使用します

```
aws backup list-backup-vaults \
--region us-east-1 \
--by-shared
```

[Copy] (コピー)

論理エアギャップボールトは、バックアップのコピージョブのターゲットにしかなれず、初期バックアップジョブのターゲットにはなれません。StartCopyJob を使用して、バックアップボールトにある既存のバックアップを、論理エアギャップボールトにコピーします。

論理エアギャップボールトへのコピージョブを作成するために使用するロールには、アクセス許可 `kms:CreateGrant` が含まれている必要があります。

CLI 入力のサンプル:

```
aws backup start-copy-job \
--region us-east-1 \
--recovery-point-arn arn:aws:resourcetype:region::snapshot/snap-12345678901234567 \
--source-backup-vault-name sourcevaultname \
--destination-backup-vault-arn arn:aws:backup:us-east-1:123456789012:backup-
vault:destinationvaultname \
--iam-role-arn arn:aws:iam::123456789012:role/service-role/servicerole
```

復元

論理エアギャップボールトからアカウントにバックアップが共有されたら、StartRestoreJob を使用してバックアップを復元できます。CLI 入力のサンプル:

```
aws backup start-restore-job \
--recovery-point-arn arn:aws:backup:us-east-1:accountnumber:recovery-
point:RecoveryPointID \
```

```
--metadata {\"availabilityzone\":\"us-east-1d\"} \
--idempotency-token TokenNumber \
--resource-type ResourceType \
--iam-role arn:aws:iam::number:role/service-role/servicerole \
--region us-east-1
```

削除

以下のサンプル CLI コマンド「DeleteBackupVault」を変更して、ボールトを削除できます。ボールト を削除できるのは、ボールト内にバックアップ (復旧ポイント) がない場合のみです。

```
aws backup delete-backup-vault
--region us-east-1
--backup-vault-name testvaultname
```

プログラムによるその他のオプションには以下のものがあります。

- CreateBackupPlan
- UpdateBackupPlan
- DescribeRecoveryPoint
- ListRecoveryPointByBackupVault
- ListProtectedResourcesByBackupVault

バックアップボールトの作成

バックアッププランを作成するか、バックアップジョブを開始する前に、少なくとも 1 つのボールトを作成する必要があります。

で AWS Backup コンソールを初めて使用すると AWS リージョン、コンソールは自動的にデフォルトのボールトを作成します。

ただし、、 AWS CLI AWS SDK、または AWS Backup を使用して を使用する場合 AWS CloudFormation、デフォルトのボールトは作成されません。独自のボールトを作成する必要があります。

必要なアクセス許可

を使用してバックアップボールトを作成するには、次のアクセス許可が必要です AWS Backup。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:DescribeKey",
        "kms:RetireGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource":
 "arn:aws:kms:region:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    {
      "Effect": "Allow",
      "Action": [
        "backup:CreateBackupVault"
      ],
      "Resource": "arn:aws:backup:region:444455556666:backup-vault:*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "backup-storage:MountCapsule"
      ],
      "Resource": "*"
    }
  ]
}
```

バックアップボールトの作成 (コンソール)

AWS Backup コンソールを使用してバックアップボールトを作成する step-by-step 手順については、「入門ガイドステップ 3: バックアップボールトの作成」の「」を参照してください。

バックアップボールトの作成 (プログラムによる)

次の AWS Command Line Interface コマンドは、バックアップボールトを作成します。

```
aws backup create-backup-vault --backup-vault-name test-vault
```

バックアップボールトに次の設定を指定することもできます。

バックアップボールト名

バックアップボールト名では大文字と小文字が区別されます。2 ~ 50 文字の英数字、ハイフン、またはアンダースコアを含める必要があります。

AWS KMS 暗号化キー

AWS KMS 暗号化キーは、このバックアップボールトのバックアップを保護します。デフォルトでは、 AWS Backup によってエイリアス aws/backup の KMS キーを作成します。そのキーを選択するか、アカウント内の他のキーを選択できます (クロスアカウント KMS キーは CLI で使用できます)。

新しい暗号化キーを作成するには、AWS Key Management Service 開発者ガイドの [キーの作成] の手順に従います。

バックアップボールトを作成して AWS KMS 暗号化キーを設定すると、そのバックアップボールトのキーを編集できなくなります。

AWS Backup ボールトで指定された暗号化キーは、特定のリソースタイプのバックアップに適用されます。バックアップの暗号化の詳細については、「セキュリティ」セクションの「でのバックアップの暗号化 AWS Backup」を参照してください。他のすべてのリソースタイプのバックアップは、ソースリソースの暗号化に使用されたキーを使用してバックアップされます。

バックアップボールトのタグ

これらのタグはバックアップボールトに関連付けられており、バックアップボールトを整理して追跡するのに役立ちます。

バックアップボールトでのアクセスポリシーの設定

では AWS Backup、バックアップボールトとそのボールトに含まれるリソースにポリシーを割り当てることができます。ポリシーを割り当てると、バックアッププランやオンデマンドバックアップを作成するアクセス権をユーザーに付与するなどの操作が可能になりますが、作成後に復旧ポイントを削除する機能は制限されます。

ポリシーを使用してリソースへのアクセスを許可または制限する方法については、IAM ユーザーガイドの「アイデンティティベースおよびリソースベースのポリシー」を参照してください。タグを使用してアクセスを管理することもできます。

次のポリシーの例をガイドとして使用して、 AWS Backup ボールトの使用時にリソースへのアクセスを制限できます。他の IAM ベースのポリシーとは異なり、 AWS Backup アクセスポリシーはActionキー内のワイルドカードをサポートしていません。

さまざまなリソースタイプの復旧ポイントを識別するために使用できる Amazon リソースネーム (ARN) のリストについては、「AWS Backup リソース ARNs」を参照して、リソース固有の復旧ポイントの ARN を確認してください。

ボールトアクセスポリシーは AWS Backup APIsへのユーザーアクセスのみを制御します。Amazon Elastic Block Store (Amazon EBS) や Amazon Realational Database Service (Amazon RDS) スナップショットなど一部のBack upタイプには、これらサービスの API を使用してもアクセスできます。これらのバックアップタイプへのアクセスを完全に管理するために、これら API へのアクセスを管理する個別のアクセスポリシーを IAM で作成できます。

AWS Backup ボールトのアクセスポリシーに関係なく、 以外のアクションのクロスアカウントアクセスは拒否backup:CopyIntoBackupVaultされます。つまり、参照されているリソースのアカウントとは異なるアカウントからの他のリクエストは拒否 AWS Backup されます。

トピック

- バックアップボールトのリソースタイプへのアクセスを拒否する
- バックアップボールトへのアクセスを拒否する
- バックアップボールトの復旧ポイントを削除するアクセスを拒否する

バックアップボールトのリソースタイプへのアクセスを拒否する

このポリシーは、バックアップボールト内のすべての Amazon EBS スナップショットに対して、指定された API 操作へのアクセスを拒否します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::Account ID:role/MyRole"
            },
            "Action": [
                "backup:UpdateRecoveryPointLifecycle",
                "backup:DescribeRecoveryPoint",
```

```
                "backup:DeleteRecoveryPoint",
                "backup:GetRecoveryPointRestoreMetadata",
                "backup:StartRestoreJob"
            ],
            "Resource": ["arn:aws:ec2:Region::snapshot/*"]
        }
    ]
}
```

バックアップボールトへのアクセスを拒否する

このポリシーは、バックアップボールトを対象とする、指定された API 操作へのアクセスを拒否します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::Account ID:role/MyRole"
            },
            "Action": [
                "backup:DescribeBackupVault",
                "backup:DeleteBackupVault",
                "backup:PutBackupVaultAccessPolicy",
                "backup:DeleteBackupVaultAccessPolicy",
                "backup:GetBackupVaultAccessPolicy",
                "backup:StartBackupJob",
                "backup:GetBackupVaultNotifications",
                "backup:PutBackupVaultNotifications",
                "backup:DeleteBackupVaultNotifications",
                "backup:ListRecoveryPointsByBackupVault"
            ],
            "Resource": "arn:aws:backup:Region:Account ID:backup-vault:backup vault
 name"
        }
    ]
}
```

バックアップボールトの復旧ポイントを削除するアクセスを拒否する

ボールトにアクセスできるかどうか、ボールトに保存されている復旧ポイントを削除できるかは、ユーザーに付与するアクセス許可によって決まります。

バックアップボールトに対するリソースベースのアクセスポリシーを作成して、バックアップボールト内のバックアップの削除を禁止する手順は、以下のとおりです。

バックアップボールトのリソースベースのアクセスポリシーを作成するには

1. にサインインし AWS Management Console、https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. 左側のナビゲーションペインで、[バックアップボールト] を選択します。
3. リストからバックアップボールトを選択します。
4. [Access policy (アクセスポリシー)] セクションに、以下の JSON の例を貼り付けます。このポリシーは、プリンシパルでないユーザーがターゲットバックアップコンテナー内の復旧ポイントを削除することを禁止します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": "*",
            "Action": "backup:DeleteRecoveryPoint",
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:userId": [
                       "AAAAAAAAAAAAAAAAAAAAA:",
                       "BBBBBBBBBBBBBBBBBBBBB",
                       "112233445566"
                    ]
                }
            }
        }
    ]
}
```

ARN を使用して IAM ID のリストを許可するには、次の例の aws:PrincipalArn グローバル条件キーを使用します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": "*",
            "Action": "backup:DeleteRecoveryPoint",
            "Resource": "*",
            "Condition": {
                "ArnNotEquals": {
                    "aws:PrincipalArn": [
                       "arn:aws:iam::112233445566:role/mys3role",
                       "arn:aws:iam::112233445566:user/shaheer",
                       "112233445566"
                    ]
                }
            }
        }
    ]
}
```

IAM エンティティの一意の ID の取得については、IAM ユーザーガイドの「一意識別子の取得」を参照してください。

これを特定のリソースタイプに制限する場合は、"Resource": "*" の代わりに、拒否する復旧ポイントタイプを明示的に含めることができます。たとえば、Amazon EBS スナップショットの場合は、リソースタイプを次のように変更します。

```
"Resource": ["arn:aws:ec2::Region::snapshot/*"]
```

5. Attach policy] (ポリシーのアタッチ) を選択します。

AWS Backup ボールトロック

> **Note**
>
> AWS Backup ボールトロックは、SEC 17a-4、CFTC、および FINRA の規制の対象となる環境での使用について、Cohasset Associates によって評価されています。 AWS Backup ボールトロックがこれらの規制にどのように関連しているかの詳細については、「Cohasset Associates Compliance Assessment」を参照してください。

AWS Backup ボールトロックはバックアップボールトのオプション機能であり、バックアップボールトのセキュリティと制御を強化するのに役立ちます。コンプライアンスモードでロックが有効になっていて、猶予期間が終了すると、顧客、アカウント/データ所有者、または AWSはボールト設定の変更または削除ができなくなります。各ボールトには 1 つのボールトロックを設定できます。

AWS Backup は、保持期間が終了するまでバックアップを利用できるようにします。いずれかのユーザー (ルートユーザーを含む) が、ロックされたボールトのライフサイクルプロパティを削除または変更しようとすると、 AWS Backup はオペレーションを拒否します。

- ガバナンスモードでロックされたボールトは、十分な IAM アクセス許可を持つユーザーがロックを解除できます。
- コンプライアンスモードでロックされたボールトは、クーリングオフ期間 (「猶予期間」) が過ぎると削除できません。猶予期間中でも、ボールトロックを解除したり、ロック設定を変更したりできます。

ボールトロックモード

ボールトロックを作成する場合、ガバナンスモードとコンプライアンスモードの 2 つのモードを選択できます。ガバナンスモードは、十分な IAM アクセス許可を持つユーザーだけがボールトを管理できるようにするためのものです。ガバナンスモードは、指定された担当者のみがバックアップボールトを変更できるようにすることで、組織がガバナンス要件を満たすのに役立ちます。コンプライアンスモードは、データ保持期間が終了するまでボールト (ひいてはその内容) が削除または変更されないことが見込まれるバックアップボールトを対象としています。コンプライアンスモードのボールトは一度ロックされるとイミュータブルになり、ロックを解除できなくなります。

ガバナンスモードでロックされたボールトは、適切な IAM アクセス許可を持つユーザーが管理または削除できます。

コンプライアンスモードのボールトロックは、どのユーザーも、また、 AWSでも変更、削除ができません。コンプライアンスモードのボールトロックには、ロックされてからイミュータブルになるまでの猶予期間が設定されています。

ボールトロックのメリット

AWS Backup ボールトロックには、次のようないくつかの利点があります。

- バックアップボールトに保存および作成するすべてのバックアップの WORM (write-once, read-many) 構成。
- バックアップボールトのバックアップ (復旧ポイント) を不注意または悪意のある削除から保護する追加の保護レイヤー。
- 保持期間の適用。これにより、特権ユーザー (AWS アカウント ルートユーザーを含む) による早期削除を防ぎ、組織のデータ保護ポリシーと手順を満たします。

コンソールを使用してバックアップボールトをロックする

Backup コンソールを使用してボールトロックを AWS Backup ボールトに追加できます。

バックアップボールトにボールトロックを追加するには:

1. にサインインし AWS Management Console、https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[バックアップボールト] を見つけます。バックアップボールトの下にネストされた、[ボールトロック] というリンクをクリックします。
3. [ボールトロックの仕組み] または [ボールトロック] で、[+ ボールトロックを作成] をクリックします。
4. [ボールトロックの詳細] ペインで、ロックを適用するボールトを選択します。
5. [ボールトロックモード] で、ボールトをロックするモードを選択します。モードの選択について詳しくは、このページで前述した「ボールトロックモード」を参照してください。
6. [保持期間] については、最小保持期間と最大保持期間を選択します (保持期間は任意です)。ボールトで作成された新しいバックアップジョブとコピージョブは、設定した保持期間に従わないと失敗します。これらの期間は、既にボールト内にある復旧ポイントには適用されません。
7. コンプライアンスモードを選択した場合、「ボールトロック開始日」というセクションが表示されます。ガバナンスモードを選択した場合、これは表示されないため、このステップはスキップできます。

コンプライアンスモードでは、クーリングオフ期間 (ボールトロックの作成からボールトとそのロックがイミュータブルで変更不能になるまでの間) があります。この期間 (「猶予時間」といいます) は自分で選択できますが、少なくとも 3 日間 (72 時間) は必要です。

> **Important**
>
> 猶予期間が過ぎると、ボールトとそのロックはイミュータブルになります。どのユーザーも、 AWSによっても変更も削除もできません。

8. 設定内容に問題がなければ、[ボールトロックを作成] をクリックします。
9. 選択したモードでこのロックを作成することを確認するには、テキストボックスに「confirm」と入力し、設定が意図したとおりであることを確認するボックスにチェックを入れます。

手順が正常に完了すると、コンソールの上部に「成功」バナーが表示されます。

バックアップボールトのロック (プログラムによる)

AWS Backup ボールトロックを設定するには、 API を使用しますPutBackupVaultLockConfiguration。含めるパラメータは、使用するボールトロックモードによって異なります。ガバナンスモードでボールトロックを作成する場合は、ChangeableForDays を含めないでください。このパラメータを含めると、ボールトロックはコンプライアンスモードで作成されます。

コンプライアンスモードのボールトロック作成の CLI サンプルを次に示します。

```
aws backup put-backup-vault-lock-configuration \
        --backup-vault-name my_vault_to_lock \
        --changeable-for-days 3 \
        --min-retention-days 7 \
        --max-retention-days 30
```

ガバナンスモードのボールトロック作成の CLI サンプルを以下に示します。

```
aws backup put-backup-vault-lock-configuration \
        --backup-vault-name my_vault_to_lock \
        --min-retention-days 7 \
        --max-retention-days 30
```

次の 4 つのオプションを設定できます。

1. **BackupVaultName**

   ロックするボールトの名前。

2. **ChangeableForDays** (コンプライアンスモードの場合のみ含む)

   このパラメータは、コンプライアンスモード でボールトロックを作成する AWS Backup ように に指示します。ガバナンスモードでロックを作成する場合は、このパラメータを省略します。

   この値は日単位で表記されます。3 以上 36,500 以下の数値でなければなりません。そうでない場合、エラーが返されます。

   このボールトロックの作成時から、指定した日付の有効期限が切れるまで、DeleteBackupVaultLockConfiguration を使用してボールトロックをボールトから削除できます。または、この間、PutBackupVaultLockConfiguration を使用して設定を変更することもできます。

   このパラメータによって決定された指定日以降、バックアップボールトはイミュータブルになり、変更または削除できません。

3. **MaxRetentionDays** (オプション)

   これは日数で表される数値です。これは、ボールトが復旧ポイントを保持する最大保持期間です。

   選択する最大保持期間は、組織のデータ保持ポリシーに沿ったものでなければなりません。データを一定期間保持するように組織から指示されている場合は、この値をその期間 (日数) に設定できます。例えば、財務データや銀行データを 7 年間 (うるう年によるものの、約 2,557 日) 保存する必要がある場合があります。

   指定しない場合、 AWS Backup ボールトロックは最大保持期間を適用しません。指定すると、ライフサイクルの保持期間が最大保持期間よりも長いこのボールトへのバックアップジョブとコピージョブは失敗します。ボールトロックの作成の前に、すでにボールトで保存されている復旧ポイントは影響されません。指定できる最長の最大保持期間は 36500 日 (約 100 年) です。

4. **MinRetentionDays** (オプション 、 に必須 CloudFormation)

   これは日数で表される数値です。これは、ボールトが復旧ポイントを保持する最小保持期間です。この設定は、組織がデータを管理するのに必要な期間に合わせて設定する必要があります。

例えば、規制や法律でデータを少なくとも 7 年間保持することが義務付けられている場合、うるう年にもよりますが、日数は約 2,557 年になります。

指定しない場合、 AWS Backup ボールトロックは最小保持期間を適用しません。指定すると、ライフサイクルの保持期間が最小保持期間よりも短いこのボールトへのバックアップジョブとコピージョブは失敗します。ボールト AWS Backup ロックの前にボールトに既に保存されている復旧ポイントは影響を受けません。指定できる最小保持期間は 1 日です。

ボールトロック設定のバックアップ AWS Backup ボールトを確認する

AWS Backup または DescribeBackupVault ListBackupVaults APIs を呼び出すことで、ボールトのボールトロックの詳細をいつでも確認できます。

ボールトロックを、バックアップボールトに適用したかを判断するには、DescribeBackupVault を呼び出し、Locked プロパティを確認します。の場合"Locked": true、次の例のように、 AWS Backup ボールトロックをバックアップボールトに適用しています。

```
{
    "BackupVaultName": "my_vault_to_lock",
    "BackupVaultArn": "arn:aws:backup:us-east-1:555500000000:backup-
vault:my_vault_to_lock",
    "EncryptionKeyArn": "arn:aws:kms:us-
east-1:555500000000:key/00000000-1111-2222-3333-000000000000",
    "CreationDate": "2021-09-24T12:25:43.030000-07:00",
    "CreatorRequestId": "ac6ce255-0456-4f84-bbc4-eec919f50709",
    "NumberOfRecoveryPoints": 1,
    "Locked": true,
    "MinRetentionDays": 7,
    "MaxRetentionDays": 30,
    "LockDate": "2021-09-30T10:12:38.089000-07:00"
}
```

前の出力では、次のオプションが確認できます。

1. Locked は、このバックアップボールトに AWS Backup ボールトロックを適用したかどうかを示すブール値です。 Trueは、 AWS Backup ボールトロックによってボールトに保存されている復旧ポイントに対する削除または更新オペレーションが失敗することを意味します (クーリングオフ猶予期間内であるかどうかにかかわらず) 。

2. LockDate は、クーリングオフ猶予期間が終了する UTC 日時です。この日時を過ぎると、このボールトでロックの削除や変更はできません。公開されているタイムコンバータを使用して、この文字列を現地時間に変換します。

"Locked":false の場合、次の例のようにボールトロックを適用していません (または以前のものが削除されていません)。

```
{
    "BackupVaultName": "my_vault_to_lock",
    "BackupVaultArn": "arn:aws:backup:us-east-1:555500000000:backup-
vault:my_vault_to_lock",
    "EncryptionKeyArn": "arn:aws:kms:us-
east-1:555500000000:key/00000000-1111-2222-3333-000000000000",
    "CreationDate": "2021-09-24T12:25:43.030000-07:00",
    "CreatorRequestId": "ac6ce255-0456-4f84-bbc4-eec919f50709",
    "NumberOfRecoveryPoints": 3,
    "Locked": false
}
```

猶予期間中のボールトロック削除 (コンプライアンスモード)

AWS Backup コンソールを使用して、猶予時間 (ボールトをロックしてから の前LockDate) にボールトロックを削除するには、

1. にサインインし AWS Management Console、https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. 左側のナビゲーションの [マイアカウント] で、[バックアップボールト] をクリックし、[バックアップボールトロック] をクリックします。
3. 削除するボールトロックをクリックし、[ボールトロックを管理] をクリックします。
4. [ボールトロックを削除] をクリックします。
5. ボールトロックを削除するかどうかを確認する警告ボックスが表示されます。テキストボックスに「confirm」と入力し、[確認] をクリックします。

すべての手順が正常に完了すると、コンソール画面の上部に [成功] バナーが表示されます。

CLI コマンドを使用して猶予時間中にボールトロックを削除するには、次の　CLI サンプルのように DeleteBackupVaultLockConfiguration を使用します。

```
aws backup delete-backup-vault-lock-configuration \
          --backup-vault-name my_vault_to_lock
```

AWS アカウント ロックされたボールトによる閉鎖

バックアップボールト AWS アカウント を含む を閉鎖 AWS し、バックアップをそのままにして アカウントを 90 日間 AWS Backup 停止します。この 90 日間にアカウントを再度開かなかった場合、ボールトロックが設定されていても AWS Backup 、 はバックアップボールトの内容 AWS を削除します。

セキュリティに関するその他の考慮事項

AWS Backup ボールトロックは、データ保護の防御にさらにセキュリティレイヤーを追加します。ボールトロックは、以下の他のセキュリティ機能と組み合わせることができます。

- 復旧ポイントの暗号化
- AWS Backup ボールトおよびリカバリポイントのアクセスポリシー 。これにより、ボールトレベルでアクセス許可を付与または拒否できます。
- AWS Backup セキュリティのベストプラクティス 。これには、 AWS サポートされているサービスによるバックアップおよび復元のアクセス許可の付与または拒否を可能にするカスタマー管理ポリシーのライブラリが含まれます。
- AWS Backup Audit Manager を使用すると、定義したコントロールのリストに対してバックアップのコンプライアンスチェックを自動化できます。

  AWS Backup API を使用したフレームワークの作成を行い、 AWS Backup Audit Manager で「バックアップは AWS Backup ボールトロックで保護されています」のコントロールを使用すると、目的のリソースがボールトロックで保護されていることを確認できます。
- リソースを非アクティブにするメカニズムは、リソースを復元する機能に影響を与える可能性があります。ロックされたボールトでは削除できませんが、アクティブ以外の状態になる可能性があります。例えば、AMI を無効にすることができる Amazon Elastic Compute Cloud 設定は、EC2 インスタンスのバックアップを復元する機能を一時的にブロックする可能性があります。これは、ボールトロックまたはリーガルホールドの影響を受けるバックアップであっても、すべての EC2 復旧ポイントに影響します。

  EC2 バックアップが無効になっている場合は、無効になっている AMI を再度有効にできます。再度有効にすると、復元の対象となります。AMI 無効機能をブロックするには、IAM ポリシーを使用して を許可しませんec2:DisableImage。

> **Note**
>
> AWS Backup ボールトロックは、S3 Glacier とのみ互換性がある Amazon S3 Glacier ボールトロック と同じ機能ではありません。 S3

バックアップボールトを削除する

偶発的または悪意のある大量削除を防ぐには、バックアップボールトのすべての復旧ポイントを削除 (またはバックアッププランのライフサイクル) した後にのみ、 AWS Backup のバックアップボールトを削除することができます。リカバリポイントを手動で削除するには、「リソースのクリーンアップ」を参照してください。

バックアップボールトを削除したら、新しいバックアップボールトを参照するようにバックアップ計画を更新します。削除されたバックアップボールトをバックアップ計画が参照していると、バックアップの作成は失敗します。

> **Note**
>
> AWS Backup デフォルトのバックアップボールトと Amazon EFS 自動バックアップボールトの 2 つのバックアップボールトを削除することはできません。

AWS Backup コンソールを使用してバックアップボールトを削除するには

1. にサインインし AWS Management Console、https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[バックアップボールト] を選択します。
3. バックアップボールトの名前を選択して、詳細ページを開きます。
4. バックアップボールトに関連付けられているバックアップを選択して削除します。
5. ボールトの削除 を選択します。確認のプロンプトが表示されたら、ボールト名を入力し、バックアップボールトの削除を選択します。

バックアップの使用

バックアップまたは復旧ポイントとは、指定された時刻における、Amazon Elastic Block Store (Amazon EBS) ボリュームや Amazon DynamoDB テーブルなどのリソースのコンテンツを表したものです。復旧ポイントは、Amazon EBS スナップショットや DynamoDB バックアップなど、 AWS サービスのさまざまなバックアップを一般的に指す用語です。復旧ポイントという用語とバックアップという用語は同じ意味で使用されます。

AWS Backup は復旧ポイントをバックアップボールトに保存します。バックアップボールトはビジネスニーズに合わせて整理できます。たとえば、20 年度の財務情報を含む一連のリソースを保存できます。リソースを復旧する必要がある場合は、 AWS Backup コンソールまたは AWS Command Line Interface （ AWS CLI) を使用して、必要なリソースを検索して復旧できます。

各復旧ポイントには一意の ID があります。一意の ID は、リカバリポイントの Amazon リソースネーム (ARN) の末尾にあります。リカバリポイント ARN および一意の ID の例については、リソースおよびオペレーション の表を参照してください。

> **Important**
>
> 追加料金を回避するには、ウォームストレージ期間を「少なくとも 1 週間」に設定して、リテンションポリシーを構成します。詳細については、「メータリング、コスト、および請求」を参照してください。

以下のセクションでは、 AWS Backupの基本的なバックアップ管理タスクの概要を説明します。

トピック

- バックアップの作成
- バックアップをコピーする
- バックアップの削除
- バックアップの編集
- バックアップの復元
- 復元テスト
- バックアップのリストの表示

バックアップの作成

では AWS Backup、バックアッププランを使用してバックアップを自動的に作成することも、オンデマンドバックアップを開始して手動で作成することもできます。

自動バックアップの作成

バックアッププランによって自動的にバックアップが作成される場合は、バックアッププランで定義されたライフサイクル設定を使用して設定されます。これらは、バックアップ計画で指定されたバックアップボールトに編成されます。また、バックアッププランに一覧表示されているタグも割り当てられます。バックアッププランの詳細については、「バックアッププランを使用したバックアップの管理」を参照してください。

オンデマンドバックアップの作成

オンデマンドバックアップを作成する場合は、作成するバックアップ用にこれらの設定を構成できます。自動または手動でバックアップが作成される場合、バックアップジョブが開始されます。オンデマンドバックアップの作成方法については、「を使用したオンデマンドバックアップの作成 AWS Backup」を参照してください。

注: オンデマンドバックアップではバックアップジョブが作成されます。バックアップジョブは 1 時間以内に (または指定した場合) Running 状態で移行します。バックアッププランに定義されている、スケジュールされた時刻以外の時間にバックアップを作成する場合は、オンデマンドバックアップを選択できます。オンデマンドバックアップは、例えばバックアップや機能をテストするためにいつでも使用できます。

オンデマンドバックアップは復元 (PITR) では使用できません。オンデマンドバックアップは、バックアップの作成時にリソースを 状態に保持しますが、PITR は一定期間の変更を記録する継続的なバックアップを使用するためです。 point-in-time

バックアップジョブのステータス

各バックアップジョブには、一意の ID があります。例えば D48D8717-0C9D-72DF-1F56-14E703BF2345 です。

バックアップジョブのステータスは、 AWS Backup バックアップコンソールの [ジョブ] ページで確認できます。バックアップジョブのステータスにはCREATED、、PENDING、RUNNING、ABORTING、ABORTED、、COMPLETED、FAILEDEXPIRED、および が含まれますPARTIAL。

増分バックアップの仕組み

多くの リソースは、 による増分バックアップをサポートしています AWS Backup。すべての一覧は、「リソース別の機能の可用性 表」の増分バックアップセクションにあります。

最初のバックアップの後の各バックアップは増分です (つまり、以前のバックアップからの変更のみをキャプチャします) が、 で作成されたすべてのバックアップは、完全な復元を可能にするために必要な参照データ AWS Backup を保持します。これは、元の (フル) バックアップがライフサイクルの期限に達して削除された場合にも当てはまります。

例えば、3 日間のライフサイクルポリシーにより、1 日目 (フル) バックアップが削除された場合、2 日目と 3 日目のバックアップを使用してフル復元を実行できます。 AWS Backup は、それを有効にするため、1 日目の必要な参照データを保持します。

ソースリソースへのアクセス

AWS Backup では、ソースリソースにアクセスしてバックアップする必要があります。例:

- Amazon EC2 インスタンスをバックアップするには、インスタンスが `running` または `stopped` の状態であってもかまいませんが、`terminated` の状態にはなりません。これは、 `running`または `stopped`インスタンスは と通信できますが AWS Backup、 `terminated`インスタンスは通信できないためです。
- 仮想マシンをバックアップするには、ハイパーバイザーのバックアップゲートウェイステータスが `ONLINE` である必要があります。詳細については、「ハイパーバイザーステータスの理解」を参照してください。
- Amazon RDS データベース、Amazon Aurora、または Amazon DocumentDB クラスターをバックアップするには、それらのリソースのステータスが `AVAILABLE` である必要があります。
- Amazon Elastic File System (Amazon EFS) をバックアップするには、ステータスが `AVAILABLE` である必要があります。
- Amazon FSx ファイルシステムをバックアップするには、ステータスが `AVAILABLE` である必要があります。ステータスが `UPDATING` の場合、バックアップリクエストはファイルシステムが `AVAILABLE` になるまでキューに入れられます。

  FSx for ONTAP は、DP (データ保護) ボリューム、LS (ロード共有) ボリューム、フルボリューム、ファイルシステム上のフルボリュームなど、特定のボリュームタイプのバックアップをサポートしていません。詳細については、「FSx for ONTAP のバックアップの使用」を参照してください。

AWS Backup は、ソースリソースの状態に関係なく、以前に作成したバックアップをライフサイクルポリシーに従って保持します。

トピック

を使用したオンデマンドバックアップの作成 AWS Backup

AWS Backup コンソールの「保護されたリソース」ページには、 AWS Backup 少なくとも 1 回バックアップされたリソースが一覧表示されます。 AWS Backup を初めて使用する場合、このページにはリソース (Amazon EBS ボリュームや Amazon RDS データベースなど) はリストされていません。リソースがバックアッププランに割り当てられていても、バックアッププランがスケジュールされたバックアップジョブを 1 回も実行したことがない場合も同様です。

注: オンデマンドバックアップでは、リソースのバックアップがすぐに開始されます。バックアッププランに定義されている、スケジュールされた時刻以外の時間にバックアップを作成する場合は、オンデマンドバックアップを選択できます。オンデマンドバックアップは、例えばバックアップや機能をテストするためにいつでも使用できます。

オンデマンドバックアップは復元 (PITR) では使用できません。オンデマンドバックアップは、バックアップが作成された時点の状態にリソースを保持しますが、PITR は一定期間の変更を記録する継続的なバックアップを使用するためです。 point-in-time

考慮事項

- アカウントに AWS Backup デフォルトのロールが存在しない場合、正しいアクセス許可を持つロールが作成されます。
- バックアップの有効期限が切れ、ライフサイクルポリシーの一部として削除のマークが付けられると、 AWS Backup は、次の 8 時間にわたってランダムに選択された時点でバックアップを削除します。このウィンドウは、一貫したパフォーマンスを確保するのに役立ちます。
- Amazon EC2 リソースの場合、 は、このステップで追加したタグに加えて、既存のグループタグと個々のリソースタグ AWS Backup を自動的にコピーします。
- AWS Backup は、デフォルトの動作として「再起動なし」の EC2 バックアップを取ります。AWS Backup は現在、Amazon EC2 で実行されているリソースをサポートしており、特定のインスタンスタイプはサポートされていません。詳細については、「Windows VSS バックアップの作成」を参照してください。

オンデマンドバックアップを作成するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ダッシュボードで、[オンデマンドバックアップを作成] を選択します。または、ナビゲーションペインで、[Protected resources (保護されたリソース)]、[Create an on-demand backup (オンデマンドバックアップを作成)] の順に選択します。
3. リソースタイプページで、バックアップするリソースタイプを選択します。例えば、Amazon DynamoDB テーブルの DynamoDB を選択します。
4. 保護するリソースの名前または ID を選択します。例えば、Amazon DynamoDB の DynamoDB テーブルの名前を選択します。
5. [今すぐバックアップを作成] が選択されていることを確認します。
6. リソースタイプがコールドストレージへの移行をサポートしている場合、コールドストレージがあります。詳細については、「リソース別の機能の可用性」の表の「コールドストレージへのライフサイクル」列を参照してください。 ???

   このバックアップをコールドストレージに移行するタイミングを指定するには、「バックアップをウォームストレージからコールドストレージに移動」を選択し、ウォームストレージの時間を指定します。
7. 合計保持期間 には、日数を指定します。コールドストレージで時間を指定した場合、保持期間はウォームストレージとコールドストレージに分割されます。

8. 既存の [Backup vault (バックアップボールト)] を選択するか、新しいバックアップボールトを作成します。[Create new Backup vault (新しいバックアップボールトを作成)] を選択すると、ボールトを作成する新しいページが開きます。完了すると、[Create on-demand backup (オンデマンドバックアップを作成)] ページに戻ります。
9. IAM ロール で、デフォルトのロールまたは作成したロールを選択します。
10. オンデマンドバックアップにタグを割り当てるには、リカバリポイント に追加されたタグ を展開し、新しいタグ を追加 を選択し、タグキーとタグ値を入力します。
11. リソースタイプが EC2 の場合、高度なバックアップ設定があります。Windows Volume Shadow Copy Service (VSS) を使用してアプリケーション整合性のあるスナップショットを作成するには、Windows VSS を選択します。
12. [オンデマンドバックアップを作成] を選択します。これにより、ジョブページが開き、ジョブのリストとジョブのステータスが表示されます。

継続的バックアップと point-in-time 復元 (PITR)

トピック

- 継続的バックアップ/ポイントインタイムリストア (PITR) でサポートされているサービス
- 継続的なバックアップを見つける
- 継続的なバックアップの復元
- 継続的バックアップの停止または削除
- 継続的バックアップのコピー
- 保持期間の変更
- バックアッププランから唯一の継続的なバックアップルールを削除する
- 同じリソースで重複する継続的なバックアップ
- P oint-in-time リカバリに関する考慮事項

一部のリソースでは、スナップショットバックアップに加えて、継続的バックアップと point-in-time リカバリ (PITR) AWS Backup もサポートしています。

継続的バックアップ では、精度から 1 秒以内 (最大 35 日間) に、 が AWS Backupサポートするリソースを選択した特定の時間に巻き戻すことで復元できます。継続的なバックアップは、最初にリソースのフルバックアップを作成し、次にリソースのトランザクションログを定期的にバックアップすることによって機能します。PITR 復元は、フルバックアップにアクセスし、トランザクションログを復元 AWS Backup するよう指示した時点まで再生することで機能します。

または、スナップショットバックアップを 1 時間ごとに作成することもできます。スナップショットバックアップは、最大 100 年間保存できます。スナップショットは、フルバックアップまたは増分バックアップ用にコピーできます。

継続的なバックアップとスナップショットバックアップにはさまざまなメリットがあるため、継続的なバックアップルールとスナップショットバックアップルールの両方でリソースを保護することをお勧めします。

注: オンデマンドバックアップでは、リソースのバックアップがすぐに開始されます。バックアッププランに定義されている、スケジュールされた時刻以外の時間にバックアップを作成する場合は、オンデマンドバックアップを選択できます。オンデマンドバックアップは、例えばバックアップや機能をテストするためにいつでも使用できます。

オンデマンドバックアップは復元 (PITR) では使用できません。オンデマンドバックアップは、バックアップが作成された時点の状態にリソースを保持しますが、PITR は一定期間の変更を記録する継続的なバックアップを使用するためです。 point-in-time

AWS Backup コンソールまたは API AWS Backup を使用して でバックアッププランを作成するときに、サポートされているリソースの継続的なバックアップをオプトインできます。

コンソールを使用して継続的なバックアップを有効にするには

1. にサインインし AWS Management Console、https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[バックアッププラン] を選択して、[バックアッププランの作成] を選択します。
3. [バックアップルール]で、[バックアップルールの追加] を選択します。
4. [バックアップルールの設定] セクションで、[サポートされているリソースの継続的なバックアップを有効にする] を選択します。

継続的バックアップ/ポイントインタイムリストア (PITR) でサポートされているサービス

AWS Backup は、以下の サービスとアプリケーションの継続的なバックアップと point-in-time リカバリをサポートします。

Amazon S3

S3 バックアップで PITR を有効にするには、バックアッププランに継続的バックアップを含める必要があります。

ソースバケットの、この元のバックアップでは PITR をアクティブにできますが、クロスリージョンまたはクロスアカウントのコピーには PITR がなく、これらのコピーから復元すると、指定されたポイントインタイムに復元されるのではなく、作成時の状態に復元されます (コピーはスナップショットコピーになります)。

RDS

バックアップスケジュール： AWS Backup プランが Amazon RDS スナップショットと継続的バックアップの両方を作成すると、 AWS Backup は、競合を防ぐために Amazon RDS メンテナンスウィンドウと調整するようにバックアップウィンドウをインテリジェントにスケジュールします。競合をさらに防止するために、Amazon RDS 自動バックアップウィンドウの手動設定は利用できません。RDS は、バックアッププランに 1 日 1 回以外のスナップショットバックアップの頻度が設定されているかどうかに関係なく、1 日に 1 回スナップショットを作成します。

設定： Amazon RDS インスタンスに AWS Backup 継続的なバックアップルールを適用した後は、Amazon RDS のそのインスタンスに継続的なバックアップ設定を作成または変更することはできません。変更を行うには、 AWS Backup コンソールまたは AWS Backup CLI を使用する必要があります。

Amazon RDS インスタンスの継続的バックアップの移行コントロールを Amazon RDS に戻します。

Console

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[バックアッププラン] を選択します。
3. そのリソースを保護する継続的なバックアップを使用して、すべての Amazon RDS バックアッププランを削除します。
4. [バックアップボールト] を選択します。バックアップボールトから継続的なバックアップ復旧ポイントを削除します。または、保持期間が経過するのを待ち、 AWS Backup が復旧ポイントを自動的に削除します。

これらのステップを完了すると、 AWS Backup はリソースの継続的なバックアップコントロールを Amazon RDS に移行します。

AWS CLI

`DisassociateRecoveryPoint` API オペレーションを呼び出します。

詳細については、「DisassociateRecoveryPoint」を参照してください。

Amazon RDS の継続的なバックアップに必要な IAM アクセス許可

- AWS Backup を使用して Amazon RDS データベースの継続的なバックアップを設定するには、バックアッププラン設定で定義された IAM ロールに API アクセス許可`rds:ModifyDBInstance`が存在することを確認します。Amazon RDS の継続的なバックアップを復元するには、復元ジョブ用に送信した IAM ロールにアクセス許可 `rds:RestoreDBInstanceToPointInTime` を追加する必要があります。`AWS Backup default service role` を使用して、バックアップとリストアを実行します。
- point-in-time 復旧に使用できる時間の範囲を記述するには、 を AWS Backup 呼び出します`rds:DescribeDBInstanceAutomatedBackupsAPI`。 AWS Backup コンソールでは、 AWS Identity and Access Management (IAM) 管理ポリシーに `rds:DescribeDBInstanceAutomatedBackups` API アクセス許可が必要です。`AWSBackupFullAccess` または `AWSBackupOperatorAccess` 管理ポリシーを使用できます。どちらのポリシーにも、必要なすべての権限があります。詳細については、「マネージドポリシー」を参照してください。

保持期間： PITR 保持期間を変更する`ModifyDBInstance`と、 は を AWS Backup 呼び出し、その変更をすぐに適用します。次のメンテナンスウィンドウが保留中の他の構成更新がある場合は、PITR の保持期間を変更すると、それらの構成更新もすぐに適用されます。詳細については、「Amazon Relational Database Service API リファレンス」の「`ModifyDBInstance`」を参照してください。

Amazon RDS 継続的バックアップのコピー：

- 増分スナップショットコピージョブは、フルスナップショットコピージョブよりも速く処理されます。新しいコピージョブが完了するまで以前のスナップショットコピーを保持しておくと、コピージョブの所要時間の短縮になる可能性があります。RDS データベースインスタンスからスナップショットをコピーする場合、以前のコピーを先に削除すると、(増分スナップショットコピーではなく) フルスナップショットコピーが作成されることに注意してください。コピーの最適化に関する詳細については、「Amazon RDS ユーザーガイド」の「増分スナップショットコピー」を参照してください。

- Amazon RDS 継続的バックアップのコピーの作成 — Amazon RDS AWS Backup ではトランザクションログのコピーが許可されていないため、Amazon RDS 継続的バックアップのコピーを作成することはできません。代わりに、 はスナップショット AWS Backup を作成し、バックアッププランで指定された頻度でスナップショットをコピーします。

復元： AWS Backup または Amazon RDS を使用して point-in-time 復元を実行できます。 AWS Backup コンソールの手順については、「Amazon RDS データベースの復元」を参照してください。Amazon RDS の手順については、Amazon RDS ユーザーガイドの「特定の時点への DB インスタンスの復元」を参照してください。

> **Tip**
>
> マルチ AZ (アベイラビリティーゾーン) データベースインスタンスを に設定`Always On`した場合、バックアップ保持期間を 0 に設定しないでください。エラーが発生した場合は、 `disassociate-recovery-point`の代わりに AWS CLI コマンドを使用し`delete-recovery-point`、Amazon RDS 設定の保持設定を 1 に変更します。

Amazon RDS の使用に関する一般的な情報については、「Amazon RDS ユーザーガイド」を参照してください。

Aurora

Aurora リソースの継続的バックアップを有効にするには、このページの最初のセクションの手順を参照してください。

Aurora クラスターをポイントインタイムに復元する手順は、Aurora クラスターのスナップショットを復元する手順のバリエーションです。

ポイントインタイムリストアを実行すると、コンソールには復元時間セクションが表示されます。このページの下にある「継続的バックアップの操作」の「継続的バックアップの復元」を参照してください。

Amazon EC2 インスタンスでの SAP HANA

point-in-time 復元 (PITR) で使用できる継続的バックアップ を作成できます (オンデマンドバックアップはリソースをその取得時の状態に保持しますが、PITR は一定期間の変更を記録する継続的バックアップを使用することに注意してください) 。

継続的バックアップにより、EC2 インスタンス上の SAP HANA データベースは、精度の 1 秒 (最大 35 日前) 以内に、選択した特定の時間に巻き戻すことで SAP HANA データベースをサポートします。継続的なバックアップは、最初にリソースのフルバックアップを作成し、次にリソースのトランザクションログを定期的にバックアップすることによって機能します。PITR 復元は、フルバックアップにアクセスし、トランザクションログを復元 AWS Backup するように指示した時点まで再生することで機能します。

AWS Backup コンソールまたは API AWS Backup を使用して でバックアッププランを作成するときに、継続的バックアップにオプトインできます。

コンソールを使用して継続的なバックアップを有効にするには

1. にサインインし AWS Management Console、https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[バックアッププラン] を選択して、[バックアッププランの作成] を選択します。
3. [バックアップルール]で、[バックアップルールの追加] を選択します。
4. [バックアップルールの設定] セクションで、[サポートされているリソースの継続的なバックアップを有効にする] を選択します。

SAP HANA データベースバックアップの PITR (point-in-time復元) を無効にすると、復旧ポイントの有効期限が切れるまで (ステータスは に等しくなります) 、ログは引き続き に送信されます AWS Backup EXPIRED)。SAP HANA 内の別のログバックアップ場所に変更して、 AWS Backupへのログの送信を停止できます。

ステータスが の継続的復旧ポイントは、継続的復旧ポイントが中断されたSTOPPEDことを示します。つまり、SAP HANA から に送信され、データベースへの増分変更 AWS Backup を示すログにギャップがあります。この期間のギャップ内に発生した復旧ポイントのステータスは STOPPED. です。

継続的バックアップ (復旧ポイント) の復元ジョブ中に発生する可能性のある問題については、本ガイドの「SAP HANA 復元のトラブルシューティング」セクションを参照してください。

継続的なバックアップを見つける

AWS Backup コンソールを使用して、継続的なバックアップを検索できます。

AWS Backup コンソールを使用して継続的なバックアップを検索するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[バックアップボールト] をクリックし、リストからバックアップボールトを選択します。
3. [バックアップ] セクションの Backup タイプ列で、Continuous 復旧ポイントをソートします。プレフィックスの継続的な復旧ポイント ID を並び替えすることもできます。

継続的なバックアップの復元

AWS Backup コンソールを使用して継続的バックアップを復元するには

- PITR 復元プロセス中に、 AWS Backup コンソールに復元時間セクションが表示されます。このセクションでは、以下のいずれか方法があります。
  - 復元可能な最新時刻に復元することを選択します。
  - 日付および時刻の指定をクリックして、保持期間内に独自の日付と時刻を入力します。

AWS Backup API を使用して継続的バックアップを復元するには

1. Amazon S3 については、AWS Backup 「 API、CLI、または SDK を使用して S3 復旧ポイントを復元する」を参照してください。
2. Amazon RDS については、AWS Backup 「API、CLI、または SDK を使用して Amazon RDS 復旧ポイント を復元する」を参照してください。

継続的バックアップの停止または削除

継続的バックアップの作成を停止することも、特定のバックアップ (point-in-time-recovery または PITR ポイント) を削除することもできます。

継続的なバックアップを停止する場合は、バックアッププランから継続的なバックアップルールを削除する必要があります。すべてのリソースの継続的バックアップを停止せずに、1 つ以上のリソースの継続的バックアップを停止する場合は、継続的バックアップを行うリソースについて、継続的バックアップルールを設定した新しいバックアッププランを作成します。代わりに、バックアップボールトから継続的バックアップ復旧ポイントを削除するだけであっても、バックアッププランでは継続的バックアップルールが引き続き実行され、新しい復旧ポイントが作成されます。

ただし、継続的バックアップルールを削除した後でも、 は削除されたバックアップルールの保持期間を AWS Backup 記憶します。指定した保持期間に基づいて、バックアップ保管庫から継続的なバックアップリカバリポイントが自動的に削除されます。

Amazon RDS リカバリポイントを削除するときは、次の点を考慮してください。

- マルチ AZ (アベイラビリティーゾーン) データベースインスタンスを に設定`Always On`した場合、バックアップ保持期間を 0 に設定しないでください。エラーが発生した場合は、`disassociate-recovery-point`の代わりに AWS CLI コマンドを使用し`delete-recovery-point`、Amazon RDS 設定の保持設定を 1 に変更します。
- Amazon RDS の point-in-time 復旧ポイント (継続的バックアップによって作成されたバックアップ) が削除されると、データベースの再起動がトリガーされ、バイナリログが無効になります。詳細については、「Amazon RDS ユーザーガイド」の「バックアップ保持期間」を参照してください。

Aurora 復旧ポイントを削除するときは、次の点を考慮してください。

Amazon Aurora リカバリポイントでこの を選択した場合、 は保持期間を 1 日 AWS Backup に設定します。ソースクラスターも削除されるまで、Aurora バックアップを完全に削除することはできません。

継続的バックアップのコピー

継続的バックアップルールでクロスアカウントコピーまたはクロスリージョンコピーも指定されている場合は、 AWS Backup は、継続的バックアップのスナップショットを作成し、そのスナップショットを送信先ボールトにコピーします。アカウントとリージョン間でのリカバリポイントのコピーの詳細については、「バックアップのコピー」を参照してください。

継続的バックアップは、送信先アカウントおよび/またはリージョンのバックアッププランルールで設定された頻度に従って、定期的なバックアップを作成します。

AWS Backup は、継続的バックアップのオンデマンドコピーをサポートしていません。

保持期間の変更

を使用して AWS Backup 、既存の継続的バックアップルールの保持期間を増減できます。最小保持期間は 1 日です。最大保持期間は 35 日です。

保持期間を長くすると、その効果は即座になります。保持期間を短くすると、 AWS Backup はデータ損失から保護するために変更を適用するまでに十分な時間が経過するまで待機します。例えば、保

持期間を 35 日から 20 日に減らした場合、 AWS Backup は 15 日が経過するまで 35 日間の継続的バックアップを保持し続けます。この設計により、変更を行った時点の過去 15 日間のバックアップが保護されます。

バックアッププランから唯一の継続的なバックアップルールを削除する

継続的なバックアップルールを使用してバックアッププランを作成し、そのルールを削除すると、は削除されたルールの保持期間を AWS Backup 記憶します。保持期間が経過すると、バックアップ保管庫から継続的なバックアップが削除されます。

同じリソースで重複する継続的なバックアップ

一般に、各リソースは、複数の継続的なバックアップルールで保護する必要があります。これは、追加の継続的なバックアップが冗長であるためです。ただし、バックアップエステートをスケールアップすると、複数のバックアッププラン、ルール、ボールトが 1 つのリソースで重複する可能性があります。 はこれらの重複を次のように AWS Backup 処理します。

継続的バックアップルールを使用して複数のバックアッププランに同じリソースを含める場合、AWS Backup は、評価する最初のバックアッププランに対してのみ継続的バックアップを作成します。他のすべてのバックアッププランのスナップショットバックアップが作成されます。

単一のバックアッププランに複数の継続的なバックアップルールを含める場合は、次の手順を実行します。

- ルールが同じバックアップボールトを指している場合、 は保持期間が最も長いルールの継続的なバックアップ AWS Backup のみを作成します。他のすべてのルールを無視します。
- ルールが別のバックアップボールトを指している場合、 はプランを無効として AWS Backup 拒否します。

P oint-in-time リカバリに関する考慮事項

point-in-time 復旧に関する以下の考慮事項に注意してください。

- スナップショットへの自動フォールバック — AWS Backup が継続的なバックアップを実行できない場合は、代わりにスナップショットバックアップを実行します。
- オンデマンドの継続的バックアップはサポート AWS Backup されません。オンデマンドの継続的バックアップは特定の時点を記録し、継続的バックアップは一定期間にわたって変化を記録するため、オンデマンドの継続的バックアップはサポートされません。

- コールドストレージへの移行はサポートされていません — 継続的なバックアップでは最大保持期間 35 日であるのに対し、コールドストレージへの移行には 90 日間の最小移行期間が必要であるため、コールドストレージへの移行はサポートされません。
- 最近のアクティビティの復元 — Amazon RDS のアクティビティでは、直近の 5 分間のアクティビティまで復元でき、Amazon S3 では直近の 15 分間のアクティビティまで復元できます。

Amazon S3 バックアップ

AWS Backup は、S3 にデータを保存するアプリケーションの一元化されたバックアップと復元を単独で、またはデータベース、ストレージ、コンピューティングのための他の AWS サービスと共にサポートします。S3 バックアップでは、多くの機能を使用できます (Backup Audit Manager を含む)。

で 1 つのバックアップポリシーを使用して AWS Backup 、アプリケーションデータのバックアップの作成を一元的に自動化できます。 は、さまざまな AWS のサービスやサードパーティーアプリケーション間でバックアップを 1 つの一元化された暗号化された場所 (バックアップボールトと呼ばれる) AWS Backup に自動的に整理するため、一元化されたエクスペリエンスを通じてアプリケーション全体のバックアップを管理できます。S3 では、継続的バックアップを作成し、S3 に保存されているアプリケーションデータを復元し、ワンクリック point-in-time でバックアップを に復元できます。

を使用すると AWS Backup、オブジェクトデータ、タグ、アクセスコントロールリスト (ACLs)、ユーザー定義メタデータなど、S3 バケットのバックアップとして次のタイプを作成できます。

- 継続的バックアップでは、過去 35 日間の任意のポイントインタイムに復元できます。S3 バケットの継続的バックアップは、1 つのバックアッププランでのみ設定してください。

  サポートされているサービスのリストと、 AWS Backup を使って連続バックアップを取る方法については「ポイントインタイムリカバリ」を参照してください。
- 定期的バックアップでは、データのスナップショットを使用して、指定した期間 (最大 99 年間) データを保持できます。定期的バックアップは、1 時間、12 時間、1 日、1 週間、または 1 年間などの頻度でスケジュールできます。 AWS Backup は、バックアッププランで定義したバックアップウィンドウ中に定期的バックアップを行います。

  がバックアッププランをリソースに適用する方法については、 AWS Backup 「バックアッププランの作成」を参照してください。

S3 バックアップではクロスアカウントコピーとクロスリージョンコピーを使用できますが、継続的バックアップのコピーには point-in-time 復元機能がありません。

S3 バケットの継続的バックアップと定期的バックアップは、どちらも同じバックアップボールトにある必要があります。

どちらのバックアップタイプでも、最初のバックアップはフルバックアップで、後続のバックアップは増分バックアップです。

> **Note**
>
> AWS Backup Amazon S3 で使用するには、S3 バケットで S3 バージョニングを有効にする必要があります。 Amazon S3 データ保護のベストプラクティスとして AWS では S3 バージョニングを推奨しているため、この前提条件を維持しています。
> S3 バージョンの場合、「ライフサイクルの有効期限を設定する」ことをお勧めします。ライフサイクルの有効期限を設定しないと、 は有効期限が切れていないすべてのバージョンの S3 データを AWS Backup バックアップして保存するため、S3 コストが増加する可能性があります。S3 ライフサイクルポリシーの設定について詳しくは、このページの指示に従ってください。

S3 バックアップタイプの比較

S3 リソースのバックアップ戦略には、継続的バックアップのみ、定期的 (スナップショット) バックアップのみ、あるいはその両方の組み合わせが含まれます。以下の情報は、組織にとって最適な方法を選択するのに役立ちます。

継続的バックアップの場合のみ、次の項目が該当します。

- 既存データの最初のフルバックアップが完了すると、S3 バケットデータの変更は発生時に追跡されます。
- 追跡された変更により、継続的バックアップの保持期間に PITR (point-in-time 復元) を使用できます。復元ジョブを実行するには、復元するポイントインタイムを選択します。
- 各継続的バックアップの保持期間は最大 35 日間です。

定期的 (スナップショット) バックアップ (定期的またはオンデマンド) の場合のみ、次の項目が該当します。

- AWS Backup は S3 バケット全体をスキャンし、各オブジェクトの ACL とタグを取得し、前のスナップショットにあったが、作成中のスナップショットには見つからなかったすべてのオブジェクトに対して Head リクエストを開始します。
- バックアップは point-in-time 一貫しています。
- 記録されたバックアップ日時は、バックアップジョブが作成された時刻ではなく、 がバケットのトラバーサル AWS Backup を完了した時刻です。
- バケットの最初のバックアップはフルバックアップです。それ以降の各バックアップは増分となり、前回のスナップショットからのデータの変化を表します。
- 定期的バックアップによって作成されたスナップショットの保持期間は最大 99 年です。

継続的バックアップと定期的/スナップショットバックアップの組み合わせの場合に、次の項目が該当します。

- 既存データ (各バケット) の最初のフルバックアップが完了すると、バケット内の変更は発生時に追跡されます。
- 継続的復旧ポイントから point-in-time 復元を実行できます。
- スナップショットは point-in-time 一貫しています。
- スナップショットは継続的復旧ポイントから直接取得されることから、バケットを再スキャンする必要がないため、処理を速められます。
- スナップショットと継続的復旧ポイントはデータ系列を共有するため、スナップショットと継続的復旧ポイント間のデータの保存は重複しません。

サポートされている S3 ストレージクラス

AWS Backup では、次の S3 ストレージクラス に保存されている S3 データをバックアップできます。

- S3 Standard
- S3 標準 - 低頻度アクセス (IA)
- S3 1 ゾーン - IA
- S3 Glacier インスタント取得
- S3 Intelligent-Tiering (S3 INT)

ストレージクラス S3 Intelligent-Tiering (INT) 内のオブジェクトのバックアップは、それらのオブジェクトにアクセスします。このアクセスにより、S3 Intelligent-Tiering がトリガーされ、それらのオブジェクトが高頻度アクセスに自動的に移動されます。

S3 標準 - 低頻度アクセス (IA) クラスや S3 1 ゾーン - IA クラスなど、低頻度アクセス階層にアクセスするバックアップは、高頻度アクセスの S3 ストレージ料金の下に移動します (低頻度アクセス階層またはアーカイブインスタントアクセス階層に適用されます) 。

Glacier Instant Retrieval を除き、アーカイブされたストレージクラスはサポートされていません。

Amazon S3 のストレージ料金の詳細については、Amazon S3の料金」を参照してください。

for Amazon S3 AWS Backup に関する考慮事項

S3 リソースをバックアップする際には、以下の点を考慮する必要があります。

- フォーカスオブジェクトメタデータのサポート： AWS Backup タグ、アクセスコントロールリスト (ACLsのメタデータをサポートします。これにより、元の作成日、バージョン ID、ストレージクラス、および ETag を除くバックアップデータとメタデータをすべて復元できます。
- S3 オブジェクトキー名は、ほとんどの UTF-8 エンコード可能な文字列で構成できます。Unicode 文字 `#x9 | #xA | #xD | #x20 to #xD7FF | #xE000 to #xFFFD | #x10000 to #x10FFFF` を使用できます。

  このリストにない文字を含むオブジェクトキー名は、バックアップから除外される場合があります。詳細については、文字に関するW3C仕様を参照してください。
- コールドストレージ移行： AWS Backupのライフサイクル管理ポリシーでは、バックアップの有効期限のタイムラインを定義できますが、現時点では S3 バックアップのコールドストレージ移行はサポートされていません。
- 同時に作成された、同じオブジェクトの複数のバージョンを含む S3 バケットのバックアップは、現時点ではサポートされていません。
- 定期的なバックアップ AWS Backup の場合、 はオブジェクトメタデータへのすべての変更を追跡するために最善を尽くします。ただし、1 分以内にタグまたは ACL を複数回更新すると、 AWS Backup `では、すべての中間状態がキャプチャされない場合があります。
- AWS Backup は現在、SSE-C で暗号化されたオブジェクトのバックアップをサポートしていません。 AWS Backup また、 は、バケットポリシー、設定、名前、アクセスポイントなどのバケット設定のバックアップもサポートしていません。

- AWS Backup は現在、 での S3 のバックアップをサポートしていません AWS Outposts。

> **Important**
>
> データ読み取りイベントをログに記録するアカウントでは、 CloudTrail ログが有効になっている S3 バケットには、アクセスログを別のターゲットバケットに保存する必要があります。 CloudTrail ログがログを記録するのと同じバケットに保存されている場合、無限ループが発生します。このループにより、予期しない不要な料金が発生する可能性があります。詳細については、「 ユーザーガイド」の「データイベントCloudTrail 」を参照してください。

S3 バックアップ完了ウィンドウ

以下の表は、S3 バケットの最初のフルバックアップの完了時間の目安となるように、さまざまなサイズのサンプルバケットを示しています。バックアップ時間は、各バケットのサイズ、内容、構成、設定によって異なります。

バケットサイズ	プロジェクト数	初期バックアップが完了するまでの推定時間
425 GB (ギガバイト)	1 億 3500 万	31 時間
800 TB (テラバイト)	6 億 7000 万	38 時間
6 PB (ペタバイト)	50 億	100 時間
370 TB (テラバイト)	75 億	180 時間

Amazon S3 のバックアップと復元のアクセス許可とポリシー

S3 リソースをバックアップ、コピー、復元するには、ロールに適切なポリシーが必要です。これらのポリシーを追加するには、「AWS 管理ポリシー」を参照してください。S3 バケットのバックアップAWSBackupServiceRolePolicyForS3Backupと復元に使用するAWSBackupServiceRolePolicyForS3Restoreロールに と を追加します。

十分なアクセス許可がない場合は、組織の管理者 (admin) アカウントの管理者に、目的のロールにポリシーを追加するよう依頼してください。

詳細については、「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」を参照してください。https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_managed-vs-inline.html

AWS Backup for S3 は、Amazon を介した S3 イベントの受信に依存しています EventBridge。S3 バケット通知設定でこの設定を無効にすると、設定がオフになっているバケットの継続的バックアップは停止します。詳細については、「 の使用 EventBridge」を参照してください。

S3 バックアップのベストプラクティスとコストに関する考慮事項

ベストプラクティス

3 億個を超えるオブジェクトを含むバケットの場合:

- 3 億個を超えるオブジェクトを含むバケットでは、バケットの最初のフルバックアップ時にバックアップ速度が 1 秒あたり最大 17,000 オブジェクトに達することがあります (増分バックアップでは速度が異なります)。3 億個未満のオブジェクトを含むバケットは、1 秒あたり 1,000 オブジェクトに近い速度でバックアップされます。
- 継続的バックアップが推奨されます。
- バックアップのライフサイクルを 35 日以上に予定している場合は、継続的バックアップが保存されているのと同じボールトにあるバケットのスナップショットバックアップを有効にすることもできます。

コストに関する考慮事項

- S3 ライフサイクルポリシーには、「期限切れのオブジェクト削除マーカーを削除」というオプション機能があります。この機能をオフにすると、削除マーカー (場合によっては数百万単位) がクリーンアッププランなしで期限切れになります。この機能のないバケットをバックアップすると、時間とコストに影響する問題が 2 つ生じます。
  - 削除マーカーはオブジェクトと同様にバックアップされます。オブジェクトと削除マーカーの比率によっては、バックアップ時間と復元時間が影響を受ける可能性があります。
  - バックアップされるオブジェクトとマーカーにはそれぞれ最低料金が適用されます。各削除マーカーには 128 KiB のオブジェクトと同じ料金がかかります。
- 少なくとも毎日、またはそれ以上の頻度でバックアップを行うアカウントでは、バックアップ内のデータについてのバックアップ間の変更が最小限であれば、継続的バックアップを使用することでコスト上のメリットが得られます。
- より大きなバケットで、変更の頻度が低いものは、継続的バックアップのメリットがあります。これは、バケット全体のスキャンとオブジェクトごとの複数のリクエストを、既存のオブジェクト

(前回のバックアップから変更されていないオブジェクト) に対して実行する必要がない場合にコスト削減につながるためです。

- 1 億個を超えるオブジェクトを含むバケットで、全体のバックアップサイズに比べて削除率が小さい場合、2 日間の保持期間の継続的バックアップと、保持期間の長いスナップショットバックアップの両方を含むバックアッププランでは、コスト面でのメリットが得られる可能性があります。
- 定期的 (スナップショット) バックアップ時間は、バケットスキャンが不要なときのバックアッププロセスの開始時間と一致します。継続的バックアップとスナップショットバックアップの両方を含むバケットでは、スナップショットバックアップは継続的復旧ポイントから取得されるため、スキャンは不要です。
- 1 つの S3-GIR (Amazon S3 Glacier Instant Retrieval) AWS Backup 内の各オブジェクトについて、は複数の呼び出しを実行するため、バックアップの実行時に取得料金が発生します。

  S3-IA ストレージクラスと S3 1 ゾーン-IA ストレージクラスのオブジェクトを持つバケットにも同様の取り出しコストが適用されます。 S3
- AWS KMS CloudTrail、、およびバックアップ戦略の一部である Amazon CloudWatch の機能では、S3 バケットデータストレージを超える追加コストが発生する可能性があります。これらの機能の調整に関する詳細については、以下を参照してください。
  - Amazon S3 ユーザーガイドの Amazon S3 バケットキーを使用した SSE-KMS のコストの削減。
  - AWS KMS イベントを除外し、S3 データイベントを無効にすることで CloudTrail コストを削減できます。
    - AWS KMS イベントを除外する: CloudTrail ユーザーガイド では、コンソールで証跡を作成する (基本イベントセレクタ) では、 AWS KMS これらのイベントを証跡からフィルタリングするイベントを除外するオプションを使用できます (デフォルト設定にはすべての KMS イベントが含まれます) 。
    - KMS イベントをログまたは除外するオプションは、証跡の管理イベントをログに記録する場合にのみ使用できます。管理イベントをログに記録しないように選択した場合は、KMS イベントはログに記録されず、KMS イベントログ設定は変更できません。
    - AWS KMS `Encrypt`、、 などの アクションは`Decrypt`、`GenerateDataKey`通常、大量のイベント (99% 以上) を生成します。これらのアクションは、[読み取り] イベントとしてログに記録されるようになりました。`Disable`、`Delete`、および `ScheduleKey` などのボリュームの小さい関連 KMS アクション (通常、KMS イベントボリュームの 0.5% 未満を占める) は、[書き込み] イベントとしてログに記録されます。
    - `Encrypt`、`Decrypt`、`GenerateDataKey` のようなボリュームの大きなイベントを除外し、`Disable`、`Delete`、`ScheduleKey` などの関連イベントを記録する場合は、[書き込み]

管理イベントを記録することを選択し、[AWS KMS イベントの除外] チェックボックスをオフにします。

- S3 データイベントを無効にする: デフォルトでは、証跡とイベントデータストアはデータイベントを記録しません。コスト削減のため、初回バックアップの前に S3 データイベントを無効にします。

- CloudWatch コストを削減するために、証跡を更新して CloudWatch ログ設定を無効にすると、CloudWatch ログへの CloudTrail イベントの送信を停止できます。

S3 バックアップの復元

を使用してバックアップした S3 データを S3 標準ストレージクラス AWS Backup に復元できます。S3 データは、元のバケットを含め、既存のバケットに復元できます。復元中に、復元ターゲットとして新しい S3 バケットを作成することもできます。S3 バックアップは、バックアップ AWS リージョン がある場所と同じ にのみ復元できます。

S3 バケット全体、またはバケット内のフォルダまたはオブジェクトを復元できます。 AWS Backup は、そのオブジェクトの現在のバージョンを復元します。

を使用して S3 データを復元するには AWS Backup、「」を参照してくださいS3 データの復元。

仮想マシンのバックアップ

AWS Backup は、オンプレミスの VMware 仮想マシン (VMsの VMware Cloud™ (VMC) および の VMware VMware Cloud™ (VMC) の VMs の一元化 AWS および自動データ保護をサポートします AWS Outposts。オンプレミスおよび VMC 仮想マシンから にバックアップできます AWS Backup。その後、 AWS Backup から、オンプレミス VM、VMC 内の VM、または VMC on AWS Outpostsに復元できます。

AWS Backup は、VM 検出、バックアップスケジューリング、保持管理、低コストのストレージ階層、クロスリージョンおよびクロスアカウントコピー、 AWS Backup ボールトロックと AWS Backup Audit Manager のサポート、ソースデータから独立した暗号化、バックアップアクセスポリシーなど、フルマネージド型の AWSネイティブ VM バックアップ管理機能も提供します。機能と詳細の完全なリストについては、「リソース別の機能の可用性 テーブル」を参照してください。

AWS Backup を使用して、VMware Cloud™ on 上の仮想マシンを保護できます AWS Outposts。AWS Outposts は、VMware Cloud™ on が接続され AWS リージョン ている に AWS Backup VM バックアップを保存します。 AWS Backup VMware VMware Cloud™ on を使用して、アプリケーションデータの低レイテンシーとローカルデータ処理のニーズを満たすために、VMware Cloud™ on

AWS Outposts AWS Backup VMs を保護できます。データレジデンシーの要件に基づいて、 AWS Outposts が接続され AWS リージョン ている親にアプリケーションデータのバックアップ AWS Backup を保存することもできます。

サポートされている VM

AWS Backup は、VMware vCenter によって管理される仮想マシンをバックアップおよび復元できます。

現在サポートされている：

- vSphere 8、7.0、および 6.7
- 1 KiB の倍数である仮想ディスクサイズ
- オンプレミスおよび 上の VMC の NFS、VMFS、および VSAN データストア AWS
- オンプレミス VMware のソース VMsにデータをコピーするための SCSI Hot-Add and Network Block Device Secure Sockets Layer (NBDSSL) AWS トランスポートモード
- VMware Cloud on 上の VMs を保護するためのホット追加モード AWS

現在サポートされていません。

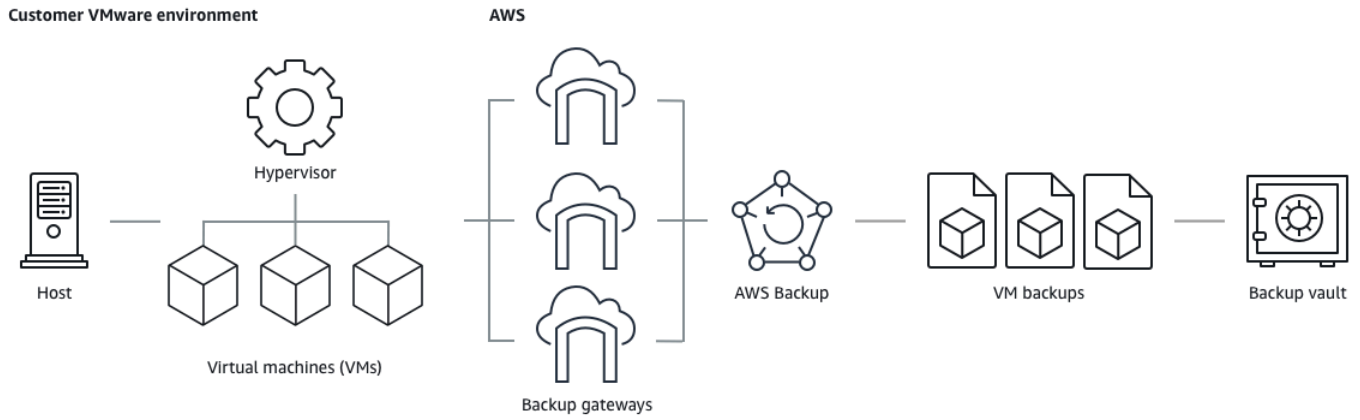
- RDM (raw ディスクマッピング) ディスクまたは NVMe コントローラーとそのディスク
- 独立した永続ディスクモードと独立した非永続ディスクモード

バックアップの整合性

AWS Backupは、デフォルトでは、仮想マシンの VMware Tools 静止設定を使用して、アプリケーションの整合性のある仮想マシンのバックアップをキャプチャします。アプリケーションが VMware Tools と互換性がある場合、バックアップはアプリケーションの一貫性を保ちます。休止機能が使用できない場合、 はクラッシュコンシステントバックアップ AWS Backup をキャプチャします。リストアをテストして、バックアップが組織のニーズを満たしていることを確認します。

Backup ゲートウェイ

Backup Gateway は、VMware VM を に接続するために VMware インフラストラクチャにデプロイするダウンロード可能な AWS Backup ソフトウェアです AWS Backup。 VMs ゲートウェイは VM 管理サーバーに接続して VM を検出し、VM を検出し、データを暗号化し、効率的にデータを AWS Backupに転送します。次の図は、Backup ゲートウェイが VM に接続する方法を示しています。



Backup ゲートウェイソフトウェアをダウンロードするには、ゲートウェイの使用 の手順に従います。

VPC (仮想プライベートクラウド) エンドポイントの詳細については、AWS Backup 「」および AWS PrivateLink 「接続」を参照してください。

Backup ゲートウェイには別に、 AWS Backup API から保持された独自の API が付属しています。Backup ゲートウェイ API アクションのリストを表示するには、「Backup ゲートウェイアクション」を参照してください。Backup ゲートウェイ API データタイプのリストを表示するには、「Backup ゲートウェイのデータタイプ」を参照してください。

エンドポイント

現在パブリックエンドポイントを使用している既存のユーザーが、VPC (Virtual Private Cloud) エンドポイントに切り替える場合は、AWS PrivateLink を使用して VPC エンドポイントで新しいゲートウェイを作成し、既存のハイパーバイザーをゲートウェイに関連付けた後、パブリックエンドポイントを含むゲートウェイを削除できます。

Backup ゲートウェイを使用するようにインフラストラクチャを構成する

Backup ゲートウェイでは、仮想マシンをバックアップおよび復元するために、次のネットワーク、ファイアウォール、およびハードウェア構成が必要です。

ネットワーク構成

バックアップゲートウェイを操作するには、許可されている特定のポートが必要です。次のポートを許可します。

1. TCP 443 アウトバウンド
   - ソース: Backup ゲートウェイ
   - 送信先： AWS
   - 使用: Backup ゲートウェイが と通信できるようにします AWS。
2. TCP 80 インバウンド
   - ソース: への接続に使用するホスト AWS Management Console
   - デスティネーション: Backup ゲートウェイ
   - 使用: ローカルシステムでバックアップゲートウェイのアクティベーションキーを取得します。ポート 80 は Backup ゲートウェイのアクティベーション中のみ使用されます。ポート 80 をパブリックにアクセス可能に AWS Backup する必要はありません。ポート 80 へのアクセスに必要なレベルはネットワークの設定によって決まります。からゲートウェイをアクティブ化する場合 AWS Management Console、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。
3. UDP 53 アウトバウンド
   - ソース: Backup ゲートウェイ
   - デスティネーション: ドメインネームサービス (DNS) サーバー
   - 使用: Backup ゲートウェイが DNS と通信できるようにします。
4. TCP 22 アウトバウンド
   - ソース: Backup ゲートウェイ
   - 送信先： AWS Support
   - 使用: AWS Support がゲートウェイにアクセスして問題に対応できるようにします。ゲートウェイの通常のオペレーションでは、このポート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開かなくてはなりません。
5. UDP 123 アウトバウンド
   - ソース: NTP クライアント
   - デスティネーション: NTP サーバー
   - 使用: 仮想マシン時間をホスト時間に同期するためにローカルシステムで使用されます。
6. TCP 443 アウトバウンド
   - ソース: Backup ゲートウェイ
   - 送信先: VMware vCenter
   - 使用: Backup ゲートウェイが VMware vCenter と通信できるようにします。
7. TCP 443 アウトバウンド

- ソース: Backup ゲートウェイ
- 送信先: ESXi ホスト
- 使用: Backup ゲートウェイが ESXi ホストと通信できるようにします。

8. TCP 902 アウトバウンド
   - ソース: Backup ゲートウェイ
   - 送信先: VMware ESXi ホスト
   - 使用: Backup ゲートウェイ経由でのデータ転送に使用されます。

上記のポートは Backup ゲートウェイに必要です。の Amazon VPC エンドポイントを設定する方法AWS Backup VPC エンドポイントの作成の詳細については、「」を参照してください AWS Backup。

ファイアウォールの設定

Backup ゲートウェイは、 と通信するために以下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 Amazon Web Services。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。Backup ゲートウェイとサービスポイント間の HTTP プロキシの使用はサポートされていません。

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

VMware で複数の NIC に対するゲートウェイの設定

複数の仮想ネットワークインターフェイス接続 (NICsと外部トラフィック (ゲートウェイから AWS) を個別にルーティングすることで、内部トラフィックと外部トラフィックに別々のネットワークを維持できます。

デフォルトでは、 AWS Backup ゲートウェイに接続された仮想マシンには 1 つのネットワークアダプタ () がありますeth0。このネットワークには、より広範なインターネットと通信するハイパーバイザー、仮想マシン、ネットワークゲートウェイ (バックアップゲートウェイ) が含まれます。

以下は、複数の仮想ネットワークインターフェイスを使ったセットアップの例です。

```
eth0:
- IP: 10.0.3.83
- routes: 10.0.3.0/24

eth1:
- IP: 10.0.0.241
- routes: 10.0.0.0/24
- default gateway: 10.0.0.1
```

- この例では、IP 10.0.3.123 を用いたハイパーバイザーへの接続となっており、ゲートウェイは eth0 を使用します。ハイパーバイザーが 10.0.3.0/24 ブロックの一部であるためです。
- IP 10.0.0.234 を用いてハイパーバイザーに接続するには、ゲートウェイは、eth1 を使用します
- ローカルネットワーク外の IP (例: 34.193.121.211) に接続するには、ゲートウェイは、10.0.0.0/24 ブロック内にあるデフォルトゲートウェイ (10.0.0.1) にフォールバックし、そのまま eth1 に接続します

ネットワークアダプタを追加する最初の手順は、vSphere クライアントで行われます。

1. VMware vSphere クライアントでゲートウェイ仮想マシンのコンテキストメニューを (右クリックで) 開き、[設定を編集] 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の [仮想ハードウェア] タブで、[新しいデバイスの追加] メニューを開き、[ネットワークアダプタ] を選択して新しいネットワークアダプタを追加します。
3.
   a. [新しいネットワーク] の詳細を展開して、新しいアダプタを設定します。
   b. [パワーオン時に接続] が選択されていることを確認します。
   c. アダプタのタイプ については、「ESXi と vCenter Server のドキュメント」の「ネットワークアダプタのタイプ」を参照してください。
4. [OK] をクリックして、新しいネットワークアダプタ設定を保存します。

追加のアダプターを設定する次のステップは、 AWS Backup ゲートウェイコンソールで行われます (これは、バックアップやその他のサービスが管理されている AWS 管理コンソールと同じインターフェイスではないことに注意してください) 。

新しい NIC をゲートウェイ VM に追加したら、以下を実行する必要があります

- [Command Prompt] に移動して、新しいアダプタをオンにします
- 新しい NIC ごとに固定 IP を設定します
- 優先する NIC をデフォルトとして設定します

そのためには、以下の操作をします

1. VMware vSphere クライアントで、ゲートウェイ仮想マシンを選択し、ウェブコンソールを起動して Backup ゲートウェイのローカルコンソールにアクセスします。
   - ローカルコンソールへのアクセスの詳細については、「VMware ESXi によるゲートウェイローカルコンソールへのアクセス」を参照してください。
2. コマンドプロンプトを終了し、[ネットワーク構成] > [固定 IP の設定] に移動し、セットアップ手順に従ってルーティングテーブルを更新します。
   a. ネットワークアダプターのサブネット内に静的 IP を割り当てます。
   b. ネットワークマスクを設定します。
   c. デフォルトゲートウェイの IP アドレスを入力します。これは、ローカルネットワーク外のすべてのトラフィックに接続するネットワークゲートウェイです。
3. クラウドに接続するアダプターをデフォルトデバイスとして指定するには、[デフォルトアダプターを設定] を選択します。
4. ゲートウェイのすべての IP アドレスは、ローカルコンソールと、VMware vSphere の仮想マシンの概要ページの両方に表示できます。

ハードウェア要件:

Backup ゲートウェイの仮想マシンホスト上で、次の最小リソースを専用できる必要があります。

- 4 つの仮想プロセッサ
- 予約済み RAM 8 GiB

VMware のアクセス権限

このセクションでは、 を使用するために必要な最低限の VMware アクセス許可を一覧表示します AWS Backup gateway。これらのアクセス権限は、Backup ゲートウェイが仮想マシンを検出、バックアップ、および復元するために必要です。

Backup ゲートウェイを VMware Cloud™ on AWS または VMware Cloud™ on で使用するには AWS Outposts、デフォルトの管理者ユーザーを使用する`cloudadmin@vmc.local`か、 CloudAdmin 専用ユーザーにロールを割り当てる必要があります。

VMware オンプレミス仮想マシンで Backup ゲートウェイを使用するには、以下に示すアクセス許可を持つ専用ユーザーを作成します。

グローバル

- メソッドを無効にする
- メソッドを有効にする
- ライセンス
- ログイベント
- カスタム属性を管理する
- カスタム属性を設定する

vSphere タギ付け

- vSphere タグの割り当てまたは割り当て解除

DataStore

- 容量を割り当てる
- データストアを参照する
- データストアを設定する (vSAN データストア用)
- 低レベルのファイル操作
- 仮想マシンのファイルを更新する

ホスト

- 構成

- [詳細設定]
- ストレージパーティションの設定

フォルダ

- フォルダの作成

ネットワーク

- ネットワークを割り当て

dvPort グループ

- 作成
- 削除

リソース

- 仮想マシンをリソースプールに割り当て

仮想マシン

- 設定の変更
  - ディスクリースを取得する
  - 既存のディスクを追加する
  - 新しいディスクを追加する
  - 高度な設定
  - 設定を変更する
  - raw デバイスを設定する
  - デバイス設定を変更する
  - ディスクを削除する
  - 注釈を設定する
  - ディスク変更の追跡を切り替え
- インベントリを編集する

  - 既存から作成する
  - 新規作成
  - 登録
  - Remove
  - 登録を解除する
- インタラクション
  - パワーオフ
  - パワーオン
- プロビジョニング
  - ディスクアクセスを許可する
  - 読み取り専用ディスクアクセスを許可する
  - 仮想マシンのダウンロードを許可する
- スナップショットの管理
  - スナップショットの作成
  - スナップショットの削除
  - スナップショットに戻す

ゲートウェイの使用

を使用して仮想マシン (VMs) をバックアップおよび復元するには AWS Backup、まず Backup ゲートウェイをインストールする必要があります。ゲートウェイは、OVF (Open Virtualization Format) テンプレート形式のソフトウェアで、 Amazon Web Services Backup をハイパーバイザーに接続して仮想マシンを自動的に検出し、バックアップと復元を可能にします。

1 つのゲートウェイで最大 4 つのバックアップジョブまたは復元ジョブを同時に実行できます。4 つ以上のジョブを同時に実行するには、ゲートウェイをさらに作成してハイパーバイザーに関連付けます。

ゲートウェイの作成

ゲートウェイを作成するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. 左のナビゲーションペインの [外部リソース] セクションで、[ゲートウェイ] をクリックします。

3. [Create gateway (ゲートウェイの作成)] を選択します。
4. [ゲートウェイの設定] セクションで、この手順に従って OVF テンプレートをダウンロードしてデプロイします。

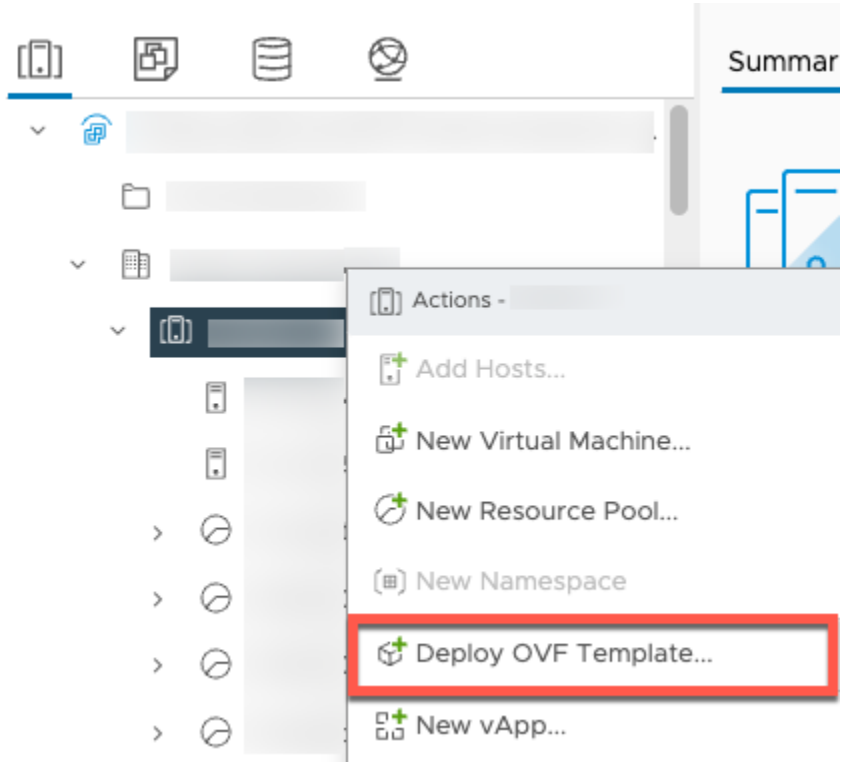
VMware ソフトウェアのダウンロード

ハイパーバイザーの接続

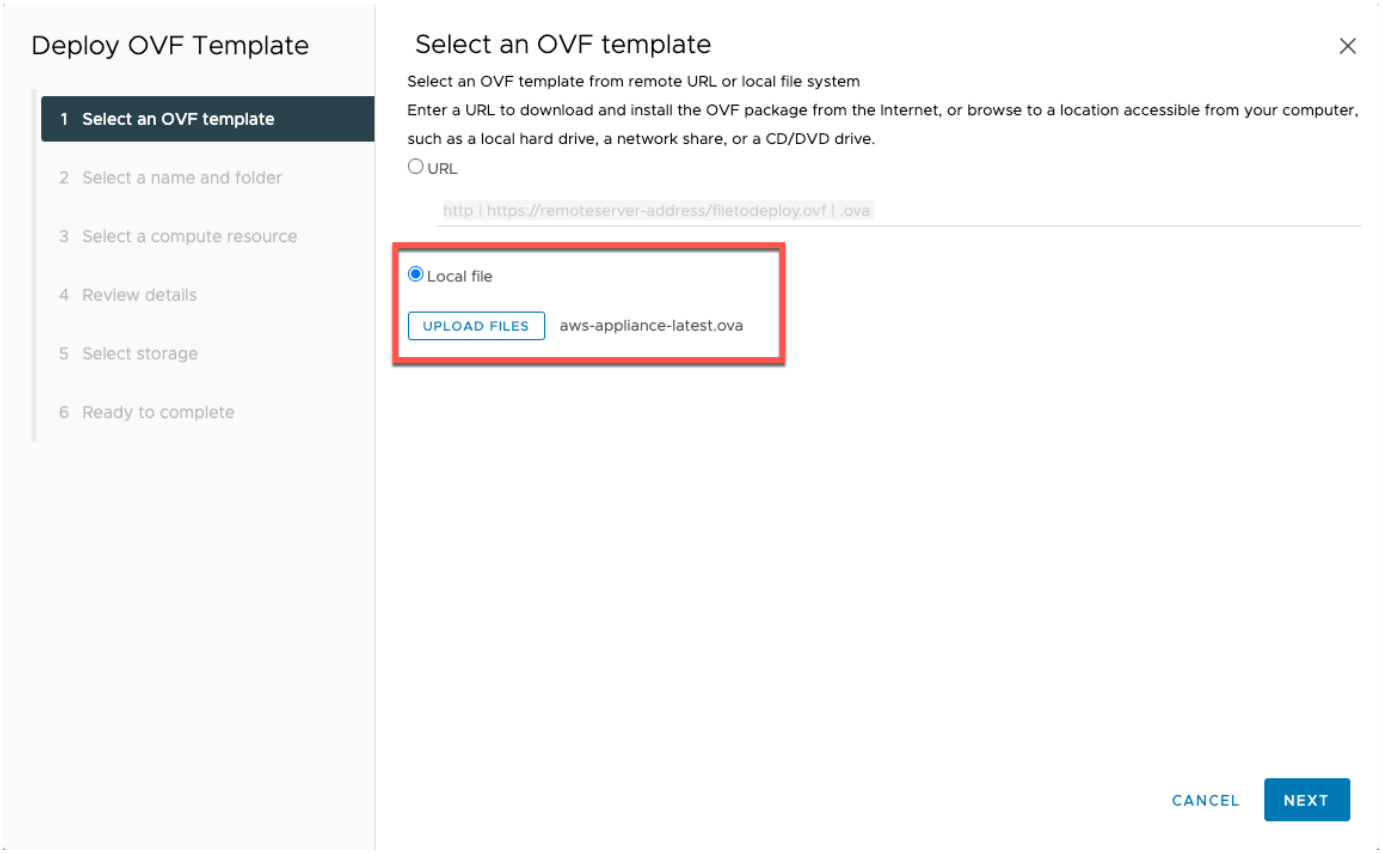
ゲートウェイはハイパーバイザー AWS Backup に接続するため、仮想マシンのバックアップを作成して保存できます。VMware ESXi でゲートウェイをセットアップするには、「OVF テンプレート」をダウンロードします。ダウンロードには約 10 分かかることもあります。

完了したら、次のステップを実行します。

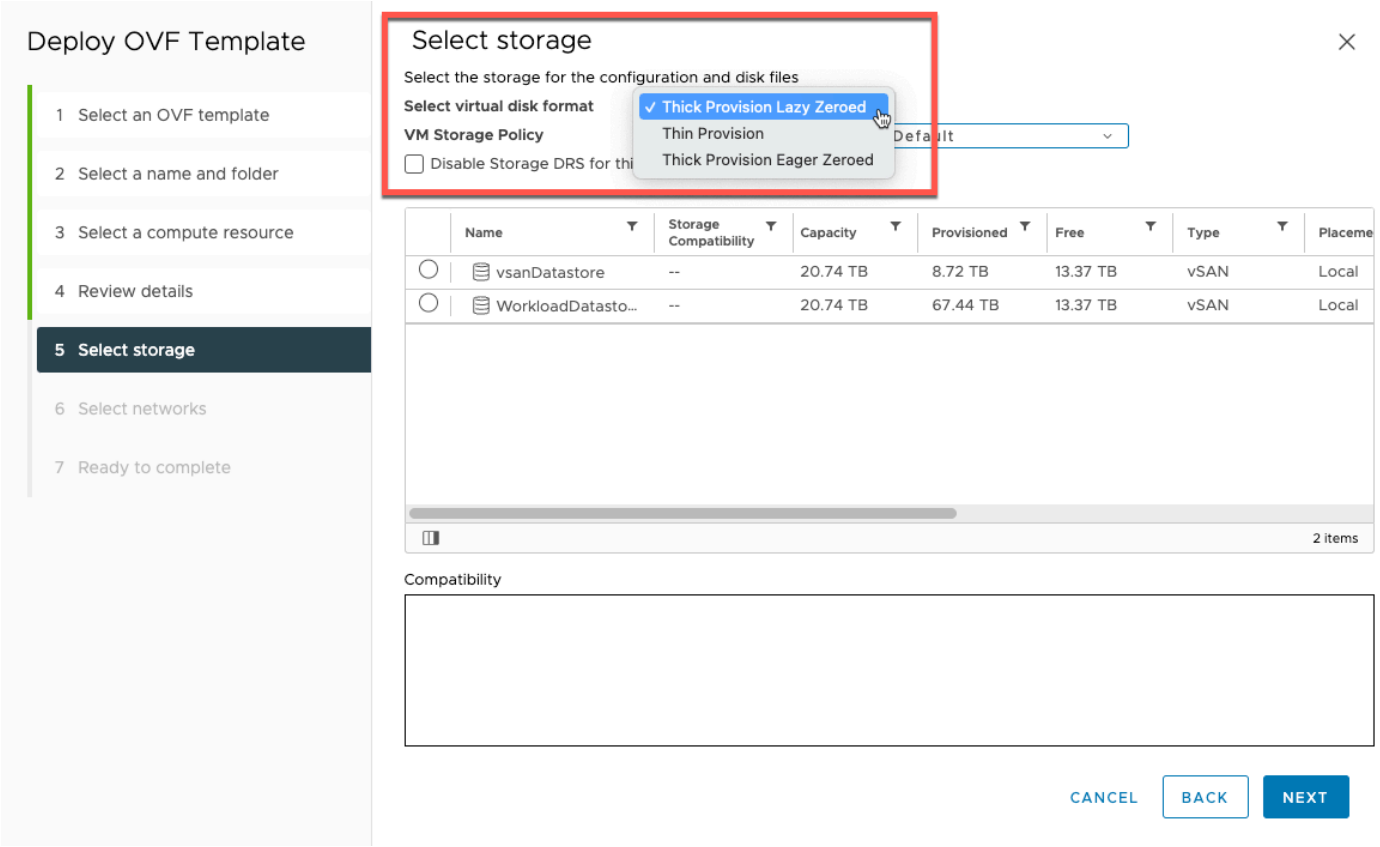
1. VMware vSphere を使用して仮想マシンのハイパーバイザーに接続します。
2. 仮想マシンの [親オブジェクト] を右クリックし、[OVF テンプレートのデプロイ] を選択します。



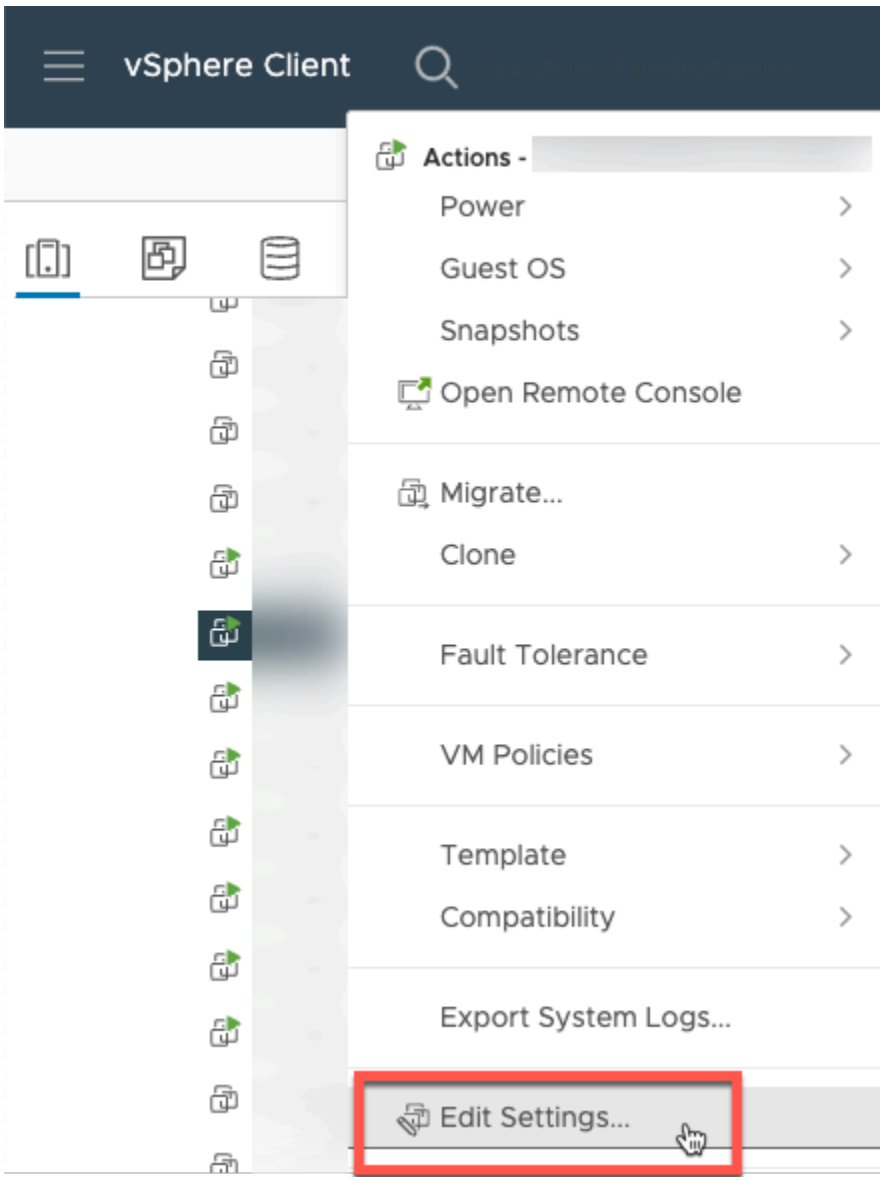
3. ローカルファイル を選択し、ダウンロードした aws-appliance-latest.ova ファイルをアップロードします。



4. デプロイウィザードの手順に従ってデプロイします。[ストレージの選択] ページで、仮想ディスクフォーマット [シックプロビジョニング Lazy Zeroed] を選択します。

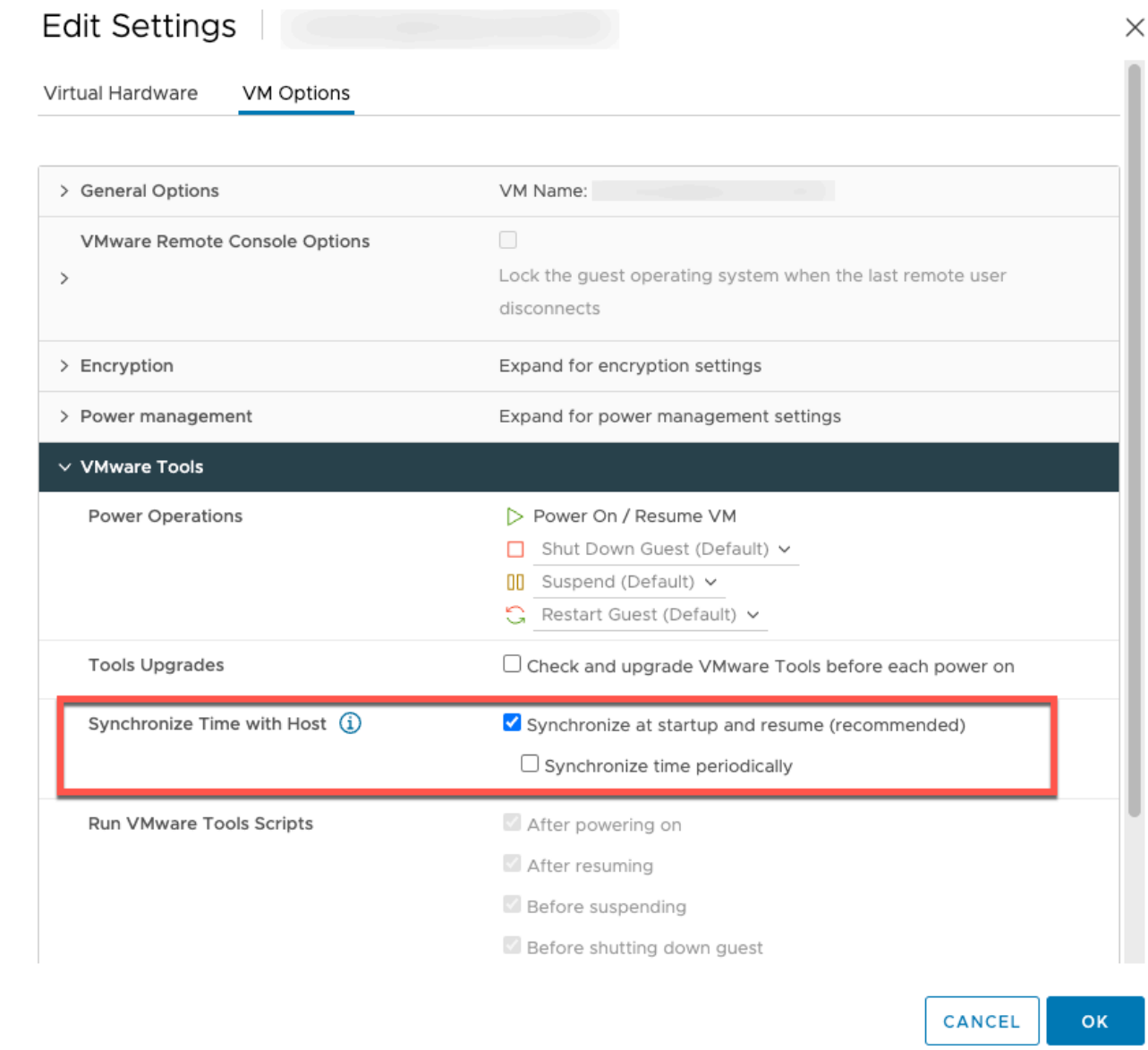


5. OVF をデプロイしたら、ゲートウェイを右クリックして [設定の編集] を選択します。

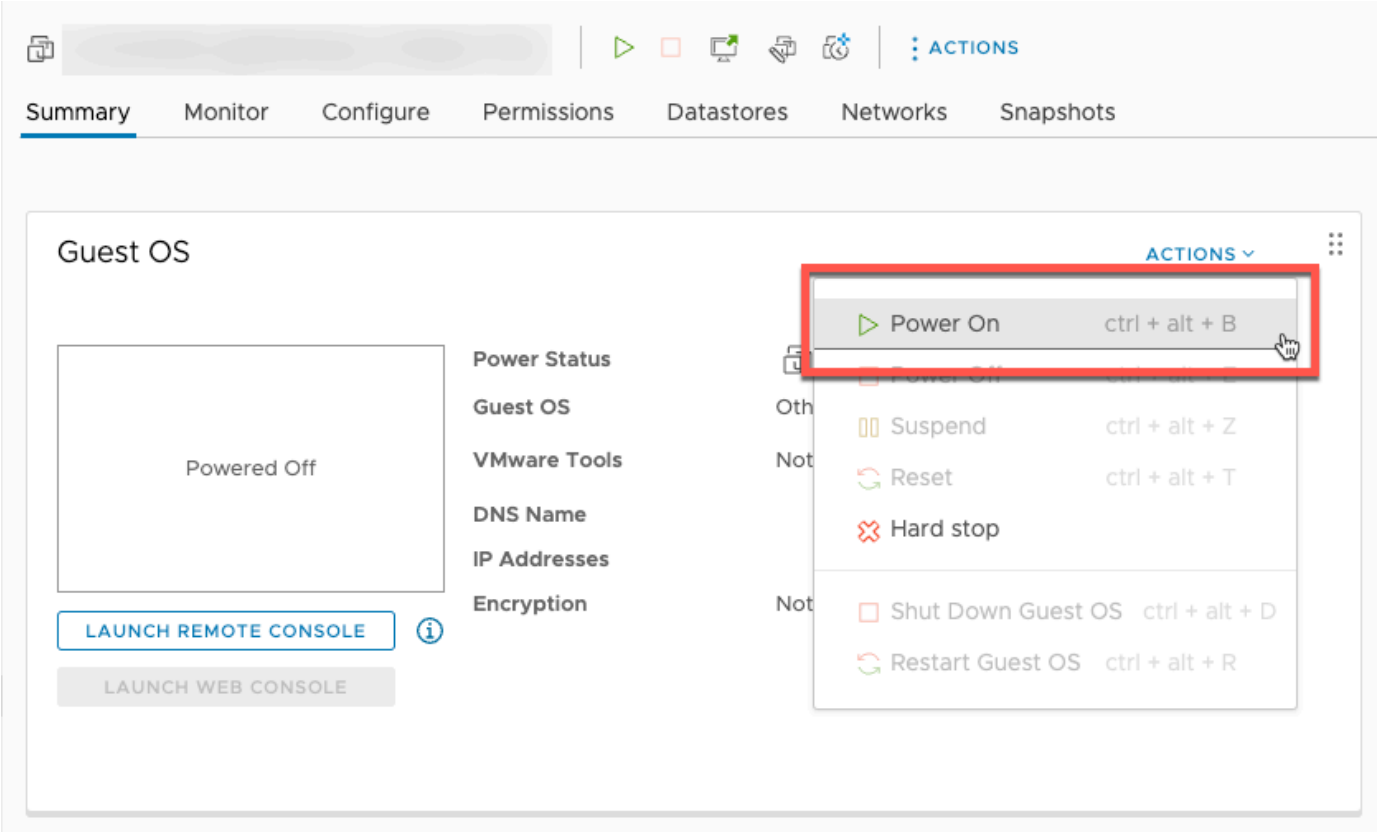


a. [VM オプション] で、[VM ツール] に移動します

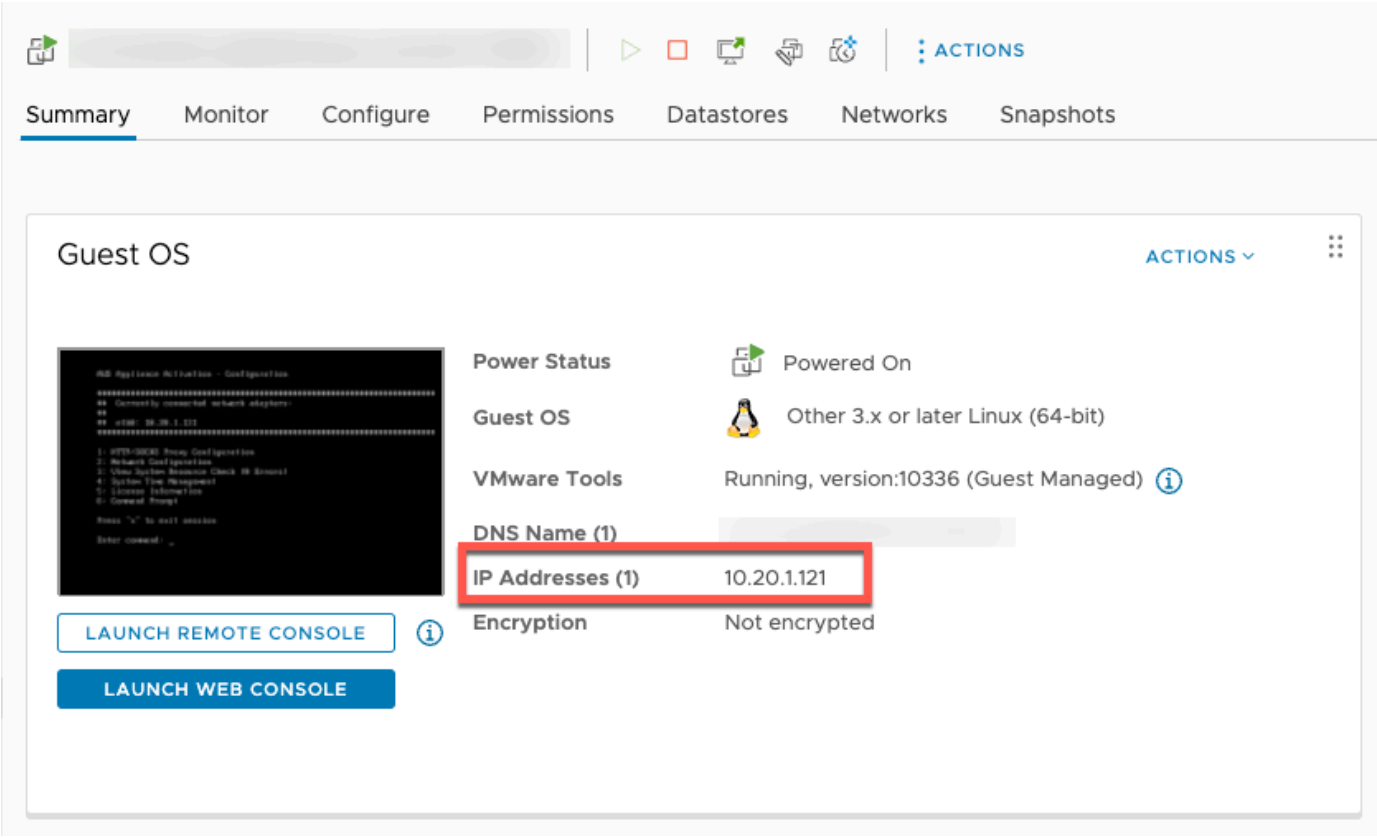
b. [ホストと時刻を同期] で、[起動時と再開時に同期する] が選択されていることを確認します。



6. [アクション] メニューから [パワーオン] を選択して、仮想マシンをオンにします。



7. VM の概要から IP アドレスをコピーし、以下に入力します。



VMware ソフトウェアをダウンロードしたら、以下の手順を実行します。

1. [ゲートウェイの接続] セクションで、ゲートウェイの IP アドレス を入力します。
   a. この IP アドレスを見つけるには、vSphere クライアントに移動します。
   b. [概要] タブでゲートウェイを選択します。
   c. IP アドレスをコピーし、 AWS Backup コンソールのテキストバーに貼り付けます。
2. [ゲートウェイの設定] セクションで、
   a. [ゲートウェイ名] を入力します。
   b. AWS リージョンを確認します。
   c. エンドポイントをパブリックにアクセス可能にするか、Virtual Private Cloud (VPC) でホストするかを選択します。
   d. 選択したエンドポイントに応じて、VPC エンドポイントの DNS 名を入力します。

      詳細については、「VPC エンドポイントの作成」を参照してください
3. [オプション] [ゲートウェイタグ] セクションでは、[キー] と [オプション] の [値] を入力してタグを割り当てることができます。複数のタグを追加するには、[別のタグを追加] をクリックします。
4. プロセスを完了するには、[ゲートウェイを作成] をクリックすると、ゲートウェイの詳細ページが表示されます。

ゲートウェイの編集または削除

ゲートウェイを編集または削除するには

1. 左のナビゲーションペインの [外部リソース] セクションで、[ゲートウェイ] をクリックします。
2. [ゲートウェイ] セクションで、ゲートウェイ名でゲートウェイを選択します。
3. ゲートウェイ名を編集するには、[編集] をクリックします。
4. ゲートウェイを削除するには、[削除] をクリックして [ゲートウェイを削除] を選択します。

   削除されたゲートウェイを再アクティブ化することはできません。ハイパーバイザーに再度接続する場合は、「ゲートウェイの作成」の手順に従ってください。
5. ハイパーバイザーに接続するには、接続されたハイパーバイザーセクションで、[接続] を選択します。

各ゲートウェイは 1 つのハイパーバイザーに接続します。ただし、複数のゲートウェイを同じハイパーバイザーに接続して、最初のゲートウェイの帯域幅を超えてそれらの間の帯域幅を増やすことができます。

6. タグを割り当て、編集、または管理するには、[タグ] セクションで、[タグの管理] を選択します。

バックアップゲートウェイの帯域幅スロットリング

> **Note**
>
> この機能は、2022 年 12 月 15 日以降にデプロイされた新しいゲートウェイで利用できるようになります。既存のゲートウェイでは、この新機能は 2023 年 1 月 30 日までにソフトウェアの自動更新により利用できるようになります。ゲートウェイを手動で最新バージョンに更新するには、 AWS CLI コマンドを使用しますUpdateGatewaySoftwareNow。

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 Backup して、ゲートウェイが使用するネットワーク帯域幅の量を制御できます。デフォルトでは、アクティブ化されたゲートウェイのレート制限は設定されていません。

帯域幅レート制限スケジュールは、 AWS Backup コンソールを使用するか、 () で AWS CLI API を使用して設定できますPutBandwidthRateLimitSchedule。帯域幅レート制限スケジュールを使用すると、制限が 1 日または 1 週間を通して自動的に変更されるように設定できます。

帯域幅レート制限は、アップロードされるすべてのデータのスループットを 1 秒あたりに平均して調整することで機能します。アップロードがマイクロ秒単位またはミリ秒単位で帯域幅レート制限を一時的に超えることもありますが、これによって長時間にわたって大きなスパイクが発生することは通常ありません。

最大 20 個の間隔を追加できます。アップロード速度の最大値は 8,000,000 (百万) メガバイト/秒 (Mbps) です。

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

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

帯域幅レート制限スケジュールを表示および編集するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. 左のナビゲーションペインで [ゲートウェイ] を選択します。[ゲートウェイ] ペインでは、ゲートウェイは名前ごとに表示されます。管理するゲートウェイ名の横にあるラジオボタンをクリックします。
3. ラジオボタンを選択すると、ドロップダウンメニューの [アクション] をクリックできるようになります。[アクション] をクリックし、[帯域幅レート制限スケジュールを編集] をクリックします。現在のスケジュールが表示されます。デフォルトでは、新規または未編集のゲートウェイには、帯域幅レート制限が定義されていません。

   > **Note**
   >
   > ゲートウェイの [詳細] ページの [スケジュールを管理] をクリックして [帯域幅の編集] ページに移動することもできます。

4. (オプション) [間隔を追加] を選択して、設定可能な新しい間隔をスケジュールに追加します。間隔ごとに、次の情報を入力します。

   a. 曜日 — 間隔を適用する定期的な曜日を選択します。選択すると、ドロップダウンメニューの下に曜日が表示されます。曜日の横にある [X] をクリックすると削除できます。

   b. 開始時刻 — [HH:MM] 24 時間形式を使用して、帯域幅間隔の開始時刻を入力します。時刻は協定世界時 (UTC) で表示されます。

      注: bandwidth-rate-limit 間隔は、指定した分の開始から始まります。

   c. 終了時刻 — [HH:MM] 24 時間形式を使用して、帯域幅間隔の終了時刻を入力します。時刻は協定世界時 (UTC) で表示されます。

      > **Important**
      >
      > bandwidth-rate-limit 間隔は、指定した分の最後に終了します。1 時間の終わりに終了する期間をスケジュールするには、「59」と入力します。連続する期間を続けてスケジュールする際に、1 時間の開始時に移行し、期間の間に中断がないようにするには、最初の期間の終了時間を「59」分と入力します。後の期間の開始時間は、「00」分と入力します。

   d. アップロード速度 — アップロード速度の制限をメガビット/秒 (Mbps) 単位で入力します。最小値は 102 メガバイト/秒 (Mbps) です。

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

> **Important**
>
> 帯域幅レート制限間隔はオーバーラップできません。間隔の開始時刻は、前の間隔の終了時刻より後で、かつ、次の間隔の開始時刻より前である必要があります。間隔の終了時刻は、次の間隔の開始時刻より前である必要があります。

6. 完了したら、[変更を保存] ボタンをクリックします。

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

GetBandwidthRateLimitSchedule アクションを使用して、指定したゲートウェイの帯域幅スロットルスケジュールを表示できます。スケジュールが設定されていない場合、スケジュールは空の間隔リストになります。を使用してゲートウェイの帯域幅スケジュール AWS CLI を取得する例を次に示します。

```
aws backup-gateway get-bandwidth-rate-limit-schedule --gateway-arn "arn:aws:backup-gateway:region:account-id:gateway/bgw-gw id"
```

ゲートウェイの帯域幅スロットルスケジュールを編集するには、PutBandwidthRateLimitSchedule アクションを使用できます。更新できるのはゲートウェイのスケジュール全体のみで、個々の間隔は変更、追加、削除できないことに注意してください。このアクションを呼び出すと、ゲートウェイの以前の帯域幅スロットルスケジュールが上書きされます。

```
aws backup-gateway put-bandwidth-rate-limit-schedule --gateway-arn "arn:aws:backup-gateway:region:account-id:gateway/gw-id" --bandwidth-rate-limit-intervals ...
```

ハイパーバイザーの操作

を完了したらゲートウェイの作成、ハイパーバイザーに接続して、 がそのハイパーバイザーによって管理される仮想マシンと連携 AWS Backup できるようにします。たとえば、VMware 仮想マシンのハイパーバイザーは VMware vCenter Server です。ハイパーバイザーに AWS Backupに必要なアクセス許可が設定されていることを確認してください。

ハイパーバイザーの追加

ハイパーバイザーを追加するには、次の手順を実行します。

1. 左のナビゲーションペインの [外部リソース] セクションで、[ハイパーバイザー] をクリックします。
2. [ハイパーバイザーの追加] を選択します。
3. [Hypervisor 設定] セクションで、ハイパーバイザー名を入力します。
4. [vCenter サーバーホスト] を選択し、ドロップダウンメニューを使用して、[IP アドレス] または [FQDN (完全修飾ドメイン名)] を選択します。対応する値を入力します。
5. AWS Backup がハイパーバイザー上の仮想マシンを検出できるようにするには、ハイパーバイザーのユーザー名 とパスワード を入力します。
6. パスワードを暗号化します。この暗号化を指定するには、ドロップダウンメニューを使用して特定のサービス管理の KMS キーまたはカスタマー管理の KMS キーを選択するか、[KMS キーを作成] を選択します。特定のキーを選択しない場合、 AWS Backup は、サービス所有のキーを使用してパスワードを暗号化します。
7. [Connecting gateway] セクションで、ドロップダウンリストを使用して、ハイパーバイザーに接続する Gateway を指定します。
8. [Test gateway connection] をクリックして、以前の入力を確認します。
9. オプションとして、[ハイパーバイザーのタグ] セクションで、[新しいタグを追加] を選択して、ハイパーバイザーにタグを割り当てることができます。
10. オプションの VMware タグマッピング: 現在使用している VMware タグを仮想マシンに追加して AWS 、タグを生成できます。
11. ロググループ設定パネルでは、Amazon CloudWatch Logs と統合してハイパーバイザーのログを維持するように選択できます (使用量に応じて標準のCloudWatch ログ料金が適用されます)。各ハイパーバイザーは、1 つのロググループに属することができます。
    a. ロググループをまだ作成していない場合は、[新しいロググループを作成する] ラジオボタンを選択します。編集中のハイパーバイザーは、このロググループに関連付けられます。
    b. 以前に別のハイパーバイザーのロググループを作成したことがある場合は、そのロググループをこのハイパーバイザーに使用できます。[既存のロググループを使用する] を選択します。
    c. CloudWatch ログ記録を使用しない場合は、ログ記録の無効化 を選択します。
12. [ハイパーバイザーの追加] をクリックし、その詳細ページに移動します。

> **Tip**
>
> Amazon CloudWatch Logs (上記のステップ 11 を参照) を使用して、エラーモニタリング、ゲートウェイとハイパーバイザー間のネットワーク接続、ネットワーク設定情報など、ハイパーバイザーに関する情報を取得できます。 CloudWatch ロググループの詳細については、「Amazon CloudWatch ユーザーガイド」の「ロググループとログストリームの使用」を参照してください。

ハイパーバイザーによって管理される仮想マシンの表示

ハイパーバイザー上の仮想マシンを表示するには、次の手順を実行します。

1. 左のナビゲーションペインの [外部リソース] セクションで、[ハイパーバイザー] をクリックします。
2. [ハイパーバイザー] セクションで、ハイパーバイザー名をクリックしてハイパーバイザーを選択し、その詳細ページに移動します。
3. [ハイパーバイザーの概要] のセクション内で、[仮想マシン] タブを選択します。
4. [接続された仮想マシン] セクションに、仮想マシンのリストが自動的に追加されます。

ハイパーバイザーに接続されたゲートウェイの表示

ハイパーバイザーに接続されているゲートウェイを表示するには、次の手順を実行します。

1. [ゲートウェイ] タブを選択します。
2. [接続されたゲートウェイ] セクションに、ゲートウェイのリストが自動的に追加されます。

ハイパーバイザーを追加のゲートウェイに接続する

バックアップと復元の速度は、ゲートウェイとハイパーバイザー間の接続の帯域幅によって制限される場合があります。1 つ以上の追加のゲートウェイをハイパーバイザーに接続することで、これらの速度を上げることができます。[接続されたゲートウェイ] セクションでこれを行うには、次のようになります。

1. [接続]を選択します。
2. ドロップダウンメニューを使用して別のゲートウェイを選択します。または、[ゲートウェイの作成] をクリックして、新しいゲートウェイを作成します。

3. [接続]を選択します。

ハイパーバイザー設定の編集

Test gateway connection 機能を使用しないと、誤ったユーザー名またはパスワードでハイパーバイザーを追加することがあります。その場合、ハイパーバイザーの接続ステータスを常に Pending にします。または、ユーザー名またはパスワードをローテーションしてハイパーバイザーにアクセスすることもできます。次のプロシージャを使用して、この情報を更新します。

すでに追加したハイパーバイザーを編集するには、次の手順を実行します。

1. 左のナビゲーションペインの [外部リソース] セクションで、[ハイパーバイザー] をクリックします。
2. [ハイパーバイザー] セクションで、ハイパーバイザー名をクリックしてハイパーバイザーを選択し、その詳細ページに移動します。
3. [編集] を選択します。
4. 一番上のパネルの名前は、[ハイパーバイザーの設定] です。
    a. vCenter サーバーホストでは、FQDN (完全修飾ドメイン名) または IP アドレスを編集することもできます。
    b. オプションとして、ハイパーバイザーの [ユーザーネーム] および [パスワード] を入力します。
5. ロググループ設定パネルでは、ハイパーバイザーのログを維持するために Amazon CloudWatch と統合することを選択できます (使用量に応じて標準CloudWatch 料金が適用されます)。各ハイパーバイザーは、1 つのロググループに属することができます。
    a. ロググループをまだ作成していない場合は、[新しいロググループを作成する] ラジオボタンを選択します。編集中のハイパーバイザーは、このロググループに関連付けられます。
    b. 以前に別のハイパーバイザーのロググループを作成したことがある場合は、そのロググループをこのハイパーバイザーに使用できます。[既存のロググループを使用する] を選択します。
    c. CloudWatch ログ記録を使用しない場合は、ログ記録の無効化 を選択します。

> **Tip**
>
> Amazon CloudWatch Logs (上記のステップ 5 を参照) を使用して、エラーモニタリング、ゲートウェイとハイパーバイザー間のネットワーク接続、ネットワーク設定情報など、ハイパーバイザーに関する情報を取得できます。 CloudWatch ロググループの詳細については、「Amazon CloudWatch ユーザーガイド」の「ロググループとログストリームの使用」を参照してください。

ハイパーバイザーをプログラムで更新するには、CLI コマンド update-hypervisor と UpdateHypervisor API コールを使用します。

ハイパーバイザー設定の削除

すでに追加されているハイパーバイザーを削除する必要がある場合は、ハイパーバイザー構成を削除して、別のハイパーバイザー構成を追加します。この削除操作は、ハイパーバイザーに接続するための構成に適用されます。ハイパーバイザーは削除されません。

すでに追加されているハイパーバイザーに接続するための構成を削除するには、次の手順を実行します。

1. 左のナビゲーションペインの [外部リソース] セクションで、[ハイパーバイザー] をクリックします。
2. [ハイパーバイザー] セクションで、ハイパーバイザー名をクリックしてハイパーバイザーを選択し、その詳細ページに移動します。
3. [削除]、[ハイパーバイザーの削除] の順に選択します。
4. オプション: ハイパーバイザーの追加 の手順を使用して、削除したハイパーバイザー構成を置き換えます。

ハイパーバイザーのステータスの理解

以下では、考えられるハイパーバイザーのステータスと、該当する場合の修復手順について説明します。ONLINE ステータスはハイパーバイザーの正常なステータスです。ハイパーバイザーは、ハイパーバイザーが管理する仮想マシンのバックアップと復元に使用されている間を通して、またはそのほとんどにおいて、このステータスになっているはずです。

ハイパーバイザーのステータス

ステータス	意味と修復
ONLINE	ハイパーバイザーを に追加し AWS Backup、ゲートウェイに関連付けられ、ネットワーク経由でそのゲートウェイに接続して、ハイパーバイザーによって管理される仮想マシンのバックアップとリカバリを実行できます。 これらの仮想マシンのオンデマンドバックアップとスケジュールバックアップはいつでも実行できます。
PENDING	ハイパーバイザーを に追加しました AWS Backup が、次のようになります。 • どのゲートウェイにも関連付けられていないか、または • 1 つ以上のゲートウェイに関連付けられているものの、それらのゲートウェイはすべて削除されているか、その他の理由でアクティブになっていません。 ハイパーバイザーのステータスを PENDING から ONLINE に変更するには、ゲートウェイを作成し、ハイパーバイザーをそのゲートウェイに接続します。
OFFLINE	ハイパーバイザーを に追加 AWS Backup してゲートウェイに関連付けましたが、ゲートウェイはネットワーク経由でハイパーバイザーに接続できません。 ハイパーバイザーのステータスを OFFLINE から ONLINE に変更するには、[ネットワーク構成] が正しいことを確認します。

ステータス	意味と修復
	問題が解決しない場合は、ハイパーバイザーの IP アドレスまたは完全修飾ドメイン名が正しいことを確認します。正しくない場合は、正しい情報を使用してハイパーバイザーを再度追加し、ゲートウェイ接続をテストします。
ERROR	ハイパーバイザーを に追加 AWS Backup してゲートウェイに関連付けましたが、ゲートウェイはハイパーバイザーと通信できません。 ハイパーバイザーのステータスを ERROR から ONLINE に変更するには、ハイパーバイザーのユーザー名とパスワードが正しいことを確認します。正しくない場合は、ハイパーバイザー構成を編集します。

次のステップ

ハイパーバイザーで仮想マシンをバックアップするには、仮想マシンのバックアップ を参照してください。

仮想マシンのバックアップ

ハイパーバイザーの追加 の後に、Backup ゲートウェイは仮想マシンを自動的に一覧表示します。仮想マシンを表示するには、左側のナビゲーションペインで [ハイパーバイザー] または [仮想マシン] のいずれかを選択します。

- [ハイパーバイザー] をクリックして、特定のハイパーバイザーによって管理されている仮想マシンのみを表示します。このビューでは、一度に 1 台の仮想マシンを操作できます。
- 仮想マシンを選択して、 に追加したすべてのハイパーバイザーのすべての仮想マシンを表示します AWS アカウント。このビューでは、複数のハイパーバイザーで一部またはすべての仮想マシンを操作できます。

選択したビューに関係なく、特定の仮想マシンでバックアップ操作を実行するには、[VM 名] をクリックして、その詳細ページを開きます。仮想マシンの詳細ページは、次の手順の開始点です。

仮想マシンのオンデマンドバックアップの作成

オンデマンドバックアップは、手動で開始するワンタイムフルバックアップです。オンデマンドバックアップを使用して、 AWS Backupのバックアップおよび復元機能をテストできます。

仮想マシンのオンデマンドバックアップを作成するには、次の手順を実行します。

1. [オンデマンドバックアップを作成] を選択します。
2. オンデマンドバックアップの設定
3. [オンデマンドバックアップを作成] を選択します。
4. バックアップジョブのステータス `Completed` がいつかを確認します。左のナビゲーションペインで [ジョブ] を選択します。
5. [Backup Job ID] を選択して、[Backup サイズ] および、[作成日] と [完了日] 間の経過時間などのバックアップジョブ情報を表示します。

増分 VM バックアップ

新しいバージョンの VMware には、ブロック変更追跡と呼ばれる機能が含まれています。この機能は、仮想マシンのストレージブロックが時間の経過とともに変化するたびにそれを追跡します。AWS Backup を使用して仮想マシンをバックアップする場合、使用可能な場合は CBT データの使用 AWS Backup を試みます。 は CBT データ AWS Backup を使用してバックアッププロセスを高速化します。CBT データがない場合、バックアップジョブは遅くなり、ハイパーバイザーリソースがより多く使用されます。CBT データが有効でない場合や、使用できない場合でも、バックアップは正常に完了します。例えば、仮想マシンまたは ESXi ホストがハードシャットダウンされた場合、CBT データは有効でなくなる可能性や、利用できなくなる可能性があります。

CBT データが無効または使用できない場合、バックアップステータスはメッセージ付きで `Successful` を読み取ります。このような場合、CBT データがない場合、メッセージは、VMware の CBT データの代わりに独自の変更検出メカニズム AWS Backup を使用してバックアップを完了したことを示します。その後のバックアップでは CBT データの使用が再試行され、ほとんどの場合、CBT データは正常に有効で使用可能になります。それでも問題が解決しない場合は、「VMware のトラブルシューティング」を参照して対処方法を確認してください。

CBT が正しく機能するためには、以下を満たしている必要があります。

- ホストは ESXi 4.0 以降である必要があります
- ディスクを所有する VM には、ハードウェアバージョン 7 以降が必要です
- CBT は仮想マシンで有効になっている必要があります (デフォルトでは有効になっています)

仮想ディスクで CBT が有効になっているかどうかを確認するには:

1. vSphere クライアントを開き、パワーオフ状態の仮想マシンを選択します。
2. 仮想マシンを右クリックして、[設定の編集] > [オプション] > [詳細/一般] > [設定パラメータ] に移動します。
3. オプション `ctkEnabled` は、`True` と等しくなければなりません。

バックアッププランにリソースを割り当てることにより、仮想マシンのバックアップを自動化させる

バックアップ計画は、ユーザー定義のデータ保護ポリシーで、 AWS サービスとサードパーティーアプリケーションで多数のデータ保護を自動化します。まず、バックアップの頻度、保持期間、ライフサイクルポリシー、その他多くのオプションを指定して、バックアッププランを作成します。バックアッププランを作成するには、「Getting started チュートリアル」を参照してください。

バックアッププランを作成したら、仮想マシンを含む AWS Backupがサポートするリソースをそのバックアッププランに割り当てます。 AWS Backup は、単一の特定のリソースの割り当てや除外、特定のタグによるリソースの追加など、アカウント内のすべてのリソースを割り当てるさまざまな方法を提供します。

仮想マシン AWS Backup のサポートでは、既存のリソース割り当て機能に加えて、仮想マシンをバックアッププランにすばやく割り当てるのに役立ついくつかの新機能が導入されています。[仮想マシン] ページでは、複数の仮想マシンにタグを割り当てたり、新しい [計画にリソースを割り当てる] 機能を使用します。これらの機能を使用して、 AWS Backup ゲートウェイによって既に検出された仮想マシンを割り当てます。

将来追加の仮想マシンを検出して割り当てる予定で、リソース割り当て手順を自動化して将来の仮想マシンを含める場合は、新しい [グループ割り当ての作成] 機能を使用します。

VMware タグ

タグは、リソースの管理、フィルタリング、検索に使用できるキーと値のペアです。

VMware タグは、カテゴリとタグ名で構成されています。VMware タグは仮想マシンをグループ化するために使用されます。タグ名は仮想マシンに割り当てられるラベルです。カテゴリはタグ名のコレクションです。

AWS タグでは、UTF-8 文字、数字、スペース、特殊文字 + - = . _ : / の中から文字を使用できます。

仮想マシンでタグを使用する場合、整理しやすいように、一致するタグを最大 10 個まで AWS Backup に追加できます。最大 10 個の VMware タグを AWS タグにマッピングできます。AWS Backup コンソール では、これらは「マイ組織 > 仮想マシン > AWS タグ」または「VMware タグ」にあります。 VMware

VMware のタグマッピング

仮想マシンでタグを使用する場合、より明確で整理しやすいように、一致するタグを最大 10 個まで AWS Backup に追加できます。マッピングはハイパーバイザー上のどの仮想マシンにも適用されます。

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. コンソールで、[ハイパーバイザーを編集] に移動します ([外部リソース]、[ハイパーバイザー] の順にクリックし、[ハイパーバイザー名] をクリックして [マッピングを管理] をクリックします)。
3. 最後のペイン VMware タグマッピング には、4 つのテキストボックスフィールドがあり、そこには、既存の VMware タグ情報を対応する AWS タグに入力できます。4 つのフィールドは、Vmware タグカテゴリ 、VMware タグ名 、AWS タグキー 、AWS タグ値 (例: Category = OS、タグ名 = Windows、 AWS タグキー = OS-Windows、 AWS タグ値 = Windows) です。
4. 希望の値を入力したら、[マッピングを追加] をクリックします。間違えた場合は、[削除] をクリックして入力した情報を削除できます。
5. マッピングを追加したら、これらの AWS タグを VMware 仮想マシンに適用するために使用する IAM ロールを指定します。

   「ポリシー AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync」には必要なアクセス許可が含まれています。使用しているロールにこのポリシーをアタッチできます (または管理者にこのポリシーをアタッチしてもらうことができます)。または、使用しているロール用のカスタムポリシーを作成することもできます。
6. 最後に、[ハイパーバイザーを追加] または [保存] をクリックします。

IAM ロールの信頼関係を変更して backup-gateway.amazonaws.com サービスと backup.amazonaws.com サービスを追加する必要があります。このサービスがないと、タグをマッピングするときにエラーが発生する可能性があります。既存のロールの信頼関係を編集するには、

1. IAM コンソールにログインします。
2. コンソールのナビゲーションペインで、[ロール] を選択します。

3. 変更するロールの名前を選択した後、詳細ページの [信頼関係] タブを選択します。
4. [ポリシードキュメント] に、次の内容を貼り付けます。

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

5. 信頼ポリシーの更新 を選択します。

詳細については、「AWS Directory Service 管理ガイド」の「既存のロールの信頼関係の編集」を参照してください。

VMware タグマッピングの表示

AWS Backup コンソールで、[外部リソース] をクリックし、次に [ハイパーバイザー] をクリックし、さらに [ハイパーバイザー名] リンクをクリックすると、選択したハイパーバイザーのプロパティが表示されます。[概要] ペインには 4 つのタブがあり、最後のタブは [VMware タグマッピング] です。マッピングがまだない場合は、「VMware タグマッピングなし」 と表示されます。

ここから、ハイパーバイザーによって検出された仮想マシンのメタデータを同期したり、ハイパーバイザーにマッピングをコピーしたり、VMware AWS タグにマッピングされたタグをバックアッププランのバックアップ選択に追加したり、マッピングを管理したりできます。

コンソールで、選択した仮想マシンにどのタグが適用されているかを確認するには、[仮想マシン]、[仮想マシン名]、[AWS タグ] または [VMware タグ] の順にクリックします。この仮想マシンに関連付けられたタグを表示したり、さらにタグを管理したりできます。

VMware タグマッピングを使用して、仮想マシンをプランに割り当てる

マッピングされたタグを使用して仮想マシンをバックアッププランに割り当てるには、次の操作を行います。

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. コンソールで、ハイパーバイザーの [詳細] ページの [VMware タグマッピング] に移動します ([外部リソース]]、[ハイパーバイザー]、[ハイパーバイザー名] を順にクリックします)。
3. マッピングされた複数のタグの横にあるチェックボックスをオンにして、それらのタグを、同じバックアッププランに割り当てます。
4. [リソースの割り当てに追加] をクリックします。
5. ドロップダウンリストから既存の [バックアッププラン] を選択します。または、[バックアッププランを作成] を選択して、新しいバックアッププランを作成します。
6. [確認] をクリックします。これにより、[リソースを割り当てる] ページが開き、値が事前入力された [タグを使用して選択を絞り込む] フィールドが表示されます。

を使用した VMware タグ AWS CLI

AWS Backup は API コールPutHypervisorPropertyMappingsを使用して、オンプレミスのハイパーバイザーエンティティプロパティを のプロパティにマッピングします AWS。

で AWS CLI、 オペレーション を使用しますput-hypervisor-property-mappings。

```
aws backup-gateway put-hypervisor-property-mappings \
--hypervisor-arn arn:aws:backup-gateway:region:account:hypervisor/hypervisorId \
--vmware-to-aws-tag-mappings list of VMware to AWS tag mappings \
--iam-role-arn arn:aws:iam::account:role/roleName \
--region AWSRegion
--endpoint-url URL
```

以下がその例です。

```
aws backup-gateway put-hypervisor-property-mappings \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--vmware-to-aws-tag-mappings VmwareCategory=OS,VmwareTagName=Windows,AwsTagKey=OS-
Windows,AwsTagValue=Windows \
--iam-role-arn arn:aws:iam::123456789012:role/SyncRole \
--region us-east-1
```

GetHypervisorPropertyMappings を使用して、プロパティマッピング情報を用いたサポートもできます。で AWS CLI、 オペレーション を使用しますget-hypervisor-property-mappings。サンプルのテンプレートを次に示します。

```
aws backup-gateway get-hypervisor-property-mappings --hypervisor-arn HypervisorARN
--region AWSRegion
```

以下がその例です。

```
aws backup-gateway get-hypervisor-property-mappings \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--region us-east-1
```

API、CLI、または SDK AWS を使用して、 でハイパーバイザーによって検出された仮想マシンのメタデータを同期する

仮想マシンのメタデータを同期できます。これを行うと、マッピングの一部である仮想マシンに存在する VMware タグが同期されます。また、仮想マシン上に存在する VMware タグにマップされた AWS タグが、 AWS 仮想マシンリソースに適用されます。

AWS Backup は API コールStartVirtualMachinesMetadataSyncを使用して、ハイパーバイザーによって検出された仮想マシンのメタデータを同期します。 AWS CLIを使用してハイパーバイザーが検出した仮想マシンのメタデータを同期するには、オペレーション start-virtual-machines-metadata-sync を使用します。

テンプレートの例:

```
aws backup-gateway start-virtual-machines-metadata-sync \
--hypervisor-arn Hypervisor ARN
--region AWSRegion
```

例：

```
aws backup-gateway start-virtual-machines-metadata-sync \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--region us-east-1
```

また、GetHypervisor を使用して、ホスト、ステータス、最新のメタデータ同期のステータスなどのハイパーバイザー情報をサポートすることも、前回成功したメタデータ同期時刻を取得することもできます。で AWS CLI、 オペレーション を使用しますget-hypervisor。

テンプレートの例:

```
aws backup-gateway get-hypervisor \
--hypervisor-arn Hypervisor ARN
--region AWSRegion
```

例：

```
aws backup-gateway get-hypervisor \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--region us-east-1
```

詳細については、「 API ドキュメントVmwareTag」および VmwareToAwsTagMapping「」を参照してください。

この機能は、2022 年 12 月 15 日以降にデプロイされた新しいゲートウェイで利用できるようになります。既存のゲートウェイでは、この新機能は 2023 年 1 月 30 日までにソフトウェアの自動更新により利用できるようになります。ゲートウェイを手動で最新バージョンに更新するには、 AWS CLI コマンドを使用します UpdateGatewaySoftwareNow。

例：

```
aws backup-gateway update-gateway-software-now \
--gateway-arn arn:aws:backup-gateway:us-east-1:123456789012:gateway/bgw-12345 \
--region us-east-1
```

タグを使用した仮想マシンの割り当て

既存のバックアッププランの 1 つに既に割り当てたタグを割り当てることで AWS Backup、 によって現在検出されている仮想マシンを他の AWS Backup リソースとともに割り当てることができます。または、新しいバックアッププランと新しいタグベースのリソースの割り当てを作成できます。バックアッププランは、バックアップジョブを実行するたびに、新しく割り当てられたリソースをチェックします。

同じタグで複数の仮想マシンにタグを付けるには、次の手順を実行します。

1. 左のナビゲーションペインで、[仮想マシン] を選択します。
2. [VM 名] の横にあるチェックボックスをオンにして、すべての仮想マシンを選択します。または、タグ付けする仮想マシン名の横にあるチェックボックスをオンにします。

3. [Add tags (タグの追加)] を選択します。
4. [キー] タグを入力します。
5. 推奨: [値] タグを入力してください。
6. [確認] を選択します。

プランへのリソースの割り当て機能を使用した仮想マシンの割り当て

で現在検出されている仮想マシン AWS Backup を既存または新規のバックアッププランに割り当てるには、リソースをプランに割り当てる機能を使用します。

プランへのリソースの割り当て機能を使用して仮想マシンを割り当てるには、次の手順を実行します。

1. 左のナビゲーションペインで、[仮想マシン] を選択します。
2. [VM 名] の横にあるチェックボックスをオンにして、すべての仮想マシンを選択します。または、複数の仮想マシン名の横にあるチェックボックスをオンにして、それらを同じバックアッププランに割り当てます。
3. [割り当て]、[計画にリソースを割り当てる] の順に選択します。
4. 「リソース割り当て名」を入力します。
5. リソース割り当て [IAM ロール] をクリックして、バックアップを作成し、リカバリーポイントを管理します。使用する特定の IAM ロールがない場合は、正しいアクセス権限を持つデフォルトロールを推奨します。
6. [バックアップ計画] セクションで、ドロップダウンリストから既存のバックアップ計画を選択します。または、[バックアッププランの作成] の順にクリックして、新しいバックアッププランを作成します。
7. リソースの割り当てを選択します。
8. オプション: Backup プランの表示を選択して、仮想マシンがバックアッププランに割り当てられていることを確認します。次に、[リソースの割り当て] セクションで、リソースの割り当ての [名前] を選択します。

グループ割り当ての作成機能を使用した仮想マシンの割り当て

仮想マシンの前述の 2 つのリソース割り当て機能とは異なり、グループ割り当ての作成機能は、 によって現在検出された仮想マシンだけでなく AWS Backup、定義したフォルダまたはハイパーバイザーで将来検出された仮想マシンも割り当てます。

また、グループ割り当ての作成機能を使用するためにチェックボックスを選択する必要はありません。

プランへのリソースの割り当て機能を使用して仮想マシンを割り当てるには、次の手順を実行します。

1. 左のナビゲーションペインで、[仮想マシン] を選択します。
2. [割り当て]、[グループ割り当ての作成] の順に選択します。
3. 「リソース割り当て名」を入力します。
4. リソース割り当て [IAM ロール] をクリックして、バックアップを作成し、リカバリーポイントを管理します。使用する特定の IAM ロールがない場合は、正しいアクセス権限を持つデフォルトロールを推奨します。
5. [リソースグループ] セクションで、[Group type] ドロップダウンメニューを選択します。選択肢は、[フォルダ] または [ハイパーバイザー] です。

   a. [フォルダ] をクリックして、ハイパーバイザー上のフォルダ内のすべての仮想マシンを割り当てます。[datacenter/vm] などの [グループ名] フォルダをクリックし、ドロップダウンメニューを使用します。[サブフォルダ] を含めることもできます。

      > **Note**
      >
      > フォルダベースの割り当てを行うには、検出プロセス中に、 は仮想マシンに検出プロセス中に見つかったフォルダを AWS Backup タグ付けします。後で仮想マシンを別のフォルダに移動した場合、 AWS Backup タグ付けのベストプラクティスにより、 は AWS タグを更新できません。この割り当て方法では、割り当てられたフォルダから移動した仮想マシンのバックアップが引き続き作成される可能性があります。

   b. [ハイパーバイザー] をクリックして、ハイパーバイザーによって管理されているすべての仮想マシンを割り当てます。ドロップダウンメニューを使用して、ハイパーバイザー ID [グループ名] を選択します。
6. [バックアップ計画] セクションで、ドロップダウンリストから既存のバックアップ計画を選択します。または、[バックアッププランの作成] の順にクリックして、新しいバックアッププランを作成します。
7. グループ割り当ての作成を選択します。

8. オプション: [Backup プランの表示] を選択して、仮想マシンがバックアッププランに割り当てられていることを確認します。[リソースの割り当て] セクションで、リソースの割り当ての [名前] を選択します。

次のステップ

仮想マシンを復元するには、「を使用した仮想マシンの復元 AWS Backup」を参照してください。

Backup ゲートウェイのサードパーティソースコンポーネントに関する情報

このセクションでは、バックアップゲートウェイ 機能を提供するために依存しているサードパーティー製のツールとライセンスについて情報を見つけることができます。

バックアップゲートウェイソフトウェアに含まれている、特定のサードパーティー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.tgz をダウンロードします。

この製品には、OpenSSL Toolkit (https://www.openssl.org/) で使用する OpenSSL プロジェクトによって開発されたソフトウェアが含まれています。

この製品には、VMware® vSphere ソフトウェア開発キット (https://www.vmware.com)。

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 アプライアンスのオープンソースコンポーネント

バックアップゲートウェイの機能を提供するために、いくつかのサードパーティ製ツールとライセンスが使用されます。

アプライアンスソフトウェアに含まれている特定のオープンソースソフトウェアコンポーネントのソースコードをダウンロードするには、次のリンクを使用します AWS 。

- 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。

この製品には、OpenSSL Toolkit (https://www.openssl.org/) で使用する OpenSSL プロジェクトによって開発されたソフトウェアが含まれています。依存するすべてのサードパーティー製ツールの関連ライセンスについては、サードパーティーのライセンスを参照してください。

VM 問題のトラブルシューティング

増分バックアップ/CBT の問題とメッセージ

障害メッセージ: **"The VMware Change Block Tracking (CBT) data was invalid during this backup, but the incremental backup was successfully completed with our proprietary change detection mechanism."**

このメッセージが続く場合は、VMware の指示に従って CBT をリセットします。

次のメッセージで、CBT がオンになっていなかったか、使用できなかったことが通知されます:「この仮想マシンでは VMware 変更ブロック追跡 (CBT) を使用できませんでしたが、増分バックアップは当社独自の変更メカニズムで正常に完了しました。」

CBT がオンになっていることを確認します。仮想ディスクで CBT が有効になっているかどうかを確認するには:

1. vSphere クライアントを開き、パワーオフ状態の仮想マシンを選択します。
2. 仮想マシンを右クリックして、[設定の編集] > [オプション] > [詳細/一般] > [設定パラメータ] に移動します。
3. オプション `ctkEnabled` は、`True` と等しくなければなりません。

オンになっている場合は、 up-to-date VMware の機能を使用していることを確認してください。ホストは ESXi 4.0 以降で、追跡対象のディスクを所有する仮想マシンはハードウェアバージョン 7 以降である必要があります。

CBT がオン (有効) になっていて、ソフトウェアとハードウェアが最新の場合は、仮想マシンをオフにしてから再びオンにします。CBT がオンになっていることを確認します。次に、バックアップをもう一度実行します。

アドバンスト DynamoDB バックアップ

AWS Backup は、Amazon DynamoDB データ保護のニーズに応じて、追加の高度な機能をサポートしています。で AWS Backupの高度な機能を有効にすると AWS リージョン、作成した DynamoDB テーブルバックアップのすべての新しい で次の機能がロック解除されます。

- コスト削減と最適化:
  - 「コールドストレージへのバックアップの階層化」でストレージコストを削減する
  - コストエクスプローラーで使用するためのコスト配分タグ付け

- ビジネス継続性
  - リージョン間の COPY
  - アカウント間のコピー
- のセキュリティ
  - 暗号化したAWS Backup ボールトでバックアップを保存し、AWS Backup ボールトロック、AWS Backup ポリシー、および暗号化キーを確保できます。
  - バックアップはソース DynamoDB テーブルからタグを継承し、これらのタグを使用してパーミッション、サービスコントロールポリシー (SCP) を設定します。

2021 年 11 月 AWS Backup 以降に にオンボーディングする新規お客様は、高度な DynamoDB バックアップ機能がデフォルトで有効になっています。具体的には、2021 年 11 月 21 日より前にバックアップボールトを作成していないお客様には、高度な DynamoDB バックアップ機能がデフォルトで有効になっています。

既存のすべての AWS Backup お客様が DynamoDB の高度な機能を有効にすることをお勧めします。高度な機能を有効にした後、ウォームバックアップストレージの価格に違いはありません。バックアップをコールドストレージに階層化することでコストを節約し、コスト配分タグを使用してコストを最適化できます。また、 のビジネス AWS Backup継続性とセキュリティ機能の利用を開始することもできます。

> **Note**
>
> の AWS Backupデフォルトのサービスロールの代わりにカスタムロールまたはポリシーを使用する場合は、次のアクセス許可ポリシーを追加または使用 (または同等のアクセス許可を追加) する必要があります。
>
> - `AWSBackupServiceRolePolicyForBackup` は、高度な DynamoDB バックアップを実行します。
> - `AWSBackupServiceRolePolicyForRestores` は、高度な DynamoDB バックアップを復元します。
>
> AWS管理ポリシーの詳細とカスタマー管理ポリシーの例については、「」を参照してくださいの管理ポリシー AWS Backup。

トピック

- コンソールを使用した高度な DynamoDB バックアップの有効化
- 高度な DynamoDB バックアップをプログラムで有効にする
- 高度な DynamoDB バックアップを編集する
- 高度な DynamoDB バックアップを復元する
- 高度な DynamoDB バックアップを削除する
- 高度な DynamoDB バックアップを有効にした場合の、完全な AWS Backup 管理のその他の利点

コンソールを使用した高度な DynamoDB バックアップの有効化

AWS Backup または DynamoDB コンソールを使用して、DynamoDB バックアップの AWS Backup 高度な機能を有効にできます。

AWS Backup コンソールから高度な DynamoDB バックアップ機能を有効にするには：

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. 左側のナビゲーションメニューから、[設定] を選択します。
3. サポートされるサービスセクションで、DynamoDB が [Enabled (有効)] であることを確認します。

   そうでない場合は、[オプトイン] を選択し、 AWS Backup サポートサービスとして DynamoDB を有効にします。
4. [DynamoDB バックアップの高度な機能] セクションで、[有効化] を選択します。
5. [Enable features] (機能の有効化) を選択します。

DynamoDB コンソールを使用して AWS Backup 高度な機能を有効にする方法については、「Amazon DynamoDB ユーザーガイド」の AWS Backup「機能の有効化」を参照してください。 DynamoDB

高度な DynamoDB バックアップをプログラムで有効にする

(CLI) を使用して AWS Command Line Interface 、DynamoDB バックアップの AWS Backup 高度な機能を有効にすることもできます。DynamoDB の高度なバックアップは、次の値を両方とも `true` に設定した場合に有効にします。

DynamoDB バックアップの AWS Backup 高度な機能をプログラムで有効にするには：

1. 次のコマンドを使用して、DynamoDB の AWS Backup 高度な機能を既に有効にしているかどうかを確認します。

```
$ aws backup describe-region-settings
```

もし "DynamoDB":true が "ResourceTypeManagementPreference" および "ResourceTypeOptInPreference" 両方の下にある場合、DynamoDB の高度なバックアップはすでに有効化しています。

次の出力のように、"DynamoDB":false のインスタンスが少なくとも 1 つある場合は、まだ高度な DynamoDB バックアップを有効にしていないので、次のステップに進みます。

```
{
  "ResourceTypeManagementPreference":{
    "DynamoDB":false,
    "EFS":true
  }
  "ResourceTypeOptInPreference":{
    "Aurora":true,
    "DocumentDB":false,
    "DynamoDB":false,
    "EBS":true,
    "EC2":true,
    "EFS":true,
    "FSx":true,
    "Neptune":false,
    "RDS":true,
    "Storage Gateway":true
  }
}
```

2. 以下の UpdateRegionSettings オペレーションを使用して、"ResourceTypeManagementPreference" および "ResourceTypeOptInPreference" の両方を "DynamoDB":true に設定します。

```
aws backup update-region-settings \
              --resource-type-opt-in-preference DynamoDB=true \
              --resource-type-management-preference DynamoDB=true
```

高度な DynamoDB バックアップを編集する

AWS Backup 高度な機能を有効にした後に DynamoDB バックアップを作成する場合、 AWS Backup を使用して次のことができます。

- リージョン間のバックアップのコピー
- アカウント間でバックアップをコピーする
- がバックアップをコールドストレージに AWS Backup 階層化するタイミングを変更する
- バックアップにタグを付ける

既存のバックアップでこれらの高度な機能を使用するには、「バックアップの編集」を参照してください。

後で DynamoDB の AWS Backup 高度な機能を無効にした場合、高度な機能を有効にした期間中に作成した DynamoDB バックアップに対してこれらのオペレーションを引き続き実行できます。

高度な DynamoDB バックアップを復元する

AWS Backup 高度な機能を有効にする前に取得した DynamoDB バックアップを復元するのと同じ方法で、 AWS Backup 高度な機能を有効にして取得した DynamoDB バックアップを復元できます。復元は、 AWS Backup または DynamoDB を使用して実行できます。

次のオプションを使用して、新しく復元されたテーブルの暗号化方法を指定できます。

- 元のテーブルと同じリージョンで復元する場合、必要に応じて復元されたテーブルの暗号化キーを指定できます。暗号化キーを指定しない場合、 AWS Backup は元のテーブルを暗号化したのと同じキーを使用して、復元されたテーブルを自動的に暗号化します。
- 元のテーブルとは異なるリージョンで復元する場合は、暗号化キーを指定する必要があります。

を使用して復元するには AWS Backup、「」を参照してくださいAmazon DynamoDB テーブルの復元。

DynamoDB を使用して復元するには、Amazon DynamoDB ユーザーガイドの「バックアップからの DynamoDB テーブルの復元」を参照してください。

高度な DynamoDB バックアップを削除する

DynamoDB のこれらの高度な機能を使用して作成されたバックアップを削除することはできません。バックアップを削除して AWS 環境全体にわたってグローバルな整合性を維持するには、 AWS Backup を使用する必要があります。

DynamoDB バックアップを削除するには、バックアップの削除 を参照してください。

高度な DynamoDB バックアップを有効にした場合の、完全な AWS Backup 管理のその他の利点

DynamoDB の AWS Backup 高度な機能を有効にすると、DynamoDB バックアップの完全な管理がに提供されます AWS Backup。そうすることで、次のような追加のメリットが得られます。

暗号化

AWS Backup は、送信先 AWS Backup ボールトの KMS キーを使用してバックアップを自動的に暗号化します。以前は、ソース DynamoDB テーブルと同じ暗号化方法を使用して暗号化されていました。これにより、データの保護に使用できる防御の数が増えます。詳細については、「でのバックアップの暗号化 AWS Backup」を参照してください。

Amazon リソースネーム (ARN)

各バックアップ ARN のサービス名前空間は awsbackup です。以前は、サービスの名前空間は dynamodb でした。別の言い方をすれば、各 ARN の始まりが `arn:aws:dynamodb` から `arn:aws:backup` に変わります。「サービス認可リファレンス」で AWS Backupの ARN について参照してください。

この変更により、ユーザーまたはバックアップ管理者は、高度な機能を有効にした後に作成された DynamoDB バックアップに適用される awsbackup サービス名前空間を使用してバックアップのためにアクセスポリシーを作成できます。awsbackup サービス名前空間を使用して、 AWS Backupによって作成される他のバックアップにポリシーを適用することもできます。詳細については、「アクセスコントロール」を参照してください。

請求明細書の請求場所

バックアップ (ストレージ、データ転送、復元、早期削除を含む) の料金は、 AWS 請求書の「バックアップ」の下に表示されます。以前は、請求額の「DynamoDB」の下に料金が表示されていました。

この変更により、 AWS Backup 請求を使用してバックアップコストを一元的にモニタリングできます。詳細については、「メータリング、コスト、および請求」を参照してください。

Amazon Timestream バックアップ

Amazon Timestream はスケーラブルな時系列データベースで、1 日に最大何兆もの時系列データポイントの保存と分析が可能です。Timestream は、最新のデータをメモリに保持し、履歴データをポリシーに従ってコストが最適化されたストレージ階層に保存することで、コストと時間の節約のために最適化されています。

Timestream データベースにはテーブルがあります。これらのテーブルにはレコードが含まれており、各レコードは時系列内の 1 つのデータポイントです。時系列は、株価、Amazon EC2 インスタンスのメモリ使用量レベル、温度読み取り値など、一定の間隔で記録された一連のレコードです。Timestream テーブルを一元的にバックアップおよび復元 AWS Backup できます。これらのテーブルのバックアップは、同じ組織 AWS リージョン 内の他のアカウントや複数のアカウントにコピーできます。

Timestream は現在、ネイティブバックアップおよび復元サービスを提供していないため、 AWS Backup を使用して Timestream テーブルの安全なコピーを作成すると、リソースにセキュリティと耐障害性をさらに強化できます。

Timestream テーブルのバックアップ

Timestream テーブルは、 AWS Backup コンソールまたは を使用してバックアップできます AWS CLI。

AWS Backup コンソールを使用して Timestream テーブルをバックアップするには、オンデマンドまたはバックアッププランの一部としての 2 つの方法があります。

オンデマンド Timestream バックアップの作成

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインを使用して、[保護されたリソース]、[オンデマンドバックアップの作成] の順に選択します。
3. [オンデマンドバックアップを作成] ページで、[Amazon Timestream] を選択します。
4. [リソースタイプ] に Timestream を選択し、バックアップするテーブル名を選択します。
5. バックアップウィンドウで、[今すぐバックアップを作成] が選択されていることを確認します。これにより、すぐにバックアップが開始され、[保護されたリソース] ページにクラスターが表示される時間を短縮できます。

6. [コールドストレージへの移行] のドロップダウンメニューで、移行設定を設定できます。
7. [保持期間] では、バックアップを保持する期間を選択できます。
8. 既存のバックアップボールトを選択するか、新しいバックアップボールトを作成します。[Create new backup vault (新しいバックアップボールトを作成)] を選択すると、ボールトを作成する新しいページが開きます。完了すると、[Create on-demand backup (オンデマンドバックアップを作成)] ページに戻ります。
9. IAM ロール で、デフォルトロール を選択します (アカウントに AWS Backup デフォルトロールが存在しない場合、正しいアクセス許可で作成されます) 。
10. オプションとして、復旧ポイントにタグを追加できます。オンデマンドバックアップに 1 つ以上のタグを割り当てる場合は、[キー] とオプションの [値]] を入力して、[タグを追加] を選択します。
11. [オンデマンドバックアップを作成] を選択します。[ジョブ] ページに移動し、ジョブのリストが表示されます。
12. クラスターの [バックアップジョブ ID] を選択すると、そのジョブの詳細が表示されます。`Completed`、`In Progress`、または `Failed` のステータスが表示されます。表示されるステータスを更新するには、[更新] ボタンをクリックします。

バックアッププランで、スケジュールされた Timestream バックアップを作成する

保護されたリソースであれば、スケジュールされたバックアップに Timestream テーブルを含めることができます。Amazon Timestream テーブルの保護をオプトインするには:

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[保護されたリソース] を選択します。
3. Amazon Timestream を [オン] に切り替えます。
4. 既存のプランまたは新しいプランに Timestream テーブルを含めるには、「コンソールへのリソースの割り当て」を参照してください。

[バックアッププランを管理] で、バックアッププランを作成して Timestream テーブルを含めるか、既存のプランを更新して Timestream テーブルを含めるかを選択できます。リソースタイプとして Timestream を追加する場合、[すべての Timestream テーブル] を追加するか、[特定のリソースタイプを選択] で、追加するテーブルの横にあるチェックボックスをオンにできます。

Timestream テーブルから最初に作成されるバックアップは、フルバックアップになります。それ以降のバックアップは増分バックアップになります。

バックアッププランを作成または変更したら、左側のナビゲーションにある [バックアッププラン] に移動します。指定したバックアッププランでは、[リソース割り当て] にクラスターが表示されるはずです。

プログラムによるバックアップ

オペレーション `start-backup-job` を使用することができます。以下のパラメータを含めます。

```
aws backup start-backup-job \
--backup-vault-name backup-vault-name \
--resource-arn arn:aws:timestream:region:account:database/database-name/table/table-
name \
--iam-role-arn arn:aws:iam::account:role/role-name \
--region AWS ##### \
--endpoint-url URL
```

Timestream テーブルのバックアップを表示する

Timestream テーブルのバックアップをコンソール内で表示および変更するには:

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. [バックアップボールト] を選択します。次に、Timestream テーブルを含むバックアップボールト名をクリックします。
3. バックアップボールトには、概要とバックアップのリストが表示されます。
   a. [復旧ポイント ID] 列のリンクをクリックするか、
   b. 復旧ポイント ID の左側にあるチェックボックスをオンにして [アクション] をクリックすると、不要になった復旧ポイントを削除できます。

Timestream テーブルを復元する

Timestream テーブルを復元する方法を確認する

Amazon EC2 インスタンス上の SAP HANA データベースのバックアップ

> **Note**
>
> がサポートするサービス AWS リージョン には、Amazon EC2 インスタンスで SAP HANA データベースのバックアップを利用できる現在サポートされている リージョンが含まれています。

AWS Backup は、Amazon EC2 インスタンス上の SAP HANA データベースのバックアップと復元をサポートします。

トピック

- を使用した SAP HANA データベースの概要 AWS Backup
- を使用して SAP HANA データベースをバックアップするための前提条件 AWS Backup
- コンソールでの SAP HANA AWS Backup バックアップオペレーション
- SAP HANA データベースのバックアップを表示する
- AWS CLI で for SAP HANA データベースを使用する AWS Backup
- SAP HANA データベースのバックアップのトラブルシューティング
- を使用する際の SAP HANA 用語の用語集 AWS Backup
- AWS Backup EC2 インスタンスでの SAP HANA データベースのリリースノートのサポート

を使用した SAP HANA データベースの概要 AWS Backup

バックアップ作成機能とデータベース復元機能に加えて、SAP 用 Amazon EC2 Systems Manager との AWS Backup の統合により、お客様は SAP HANA データベースを識別してタグ付けすることができます。

AWS Backup は Backint Agent AWS と統合され、SAP HANA のバックアップと復元を実行します。詳細については、「AWS Backint」を参照してください。

を使用して SAP HANA データベースをバックアップするための前提条件 AWS Backup

バックアップと復元を実行する前に、いくつかの前提条件を満たす必要があります。これらのステップを実行するには、SAP HANA データベースへの管理アクセスと、 AWS アカウントで新しい IAM ロールとポリシーを作成するためのアクセス許可が必要です。

Amazon EC2 Systems Manager で以下の前提条件を満たします。

1. SAP HANA データベースを実行している Amazon EC2 インスタンスに必要なアクセス許可を設定する
2. での認証情報の登録 AWS Secrets Manager
3. AWS Backint と AWS Systems Manager for SAP Agents をインストールする
4. SSM エージェントを検証する
5. パラメータを確認する
6. SAP HANA データベースを登録する

各 HANA インスタンスは 1 回だけ登録するのがベストプラクティスです。複数の登録を行うと、同じデータベースに対して複数の ARNs が発生する可能性があります。単一の ARN と登録を維持すると、バックアッププランの作成とメンテナンスが簡単になり、バックアップの計画外の重複を減らすこともできます。

コンソールでの SAP HANA AWS Backup バックアップオペレーション

SAP セットアップの前提条件と SSM が完了すると、EC2 ででの SAP HANA データベースのバックアップと復元が可能になります。

SAP HANA リソース保護のオプトイン

AWS Backup を使用して SAP HANA データベースを保護するには、保護されたリソースの 1 つとして SAP HANA をオンにする必要があります。オプトインするには、以下の操作を行います。

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. 左側のナビゲーションペインで [設定] を選択します。
3. [サービスのオプトイン] で、[リソースを設定] を選択します。
4. [SAP HANA on Amazon EC2] にオプトインします。
5. [確認] をクリックします。

これで、Amazon EC2 での SAP HANA のサービスオプトインが有効になります。

SAP HANA データベースのスケジュールされたバックアップを作成する

既存のバックアッププランを編集して、SAP HANA リソースを追加することも、SAP HANA リソース専用の新しいバックアッププランを作成することもできます。

新しいバックアッププランの作成を選択する場合は、次の 3 つのオプションがあります。

1. オプション 1: テンプレートから始める
    1. バックアッププランテンプレートを選択します。
    2. バックアッププラン名を指定します。
    3. [プランを作成] をクリックします。
2. オプション 2: 新しいプランを作成する
    1. バックアッププラン名を指定します。
    2. オプションとして、バックアッププランに追加するタグを指定します。
    3. バックアップルール設定を指定します。
        a. バックアップルール名を指定します。
        b. 既存のボールトを選択するか、新しいバックアップボールトを作成します。これが、バックアップが保存される場所です。
        c. バックアップ頻度を指定します。
        d. バックアップウィンドウを指定します。

            注: コールドストレージへの移行は現在サポートされていません。
        e. 保持期間を指定します。

            コピー先へのコピーは現在サポートされていません。
        f. (オプション) 復旧ポイントに追加するタグを指定します。
    4. [プランを作成] をクリックします。
3. オプション 3: JSON を使用したプランの定義
    1. 既存のバックアッププランの JSON 式を変更するか、新しい式を作成して、バックアッププランの JSON を指定します。
    2. バックアッププラン名を指定します。
    3. [JSON を検証] をクリックします。

バックアッププランが正常に作成されたら、次のステップでバックアッププランにリソースを割り当てることができます。

どのプランを使用する場合でも、必ずリソースを割り当てます。システムデータベースとテナントデータベースを含め、どの SAP HANA データベースを割り当てるかを選択できます。また、特定のリソース ID を除外することもできます。

SAP HANA データベースのオンデマンドバックアップを作成する

作成後すぐに実行されるフルオンデマンドバックアップを作成できます。Amazon EC2 インスタンス上の SAP HANA データベースのオンデマンドバックアップはフルバックアップであり、増分バックアップはサポートされていないことに注意してください。

これで、オンデマンドバックアップが作成されました。指定したリソースのバックアップが開始されます。コンソールは、ジョブの進行状況を確認できる [バックアップジョブ] ページに移動します。画面上部の青いバナーにあるバックアップジョブ ID をメモしておきます。バックアップジョブのステータスを簡単に確認するために必要となるためです。バックアップが完了すると、ステータスは `Completed` に進みます。バックアップには最大で数時間かかることもあります。

[バックアップジョブリスト] を更新して、ステータスの変更を確認します。[バックアップジョブ ID] を検索してクリックすると、詳細なジョブステータスを表示することもできます。

SAP HANA データベースの継続的バックアップ

point-in-time 復元 (PITR) で使用できる継続的なバックアップ を作成できます (オンデマンドバックアップはリソースをその取得時の状態に保持しますが、PITR は一定期間の変更を記録する継続的なバックアップを使用することに注意してください)。

継続的バックアップにより、EC2 インスタンス上の SAP HANA データベースは、精度の 1 秒 (最大 35 日前) 以内に、選択した特定の時間に巻き戻すことで SAP HANA データベースをサポートします。継続的なバックアップは、最初にリソースのフルバックアップを作成し、次にリソースのトランザクションログを定期的にバックアップすることによって機能します。PITR 復元は、フルバックアップにアクセスし、トランザクションログを復元 AWS Backup するように指示した時点まで再生することで機能します。

AWS Backup コンソールまたは API AWS Backup を使用して でバックアッププランを作成するときに、継続的バックアップにオプトインできます。

コンソールを使用して継続的なバックアップを有効にするには

1. にサインインし AWS Management Console、https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[バックアッププラン] を選択して、[バックアッププランの作成] を選択します。

3. [バックアップルール]で、[バックアップルールの追加] を選択します。
4. [バックアップルールの設定] セクションで、[サポートされているリソースの継続的なバックアップを有効にする] を選択します。

SAP HANA データベースバックアップの PITR (point-in-time復元) を無効にすると、復旧ポイントの有効期限が切れるまで (ステータスは に等しくなります) 、ログは引き続き に送信されます AWS Backup EXPIRED)。SAP HANA 内の別のログバックアップ場所に変更して、 AWS Backupへのログの送信を停止できます。

ステータスが の継続的復旧ポイントは、継続的復旧ポイントが中断されたSTOPPEDことを示します。つまり、SAP HANA から に送信され、データベースへの増分変更 AWS Backup を示すログにギャップがあります。この期間のギャップ内に発生した復旧ポイントのステータスは STOPPED. です。

継続的バックアップ (復旧ポイント) の復元ジョブ中に発生する可能性のある問題については、本ガイドの「SAP HANA 復元のトラブルシューティング」セクションを参照してください。

SAP HANA データベースのバックアップを表示する

バックアップジョブのステータスを表示する:

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで ジョブを選択します。
3. バックアップジョブ、復元ジョブ、またはコピージョブを選択すると、ジョブのリストが表示されます。
4. ジョブ ID を検索してクリックすると、詳細なジョブステータスが表示されます。

ボールト内のすべての復旧ポイントを表示する:

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[バックアップボールト] を選択します。
3. バックアップボールトを検索してクリックすると、そのボールト内のすべての復旧ポイントが表示されます。

保護されたリソースの詳細を表示する:

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

2. ナビゲーションペインで、[保護されたリソース] を選択します。
3. リソースタイプでフィルタリングして、そのリソースタイプのすべてのバックアップを表示することもできます。

AWS CLI で for SAP HANA データベースを使用する AWS Backup

バックアップコンソール内の各アクションには、対応する API 呼び出しがあります。

プログラムで とそのリソースを設定 AWS Backup および管理StartBackupJobするには、 API コールを使用して EC2 インスタンス上の SAP HANA データベースをバックアップします。

CLI コマンドとして `start-backup-job` を使用します。

SAP HANA データベースのバックアップのトラブルシューティング

ワークフロー中にエラーが発生した場合は、次のエラー例と推奨される解決策を参照してください。

Python の前提条件

- エラー: SSM for SAP 以降、Python バージョンに関連する Zypper エラー。Python 3.6 AWS Backup が必要ですが、SUSE 12 SP5 はデフォルトで Python 3.4 をサポートしています。

  解決策： 次の手順を実行して、複数のバージョンの Python を SUSE12 SP5 にインストールします。

  1. update-alternatives コマンドを実行して、Python 3 のシンボリックリンクを '/usr/local/bin/' で作成します。これは、'/usr/bin/python3' を直接使用しません。このコマンドは、Python 3.4 をデフォルトバージョンとして設定します。コマンドは次のとおりです。 `# sudo update-alternatives –install /usr/local/bin/python3 python3 /usr/bin/python3.45`
  2. 次のコマンドを実行して、代替設定に Python 3.6 を追加します。 `# sudo update-alternatives –install /usr/local/bin/python3 python3 /usr/bin/python3.62`
  3. 次のコマンドを実行して、代替設定を Python 3.6 に変更します。 `# sudo update-alternatives –config python3`

     次の出力が表示されます。

```
There are 2 choices for the alternative python3 (providing /usr/local/bin/python3).
 Selection Path Priority Status
```

```
* 0 /usr/bin/python3.4 5 auto mode
 1 /usr/bin/python3.4 5 manual mode
 2 /usr/bin/python3.6 2 manual mode
Press enter to keep the current choice[*], or type selection number:
```

4. Python 3.6 に対応する番号を入力します。
5. Python のバージョンを確認し、Python 3.6 が使用されていることを確認します。
6. （ オプションですが、推奨) Zypper コマンドが期待どおりに動作することを確認します。

SAP の検出と登録のための Amazon EC2 Systems Manager

- エラー: および SSM のパブリックエンドポイントへのアクセスがブロックされたため、SSM for SAP はワークロードを検出できませんでした。 AWS Secrets Manager

  解決策： SAP HANA データベースからエンドポイントにアクセスできるかどうかをテストします。それらに到達できない場合は、 の Amazon VPC エンドポイントと SAP の AWS Secrets Manager SSM を作成できます。

  1. コマンド を実行して、HANA DB の Amazon EC2 ホストから Secrets Manager `aws secretsmanager get-secret-value –secret-id hanaeccsbx_hbx_database_awsbkp` へのアクセスをテストします。コマンドが値を返さない場合、ファイアウォールは Secrets Manager サービスエンドポイントへのアクセスをブロックしています。ログは「Secrets Manager からシークレットを取得する」のステップで停止します。
  2. コマンド を実行して、SSM for SAP `aws ssm-sap list-registration` エンドポイントへの接続をテストします。コマンドが値を返さない場合、ファイアウォールは SSM for SAP エンドポイントへのアクセスをブロックしています。

     エラーの例: `Connection was closed before we received a valid response from endpoint URL: “https://ssm-sap.us-west-2.amazonaws.com/register-application"`。

  エンドポイントに到達できない場合、続行するには 2 つのオプションがあります。

  - Secrets Manager および SSM for SAP のパブリックサービスエンドポイントへのアクセスを許可するには、ファイアウォールポートを開きます。
  - Secrets Manager と SSM for SAP 用の VPC エンドポイントを作成し、次の操作を行います。
    - Amazon VPC が DNSSupport および DNSHostname に対して有効になっていることを確認します。

  - VPC エンドポイントでプライベート DNS 名を許可が有効になっていることを確認します。
  - SSM for SAP の検出が正常に完了すると、ログにホストが検出されたことが示されます。
- サービスのパブリックエンドポイントへのアクセス AWS Backup がブロックされたため、エラー: AWS Backup および Backint 接続が失敗します。 は、 `time="2024-01-03T11:39:15-08:00" level=error msg="Storage configuration validation failed: missing backup data plane Id"` または のようなエラーを表示する`aws-backint-agent.log`ことがありますlevel=fatal msg="Error performing backup missing backup data plane Id。また、コンソールには AWS Backup `Fatal Error: An internal error occured.`

  解決策: エンドポイントに到達できない場合、次の 2 つのオプションを使用できます。

  - ファイアウォールポートを開いて、パブリックサービスエンドポイント (HTTPS) へのアクセスを許可します。このオプションを使用すると、DNS はパブリック IP アドレスを介して AWS サービスへのリクエストを解決します。
  - VPC エンドポイントを作成すると、 に必要な AWS サービスとの間でトラフィックがプライベートにルーティングされます AWS Backup。このオプションを使用すると、DNS はプライベート IP アドレスを介してそれらのサービスのリクエストを解決します。このオプションでは、リクエストをプライベートエンドポイントに転送するルールを追加するために、DNS サーバーの更新が必要になる場合があります。
- エラー: HANA パスワードに特殊文字が含まれているため、SSM for SAP 登録が失敗します。エラーの例には、HANA データベースの Amazon EC2 インスタンスからテストされた `systemdb`および `hdbsql`を使用して接続`tenantdb`をテストした後`Error connecting to database HBX/HBX when validating its credentials.`、またはテスト`Discovery failed because credentials for HBX/SYSTEMDB either not provided or cannot be validated.`した後が含まれます。

  ジョブページの AWS Backupコンソールでは、バックアップジョブの詳細にエラー `FAILED` を含む のステータスが表示されることがありますMiscellaneous: b’* 10: authentication failed SQLSTATE: 28000\n’。

  解決策: パスワードに $ などの特殊文字が含まれていないことを確認します。
- エラー: **`b’* 447: backup could not be completed: [110507] Backint exited with exit code 1 instead of 0. console output: time...`**

  解決策： AWS BackInt Agent for SAP HANA のインストールが正常に完了していない可能性があります。AWS Backint エージェントと Amazon EC2 Systems Manager エージェントを SAP アプリケーションサーバーにデプロイするプロセスを再試行します。 Amazon EC2 Systems Manager

- エラー: コンソールは登録後にログファイルと一致しません。

  検出ログには、特殊文字を含むパスワードが原因で HANA DB に接続しようとしたときに失敗した登録が表示されますが、SSM for SAP Application Manager for SAP コンソールには登録が成功したことは確認されません。コンソールに正常に登録されたがログに表示されない場合、バックアップは失敗します。

  登録ステータスを確認します。

  1. SSM コンソールにログインする
  2. 左側のナビゲーションから Run Command を選択します。
  3. テキストフィールドのコマンド履歴 で`Instance ID:Equal:`、登録に使用したインスタンスと等しい値で を入力します。これにより、コマンド履歴がフィルタリングされます。
  4. コマンド ID 列を使用して、ステータスが のコマンドを検索します`Failed`。次に、-AWSSystemsManagerSAPDiscovery のドキュメント名を見つけます。
  5. で AWS CLI、 コマンドを実行します`aws ssm-sap register-application status`。返された値が の場合`Error`、登録は失敗しました。

  解決策: HANA パスワードに特殊文字 (「$」など) が含まれていないことを確認します。

SAP HANA データベースのバックアップの作成

- エラー: AWS Backup コンソールは、SystemDB または TenantDB のオンデマンドバックアップが作成されると、「致命的エラー」というメッセージを表示します。これは、パブリックエンドポイント cell-1.prod.us-west-2.storage.cryo.aws.a2z.com にアクセスできないために発生します。これは、このエンドポイントへのアクセスをブロックするクライアント側のファイアウォールが原因で発生します。

  `aws-backint-agent.log` は、`level=error msg="Storage configuration validation failed: missing backup data plane Id"` や などのエラーを表示できます。`level=fatal msg="Error performing backup missing backup data plane Id."`

  解決策: パブリックエンドポイント cell-1.prod.us-west-2.storage.cryo.aws.a2z.com へのファイアウォールアクセスを開きます。

- エラー: `Database cannot be backed up while it is stopped`。

解決策: バックアップするデータベースがアクティブであることを確認してください。データベースデータとログは、データベースがオンラインの場合のみ、バックアップできます。

- エラー: `Getting backup metadata failed. Check the SSM document execution for more details.`

  解決策: バックアップするデータベースがアクティブであることを確認してください。データベースデータとログは、データベースがオンラインの場合のみ、バックアップできます。

バックアップログのモニタリング

- エラー: `Encountered an issue with log backups, please check SAP HANA for details.`

  解決策： SAP HANA をチェックして、ログのバックアップが SAP HANA AWS Backup から に送信されていることを確認します。
- エラー: `One or more log backup attempts failed for recovery point.`

  解決策: 詳細については SAP HANA を確認します。SAP HANA AWS Backup から にログバックアップが送信されていることを確認します。
- エラー: `Unable to determine the status of log backups for recovery point.`

  解決策: 詳細については SAP HANA を確認します。SAP HANA AWS Backup から にログバックアップが送信されていることを確認します。
- エラー: `Log backups for recovery point %s were interrupted due to a restore operation on the database.`

  解決策: 復元ジョブが完了するまで待ちます。ログバックアップが再開されるはずです。

を使用する際の SAP HANA 用語の用語集 AWS Backup

データバックアップタイプ： SAP HANA は、フルバックアップと INC (インクリメンタル) の 2 種類のデータバックアップをサポートしています。各バックアップオペレーションで使用されるタイプ AWS Backup を最適化します。

カタログバックアップ： SAP HANA は、カタログ .interacts という独自のマニフェストをこのカタログに保持します。 AWS Backup 新しいバックアップを行うたびに、カタログにエントリが作成されます。

継続的ログバックアップ (トランザクションログ): ポイントインタイムリカバリ (PITR) 機能では、SAP HANA は最新のバックアップ以降のすべてのトランザクションを追跡します。

システムコピー: 復元先のデータベースが、復旧ポイントの作成元のソースデータベースと異なる復元ジョブ。

破壊的復元: 破壊的復元は、復元ジョブのータイプで、復元されたデータベースがソースまたは既存のデータベースを削除または上書きするものです。

フル: フルバックアップはデータベース全体のバックアップです。

INC: 増分バックアップは、前回のバックアップ以降に SAP HANA データベースに加えられたすべての変更のバックアップです。

詳細については、「AWS 用語集」を参照してください。

AWS Backup EC2 インスタンスでの SAP HANA データベースのリリースノートのサポート

現時点ではサポートされていない機能が、以下のとおりあります。

- クロスアカウントコピーおよびクロスリージョンコピーはサポートされていません。
- Backup Audit Manager とレポートは現在サポートされていません。
- がサポートするサービス AWS リージョン には、Amazon EC2 インスタンスでの SAP HANA データベースバックアップで現在サポートされている リージョンが含まれています。

Amazon Redshift バックアップ

Amazon Redshift はフルマネージド型のスケーラブルなクラウドデータウェアハウスで、迅速、簡単、安全な分析により、インサイトを得るまでの時間を短縮します。を使用して AWS Backup 、変更不可能なバックアップ、個別のアクセスポリシー、バックアップジョブと復元ジョブの一元的な組織ガバナンスでデータウェアハウスを保護できます。

Amazon Redshift データウェアハウスは、ノードと呼ばれるコンピューティングリソースのコレクションであり、cluster. AWS Backup can と呼ばれるグループに編成されています。

Amazon Redshift の詳細については、「Amazon Redshift 入門ガイド」、「Amazon Redshift データベースデベロッパーガイド」、および「Amazon Redshift クラスター管理ガイド」を参照してください。

Amazon Redshift でプロビジョニングされたクラスターのバックアップ

Amazon Redshift クラスターは、 AWS Backup コンソールを使用して保護することも、API または CLI を使用してプログラムで保護することもできます。これらのクラスターは、バックアッププランの一環として定期的なスケジュールでバックアップすることも、必要に応じてオンデマンドバックアップでバックアップすることもできます。

単一のテーブル (「項目レベルの復元」とも呼ばれます) またはクラスター全体を復元できます。テーブルは単独ではバックアップできないことに注意してください。クラスターをバックアップすると、テーブルはクラスターの一部としてバックアップされます。

AWS Backup を使用すると、リソースを一元的に表示できます。ただし、Amazon Redshift が唯一のリソースである場合は、Amazon Redshift の自動スナップショットスケジューラを引き続き使用できます。を介して手動スナップショット設定を管理することを選択した場合、Amazon Redshift を使用して手動スナップショット設定を引き続き管理することはできません AWS Backup。

Amazon Redshift クラスターは、 AWS Backup コンソールまたは を使用してバックアップできます AWS CLI。

AWS Backup コンソールを使用して Amazon Redshift クラスターをバックアップするには、オンデマンドまたはバックアッププランの一部としての 2 つの方法があります。

オンデマンド Amazon Redshift バックアップを作成する

詳細については、「オンデマンドバックアップタイプの作成」ページを参照してください。

手動スナップショットを作成するには、Amazon Redshift リソースを含むバックアッププランを作成するときに、継続的バックアップチェックボックスをオフのままにします。

バックアッププランで、スケジュールされた Amazon Redshift バックアップを作成する

保護されたリソースであれば、スケジュールされたバックアップに Amazon Redshift クラスターを含めることができます。Amazon Redshift テーブルの保護をオプトインするには:

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[保護されたリソース] を選択します。
3. Amazon Redshift を [オン] に切り替えます。
4. Amazon Redshift クラスターを既存または新規のプランに含めるには、「コンソールへのリソースの割り当て」を参照してください。

[バックアッププランを管理] では、バックアッププランを作成して、Amazon Redshift クラスターを含めるか、既存のプランを更新して Amazon Redshift クラスターを含めるかを選択できます。リソースタイプとして Amazon Redshift を追加する場合、[すべての Redshift クラスター] を追加するか、クラスターの横にあるチェックボックスをオンします。

プログラムによるバックアップ

JSON ドキュメントでバックアッププランを定義し、 AWS Backup コンソールまたは を使用して指定することもできます AWS CLI。プログラムでバックアッププランを作成する方法については、「JSON ドキュメントと AWS Backup CLI を使用したバックアッププランの作成」を参照してください。

API を用いると、以下の操作が行えます。

- バックアップジョブを開始する
- バックアップジョブの説明を表示する
- 復旧ポイントのメタデータを取得する
- リソース別に復旧ポイントを一覧表示する
- 復旧ポイントのタグを一覧表示する

Amazon Redshift クラスターバックアップを表示する

Amazon Redshift テーブルのバックアップをコンソール内で表示および変更するには:

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. [バックアップボールト] を選択します。次に、Amazon Redshift クラスターを含むバックアップボールト名をクリックします。
3. バックアップボールトには、概要とバックアップのリストが表示されます。[復旧ポイント ID] 列のリンクをクリックできます。
4. 1 つまたは複数の復旧ポイントを削除するには、削除するボックスにチェックを入れます。[アクション] ボタンで、[削除] を選択できます。

Amazon Redshift クラスターの復元

詳細については、「Amazon Redshift クラスターの復元」を参照してください。

Amazon Relational Database Service のバックアップ

Amazon RDS と AWS Backup

Amazon RDS インスタンスとクラスターをバックアップするオプションを検討するときは、作成して使用するバックアップの種類を明確にすることが重要です。Amazon RDS を含むいくつかの AWS リソースは、独自のネイティブバックアップソリューションを提供します。

Amazon RDS には、自動バックアップと手動バックアップを作成するオプションがあります。Amazon RDS の用語では、バックアッププランに含まれる復旧ポイントを含め AWS Backup、によって作成されたすべての復旧ポイントが手動バックアップを検討しています。

AWS Backup を使用して Amazon RDS インスタンスのバックアップ (復旧ポイント) を作成する場合、 AWS Backup は、Amazon RDS を使用して自動バックアップを作成したことがあるかどうかをチェックします。自動バックアップが存在する場合、 はこのスナップショットのコピーを作成します (AWS Backup `copy-db-snapshot` オペレーション) 。既存のバックアップが存在しない場合、はコピー (`create-db-snapshot` オペレーション) の代わりに、指定したインスタンスのスナップショット AWS Backup を作成します。

いずれかのオペレーションによって作成された AWS Backupによって作成された最初のスナップショットは、完全なスナップショットが 1 つになります。フルバックアップが存在する限り、この後続のコピーはすべて増分バックアップになります。

> **Important**
>
> AWS Backup バックアッププランが Amazon RDS インスタンスの複数の日次スナップショットを作成するようにスケジュールされていて、それらのスケジュールされたAWS Backup バックアップ開始ウィンドウの 1 つが Amazon RDS Backup ウィンドウ と一致すると、バックアップのデータ系統が非同一バックアップに分岐し、計画外の競合するバックアップを作成できます。これを防ぐには、 AWS Backup バックアッププランまたは Amazon RDS ウィンドウが時間と一致しないようにしてください。

Amazon RDS の継続的バックアップとポイントインタイム復元

継続的なバックアップには AWS Backup 、 を使用して Amazon RDS リソースの完全バックアップを作成し、トランザクションログを使用してすべての変更をキャプチャすることが含まれます。一定の時間間隔で撮影された以前のスナップショットを選択する代わりに、復元したい時点まで巻き戻すことで、よりきめ細かな作業を実現できます。

詳細については、「継続的バックアップと PITR がサポートするサービス」と「継続的バックアップ設定の管理」を参照してください。

Amazon RDS マルチアベイラビリティゾーンのバックアップ

AWS Backup は、Amazon RDS for MySQL および for PostgreSQL マルチ AZ (アベイラビリティーゾーン) のデプロイオプションをバックアップし、1 つのプライマリデータベースインスタンスと 2 つの読み取り可能なスタンバイデータベースインスタンスでサポートします。

マルチアベイラビリティーゾーンのバックアップは、以下のリージョンで利用可能です。アジアパシフィック (シドニー) リージョン、アジアパシフィック (東京) リージョン、欧州 (アイルランド) リージョン、米国東部 (オハイオ) リージョン、米国西部 (オレゴン) リージョン、欧州 (ストックホルム) リージョン、アジアパシフィック (シンガポール) リージョン、米国東部 (バージニア北部) リージョン、および欧州 (フランクフルト) リージョンです。

マルチ AZ 配置オプションは、書き込みトランザクションを最適化するものであり、読み込み容量の追加、書き込みトランザクションの待ち時間の短縮、(書き込みトランザクションの遅延の一貫性に影響する) ネットワークジッターからの耐障害性、および高い可用性と耐久性を必要とするワークロードに最適です。

マルチ AZ クラスターを作成するには、エンジンタイプとして MySQL または PostgreSQL のいずれかを選択できます。

AWS Backup コンソールには、次の 3 つのデプロイオプションがあります。

- マルチ AZ DB クラスター: 1 つのプライマリ DB インスタンスと 2 つの読み取り可能なスタンバイ DB インスタンスを含む DB クラスターを作成します。これらは、各 DB インスタンスは異なるアベイラビリティーゾーンにあります。サーバー対応ワークロードに高可用性とデータ冗長性を提供し、容量を増やします。
- マルチ AZ DB インスタンス: プライマリ DB インスタンスとスタンバイ DB インスタンスが別個のアベイラビリティーゾーンに作成されます。これにより高い可用性とデータの冗長性が得られますが、スタンバイ DB インスタンスは読み取りワークロードの接続をサポートしていません。
- 単一の DB インスタンス: スタンバイ DB インスタンスのない単一の DB インスタンスを作成します。

Amazon RDS のバックアップを作成するには、「バックアップの作成」のうち、「バックアッププランの一環としてのバックアップのスケジュール」、または、「オンデマンドバックアップの作成」を参照してください。

> **Note**
>
> ポイントインタイムリカバリ (PITR) はインスタンスをサポートしていますが、クラスターはサポートしていません。
> マルチ AZ DB クラスターのスナップショットのコピーはサポートされていません。

マルチ AZ クラスターと RDS インスタンスの違い

1 つのアベイラビリティーゾーンまたは 2 つのアベイラビリティーゾーンにあるバックアップは、RDS インスタンスです。3 つ以上のインスタンスを含むデプロイとバックアップは、Amazon Aurora、Amazon Neptune、Amazon DocumentDB クラスターと同様に、クラスターです。

ARN (Amazon リソースネーム) は、インスタンスとクラスターのどちらを使用するかによってレンダリングが異なります。

RDS インスタンスの ARN: `arn:aws:rds:`*`region`*`:` *`account`*`:db:`*`name`*

RDS マルチアベイラビリティクラスター:`arn:aws:rds:`*`region`*`:`*`account`* `:cluster:`*`name`*

詳細については、「Amazon RDS ユーザーガイド」の「マルチ AZ DB クラスターのデプロイ」を参照してください。

マルチ AZ DB クラスタースナップショットの作成に関する詳細については、「Amazon RDS ユーザーガイド」を参照してください。

AWS CloudFormation スタックバックアップ

CloudFormation スタックは、1 つのユニットとしてバックアップできる複数のステートフルリソースとステートレスリソースで構成されます。つまり、スタックをバックアップし、その中のリソースを復元することで、複数のリソースを含むアプリケーションをバックアップおよび復元できます。スタック内のすべてのリソースは、スタックの AWS CloudFormation テンプレートで定義されます。

スタックがバックアップされると、 CloudFormation テンプレートとスタック AWS Backup で CloudFormation がサポートする追加リソースごとに復旧ポイントが作成されます。これらの復旧ポイントは、複合と呼ばれる包括的な復旧ポイントにまとめられます。

この複合復旧ポイントは復元できませんが、ネストされた復旧ポイントは復元できます。コンソールまたは AWS CLIを使用して、複合バックアップ内の 1 つのネストされたバックアップからすべてのネストされたバックアップまで復元できます。

CloudFormation アプリケーションスタックの用語

- 複合復旧ポイント: ネストされた復旧ポイントやその他のメタデータをグループ化するために使用される復旧ポイントです。
- ネストされた復旧ポイント : CloudFormation スタックの一部であり、複合復旧ポイントの一部としてバックアップされるリソースの復旧ポイント。ネストされた復旧ポイントは、それぞれ、1 つの複合復旧ポイントのスタックに属します。
- 複合ジョブ : スタック内の個々のリソースの他のバックアップジョブを CloudFormationトリガーできるスタックのバックアップ、コピー、または復元ジョブ。
- ネストされたジョブ： AWS CloudFormation スタック内のリソースのバックアップ、コピー、または復元ジョブ。

CloudFormation スタックバックアップジョブ

バックアップ作成のプロセスは、バックアップジョブと呼ばれます。 CloudFormation スタックバックアップジョブのステータスは です。バックアップジョブが終了すると、ステータスは `Completed` になります。これは AWS CloudFormation 復旧ポイント (バックアップ) が作成されたことを意味します。

CloudFormation スタックは、 コンソールを使用してバックアップすることも、プログラムでバックアップすることもできます。 CloudFormation スタックを含むリソースをバックアップするには、このデAWS Backup ベロッパーガイドの「バックアップの作成」を参照してください。

CloudFormation スタックは API コマンド を使用してバックアップできます`StartBackupJob`。ドキュメントとコンソールは、複合復旧ポイントとネストされた復旧ポイントを指していることに注意してください。API 言語では「親復旧ポイントと子復旧ポイント」という用語が同じ文脈上の関係で使用されています。

CloudFormation スタックには、CloudFormation テンプレート によって示されるすべての AWS リソースが含まれています。テンプレートには AWS Backupによってまだサポートされていないリソースが含まれている場合があることに注意してください。テンプレートに AWS サポートされているリソースとサポートされていないリソースの組み合わせが含まれている場合、 AWS Backup は引き続きテンプレートを複合スタックにバックアップしますが、Backup は Backup がサポートするサービスの復旧ポイントのみを作成します。 CloudFormation テンプレートに含まれるすべてのリソースタイプは、特定のサービスにオプトインしていない場合でも、バックアップに含まれます (コンソール設定でサービスを「有効」にする) 。 AWS Backup がサポートするネストされたバック

アップ (復旧ポイント) は復元できますが、ネストされたスタックは、バックアップまたは復元できません。

AWS CloudFormation 復旧ポイント

復旧ポイントのステータス

スタックのバックアップジョブが終了すると (ジョブステータスが Completed になると)、スタックのバックアップの作成が完了となります。このバックアップは複合復旧ポイントとも呼ばれます。複合復旧ポイントには、Completed、Failed、Partial のいずれかのステータスがあります。バックアップジョブに一定のステータスがありますが、復旧ポイント (バックアップとも呼ばれます) にも別個のステータスがあることに注意してください。

完了したバックアップジョブとは、スタック全体と 内のリソースが によって保護されていることを意味します AWS Backup。失敗ステータスは、バックアップジョブが失敗したことを示します。失敗の原因となった問題が修正されたら、バックアップを再度作成する必要があります。

Partial ステータスは、スタック内のすべてのリソースがバックアップされたわけではないことを意味します。これは、 CloudFormation テンプレートに現在 でサポートされていないリソースが含まれている場合や AWS Backup、スタック内のリソース (ネストされたリソース) に属する 1 つ以上のバックアップジョブのステータスが 以外の場合に発生する可能性がありますCompleted。Completed 以外のステータスになったリソースがあれば、オンデマンドバックアップを手動で作成して、このリソースを再実行できます。スタックのステータスが Completed になるべきところが、Partial として表示されている場合は、上記のどの条件がスタックに当てはまるかを確認してください。

複合復旧ポイント内のネストされたリソースのそれぞれに、個別の復旧ポイントがあり、それぞれに独自のステータス (Completed または Failed) があります。ネストされた復旧ポイントで、ステータスが Completed のものは、復元できます。

復旧ポイントを管理する

複合復旧ポイント (バックアップ) はコピーでき、ネストされた復旧ポイントはコピー、削除、関連付け解除、または復元ができます。ネストされたバックアップを含む複合復旧ポイントは削除できません。複合復旧ポイント内の、ネストされた復旧ポイントを削除した後、または関連付けを解除した後は、複合復旧ポイントを手動で削除することも、バックアッププランのライフサイクルによって削除されるまでそのままにしておくこともできます。

復旧ポイントを削除する

復旧ポイントは、 AWS Backup コンソールまたは を使用して削除できます AWS CLI。

AWS Backup コンソールを使用して復旧ポイントを削除するには、

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. 左側のナビゲーションで、[保護されたリソース] をクリックします。テキストボックスに「」と入力CloudFormationすると、スタックのみ CloudFormationが表示されます。
3. 複合復旧ポイントは [復旧ポイント] ペインに表示されます。各復旧ポイント ID の左側にある [プラス記号 (+)] をクリックすると各複合復旧ポイントが展開され、複合に含まれるネストされた復旧ポイントのすべてが表示されます。任意の復旧ポイントの左側にあるチェックボックスをオンにすると、削除する復旧ポイントの選択にその復旧ポイントを含めることができます。
4. [削除] ボタンをクリックします。

コンソールを使用して 1 つ以上の複合復旧ポイントを削除すると、警告ボックスが表示されます。この警告ボックスでは、複合スタック内のネストされた復旧ポイントを含め、複合復旧ポイントを削除する意図の確認を求められます。

API を使用して復旧ポイントを削除するには、コマンド `DeleteRecoveryPoint` を使用します。

で API を使用する場合は AWS Command Line Interface 、複合ポイントを削除する前に、ネストされたすべての復旧ポイントを削除する必要があります。ネストされた復旧ポイントがまだ含まれている複合スタックバックアップ (復旧ポイント) を削除するための API リクエストを送信すると、リクエストはエラーを返します。

ネストされた復旧ポイントと複合復旧ポイントの関連付けを解除する

ネストされた復旧ポイントと複合復旧ポイントの関連付けを解除できます (例えば、ネストされた復旧ポイントをそのままにしておき、複合復旧ポイントを削除する場合など)。両方の復旧ポイントはそのまま残りますが、接続は解除されます。つまり、ネストされた復旧ポイントとの関連付けが解除されると、複合復旧ポイントで実行された操作は、ネストされた復旧ポイントには適用されなくなります。

コンソールを使用して復旧ポイントの関連付けを解除することも、API `DisassociateRecoveryPointFromParent` を呼び出すこともできます。[API 呼び出しでは、複合復旧ポイントを指すのに「親」という用語が使用されることに注意してください。]

復旧ポイントをコピーする

複合復旧ポイントをコピーすることも、リソースがクロスアカウントおよびクロスリージョンコピーをサポートしている場合は、ネストされた復旧ポイントをコピーすることもできます。

AWS Backup コンソールを使用して復旧ポイントをコピーするには：

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. 左側のナビゲーションで、[保護されたリソース] をクリックします。テキストボックスに「」と入力CloudFormationすると、スタックのみ CloudFormationが表示されます。
3. 複合復旧ポイントは [復旧ポイント] ペインに表示されます。各復旧ポイント ID の左側にある [プラス記号 (+)] をクリックすると各複合復旧ポイントが展開され、複合に含まれるネストされた復旧ポイントのすべてが表示されます。任意の復旧ポイントの左側にある [放射状の円] ボタンをクリックすると、その復旧ポイントをコピーできます。
4. 選択したら、ペインの右上隅にある [コピー] ボタンをクリックします。

複合復旧ポイントをコピーしても、コピー機能をサポートしないネストされた復旧ポイントは、コピーされたスタックには含まれません。複合復旧ポイントのステータスは `Partial` になります。

よくある質問

1. 「アプリケーションバックアップには何が含まれていますか?」

   を使用して定義されたアプリケーションの各バックアップの一部として CloudFormation、テンプレート、テンプレート内の各パラメータの処理された値、および でサポートされているネストされたリソース AWS Backup がバックアップされます。ネストされたリソースは、CloudFormation スタックの一部ではない個々のリソースがバックアップされるのと同じ方法でバックアップされます。`no-echo` と表示されたパラメータの値はバックアップされないことに注意してください。

2. 「ネストされた AWS CloudFormation スタックがあるスタックをバックアップできますか？」

   はい。ネストされた CloudFormation スタックを含むスタックは、バックアップに含めることができます。

3. 「*`Partial`* ステータスはバックアップの作成に失敗したことを意味しますか?」

   いいえ。一部のステータスでは、一部の復旧ポイントがバックアップされたものの、一部はバックアップされなかったことが示されます。`Completed` バックアップ結果を期待していたかどうかを確認するには、次の 3 つの条件があります。

   a. CloudFormation スタックには、現在 でサポートされていないリソースが含まれていますか AWS Backup？ サポートされているリソースのリストについては、「 デベロッパーガイド」の「サポートされている AWS リソースとサードパーティーアプリケーション」を参照してください。

b. スタック内のリソースに属する 1 つ以上のバックアップジョブが成功しなかったため、ジョブを再実行する必要があります。

c. ネストされた復旧ポイントが削除されたか、複合復旧ポイントとの関連付けが解除されました。

4. CloudFormation 「スタックバックアップでリソースを除外するにはどうすればよいですか？」

   CloudFormation スタックをバックアップするときに、バックアップの一部からリソースを除外できます。コンソールでは、バックアッププランの作成とバックアッププランの更新のプロセス中に、リソースを割り当てるステップがあります。このステップには、リソース選択セクションがあります。特定のリソースタイプを含めることを選択し、バックアップするリソースとして を含めた CloudFormation場合は、選択したリソースタイプ から特定のリソース IDs を除外できます。タグを使用して、スタック内のリソースを除外することもできます。

   CLI を使用すると、次の操作ができます。

   - `NotResources` CloudFormation スタックから特定のリソースを除外するバックアッププランの 。
   - `StringNotLike` タグを使用して項目を除外する。

5. 「ネストされたリソースではどのような種類のバックアップがサポートされていますか?」

   ネストされたリソースのバックアップは、これらのリソース AWS Backup に対して がサポートするバックアップの種類に応じて、完全バックアップまたは増分バックアップのいずれかになります。詳細については、「増分バックアップの仕組み」を参照してください。ただし、PITR (point-in-time 復元) は Amazon S3 および Amazon RDS ネストされたリソースではサポートされていないことに注意してください。

6. CloudFormation 「スタックの一部である変更セットはバックアップされていますか？」

   いいえ。変更セットは CloudFormation スタックバックアップの一部としてバックアップされません。

7. AWS CloudFormation 「スタックのステータスはバックアップにどのように影響しますか？」

   CloudFormation スタックのステータスは、バックアップに影響する可能性があります。`COMPLETE` を含むステータス (`CREATE_COMPLETE`、`ROLLBACK_COMPLETE`、`UPDATE_COMPLETE`、`UPDATE_ROLLBACK_COMPLETE`、

または IMPORT_ROLLBACK_COMPLETE などのステータス) であるスタックはバックアップが可能です。

新しいテンプレートのアップロードが失敗し、スタックが ROLLBACK_COMPLETE のステータスに移行した場合、新しいテンプレートはバックアップされますが、ネストされたリソースのバックアップはロールバックされたリソースに基づいて行われます。

8. 「アプリケーションスタックのライフサイクルは、他の復旧ポイントのライフサイクルとどう違うのですか?」

   ネストされた復旧ポイントのライフサイクルは、その復旧ポイントが属するバックアッププランによって決まります。複合復旧ポイントは、ネストされた復旧ポイントのすべてのライフサイクルが最も長いものによって決まります。複合復旧ポイント内にあるネストされた復旧ポイントのうち最後に残っているものが削除されるか、関連付けが解除されると、複合復旧ポイントも削除されます。

9. のタグを復旧ポイント CloudFormation にコピーする方法

   はい。これらのタグは、ネストされた復旧ポイントのそれぞれにコピーされます。

10. 「複合復旧ポイントとネストされた復旧ポイント (バックアップ) を削除する順序はありますか?」

    はい。一部のバックアップは、他のバックアップを削除する前に削除する必要があります。ネストされた復旧ポイントを含む複合バックアップは、複合バックアップ内の復旧ポイントのすべてが削除されるまで削除できません。複合復旧ポイントに、ネストされた復旧ポイントが含まれなくなったら、手動で削除できます。それ以外の場合は、バックアッププランのライフサイクルに従って削除されます。

スタック内のアプリケーションを復元する

ネストされた復旧ポイントの復元に関する詳細については、「アプリケーションスタックのバックアップを復元する方法」を参照してください。

Windows VSS バックアップの作成

を使用すると AWS Backup、Amazon EC2 インスタンスで実行されている VSS (ボリュームシャドウコピーサービス) 対応 Windows アプリケーションをバックアップおよび復元できます。アプリケーションに Windows VSS に登録された VSS ライターがある場合、 はそのアプリケーションと整合性のあるスナップショット AWS Backup を作成します。

他のリソースの保護に使用されるのと同じマネージドバックアップサービスを使用しながら、一貫した復元を実行できます AWS 。EC2 でアプリケーション整合性の高い Windows バックアップを使用すると、従来のバックアップツールと同じ整合性設定とアプリケーション認識が得られます。

> **Note**
>
> AWS Backup は現在、Amazon EC2 で実行されているリソースのアプリケーション整合性のあるバックアップのみをサポートしています。特に、既存のインスタンスをバックアップから作成された新しいインスタンスに置き換えることで、アプリケーションデータを復元できるバックアップシナリオをサポートしています。Windows VSS バックアップでは、すべてのインスタンスタイプまたはアプリケーションがサポートされているわけではありません。

詳細については、「Amazon EC2 ユーザーガイド」の「VSS アプリケーション整合性のあるスナップショットの作成Amazon EC2」を参照してください。

Amazon EC2 を実行する VSS 対応の Windows リソースをバックアップおよび復元するには、必要な前提条件のタスクを完了するための次の手順を実行します。手順については、「Windows インスタンス用 Amazon EC2 ユーザーガイド」の「開始する前に」を参照してください。

1. で SSM エージェントをダウンロード、インストール、設定します AWS Systems Manager。このステップは必須です。手順については、Systems Manager ユーザーガイドの「Windows Server 用 Amazon EC2 インスタンスでの SSM エージェントの使用」を参照してください。 AWS
2. Windows VSS (ボリュームシャドウコピーサービス) のバックアップを取る前に、IAM ロールに IAM ポリシーを追加し、Amazon EC2 インスタンスにロールをアタッチします。手順については、Amazon EC2 ユーザーガイド」の「VSS 対応スナップショットの IAM ロールを作成する」を参照してください。IAM ポリシーの例については、「の管理ポリシー AWS Backup」を参照してください。
3. VSS コンポーネントをダウンロードして EC2 インスタンスでの Windows にインストールする
4. で VSS を有効にします AWS Backup。

    1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
    2. ダッシュボードで、オンデマンドバックアップの作成またはバックアッププランの管理から作成するバックアップのタイプを選択します。バックアップタイプに必要な情報を入力します。
    3. リソースを割り当てる場合は、[EC2] を選択します。Windows VSS バックアップは、現在 EC2 インスタンスでのみサポートされています。

4. [詳細設定] セクションで、[Windows VSS] を選択します。これにより、アプリケーション整合性のある Windows VSS バックアップを作成できます。
5. バックアップを作成します。

ステータスが Completed のバックアップジョブは、VSS 部分が成功することを保証するものではありません。VSS の組み込みはベストエフォート方式で行われます。次の手順を実行して、バックアップがアプリケーション整合性があるのか、クラッシュコンシステントであるのか、失敗しているのかを判断してください。

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. 左側のナビゲーションの [マイアカウント] で [ジョブ] をクリックします。
3. ステータスが Completed の場合、アプリケーション整合性がある (VSS) ジョブが成功したことを示します。

   ステータスが Completed with issues の場合、VSS 操作が失敗したため、クラッシュコンシステントバックアップだけが成功したことを示します。このステータスにはポップオーバーメッセージ "Windows VSS Backup Job Error encountered, trying for regular backup" も表示されます。

   バックアップに失敗した場合、ステータスは Failed になります。
4. バックアップジョブの追加の詳細を表示するには、個々のジョブをクリックします。例えば、詳細で Windows VSS Backup attempt failed because of timeout on VSS enabled snapshot creation が読み取られる場合があります。

ジョブが成功した Windows 以外のターゲットまたは VSS コンポーネント以外のターゲットを持つ VSS 対応バックアップは、VSS なしでクラッシュコンシステントになります。

サポートされていない Amazon EC2 インスタンス

次の Amazon EC2 インスタンスタイプは、小規模なインスタンスであり、バックアップを正常に取得しない可能性があるため、VSS 対応の Windows バックアップではサポートされません。

- t3.nano
- t3.micro
- t3a.nano
- t3a.micro

- t2.nano
- t2.micro

Amazon EBS と AWS Backup

Amazon EBS リソースのバックアッププロセスは、他のリソースタイプのバックアップに使用される手順と似ています。

- オンデマンドバックアップを作成する
- スケジュールされたバックアップを作成する

以下のセクションで、リソース固有の情報を紹介します。

コールドストレージ用の Amazon EBS アーカイブ階層

EBS は、バックアップのコールドストレージへの移行に対応するリソースの 1 つです。詳細については、「ライフサイクルとストレージ階層」を参照してください。

> **Note**
>
> この機能は、中国 (北京) 、中国 (寧夏) 、 AWS GovCloud （米国東部) 、 AWS GovCloud （米国西部) の各リージョンでは使用できません。

Amazon EBS マルチボリュームのクラッシュコンシステントバックアップ

デフォルトでは、 は Amazon EC2 インスタンスにアタッチされている Amazon EBS ボリュームのクラッシュコンシステントバックアップ AWS Backup を作成します。クラッシュの一貫性は、同じ Amazon EC2 インスタンスにアタッチされたすべての Amazon EBS ボリュームのスナップショットがまったく同じ瞬間に取得されることを意味します。アプリケーションの状態のクラッシュコンシステントを確保するために、インスタンスを停止したり、複数の Amazon EBS ボリューム間で調整する必要がなくなりました。

マルチボリュームのクラッシュコンシステントなスナップショットはデフォルトの AWS Backup 機能であるため、この機能を使用するには別の操作を行う必要はありません。Amazon EBS ボリュームは、次のいずれかの手順を使用してバックアップできます。

EBS スナップショット復旧ポイントの作成に使用されるロールは、そのスナップショットに関連付けられます。この同じロールを使用して、そのロールによって作成された復旧ポイントを削除したり、復旧ポイントをアーカイブ階層に移行したりする必要があります。

Amazon EBS スナップショットロックと AWS Backup

AWS Backup Amazon EBS スナップショットロックが適用されている AWS Backup マネージド Amazon EC2 AMI に関連付けられた マネージド Amazon EBS スナップショットおよびスナップショットは、スナップショットロック期間がバックアップライフサイクルを超える場合、リカバリポイントライフサイクルの一部として削除できない場合があります。この場合、復旧ポイントのステータスは EXPIRED になります。これらの復旧ポイントは、最初に Amazon EBS Snapshot Lock の解除を選択すると、手動で削除できます。

Amazon EBS リソースの復元

Amazon EBS ボリュームを復元するには、「Amazon EBS ボリュームの復元」の手順に従います。

バックアップへのタグのコピー

一般に、 は保護するリソースのタグを復旧ポイント AWS Backup にコピーします。復元中にタグをコピーする方法について詳しくは、「復元中にタグをコピーする」を参照してください。

例えば、Amazon EC2 ボリュームをバックアップすると、 はグループタグと個々のリソースタグを結果のスナップショット AWS Backup にコピーします。ただし、以下を条件とします。

- バックアップにメタデータタグを保存するために必要なリソース固有のアクセス権限の一覧については、「バックアップにタグを割り当てるのに必要なアクセス権限」を参照してください。
- 元々リソースに関連付けられているタグと、バックアップ中に割り当てられたタグは、バックアップボールトに保存されている復旧ポイントに最大 50 個割り当てられます (これは AWS 制限です)。バックアップ中に割り当てられるタグが優先され、両方のタグのセットがアルファベット順にコピーされます。
- DynamoDB は、最初に アドバンスト DynamoDB バックアップ を有効にしない限り、バックアップへのタグの割り当てをサポートしません。
- Amazon EC2 インスタンスにアタッチされている Amazon EBS ボリュームは、ネストされたリソースです。Amazon EC2 インスタンスにアタッチされている Amazon EBS ボリュームのタグは、ネストされたタグです。 は、ネストされたタグのコピーを AWS Backup ベストエフォートで試行しますが、失敗した場合は、それらなしでバックアップを作成し、完了ステータスを報告します。

- Amazon EC2 バックアップがイメージリカバリポイントとスナップショットのセットを作成すると、 AWS Backup はタグを結果の AMI にコピーします。 AWS Backup また、 は、Amazon EC2 インスタンスに関連付けられたボリュームから結果のスナップショットにタグをコピーしようとベストエフォートで試みます。

バックアップを別の にコピーすると AWS リージョン、 AWS Backup は元のバックアップのすべてのタグを送信先 にコピーします AWS リージョン。

バックアップジョブの停止

バックアップジョブ AWS Backup は、開始後に で停止できます。これを行うと、バックアップは作成されず、バックアップジョブのレコードが [中止] のステータスで保持されます。

AWS Backup コンソールを使用してバックアップジョブを停止するには

1. にサインインし AWS Management Console、https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. 左側のナビゲーションペインで、[Jobs (ジョブ)] を選択します。
3. 停止するバックアップジョブを選択します。
4. バックアップジョブの詳細ペインで、[Stop (停止)] を選択します。

バックアップをコピーする

バックアップは、複数の またはオンデマンド AWS アカウント AWS リージョン にコピーすることも、ほとんどのリソースタイプのスケジュールされたバックアッププランの一部として自動的にコピーすることもできます。詳細については、「」を参照してくださいthe section called “リソース別の機能の可用性”。

Amazon RDS および Aurora を除き、サポートされているほとんどのリソースについて、クロスアカウントおよびクロスリージョンコピーのシーケンスを自動化することもできます。Amazon RDS および Aurora スナップショットの場合、 は、これらのサービスが暗号化キーを作成する方法により、クロスアカウントコピーまたはクロスリージョンコピーの自動化 AWS Backup のみをサポートします (マルチ AZ DB クラススナップショットのコピーはサポートされていません)。

リソースタイプによっては、継続的バックアップ機能と、クロスリージョンおよびクロスアカウントコピーの両方が可能なリソースタイプがあります。継続的バックアップのクロスリージョンコピーまたはクロスアカウントコピーが作成されると、コピーされた復旧ポイント (バックアップ) はスナッ

プショット (定期的) バックアップになります。リソースタイプ に応じて、スナップショットは増分コピーでもフルコピーでもかまいません。これらのコピーには PITR (ポイントインタイムリカバリ) は使用できません。

コピーは、作成日や保持期間など、ソース設定を保持します。作成日とは、コピーが作成された日時ではなく、ソースが作成された日時を指します。

注: コピーが期限切れにならないように設定されている場合でも、ソース設定はコピーの有効期限設定よりも優先されます。有効期限なしに設定されたコピーでも、ソースの有効期限を保持します。

バックアップコピーを期限切れにならないようにする場合は、ソースバックアップを期限切れにならないように設定するか、コピーの作成後 100 年後に有効期限を指定します。

内容

- でのバックアップコピーの作成 AWS リージョン
- でのバックアップコピーの作成 AWS アカウント

でのバックアップコピーの作成 AWS リージョン

を使用すると AWS Backup、バックアップをオンデマンド AWS リージョン で複数の にコピーすることも、スケジュールされたバックアッププランの一部として自動的にコピーすることもできます。リージョン間のレプリケーションは、本番稼働用データから最小限の距離だけ離してバックアップを保存するビジネス継続性またはコンプライアンス要件がある場合に特に役立ちます。ビデオチュートリアルについては、「バックアップのクロスリージョンコピーの管理」を参照してください。

バックアップを新しい に AWS リージョン 初めてコピーすると、 はバックアップを完全に AWS Backup コピーします。一般的に、サービスが増分バックアップをサポートしている場合、同じ 内のそのバックアップの後続のコピーは増分 AWS リージョン になります。 AWS Backup は、コピー先ボールトのカスタマーマネージドキーを使用してコピーを再暗号化します。

例外は Amazon EBS で、コピーオペレーション中にスナップショットの暗号化ステータスを変更すると、完全な (増分ではない) コピーになります。

要件

- AWS Backupがサポートするほとんどのリソースは、クロスリージョンバックアップをサポートしています。詳細については、「リソース別の機能の可用性」を参照してください。
- ほとんどの AWS リージョンはクロスリージョンバックアップをサポートしています。詳細については、「による機能の可用性 AWS リージョン」を参照してください。

- AWS Backup は、コールド階層のストレージのクロスリージョンコピーをサポートしていません。

特定のリソースとのクロスリージョンコピーに関する考慮事項

Amazon RDS

オプショングループを別の にコピーすることはできません AWS リージョン。これを試みると、「スナップショットには次のオプションを含むターゲットオプショングループが必要です: ...」などのエラーが表示されることがあります。

Amazon RDS スナップショットの新しいクロスリージョンコピーを作成する AWS リージョン ときは、ターゲットに同じオプショングループを入力する必要があります。

オンデマンドのクロスリージョンバックアップの実行

既存のバックアップをオンデマンドでコピーするには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. [バックアップボールト] を選択します。
3. コピーする復旧ポイントが含まれるボールトを選択します。
4. バックアップセクションで、コピーする復旧ポイントを選択します。
5. [アクション] ドロップダウンボタンを使用して [コピー] を選択します。
6. 次の値を入力します。

   送信先にコピーする

   コピー AWS リージョン 先を選択します。コピーごとに新しいコピールールを新しい送信先に追加できます。

   送信先のバックアップボールト

   送信先のバックアップボールトを選択します。

   コールドストレージへの移行

   バックアップコピーをコールドストレージに移行するタイミングを選択します。コールドストレージに移行されたバックアップは、そこに最低 90 日保存される必要があります。この値は、コピーがコールドストレージに移行された後は変更できません。

コールドストレージに移行できるリソースの一覧については、リソース別の機能の可用性 表の「コールドストレージへのライフサイクル」セクションを参照してください。他のリソースでは、コールドストレージ式は無視されます。

保持期間

コピーが削除される作成後の日数を指定します。これは、[コールドストレージへの移行] の値より 90 日以上大きい数値にする必要があります。[常時] の保持期間では、コピーは無期限に保持されます。

IAM ロール

コピーの作成時に AWS Backup が使用する IAM ロールを選択します。ロールは、 がロールを AWS Backup 引き受けることができる信頼されたエンティティとして AWS Backup リストされている必要もあります。デフォルト を選択し、 AWS Backup デフォルトのロールがアカウントに存在しない場合、正しいアクセス許可を持つロールが作成されます。

7. [コピー] を選択します。

クロスリージョンバックアップのスケジュール

スケジュールバックアッププランを使用して、バックアップを AWS リージョン間でコピーできます。

スケジュールバックアッププランを使用してバックアップをコピーするには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. マイアカウントで、[バックアッププラン] を選択してから、「バックアッププランを作成する」を選択します。
3. リポジトリの [バックアッププランの作成] ページで、[新しいプランを構築する] を選択します。
4. [バックアッププラン名] で、バックアッププランの名前を入力します。
5. [バックアップルールの設定] セクションで、バックアップスケジュール、バックアップウィンドウ、ライフサイクルルールを定義するバックアップルールを追加します。後でバックアップルールを追加できます。

   a. [バックアップルール名] にルールの名前を入力します。

   b. [バックアップボールト] で、リストから [ボールト] を選択します。このバックアップのリカバリポイントは、このボールトに保存されます。新しいバックアップボールトを作成します。

c. [バックアップ頻度] で、バックアップを取る頻度を選択します。

d. PITR をサポートするサービスの場合、この機能が必要な場合は、継続的バックアップの point-in-time 復旧を有効にする (PITR) を選択します。PITR をサポートするサービスの一覧については、リソース別の機能の可用性 表の該当するセクションを参照してください。

e. バックアップウィンドウで、[バックアップウィンドウのデフォルトを使用する (推奨)] を選択します。バックアップウィンドウをカスタマイズできます。

f. [送信先にコピー] で、バックアップコピーの送信先 AWS リージョン を選択します。バックアップはこのリージョンにコピーされます。コピーごとに新しいコピールールを新しい送信先に追加できます。次に、以下の値を入力します:

別のアカウントのボールトにコピー

このオプションは切り替えないでください。クロスアカウントコピーの詳細については、「 でのバックアップコピーの作成 AWS アカウント」を参照してください。

送信先のバックアップボールト

がバックアップ AWS Backup をコピーする送信先リージョンのバックアップボールトを選択します。

クロスリージョンコピー用の新しいバックアップボールトを作成する場合は、「バックアップボールトの新規作成」を選択します。ウィザードに情報を入力します。続いて、[バックアップボールトを作成する] を選択します。

6. [プランを作成] を選択します。

でのバックアップコピーの作成 AWS アカウント

を使用すると AWS Backup、オンデマンド AWS アカウント で複数の にバックアップすることも、スケジュールされたバックアッププランの一部として自動的にバックアップすることもできます。運用上またはセキュリティ上の理由から、組織 AWS アカウント 内の 1 つ以上の にバックアップを安全にコピーする場合は、クロスアカウントバックアップを使用します。元のバックアップが誤って削除された場合は、コピー先アカウントからコピー元のアカウントにバックアップをコピーし、復元を開始できます。これを行うには、その前に、 AWS Organizations サービスの同じ組織に属する 2 つのアカウントを持つ必要があります。詳細については、Organizations ユーザーガイドの「チュートリアル: 組織の作成と設定」を参照してください。

コピー先アカウントで、バックアップボールトを作成する必要があります。次に、コピー先アカウントのバックアップを暗号化するカスタマーマネージドキーと、コピーするリソース AWS Backup

へのアクセスを に許可するリソースベースのアクセスポリシーを割り当てます。ソースアカウントで、リソースがカスタマー管理キーで暗号化されている場合は、このカスタマー管理キーをコピー先アカウントと共有する必要があります。その後、バックアッププランを作成し、 AWS Organizations で組織単位の一部であるコピー先アカウントを選択できます。

バックアップを初めてクロスアカウントにコピーすると、 はバックアップを完全に AWS Backup コピーします。一般的に、サービスが増分バックアップをサポートしている場合、同じアカウント内のそのバックアップの後続のコピーは増分です。 AWS Backup は、コピー先ボールトのカスタマーマネージドキーを使用してコピーを暗号化します。

要件

- AWS アカウント の複数の にまたがるリソースを管理する前に AWS Backup、アカウントは AWS Organizations サービス内の同じ組織に属している必要があります。
- でサポートされているほとんどのリソースは、クロスアカウントバックアップ AWS Backup をサポートしています。詳細については、「リソース別の機能の可用性」を参照してください。
- ほとんどの AWS リージョンでは、クロスアカウントバックアップがサポートされています。詳細については、「による機能の可用性 AWS リージョン」を参照してください。
- AWS Backup は、コールド階層のストレージ用のクロスアカウントコピーをサポートしていません。

クロスアカウントバックアップのセットアップ

クロスアカウントバックアップを作成するには何が必要か

- ソースアカウント

  ソースアカウントは、本番稼働用 AWS リソースとプライマリバックアップが存在するアカウントです。

  ソースアカウントユーザーがクロスアカウントのバックアップ操作を開始します。ソースアカウントユーザーまたはロールには、操作を開始するための適切な API 権限が必要です。適切なアクセス許可は`AWSBackupFullAccess`、 AWS Backup オペレーションへのフルアクセスを可能にする AWS マネージドポリシー、または などのアクションを許可するカスタマー管理ポリシーです`ec2:ModifySnapshotAttribute`。ポリシータイプの詳細については、「AWS Backup 管理ポリシー」を参照してください。
- コピー先アカウント

コピー先アカウントは、バックアップのコピーを保持するアカウントです。アカウントは複数選択できます。コピー先アカウントは、 AWS Organizationsのソースアカウントと同じ組織にある必要があります。

コピー先バックアップボールトのアクセスポリシー `backup:CopyIntoBackupVault` を「許可」する必要があります。このポリシーが存在しない場合、コピー先アカウントへのコピーの試行は拒否されます。

- の管理アカウント AWS Organizations

  管理アカウントは、 AWS アカウントでクロスアカウントバックアップを管理するために使用する AWS Organizationsによって定義された組織内のプライマリアカウントです。クロスアカウントバックアップを使用するには、サービスの信頼も有効にする必要があります。サービスの信頼を有効にすると、組織内の任意のアカウントをコピー先アカウントとして使用できます。コピー先アカウントから、クロスアカウントのバックアップに使用するボールトを選択できます。
- AWS Backup コンソールでクロスアカウントバックアップを有効にする

セキュリティについては、「クロスアカウントバックアップのセキュリティに関する考慮事項」を参照してください。

クロスアカウントバックアップを使用するには、クロスアカウントバックアップ機能を有効にする必要があります。次に、アクセスポリシー `backup:CopyIntoBackupVault` をコピー先バックアップボールトに「許可」する必要があります。

クロスアカウントバックアップを有効にする

1. AWS Organizations 管理アカウントの認証情報を使用してログインします。クロスアカウントバックアップは、これらの認証情報を使用してのみ有効または無効にできます。
2. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
3. [マイアカウント] で、[設定] を選択します。
4. [クロスアカウントバックアップ] で、[有効] を選択します。
5. [バックアップボールト] で、コピー先ボールトを選択します。

   クロスアカウントコピーの場合、ソースボールトと宛先ボールトは異なるアカウントにあります。必要に応じて、送信先アカウントを所有するアカウントに切り替えます。
6. [アクセスポリシー] セクションで、`backup:CopyIntoBackupVault` を [許可] します。たとえば、[アクセス許可の追加] を選択し、その後、[組織からのバックアップボー

ルトへのアクセスを許可する] を選択します。以外のクロスアカウントアクションは拒否backup:CopyIntoBackupVaultされます。

7. これで、組織内のどのアカウントでも、バックアップ保管庫の内容を組織内の他のアカウントと共有できるようになりました。詳細については、「バックアップボールトを別の AWS アカウントと共有する」を参照してください。他のアカウントのバックアップボールトの内容を受信できるアカウントを制限するには、アカウントをコピー先アカウントとして設定する を参照してください。

クロスアカウントバックアップのスケジュール

スケジュールバックアッププランを使用して、バックアップを AWS アカウント間でコピーできます。

スケジュールバックアッププランを使用してバックアップをコピーするには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. マイアカウントで、[バックアッププラン] を選択してから、「バックアッププランを作成する」を選択します。
3. リポジトリの [バックアッププランの作成] ページで、[新しいプランを構築する] を選択します。
4. [バックアッププラン名] で、バックアッププランの名前を入力します。
5. [バックアップルールの設定] セクションで、バックアップスケジュール、バックアップウィンドウ、ライフサイクルルールを定義するバックアップルールを追加します。後でバックアップルールを追加できます。

   [ルール名] にルールの名前を入力します。
6. [Frequency (頻度)] の [Schedule (スケジュール)] セクションで、バックアップを実行する頻度を選択します。
7. バックアップウィンドウで、「バックアップウィンドウのデフォルトを使用する (推奨)」を選択します。バックアップウィンドウをカスタマイズできます。
8. [バックアップボールト] で、リストから [ボールト] を選択します。このバックアップのリカバリポイントは、このボールトに保存されます。新しいバックアップボールトを作成します。
9. コピーの生成-オプションセクションで、次の値を入力します。

送信先リージョン

バックアップコピー AWS リージョン の送信先を選択します。バックアップはこのリージョンにコピーされます。コピーごとに新しいコピールールを新しい送信先に追加できます。

別のアカウントのボールトにコピー

このオプションを切り替えて選択します。このオプションを選択すると、青に変わります。外部ボールト ARN オプションが表示されます。

外部ボールト ARN

コピー先リソースの Amazon リソースネーム (ARN) に入力します。ARN は、アカウント ID とその を含む文字列です AWS リージョン。 AWS Backup はバックアップを送信先アカウントのボールトにコピーします。コピー先リージョンリストは、外部ボールト ARN 内のリージョンに自動的に更新されます。

バックアップボールトのアクセスを許可するために、[許可] を選択します。次に開いたウィザードで [許可] を選択します。

AWS Backup には、指定された値にバックアップをコピーするために外部アカウントにアクセスするためのアクセス許可が必要です。ウィザードには、このアクセスを提供する次のポリシー例が表示されます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow account to copy into backup vault",
      "Effect": "Allow",
      "Action": "backup:CopyIntoBackupVault",
      "Resource": "*",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:root"
      }
    }
  ]
}
```

コールドストレージへの移行

バックアップコピーをコールドストレージに移行するタイミングと、コピーの有効期限 (削除) を選択します。コールドストレージに移行されたバックアップは、そこに最低 90 日保存される必要があります。この値は、コピーがコールドストレージに移行された後は変更できません。

コールドストレージに移行できるリソースの一覧については、リソース別の機能の可用性 表の「コールドストレージへのライフサイクル」セクションを参照してください。他のリソースでは、コールドストレージ式は無視されます。

[有効期限切れ] で、コピーが作成されてから削除されるまでの日数を指定します。これは、[コールドストレージへの移行] の値より 90 日以上大きい数値にする必要があります。

> **Note**
>
> バックアップの有効期限が切れ、ライフサイクルポリシーの一部として削除対象としてマークされると、 はランダムに選択された時点で次の 8 時間にわたってバックアップ AWS Backup を削除します。このウィンドウは、一貫したパフォーマンスを確保するのに役立ちます。

10. リカバリポイントに追加されたタグをクリックして、リカバリポイントにタグを追加します。
11. 詳細バックアップ設定で、Windows VSS を選択して、EC2 で実行されている選択したサードパーティソフトウェアのアプリケーション対応スナップショットを有効にします。
12. [プランを作成] を選択します。

オンデマンドのクロスアカウントバックアップの実行

バックアップは、オンデマンド AWS アカウント で別の にコピーできます。

バックアップをオンデマンドでコピーするには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. マイアカウントで、[バックアップボールト] をクリックして、すべてのバックアップボールトを一覧表示します。バックアップボールトの名前またはタグでフィルタリングできます。
3. コピーするバックアップの [復旧ポイント ID] を選択します。
4. [コピー] を選択します。

5. [バックアップの詳細] を開いて、コピーするリカバリポイントに関する情報を表示します。
6. [設定のコピー] セクションで、[コピー先リージョン] リストからオプションを選択します。
7. [別のアカウントのボールトにコピー] をオンにします。このオプションを選択すると、青に変わります。
8. コピー先リソースの Amazon リソースネーム (ARN) に入力します。ARN は、アカウント ID とその を含む文字列です AWS リージョン。 AWS Backup はバックアップを送信先アカウントのボールトにコピーします。コピー先リージョンリストは、外部ボールト ARN 内のリージョンに自動的に更新されます。
9. バックアップボールトのアクセスを許可するために、[許可] を選択します。次に開いたウィザードで [許可] を選択します。

   コピーを作成するには、ソースアカウントにアクセスするためのアクセス許可 AWS Backup が必要です。ウィザードには、このアクセスを提供するポリシーの例が表示されます。このポリシーを以下に示します。

   ```
   {
     "Version": "2012-10-17",
     "Statement": [
       {
         "Sid": "Allow account to copy into backup vault",
         "Effect": "Allow",
         "Action": "backup:CopyIntoBackupVault",
         "Resource": "*",
         "Principal": {
           "AWS": "arn:aws:iam::account-id:root"
         }
       }
     ]
   }
   ```

10. コールドストレージへの移行については、バックアップコピーをコールドストレージに移行するタイミングと、コピーの有効期限 (削除) を選択します。コールドストレージに移行されたバックアップは、そこに最低 90 日保存される必要があります。この値は、コピーがコールドストレージに移行された後は変更できません。

    コールドストレージに移行できるリソースの一覧については、リソース別の機能の可用性 表の「コールドストレージへのライフサイクル」セクションを参照してください。他のリソースでは、コールドストレージ式は無視されます。

[有効期限切れ] で、コピーが作成されてから削除されるまでの日数を指定します。これは、[コールドストレージへの移行] の値より 90 日以上大きい数値にする必要があります。

11. IAM ロールで、バックアップをコピーできるようにする権限を持つ IAM ロール (デフォルトロールなど) を指定します。コピーの行為は、コピー先アカウントのサービスにリンクされたロールによって実行されます。
12. [コピー] を選択します。コピーするリソースのサイズによっては、この処理が完了するまでに数時間かかる場合があります。コピージョブが完了すると、[ジョブ] メニュー内の [コピージョブ] タブ内にコピーされます。

暗号化キーとクロスアカウントコピー

クロスアカウントコピーの暗号化キーは、リソースタイプによって異なります。ソースバックアップボールトの暗号化キーフル AWS Backup 管理を使用するリソース。カスタマーマネージド KMS キーは、これらのリソースタイプのクロスアカウントコピー暗号化に使用できます。

によって完全に管理されていないリソースタイプ AWS Backup には、同じソース KMS キーとリソース KMS キーがあります。 AWS マネージド KMS キーを使用したクロスアカウントコピーは、によって完全に管理されていないこれらのタイプのリソースではサポートされていません AWS Backup。

クロスアカウントコピーの失敗のトラブルシューティングに関するその他のヘルプについては、「AWS ナレッジセンター」を参照してください。

クロスアカウントコピー中、ソースアカウントの KMS キーポリシーは、KMS キーポリシーで送信先アカウントを許可する必要があります。

ある から別の AWS アカウント へのバックアップの復元

AWS Backup は、リソースの 1 つの から別の AWS アカウント への復旧をサポートしていません。ただし、あるアカウントから別のアカウントにバックアップをコピーし、そのアカウントで復元することはできます。たとえば、アカウント A からアカウント B にバックアップを復元することはできませんが、アカウント A からアカウント B にバックアップをコピーし、アカウント B で復元できます。

あるアカウントから別のアカウントへのバックアップの復元は、2 つのステップです。

アカウントから別のアカウントにバックアップを復元するには

1. ソースから復元先の AWS アカウント アカウントにバックアップをコピーします。手順については、「クロスアカウントバックアップのセットアップ」を参照してください。
2. リソースに適切な指示に従って、バックアップを復元します。

バックアップボールトを別の AWS アカウントと共有する

AWS Backup では、バックアップボールトを 1 つ以上のアカウント、または の組織全体と共有できます AWS Organizations。コピー先のバックアップボールトをソース AWS アカウント、ユーザー、または IAM ロールと共有できます。

コピー先のBackup ボールトを共有するには

1. [AWS Backup] を選択してから、[バックアップボールト] を選択します。
2. 共有するバックアップボールトの名前を選択します。
3. [アクセスポリシー] ペインで、[アクセス許可の追加] のドロップダウンを選択します。
4. アカウントレベルのBackup ボールトへのアクセスを許可するを選択します。または、組織レベルまたはロールレベルのアクセスを許可するかを選択できます。
5. このコピー先バックアップボールトと共有するアカウントのうち、AccountID を入力します。
6. [ポリシーを保存]を選択します。

IAM ポリシーを使用して、バックアップボールトを共有できます。

コピー先のバックアップボールトを AWS アカウント または IAM ロールで共有します。

次のポリシーは、バックアップボールトとアカウント番号の 4444555566666 および SomeRoleアカウント番号 111122223333 の IAM ロールを共有します。

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":{
        "AWS":[
          "arn:aws:iam::444455556666:root",
          "arn:aws:iam::111122223333:role/SomeRole"
```

```
        ]
      },
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*"
    }
  ]
}
```

で組織単位を送信先バックアップボールトを共有する AWS Organizations

次のポリシーでは、PrincipalOrgPaths を使用してバックアップボールトを組織部門と共有します。

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":"*",
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*",
      "Condition":{
        "ForAnyValue:StringLike":{
          "aws:PrincipalOrgPaths":[
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/",
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/ou-jkl0-awsddddd/*"
          ]
        }
      }
    }
  ]
}
```

の組織と送信先バックアップボールトを共有する AWS Organizations

次のポリシーは、バックアップボールトを組織とPrincipalOrgID "o-a1b2c3d4e5"で共有します。

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":"*",
```

```
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*",
      "Condition":{
        "StringEquals":{
          "aws:PrincipalOrgID":[
            "o-a1b2c3d4e5"
          ]
        }
      }
    }
  ]
}
```

アカウントをコピー先アカウントとして設定する

AWS Organizations 管理アカウントを使用してクロスアカウントバックアップを初めて有効にすると、メンバーアカウントのユーザーは、自分のアカウントを送信先アカウントとして設定できます。AWS Organizations で次のサービスコントロールポリシー (SCP) を 1 つ以上設定し、コピー先アカウントを制限することをお勧めします。 AWS Organizations ノードへのサービスコントロールポリシーのアタッチの詳細については、「サービスコントロールポリシーのアタッチとデタッチ」を参照してください。

タグを使用してコピー先アカウントを制限する

AWS Organizations ルート、OU、または個々のアカウントにアタッチされると、このポリシーは、そのルート、OU、またはアカウントから、 にタグ付けしたバックアップボールトを持つアカウントのみに宛先をコピーしますDestinationBackupVault。アクセス許可 `"backup:CopyIntoBackupVault"` は、バックアップボールトの動作を制御し、この場合はどのコピー先バックアップボールトが有効かを制御します。このポリシーと、承認されたコピー先ボールトに適用される対応するタグを使用して、クロスアカウントコピーのコピー先を承認済みアカウントとバックアップボールトのみに制限します。

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Deny",
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*",
      "Condition":{
        "Null":{
```

```
          "aws:ResourceTag/DestinationBackupVault":"true"
        }
      }
    }
  ]
}
```

アカウント番号とボールト名を使用してコピー先アカウントを制限する

AWS Organizations ルート、OU、または個々のアカウントにアタッチすると、このポリシーは、そのルート、OU、またはアカウントから発信されるコピーを 2 つの送信先アカウントのみに制限します。アクセス許可 "backup:CopyFromBackupVault" は、バックアップボールト内の復旧ポイントの動作を制御します。この場合は、その復旧ポイントをコピーできるコピー先も制御されます。コピー元のボールトは、1 つまたは複数のコピー先のバックアップボールト名が cab- で始まる場合のみ、最初のコピー先アカウント (112233445566) へのコピーを許可します。コピー元のボールトは、コピー先が fort-knox という名前の単一バックアップボールトである場合、2 つ目のコピー先アカウント (123456789012) へのコピーのみ許可します。

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Deny",
      "Action":"backup:CopyFromBackupVault",
      "Resource":"arn:aws:ec2:*:snapshot/*",
      "Condition":{
        "ForAllValues:ArnNotLike":{
          "backup:CopyTargets":[
            "arn:aws:backup:*:112233445566:backup-vault:cab-*",
            "arn:aws:backup:us-west-1:123456789012:backup-vault:fort-knox"
          ]
        }
      }
    }
  ]
}
```

で組織単位を使用して送信先アカウントを制限する AWS Organizations

ソースアカウントを含む AWS Organizations ルートまたは OU にアタッチする場合、またはソースアカウントにアタッチする場合、次のポリシーは、宛先アカウントを 2 つの指定された OUs。

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Deny",
      "Action":"backup:CopyFromBackupVault",
      "Resource":"*",
      "Condition":{
        "ForAllValues:StringNotLike":{
          "backup:CopyTargetOrgPaths":[
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/",
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/ou-jkl0-awsddddd/*"
          ]
        }
      }
    }
  ]
}
```

クロスアカウントバックアップのセキュリティに関する考慮事項

AWS Backupでクロスアカウントバックアップを実行する場合は、次の点に注意してください。

- デスティネーションボールトを既定のボールトにすることはできません。これは、デフォルトのボールトが他のアカウントと共有できないキーで暗号化されているためです。
- クロスアカウントバックアップを無効にした後も、クロスアカウントバックアップが最大 15 分間実行されることがあります。これは結果整合性が原因で、クロスアカウントバックアップを無効にした後でも、クロスアカウントジョブが開始または完了することがあります。
- コピー先アカウントが後で組織を離れる場合、そのアカウントはバックアップを保持します。潜在的なデータ漏洩を回避するには、コピー先アカウントにアタッチされたサービスコントロールポリシー (SCP) 内の `organizations:LeaveOrganization` アクセス許可を拒否します。SCP の詳細については、Organizations ユーザーガイドの「組織からのメンバーアカウントの削除」を参照してください。
- クロスアカウントコピー中にコピージョブロールを削除した場合、コピージョブの完了時にソースアカウントからスナップショットの共有を解除 AWS Backup することはできません。この場合、バックアップジョブは終了しますが、コピージョブのステータスは「スナップショットの共有解除に失敗しました。」と表示されます。

バックアップの削除

AWS Backup バックアッププランの作成時にライフサイクルを設定することで、不要になったバックアップを自動的に削除するために を使用することをお勧めします。例えば、バックアッププランのライフサイクルを 1 年間保持するように設定した場合、 AWS Backup は 2022 年 1 月 1 日に、または 2021 年 1 月 1 日から数時間以内に作成した復旧ポイントを自動的に削除します (パフォーマンスを維持するために、復旧ポイントの有効期限が切れてから 8 時間以内に削除をAWS Backup ランダム化します)。ライフサイクル保持ポリシーの設定の詳細については、「バックアッププランの作成」を参照してください。

ただし、1 つまたは複数のリカバリポイントを手動で削除することもできます。例:

- EXPIRED 復旧ポイントがあります。これらは、バックアッププランの作成に使用した元の IAM ポリシーを削除または変更したため、 を自動的に削除 AWS Backup できませんでした。削除 AWS Backup しようとすると、そのアクセス許可が付与されていなかった。

  AWS マネージド Amazon EBS または Amazon EC2 復旧ポイントに Amazon EBS スナップショットロックが適用され、通常は復旧ポイントが削除されるライフサイクルプロセスを完了 AWS Backup できない場合にも、期限切れの復旧ポイントが作成されることがあります。このような期限切れの復旧ポイントは、Amazon EC2 コンソールと API、または Amazon EBS コンソールと API から復元できることに注意してください。

  > ⚠ Warning
  >
  > 期限切れの回復ポイントは引き続きアカウントに保存されます。これにより、ストレージコストが増加する可能性があります。

  2021 年 8 月 6 日以降、 AWS Backup はターゲット復旧ポイントをバックアップボールトに期限切れとして表示します。バックアップを削除できなかった理由を説明するポップオーバーステータスメッセージの赤い [Expired] ステータス上にマウスを置くことができます。[更新] をクリックして、最新の情報を受信します。
- バックアッププランを設定したとおりに動作させたくありません。バックアッププランの更新は、作成する将来のリカバリポイントに影響しますが、すでに作成したリカバリポイントには影響しません。詳細については、「バックアッププランの更新」を参照してください。
- テストやチュートリアルを終えたら、クリーンアップする必要があります。

バックアップを手動で削除する

回復ポイントを手動で削除するには

1. AWS Backup コンソールのナビゲーションペインで、バックアップボールト を選択します。
2. [バックアップボールト] ページで、バックアップを保存したバックアップボールトを選択します。
3. 復旧ポイントを選択し、[アクション] ドロップダウンで、[削除] を選択します。
4. 1. リストに継続的なバックアップが含まれている場合は、次のいずれかのオプションを選択します。各継続的バックアップには、1 つのリカバリポイントがあります。
   - バックアップデータを完全に削除するか復旧ポイントを削除します。これらのオプションのいずれかを選択すると、今後の継続的なバックアップを停止し、既存の継続的なバックアップデータも削除します。

     > **Note**
     >
     > Amazon S3、Amazon RDS、および Aurora の継続的バックアップに関する考慮事項継続的バックアップと point-in-time 復元 (PITR)については、「」を参照してください。

   - 継続的バックアップデータを保持するか、復旧ポイント の関連付けを解除します。これらのオプションのいずれかを選択すると、今後の継続的バックアップは停止しますが、保持期間の定義に従って期限が切れるまで、既存の継続的バックアップデータは保持されます。

     関連付けが解除された Amazon S3 継続的復旧ポイント (バックアップ) はバックアップボールトに残りますが、その状態は に移行しますSTOPPED。

   2. リストされているすべての復旧ポイントを削除するには、delete と入力し、[復旧ポイントの削除] を選択します。
   3. AWS Backup は、削除のために復旧ポイントの送信を開始し、進行状況バーを表示します。ブラウザタブを開いたままにしておき、送信プロセス中はこのページから移動しないでください。
   4. 送信プロセスの最後に、バナーに AWS Backup ステータスが表示されます。このステータスは、
      - 正常に送信されました。各リカバリポイントの削除ステータスについて、[進行状況を閲覧する] を選択することもできます。

- 送信に失敗しました。各リカバリポイントの削除ステータスについて、[進行状況を閲覧する] または、[Try again] を選択することもできます。
- 一部のリカバリポイントが正常に送信され、他のリカバリポイントの送信に失敗した混合結果。

5. 「進行状況を閲覧する」を選択すると、バックアップごとに削除ステータスを確認することができます。削除ステータスが [Failed] または [Expired] の場合、そのステータスをクリックして理由を確認できます。[失敗した削除を再試行する] を選択することもできます。

手動削除のトラブルシューティング

まれに、削除リクエストを完了しない AWS Backup 場合があります。 AWS Backup は、サービスにリンクされたロール`AWSServiceRoleForBackup`を使用して削除を実行します。

削除リクエストが失敗した場合は、IAM ロールにサービスにリンクされたロールを作成するアクセス権限があることを確認します。具体的には、IAM ロールに `iam:CreateServiceLinkedRole` action があることを確認します。そうでない場合は、バックアップの作成に使用したロールにこのアクセス許可を追加します。このアクセス許可を追加する AWS Backup と、 は手動で削除を実行できます。

IAM ロールに `iam:CreateServiceLinkedRole` アクションがある場合、リカバリポイントはまだ `DELETING` ステータスで、お客様の問題を調査している可能性があります。以下の手順で、手動削除を完了します。

1. 2-3 日後に戻ってくるリマインダーを設定します。
2. 2-3日後、最初の手動削除操作の結果である最近の `EXPIRED` 削除ポイントをチェックします。
3. それらの `EXPIRED` 復旧ポイントを手動で削除します。

ロールの詳細については、「サービスにリンクされたロールの使用」と「IAM アイデンティティアクセス許可の追加と削除」を参照してください。

バックアップの編集

を使用してバックアップを作成したら AWS Backup、バックアップのライフサイクルまたはタグを変更できます。ライフサイクルにより、バックアップがいつコールドストレージに移行するか、およびいつ期限切れになるかが定義されます。 AWS Backup は、お客様が定義するライフサイクルに従って自動的にバックアップを移行し、期限切れにします。

コールドストレージに移行できるリソースの一覧については、リソース別の機能の可用性 表の「コールドストレージへのライフサイクル」セクションを参照してください。他のリソースでは、コールドストレージ式は無視されます。

> **Note**
>
> AWS Backup コンソールを使用したバックアップのタグの編集は、Amazon Elastic File System (Amazon EFS) ファイルシステムおよび Advanced Amazon DynamoDB のバックアップでのみサポートされます。
> 他のリソースの作成時に復旧ポイントに追加されたタグは引き続き表示されますが、グレー表示されて編集できません。これらのタグは AWS Backup コンソールでは編集できませんが、サービスのコンソールまたは API を使用して、これらの他のサービスのバックアップのタグを編集できます。

コールドストレージに移行されたバックアップは、そこに最低 90 日保存される必要があります。したがって、「保持期間」の設定は、「コールドへの移行 (日数)」設定から 90 日以上あける必要があります。「コールドへの移行 (日数)」設定を更新する場合、値はバックアップの経過時間 + 1 日以上にする必要があります。バックアップがコールドに移行された後で、「コールドへの移行 (日数)」設定を変更することはできません。

次の例では、バックアップのライフサイクルを更新する方法について説明します。

バックアップのライフサイクルを編集するには

1. にサインインし AWS Management Console、https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[バックアップボールト] を選択します。
3. [Backups (バックアップ)] セクションで、バックアップを選択します。
4. バックアップ詳細ページで、[Edit (編集)] を選択します。
5. ライフサイクル設定を構成して、[Save (保存)] を選択します。

バックアップの復元

復元方法

コンソールの復元手順と、 AWS Backupがサポートする各リソースタイプのドキュメントへのリンクについては、このページの下部にあるリンクを参照してください。

バックアップをプログラムで復元するには、StartRestoreJob API オペレーションを使用します。

リソースの復元に必要な設定値 (「メタデータの復元」) は、復元するリソースによって異なります。バックアップの作成に使用した設定メタデータを取得するには、GetRecoveryPointRestoreMetadata を呼び出します。復元メタデータのサンプルは、このページの下部にあるリンクでもご覧いただけます。

コールドストレージからの復元には、通常、ウォームストレージからの復元よりも 4 時間長くかかります。

復元ごとに、固有のジョブ ID (例: 1323657E-2AA4-1D94-2C48-5D7A423E7394) を持つジョブが作成されます。

> **Note**
>
> AWS Backup は、復元時間に関するサービスレベルアグリーメント (SLAsを提供しません。復元にかかる時間は、同じリソースを含む復元であっても、システムの負荷と容量によって異なる場合があります。

破壊でない復元

AWS Backup を使用してバックアップを復元すると、復元するバックアップを含む新しいリソースが作成されます。これは、復元アクティビティによって既存のリソースが破壊されるのを防ぐためです。

復元テスト

リソースでテストを実施して、復元方法をシミュレートできます。これにより、組織の目標復旧時間 (RTO) を満たしているかどうかを判断し、将来の復元ニーズに備えることができます。

詳細については、「復元テスト」を参照してください。

復元中にタグをコピーする

> **Note**
>
> Amazon EC2 インスタンス、仮想マシン、Amazon Timestream リソース上の Amazon DynamoDB、Amazon S3、SAP HANA の復元では、現在この機能は利用できません。

序章

バックアップ時にタグが、保護されたリソースに属していた場合は、リソースを復元するときにタグをコピーできます。タグは、キーと値のペアを含むラベルで、リソースの特定と検索に役立ちます。復元ジョブを開始すると、バックアップされた元のリソースに属していたタグを、復元対象のリソースに追加できます。

復元ジョブ中にタグの追加を選択すると、復元ジョブの完了後にリソースに手動でタグを適用する手間と労力を省くことができます。これは、復元されたリソースに新しいタグを追加することとは異なることに注意してください。

コンソールフローでバックアップを復元すると、ソースタグがデフォルトでコピーされます。復元されたリソースへのタグのコピーをオプトアウトする場合は、コンソールでチェックボックスをオフにします。

API オペレーション `StartRestoreJob` では、パラメータ `CopySourceTagsToRestoredResource` はデフォルトで `false` に設定され、復元するリソースから元のソースタグが除外されます。元のソースからのタグを含める場合は、これを `True` に設定します。

考慮事項

- リソースには、復元されたリソースを含め、最大 50 個のタグを含めることができます。タグの制限の詳細については、「AWS リソースのタグ付け」を参照してください。
- タグをコピーするための復元用に使用するロールに正しいアクセス許可があることを確認してください。復元用のデフォルトロールには必要なアクセス許可が含まれています。カスタムロールには、リソースにタグを付けるための追加のアクセス許可が含まれている必要があります。
- 現在、復元タグの包含では、VMware Cloud™ on AWS、VMware Cloud™ on AWS Outposts、オンプレミスシステム、Amazon EC2 インスタンス上の SAP HANA、Timestream、DynamoDB 、Advanced DynamoDB 、および Amazon S3 のリソースはサポートされていません。

- 継続的バックアップでは、最新のバックアップ時点で元のリソースにあったタグが、復元されたリソースにコピーされます。
- 項目レベルの復元ではタグはコピーされません。
- バックアップジョブの完了後にバックアップに追加されたタグで、バックアップ前に元のリソースには存在しなかったものは、復元されたリソースにはコピーされません。2023 年 5 月 22 日以降に作成されたバックアップのみが、復元時にタグコピーの対象となります。

タグと特定のリソースとの相互作用

- 「Amazon EC2」
  - 復元された Amazon EC2 インスタンスに適用されるタグは、アタッチされた復元された Amazon EBS ボリュームにも適用されます。
  - ソースインスタンスにアタッチされた EBS ボリュームに適用されたタグは、復元されたインスタンスにアタッチされたボリュームにコピーされません。タグに基づいて EBS ボリュームへのアクセスをユーザーに許可または拒否する IAM ポリシーがある場合は、ポリシーが有効であることを確認するために、復元されたボリュームに必要なタグを手動で再割り当てする必要があります。
- Amazon EFS リソースを復元するときは、新しいファイルシステムにコピーする必要があります。既存のファイルシステムに復元する場合、タグをコピーすることはできません。
- Amazon RDS
  - バックアップされた RDS クラスターがまだアクティブな場合、このクラスターのタグがコピーされます。
  - 元のクラスターがアクティブでなくなった場合は、代わりにクラスターのスナップショットのタグがコピーされます。
  - `CopySourceTagsToRestoredResource` のブール値パラメータが `True` または `False` に設定されているかどうかに関係なく、バックアップ時にリソースに存在していたタグは復元中にコピーされます。ただし、スナップショットにタグが含まれていない場合は、上記のブール値設定が使用されます。
- Amazon Redshift クラスターには、デフォルトで復元ジョブ中にタグが常に含まれます。

コンソール経由でのタグのコピー

1. AWS Backup コンソールを開きます。

2. ナビゲーションペインで、[保護されたリソース] を選択し、復元する Amazon S3 リソース ID を選択します。
3. [リソースの詳細] ページには、選択したリソース ID の復旧ポイントのリストが表示されます。リソースを復元するには:
   a. [バックアップ] ペインで、リソースの復旧ポイント ID を選択します。
   b. ペインの右上隅にある [復元] を選択します (または、バックアップボールトに移動して復元ポイントを探し、[アクション]]、[復元] の順でクリックします)。
4. 「バックアップの復元」ページで、「タグによる復元」という名前のパネルを探します。元のリソースのすべてのタグを含めるには、このボックスをオンのままにします (コンソールでは、このボックスはデフォルトでオンになっていることに注意してください)。
5. 希望の設定とロールをすべて選択したら、[バックアップを復元] をクリックします。

プログラムでタグを含めるには

API オペレーション `StartRestoreJob` を使用します。次のブール値パラメータが `True` に設定されていることを確認します。

```
CopySourceTagsToRestoredResource = true
```

ブール値パラメータが `CopySourceTagsToRestoredResource = True` の場合、復元ジョブは、元のリソースから、復元されたマテリアルにタグをコピーします。

> **Important**
>
> サポートされていないリソース (VMware 、オンプレミスシステム、EC2 インスタンス上の SAP HANA AWS Outposts、Timestream、DynamoDB、Advanced DynamoDB、Amazon S3) にこのパラメータが含まれている場合、復元ジョブは失敗します。

```
{
    "RecoveryPointArn": "arn:aws:ec2:us-east-1::image/ami-1234567890a1b234",
    "Metadata": {
        "InstanceInitiatedShutdownBehavior": "stop",
        "DisableApiTermination": "false",
        "EbsOptimized": "false",
        "InstanceType": "t1.micro",
```

```
        "SubnetId": "subnet-123ab456cd7efgh89",
        "SecurityGroupIds": "[\"sg-0a1bc2d345ef67890\"]",
        "Placement": "{\"GroupName\":null,\"Tenancy\":\"default\"}",
        "HibernationOptions": "{\"Configured\":false}",
        "IamInstanceProfileName": "UseBackedUpValue",
        "aws:backup:request-id": "1a2345b6-cd78-90e1-2345-67f890g1h2ij"
    },
    "IamRoleArn": "arn:aws:iam::123456789012:role/EC2Restore",
    "ResourceType": "EC2",
    "IdempotencyToken": "34ab5678-9012-3c4d-5678-efg9h01f23i4",
    "CopySourceTagsToRestoredResource": true
}
```

タグ復元に関する問題のトラブルシューティング

エラー: アクセス許可が不十分である

対処法: 復元したリソースにタグを追加できるように、復元ロールに必要なアクセス許可があることを確認します。復元用のデフォルトのAWS マネージドサービスロールポリシー にはAWSBackupServiceRolePolicyForRestores、このタスクに必要なアクセス許可が含まれています。

カスタムロールの使用を選択する場合は、以下のアクセス許可があることを確認してください。

- `elasticfilesystem:TagResource`
- `storagegateway:AddTagsToResource`
- `rds:AddTagsToResource`
- `ec2:CreateTags`
- `cloudformation:TagResource`

詳細については、「API アクセス許可」を参照してください。

ジョブステータスの復元

復元ジョブのステータスは、 AWS Backup コンソールの [ジョブ] ページで確認できます。復元ジョブのステータスには、[保留中]、[実行中]、[完了]、[中止]、[失敗] があります。

トピック

- S3 データの復元

- を使用した仮想マシンの復元 AWS Backup
- FSx ファイルシステムの復元
- Amazon EBS ボリュームの復元
- Amazon EFS ファイルシステムの復元
- Amazon DynamoDB テーブルの復元
- RDS データベースの復元
- Amazon Aurora クラスターの復元
- Amazon EC2 インスタンスの復元
- Storage Gateway ボリュームの復元
- Amazon Timestream テーブルを復元する
- Amazon Redshift クラスター を復元する
- Amazon EC2 インスタンスで SAP HANA データベースを復元する
- DocumentDB クラスターの復元
- Neptune クラスターの復元
- CloudFormation スタックバックアップの復元

S3 データの復元

を使用してバックアップした S3 データを S3 Standard ストレージクラス AWS Backup に復元できます。バケット内のすべてのオブジェクトまたは特定のオブジェクトを復元できます。既存のバケットまたは新しいバケットに復元できます。

Amazon S3 の復元アクセス許可

リソースの復元を開始する前に、使用しているロールに十分なアクセス許可があることを確認してください。

詳細については、ポリシーに関する次のエントリを参照してください。

1. `AWSBackupServiceRolePolicyForS3Restore`
2. `AWSBackupServiceRolePolicyForRestores`
3. の管理ポリシー AWS Backup

Amazon S3 の復元に関する考慮事項

- AWS Backup はすべての S3 バージョンのバックアップを作成しますが、いつでもバージョンスタックから最新バージョンのみを復元します。
- 送信先バケットでアクセスコントロールリスト (ACL) を有効にする必要があります。有効にしないと、ジョブは失敗します。ACL を有効にするには、「ACL の設定ページ」の指示に従ってください。
- ソースバケットに同じ名前または同じバージョン ID のオブジェクトがある場合、オブジェクトの復元はスキップされます。
- 特定のオブジェクトを復元すると、オブジェクトの現在のバージョンを復元できます。
- 元の S3 バケットに復元すると、
  - AWS Backup は破壊的な復元を実行しません。つまり、 AWS Backup はバージョンに関係なく、既存のオブジェクトの代わりにバケットにオブジェクトを配置しません。
  - 最新バージョンの削除マーカーはオブジェクトが存在しないものとして扱われるため、復元が発生する可能性があります。
  - AWS Backup は、復元中にバケットからオブジェクト (削除マーカーなし) を削除しません (例: バックアップ中に存在しなかったバケット内のキーは残ります) 。
- クロスリージョンコピーの復元
  - S3 バックアップはクロスリージョンコピーができますが、復元ジョブは元のバックアップまたはコピーが置かれている同じリージョンでのみなされます。

    Example

    例: 米国東部 (バージニア北部) リージョンで作成された S3 バケットは、カナダ (中部) リージョンにコピーできます。復元ジョブは、米国東部 (バージニア北部) リージョンの元のバケットを使用して開始し、そのリージョンに復元できます。または、カナダ (中部) リージョンのコピーを使用して復元ジョブを開始し、そのリージョンに復元することもできます。
  - 元の暗号化メソッドを使用して、別のリージョンからコピーされた復旧ポイント (バックアップ) を復元することはできません。クロスリージョンコピー AWS KMS 暗号化は Amazon S3 リソースでは使用できません。代わりに、復元ジョブに別の暗号化タイプを使用します。

AWS Backup コンソールを使用して Amazon S3 復旧ポイントを復元する

AWS Backup コンソールを使用して Amazon S3 データを復元するには：

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[保護されたリソース] を選択し、復元する Amazon S3 リソース ID を選択します。
3. [リソースの詳細] ページには、選択したリソース ID の復旧ポイントのリストが表示されます。リソースを復元するには:

   a. [バックアップ] ペインで、リソースの復旧ポイント ID を選択します。

   b. ペインの右上隅にある [復元] を選択します。

      (または、バックアップボールトに移動して復旧ポイントを探し、[アクション]、[復元] の順にクリックすることもできます)。
4. 継続的バックアップを復元する場合は、[復元時刻] ペインで、次のいずれかのオプションを選択します。

   a. デフォルトをそのまま使用して、[復元可能な最新の時刻] に復元します。

   b. [日付および時刻を指定] をクリックして、復元します。
5. [設定] ペインで、バケット全体を復元するか、項目レベルの復元を実行するかどうかを指定します。

   a. 項目レベルの復元 を選択した場合、各項目の S3 URI を指定して、そのオブジェクトを一意に識別することで、復元ジョブごとに最大 5 つの項目 (バケット内のオブジェクトまたはフォルダ) を復元します。

      S3 バケット URI の詳細については、「Amazon Simple Storage Service ユーザーガイド」の「バケットにアクセスするためのメソッド」を参照してください。

   b. [アイテムを追加] をクリックして、復元する別のアイテムを指定します。
6. [復元先] を選択します。ソースバケットに復元する、既存のバケットを使用する、または新しいバケットの作成のいずれかを実行できます。

> **Note**
>
> 復元先バケットでバージョニングが有効になっている必要があります。選択したバケットがこの要件を満たしていない場合は、 から AWS Backup 通知されます。

a. 既存のバケットを使用する を選択した場合は、ドロップダウンメニューから送信先 S3 バケットを選択します。このバケットには、現在の AWS リージョン内のすべての既存のバケットが表示されます。

b. [新しいバケットの作成] を選択すると、[新しいバケット名] が入力されます。新しいバケットはデフォルトで S3 バージョニングが有効になっています。パブリックアクセスのブロック (BPA) 設定はデフォルトでオフに切り替わります。S3 でバケットを作成した後で、これらの設定を変更できます。

7. S3 バケット内のオブジェクトの暗号化には、復元されたオブジェクトの暗号化 を選択できます。[元の暗号化キーを使用 (デフォルト)]、[Amazon S3 キー (SSE-S3)]、または [AWS Key Management Service キー (SSE-KMS)] を使用してください。

   これらの設定は、S3 バケット内のオブジェクトの暗号化にのみ適用されます。これはバケット自体の暗号化には影響しません。

   a. 元の暗号化キーを使用する (デフォルト) は、ソースオブジェクトで使用されるのと同じ暗号化キーを持つオブジェクトを復元します。ソースオブジェクトが暗号化されていない場合、このメソッドは暗号化なしでオブジェクトを復元します。

      この復元オプションでは、オプションで代替の暗号化キーを選択して、元のキーが使用できない場合は復元オブジェクトを暗号化できます (複数可) 。

   b. [Amazon S3 キー (SSE-S3)] を選択した場合は、他のオプションを指定する必要はありません。

   c. AWS Key Management Service キー (SSE-KMS) を選択した場合、AWS マネージドキー (aws/s3)、 AWS KMS キーから選択、または AWS KMS キー ARN を入力を選択できます。

      i. AWS マネージドキー (aws/s3) を選択した場合は、他のオプションを指定する必要はありません。

      ii. AWS KMS キー から選択する場合は、ドロップダウンメニューからキーを選択します AWS KMS 。または、[キーの作成] を選択します。

      iii. AWS KMS キー ARN を入力する場合は、テキストボックスに ARN を入力します。または、[キーの作成] を選択します。

8. [ロールを復元] ペインで、この復元のために AWS Backup が引き受ける IAM ロールを選択します。

9. [バックアップを復元] を選択します。[復元ジョブ] ペインが表示されます。ページ上部のメッセージには、復元ジョブに関する情報が表示されます。

AWS Backup API、CLI、または SDK を使用して Amazon S3 リカバリポイントを復元する

StartRestoreJob を使用します。Amazon S3 復元中に、以下のメタデータを指定できます。

```
// Mandatory metadata:
DestinationBucketName // The destination bucket for your restore.
ItemsToRestore // A list of up to five paths of individual objects to restore. Only
 required for item-level restore.
NewBucket // Boolean to indicate whether to create a new bucket.
Encrypted // Boolean to indicate whether to encrypt the restored data.
CreationToken // An idempotency token.
EncryptionType // The type of encryption to encrypt your restored objects. Options
 are original (same encryption as the original object), SSE-S3, or SSE-KMS).
RestoreTime // The restore time (only valid for continuous recovery points where it is
 required, in format 2021-11-27T03:30:27Z).

// Optional metadata:
KMSKey // Specifies the SSE-KMS key to use. Only needed if encryption is SSE-KMS.
aws:backup:request-id
```

復旧ポイントのステータス

復旧ポイントには、その状態を示すステータスが表示されます。

PARTIAL ステータスは、バックアップウィンドウが閉じられる前にリカバリポイントを作成 AWS Backup できなかったことを示します。API を使用してバックアッププランウィンドウを増やすには、「」を参照してくださいUpdateBackupPlan。コンソールを使用して、バックアッププランを選択、編集して、バックアッププランのウィンドウを増やすこともできます。

EXPIRED ステータスは、復旧ポイントが保持期間を超過したが、アクセス許可 AWS Backup がないか、削除できないことを示します。これらの復旧ポイントを手動で削除するには、「開始方法」の「リソースのクリーンアップ」セクションの「ステップ 3: 復旧ポイントの削除」を参照してください。

STOPPED ステータスは、継続的バックアップが無効になるような操作をユーザーが行った場合の継続的バックアップ時に発生します。これは、アクセス許可の削除、バージョニングの無効化、Amazon に送信されるイベントの無効化 EventBridge、または によって設定された EventBridge ルールの無効化が原因である可能性があります AWS Backup。

STOPPED ステータスを解決するには、要求されたアクセス許可がすべて揃っていて、S3 バケットでバージョニングが有効になっていることを確認してください。これらの条件が満たされると、実行されるバックアップルールの次のインスタンスでは、新しい継続的復旧ポイントが作成されます。停止ステータスの復旧ポイントは削除する必要はありません。

を使用した仮想マシンの復元 AWS Backup

仮想マシンは、VMware 、VMware Cloud on AWS、VMware Cloud on AWS Outposts、Amazon EBS ボリューム、または Amazon EC2 インスタンス に復元できます。仮想マシンを EC2 に復元 (または移行) するにはライセンスが必要です。デフォルトでは、 にはライセンス AWS が含まれます (料金が適用されます) 。詳細については、VM Import/Export ユーザーガイドの「ライセンスオプション」を参照してください。

VMware 仮想マシンは、 AWS Backup コンソールまたは を使用して復元できます AWS CLI。仮想マシンが復元されると、VMware Tools フォルダは含まれません。VMware Tools を再インストールするには、VMware のドキュメントを参照してください。

AWS Backup 仮想マシンの復元は非破壊的です。つまり、復元中に既存の仮想マシンが上書き AWS Backup されることはありません。代わりに、復元ジョブは新しい仮想マシンをデプロイします。

タスク

- VM を Amazon EC2 インスタンスに復元する際の考慮事項
- AWS Backup コンソールを使用して仮想マシンの復旧ポイントを復元する
- を使用して仮想マシンの復旧ポイントを復元 AWS CLI する

VM を Amazon EC2 インスタンスに復元する際の考慮事項

- 仮想マシンを EC2 に復元 (または移行) するにはライセンスが必要です。デフォルトでは、 AWS にはライセンスが含まれます (有料)。詳細については、VM Import/Export ユーザーガイドの「ライセンスオプション」を参照してください。
- 各仮想マシンのディスクには 5 TB (テラバイト) の上限があります。
- 仮想マシンをインスタンスに復元するときにキーペアを指定することはできません。キーペアは、起動`authorized_keys`中 (インスタンスユーザーデータを使用) または起動後 (Amazon EC2 ユーザーガイドのこのトラブルシューティングセクションで説明) に追加できます。
- VM Import/Export ユーザーガイドのAmazon EC2 へのインポートとエクスポートがオペレーティングシステムでサポートされていることを確認します」。

- VM Import/Export ユーザーガイドの VMsAmazon EC2 への VM のインポートに関する制限事項」を確認してください。
- を使用して Amazon EC2 インスタンスに復元する場合は AWS CLI、 を指定する必要があります`"RestoreTo":"EC2Instance"`。他のすべての属性にはデフォルト値があります。

AWS Backup コンソールを使用して仮想マシンの復旧ポイントを復元する

AWS Backup コンソールの左側のナビゲーションペインにある複数の場所から仮想マシンを復元できます。

- Hypervisor を選択して、 AWS Backupに接続されているハイパーバイザーによって管理されている仮想マシンのリカバリポイントを表示します。
- 仮想マシンを選択して、 AWS Backupに接続されているすべてのハイパーバイザの仮想マシンのリカバリポイントを表示します。
- バックアップボールトを選択すると、特定の AWS Backup ボールトに保存されている復旧ポイントが表示されます。
- 保護されたリソースを選択すると、 AWS Backup 保護されたすべてのリソースの復旧ポイントが表示されます。

Backup ゲートウェイとの接続がなくなった仮想マシンを復元する必要がある場合は、[バックアップボールト] または [保護されたリソース] の順にクリックして、復元ポイントを確認します。

オプション

- VMware への復元
- Amazon EBS ボリュームへの復元
- Amazon EC2 インスタンスへの復元

仮想マシンを VMware 、VMware Cloud on AWS、および VMware Cloud on に復元するには AWS Outposts

1. [ハイパーバイザー] ビューまたは [仮想マシン] ビューで、復元する VM 名を選択します。[保護されたリソース] ビューで、仮想マシンの表示、選択リソース ID をクリックして、復元します。
2. [復元ポイント ID] の横にある放射状ボタンをクリックして、復元します。

3. [復元] を選択します。
4. [復元タイプ] を選択します。

   a. 完全な復元では、仮想マシンのすべてのディスクが復元されます。

   b. ディスクレベル復元では、ユーザーが定義した 1 つ以上のディスクを復元します。ドロップダウンメニューを使用して、復元するディスクを選択します。

5. [復元場所] を選択します。オプションは、VMware、VMware Cloud on AWS、VMware Cloud on AWS Outpostsです。
6. 完全な復元を実行する場合は、次のステップに進んでください。ディスクレベル復元を実行する場合、VM ディスクの下にドロップダウンメニューが表示されます。復元するブートできるボリュームを 1 つ以上選択します。
7. ドロップダウンメニューから Hypervisor を選択し、復元された仮想マシンを管理する
8. 復元された仮想マシンについては、組織の仮想マシンのベストプラクティスを使用して、以下を指定します。

   a. 名前

   b. パス (`/datacenter/vm` など)

   c. コンピューティングリソース名 (VMHost やクラスタなど)

      ホストがクラスターの一部である場合、そのホストには復元できず、特定のクラスターにのみ復元できます。

   d. データストア

9. ロールの復元を使用する場合、次のいずれかを選択します。デフォルトロール (推奨) またはドロップダウンメニューを使用して、IAM ロールを選択する。
10. [バックアップを復元] を選択します。
11. オプション: 復元ジョブのステータスが `Completed` となっているタイミングを確認します。左のナビゲーションペインで [ジョブ] を選択します。

仮想マシンを Amazon EBS ボリュームに復元するには

1. [ハイパーバイザー] ビューまたは [仮想マシン] ビューで、復元する VM 名を選択します。[保護されたリソース] ビューで、仮想マシンの表示、選択リソース ID をクリックして、復元します。
2. [復元ポイント ID] の横にある放射状ボタンをクリックして、復元します。

3. [復元] を選択します。
4. [復元タイプ] を選択します。

   - ディスク復元では、ユーザーが定義した 1 つのディスクを復元します。ドロップダウンメニューを使用して、復元するディスクを選択します。

5. [復元場所] を [Amazon EBS] として選択します。
6. [VM ディスク] ドロップダウンメニューで、復元するブートできるボリュームを選択します。
7. [EBS ボリュームタイプ] では、ボリュームタイプを選択します。
8. アベイラビリティーゾーンを選択します。
9. 暗号化 (オプション)。EBS ボリュームを暗号化する場合は、このボックスをオンにします。
10. メニューから KMS キーを選択します。
11. ロールを復元するには、デフォルトロール (推奨) または IAM ロール を選択します。
12. [バックアップを復元] を選択します。
13. オプション: 復元ジョブのステータスが `Completed` となっているタイミングを確認します。左のナビゲーションペインで [ジョブ] を選択します。
14. オプション: マネージドボリュームをマウントし、復元した Amazon EBS ボリューム上のデータにアクセスする方法の詳細については、「Amazon EBS ボリューム全体で LVM 論理ボリュームを作成する方法を教えてください」をご覧ください。

仮想マシンを Amazon EC2 インスタンスに復元するには

1. [ハイパーバイザー] ビューまたは [仮想マシン] ビューで、復元する VM 名を選択します。[保護されたリソース] ビューで、仮想マシンの表示、選択リソース ID をクリックして、復元します。
2. [復元ポイント ID] の横にある放射状ボタンをクリックして、復元します。
3. [復元] を選択します。
4. [復元タイプ] を選択します。

   - 完全な復元では、ルートレベルのフォルダとファイルを含め、ファイルシステムが完全に復元されます。

5. [復元場所] を [Amazon EC2] として選択します。
6. インスタンスタイプ で、新しいインスタンスでアプリケーションを実行するために必要なコンピューティングとメモリの組み合わせを選択します。

> **Tip**
>
> 元の仮想マシンの仕様と一致するか、それを超えるインスタンスタイプを選択します。詳細については、「Amazon EC2 インスタンスタイプガイド」を参照してください。

7. Virtual Private Cloud (VPC) では、インスタンスのネットワーク環境を定義する Virtual Private Cloud (VPC) を選択します。
8. サブネット で、VPC 内のサブネットのいずれかを選択します。インスタンスは、サブネットアドレス範囲からプライベート IP アドレスを受け取ります。
9. セキュリティグループ では、インスタンスへのトラフィックのファイアウォールとして機能するセキュリティグループを選択します。
10. ロールの復元 で、デフォルトロール (推奨) または IAM ロール を選択します。
11. オプション： 起動時にインスタンスでスクリプトを実行するには、詳細設定を展開し、スクリプトをユーザーデータ に入力します。
12. [バックアップを復元] を選択します。
13. オプション: 復元ジョブのステータスが `Completed` となっているタイミングを確認します。左のナビゲーションペインで [ジョブ] を選択します。

を使用して仮想マシンの復旧ポイントを復元 AWS CLI する

`StartRestoreJob` を使用します。

Amazon EC2 および Amazon EBS に仮想マシンを復元する場合は、以下のメタデータを指定できます。

```
RestoreTo
InstanceType
VpcId
SubnetId
SecurityGroupIds
IamInstanceProfileName
InstanceInitiatedShutdownBehavior
HibernationOptions
DisableApiTermination
Placement
CreditSpecification
RamdiskId
```

```
KernelId
UserData
EbsOptimized
LicenseSpecifications
KmsKeyId
AvailabilityZone
EbsVolumeType
IsEncrypted
ItemsToRestore
RequireIMDSv2
```

VMware 、VMware Cloud on 、VMware Cloud VMware on AWS Outpost への仮想マシンの復元には AWS、次のメタデータを指定できます。 VMware

```
RestoreTo
HypervisorArn
VMName
VMPath
ComputeResourceName
VMDatastore
DisksToRestore
ItemsToRestore
```

この例では、VMware への完全な復元を実行する方法を示します。

```
'{"RestoreTo":"VMware","HypervisorArn":"arn:aws:backup-gateway:us-
east-1:209870788375:hypervisor/hype-9B1AB1F1","VMName":"name","VMPath":"/Labster/
vm","ComputeResourceName":"Cluster","VMDatastore":"vsanDatastore","DisksToRestore":"[{\"DiskId
\":\"2000\",\"Label\":\"Hard disk 1\"}]","vmId":"vm-101"}'
```

FSx ファイルシステムの復元

AWS Backup を使用して Amazon FSx ファイルシステムを復元する場合に使用できる復元オプションは、ネイティブ Amazon FSx バックアップを使用する場合と同じです。バックアップの復旧ポイントを使用して、新しいファイルシステムを作成し、別のファイルシステムの point-in-time スナップショットを復元できます。

Amazon FSx ファイルシステムを復元する場合、 は新しいファイルシステム AWS Backup を作成し、データを入力します (Amazon FSx for NetApp ONTAP では、ボリュームを既存のファイルシステムに復元できます) 。これは、ネイティブの Amazon FSx がファイルシステムをバックアップお

よび復元する方法に似ています。新しいファイルシステムへのバックアップの復元には、新しいファイルシステムの作成と同じ時間がかかります。バックアップから復元されたデータは、ファイルシステムに遅延ロードされます。したがって、プロセス中にレイテンシーがわずかに長くなる可能性があります。

> **Note**
>
> 既存の Amazon FSx ファイルシステムに復元することはできません。また、個々のファイルやフォルダを復元することはできません。
> FSx for ONTAP は、DP (データ保護) ボリューム、LS (ロード共有) ボリューム、フルボリューム、ファイルシステム上のフルボリュームなど、特定のボリュームタイプのバックアップをサポートしていません。詳細については、「FSx for ONTAP のバックアップの使用」を参照してください。
> AWS Backup Amazon FSx ファイルシステムの復旧ポイントを含むボールトは、 の外部に表示されます AWS Backup。Amazon FSx を使用してリカバリポイントを復元することはできますが、削除することはできません。

組み込みの Amazon FSx 自動バックアップ機能によって作成されたバックアップは、 AWS Backup コンソールから確認できます。を使用してこれらのバックアップを復元することもできます AWS Backup。ただし、これらのバックアップを削除したり、 を使用して Amazon FSx ファイルシステムの自動バックアップスケジュールを変更したりすることはできません AWS Backup。

AWS Backup コンソール、API、または AWS Backup を使用して作成されたバックアップを復元できます AWS CLI。このセクションでは、 AWS Backup コンソールを使用して Amazon FSx ファイルシステムを復元する方法について説明します。

AWS Backup コンソールを使用して Amazon FSx リカバリポイントを復元する

FSx for Windows File Server ファイルシステムの削除

FSx for Windows File Server ファイルシステムを削除するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[Protected resources (保護されたリソース)] を選択し、復元する Amazon FSx リソース ID を選択します。
3. [リソースの詳細] ページには、選択したリソース ID の復旧ポイントのリストが表示されます。リソースのリカバリポイント ID を選択します。

4. ペインの右上隅にある [復元] をクリックして、バックアップの復元ページを開きます。
5. [ファイルシステムの詳細] セクションで、バックアップの ID は [Backup ID] で示し、ファイルシステムの種類を [ファイルシステムのタイプ] で示します。FSx for Windows File Server と FSx for Lustre ファイルシステムの両方を復元できます。
6. [デプロイタイプ] にデフォルトを入力します。復元中にファイルシステムのデプロイメントタイプを変更することはできません。
7. [ストレージタイプ] を選択して使用します。ファイルシステムのストレージ容量が 2,000 GiB 未満の場合は、HDDストレージタイプを使用できません。
8. [スループット容量] で、[推奨スループット容量] を選択して推奨される 16 MB /秒 (MBps) レートを使用するか、スループット容量の指定を選択して新しいレートを入力します。
9. [Network and Security] セクションで、必要な情報を入力します。
10. FSx for Windows File Server システムを復元する場合は、Windows 認証ファイルシステムへのアクセスに使用される情報。新しいファイルを作成することもできます。

    > **Note**
    >
    > バックアップを復元するときに、ファイルシステム上の Active Directory のタイプを変更することはできません。

    Microsoft Active Directory の詳細については、「FSx for Windows File Server ユーザーガイド」の「Amazon FSx for Windows File Server でアクティブディレクトリを操作する」を参照してください。
11. (オプション) [バックアップとメンテナンス] セクションで、バックアップ設定を行うための情報を入力します。
12. [復元ロール] セクションで IAM ロールを選択し、 AWS Backup を使用して、お客様に代わってバックアップを作成および管理します。このデフォルトロールを選択することが推奨されます。デフォルトロールがアカウントに存在しない場合は、適切なアクセス許可を備えたものが自動的に作成されます。独自の IAM ロールを指定することもできます。
13. すべてのエントリを確認し、[バックアップの復元] を選択します。

Amazon FSx for Lustre ファイルシステムの作成

AWS Backup は、永続的ストレージデプロイタイプを持ち、Amazon S3 などのデータリポジトリにリンクされていない Amazon FSx for Lustre ファイルシステムをサポートします。

Amazon FSx for Lustre ファイルシステムを作成するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[Protected resources (保護されたリソース)] を選択し、復元する Amazon FSx リソース ID を選択します。
3. [リソースの詳細] ページには、選択したリソース ID の復旧ポイントのリストが表示されます。リソースのリカバリポイント ID を選択します。
4. ペインの右上隅にある [復元] をクリックして、[Restore backup to new file system] ページを開きます。
5. [設定] セクションで、バックアップの ID は [Backup ID] で示し、ファイルシステムの種類を [ファイルシステムのタイプ] で示します。ファイルシステムのタイプは [Lustre] になっている必要があります。
6. (オプション) [Name (名前)] にファイルシステムの名前を入力します。
7. デプロイタイプ を選択します。 は永続デプロイタイプ AWS Backup のみをサポートします。復元中にファイルシステムのデプロイメントタイプを変更することはできません。

   永続的なデプロイタイプは、長期保存用です。FSx for Lustre デプロイオプションの詳細については、「Amazon FSx for Lustre ユーザーガイド」の「Amazon FSx for Lustre ファイルシステムで使用可能なデプロイオプションを使用する」を参照してください。
8. 使用する [ユニットストレージあたりのスループット] を選択します。
9. [ストレージキャパシティ] を指定します。32 GiB から 64,436 GiB の間の容量を入力します。
10. [Network and Security] セクションで、必要な情報を入力します。
11. (オプション) [バックアップとメンテナンス] セクションで、バックアップ設定を行うための情報を入力します。
12. [復元ロール] セクションで IAM ロールを選択し、 AWS Backup を使用して、お客様に代わってバックアップを作成および管理します。このデフォルトロールを選択することが推奨されます。デフォルトロールがアカウントに存在しない場合は、適切なアクセス許可を備えたものが自動的に作成されます。IAM ロールを指定することもできます。
13. すべてのエントリを確認し、[バックアップを復元] を選択します。

Amazon FSx for NetApp ONTAP ボリュームの復元

Amazon FSx for NetApp ONTAP ボリュームを復元するには：

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

2. ナビゲーションペインで、[Protected resources (保護されたリソース)] を選択し、復元する Amazon FSx リソース ID を選択します。
3. [リソースの詳細] ページには、選択したリソース ID の復旧ポイントのリストが表示されます。リソースのリカバリポイント ID を選択します。
4. ペインの右上隅にある [Restore] (復元) をクリックして、[Restore] (復元) ページを開きます。

   最初のセクションである [File system details] (ファイルシステムの詳細) には、リカバリポイント ID、ファイルシステム ID、ファイルシステムタイプが表示されます。
5. [Restore options] (復元オプション) には、複数の選択肢があります。まず、ドロップダウンメニューから [File system] (ファイルシステム) を選択します。
6. 次に、ドロップダウンメニューから優先する [Storage virtual machine] (ストレージ仮想マシン) を選択します。
7. ボリューム名を入力します。
8. ボリュームがマウントされるファイルシステム内の場所である [Junction Path] (ジャンクションパス) を指定します。
9. 作成する [Volume size] (ボリュームサイズ) をメガバイト (MB) 単位で指定します。
10. (オプション) チェックボックスをオンにすると、[Enable storage efficiency] (ストレージ効率を有効にする) を選択できます。これにより、重複排除と圧縮が可能になります。
11. [Capacity pool tiering policy] (容量プールの階層化ポリシー) ドロップダウンメニューで、階層設定を選択します。
12. 復元アクセス許可 AWS Backup で、バックアップの復元に使用する IAM ロールを選択します。
13. すべてのエントリを確認し、[バックアップを復元] を選択します。

Amazon FSx for OpenZFS ファイルシステムの復元

FSx for OpenZFS ファイルシステムを復元するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[Protected resources (保護されたリソース)] を選択し、復元する Amazon FSx リソース ID を選択します。
3. [リソースの詳細] ページには、選択したリソース ID の復旧ポイントのリストが表示されます。リソースのリカバリポイント ID を選択します。
4. ペインの右上隅にある [復元] をクリックして、バックアップの復元ページを開きます。

[ファイルシステムの詳細] セクションで、バックアップの ID は [Backup ID] で示し、ファイルシステムの種類を [ファイルシステムのタイプ] で示します。ファイルシステムのタイプは FSx for OpenZFS でなければなりません。

5. [復元オプション] では、[クイック復元] または [標準復元] を選択できます。クイック復元では、ソースファイルシステムのデフォルト設定が使用されます。クイック復元を行う場合は、ステップ 7 に進みます。

   標準復元を選択した場合は、以下の設定を追加で指定します。

   a. プロビジョンド SSD IOPS: 自動ラジオボタンを選択するか、可能な場合は [ユーザープロビジョニングオプション] を選択できます。

   b. スループットキャパシティ: 64MB/秒の [推奨スループットキャパシティ] を選択するか、[スループットキャパシティを指定する] を選択できます。

   c. (オプション) VPC セキュリティグループ: [VPC セキュリティグループ] を指定して、ファイルシステムのネットワークインターフェイスに関連付けることができます。

   d. 暗号化キー : AWS Key Management Service キーを指定して、復元された保管中のファイルシステムデータを保護します。

   e. (オプション) ルートボリューム設定: この設定はデフォルトでは折りたたまれています。[下向きのカラット (矢印)] をクリックすると展開できます。バックアップからファイルシステムを作成すると、新しいファイルシステムが作成されます。ボリュームとスナップショットは、ソースの設定を保持します。

   f. (オプション) バックアップとメンテナンス: スケジュールされたバックアップを設定するには、[下向きのカラット (矢印)] をクリックしてセクションを展開します。バックアップウィンドウ、時間と分、保持期間、週ごとのメンテナンスウィンドウを選択できます。

6. (オプション) ボリューム名を入力できます。

7. SSD ストレージ容量には、ファイルシステムのストレージ容量が表示されます。

8. ファイルシステムにアクセスできる [仮想プライベートクラウド (VPC)] を選択します。

9. [サブネット] ドロップダウンメニューで、ファイルシステムのネットワークインターフェイスが存在するサブネットを選択します。

10. 「ロールの復元」セクションで、 AWS Backup がユーザーに代わってバックアップを作成および管理するために使用する IAM ロールを選択します。このデフォルトロールを選択することが推奨されます。デフォルトロールがアカウントに存在しない場合は、適切なアクセス許可を備えたものが自動的に作成されます。IAM ロールも選択できます。

11. すべてのエントリを確認し、[バックアップを復元] を選択します。

AWS Backup API、CLI、または SDK を使用して Amazon FSx リカバリポイントを復元する

API または CLI を使用して Amazon FSx を復元するには、`StartRestoreJob` を使用します。Amazon FSx の復元中に、次のメタデータを指定できます。

```
FileSystemId
FileSystemType
StorageCapacity
StorageType
VpcId
KmsKeyId
SecurityGroupIds
SubnetIds
DeploymentType
WeeklyMaintenanceStartTime
DailyAutomaticBackupStartTime
AutomaticBackupRetentionDays
CopyTagsToBackups
WindowsConfiguration
LustreConfiguration
OntapConfiguration
OpenZFSConfiguration
aws:backup:request-id
```

FSx for Windows File Server メタデータの復元

FSx for Windows File Server のリストア中に、次のメタデータを指定できます。

- ThroughputCapacity
- PreferredSubnetId
- ActiveDirectoryId

FSx for Lustre メタデータの復元

FSx for Lustre の復元中に、次の `PerUnitStorageThroughput` および `DriveCacheType` を指定できます。

FSx for ONTAP の復元メタデータ

FSx for ONTAP の復元中に、次のメタデータを指定できます。

- 作成するボリュームの名前 #name
- OntapConfiguration: # ontap 設定
- `junctionPath`
- `sizeInMegabytes`
- `storageEfficiencyEnabled`
- `storageVirtualMachineId`
- `tieringPolicy`

FSx for OpenZFS メタデータの復元

FSx for OpenZFS の復元中に、次のメタデータを指定できます。

- `ThroughputCapacity`
- `DesklopsConfiguration`
- IOPS を指定する場合、0 から 160,000 までの値を含める必要がありますが、モードは含めないでください。

CLI 復元コマンドの例

```
aws backup start-restore-job --recovery-point-arn "arn:aws:fsx:us-west-2:1234:backup/
backup-1234" --iam-role-arn "arn:aws:iam::1234:role/Role" --resource-
type "FSx" --region us-west-2 --metadata 'SubnetIds="[\"subnet-1234\",
\"subnet-5678\"]",StorageType=HDD,SecurityGroupIds="[\"sg-bb5efdc4\",
\"sg-0faa52\"]",WindowsConfiguration="{\"DeploymentType\": \"MULTI_AZ_1\",
\"PreferredSubnetId\": \"subnet-1234\",\"ThroughputCapacity\": \"32\"}"'
```

メタデータの復元例:

```
"restoreMetadata":  "{\"StorageType\":\"SSD\",\"KmsKeyId\":\"arn:aws:kms:us-
east-1:123456789012:key/123456a-123b-123c-defg-1h2i2345678\",\"StorageCapacity
\":\"1200\",\"VpcId\":\"vpc-0ab0979fa431ad326\",\"FileSystemType\":\"LUSTRE\",
\"LustreConfiguration\":\"{\\\"WeeklyMaintenanceStartTime\\\":\\\"4:10:30\\\",\\
\"DeploymentType\\\":\\\"PERSISTENT_1\\\",\\\"PerUnitStorageThroughput\\\":50,\\
\"CopyTagsToBackups\\\":true}\",\"FileSystemId\":\"fs-0ca11fb3d218a35c2\",\"SubnetIds
\":\"[\\\"subnet-0e66e94eb43235351\\\"]\"}"
```

Amazon EBS ボリュームの復元

Amazon Elastic Block Store (Amazon EBS) スナップショットを復元すると、 は Amazon EC2 インスタンスにアタッチできる新しい Amazon EBS ボリューム AWS Backup を作成します。

スナップショットを EBS ボリュームとして復元するか、 AWS Storage Gateway ボリュームとして復元するかを選択できます。

AWS Backup コンソールを使用して Amazon EBS 復旧ポイントを復元する

Amazon EBS ボリュームを復元するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[Protected resources (保護されたリソース)] を選択し、復元する EBS リソース ID を選択します。
3. [リソースの詳細] ページには、選択したリソース ID の復旧ポイントのリストが表示されます。リソースを復元するには、[バックアップ] ペインで、リソースの復旧ポイント ID の横にあるラジオボタンをクリックします。ペインの右上隅にある [復元] を選択します。
4. リソースの復元パラメータを指定します。入力する復元パラメータは、選択したリソースタイプに固有です。

   リソースタイプ で、このバックアップを復元するときに作成する AWS リソースを選択します。
5. [EBS ボリューム] を選択した場合は、[ボリュームタイプ]、[サイズ (GiB)] の値を指定し、[アベイラビリティーゾーン] を選択します。

   - スループットの後に、オプションで [このボリュームを暗号化する] チェックボックスが表示されます。EBS 復旧ポイントが暗号化されている場合、このオプションはアクティブなままになります。

     KMS キーを指定するか、 AWS KMS キーを作成できます。

   Storage Gateway ボリュームを選択すると、到達可能な状態のゲートウェイが選択されます。また、iSCSI ターゲット名も選択してください。

   - 保管型ボリュームゲートウェイを使用する場合、ディスク ID を選択してください。
   - キャッシュボリュームゲートウェイを使用する場合、少なくとも保護されたリソースと同じ大きさの容量を選択します。

6. 復元ロール で、この復元のために AWS Backup が引き受ける IAM ロールを選択します。

> **Note**
>
> アカウントに AWS Backup デフォルトのロールが存在しない場合、適切なアクセス許可を持つデフォルトのロールが作成されます。このデフォルトロールを削除するか、使用不能にすることができます。

7. [バックアップを復元] を選択します。

   [復元ジョブ] ペインが表示されます。ページ上部のメッセージには、復元ジョブに関する情報が表示されます。

アーカイブされた EBS スナップショットを復元する場合、スナップショットが一時的にコールドストレージからウォームストレージに移動し、新しい EBS ボリュームが作成されます。この種の復元では、1 回限りの取り出し料金が発生します。この復元期間中に、ウォームストレージとコールドストレージの両方のストレージコストが請求されます。コールドストレージの EBS ボリュームを Backup ゲートウェイボリュームに復元することはできません。

コールドストレージにアーカイブされた EBS スナップショットは、AWS Backup コンソールまたはコマンドラインを使用して復元できます。コールドストレージからの復元には最大 72 時間かかる場合があります。詳細については、「Amazon EBS ユーザーガイド」の「Amazon EBS スナップショットのアーカイブ」を参照してください。

Console

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. [バックアップボールト] > *[####]* > [アーカイブされた EBS スナップショットを復元する] に移動します。
3. [設定] セクションで、アーカイブされたスナップショットを一時的に復元する日数を、0 ~ 180 の値を入力して指定します。
4. その他の設定 (ボリュームタイプ、サイズ、IOPS、アベイラビリティーゾーン、スループット、暗号化) を入力します。
5. 使用している復元ロールを選択します。
6. [バックアップを復元] を選択します。確認ポップアップでスナップショットと復元タイプを確認します。次に、[スナップショットを復元] を選択します。

AWS CLI

1. start-restore-job を使用します。
2. パラメータを指定します。
3.
4.
5.

AWS Backup API、CLI、または SDK を使用して Amazon EBS リカバリポイントを復元する

API または CLI を使用して Amazon EBS を復元するには、StartRestoreJob を使用します。Amazon EBS の復元中に、次のメタデータを指定できます。

```
availabilityZone
volumeType
volumeSize
iops
throughput
temporaryRestoreDays
encrypted // if set to true, encryption will be enabled as volume is restored
kmsKeyId // if included, this key will be used to encrypt the restored volume instead
 of default KMS Key Id
aws:backup:request-id
```

例：

```
"restoreMetadata": "{\"encrypted\":\"false\",\"volumeId\":\"vol-04cc95f3490b5ceea\",
\"availabilityZone\":null}"
```

Amazon EFS ファイルシステムの復元

Amazon Elastic File System (Amazon EFS) インスタンスを復元する場合、完全な復元または項目レベルの復元を実行できます。

完全な復元

完全な復元を実行すると、ファイルシステム全体が復元されます。

AWS Backup は、Amazon EFS による破壊的復元をサポートしていません。破壊リストアとは、リストアされたファイルシステムが、ソースまたは既存のファイルシステムを削除または上書きするときです。代わりに、 AWS Backup ファイルシステムをルートディレクトリの別のリカバリディレクトリにリストアします。

項目レベルの復元

項目レベルの復元を実行すると、 は特定のファイルまたはディレクトリ AWS Backup を復元します。ファイルシステムのルートへの相対パスを指定する必要があります。たとえば、ファイルシステムが `/user/home/myname/efs` にマウントされていて、ファイルパスが `user/home/myname/efs/file1` である場合は、「**`/file1`**」と入力します。パスでは、大文字と小文字が区別されます。ワイルドカード文字はサポートされていません。ファイルシステムがアクセスポイントを使用してマウントされている場合、パスはホスト内のパスとは異なる場合があります。

コンソールを使用して EFS 復元を実行するとき、最大 10 個の項目を選択できます。CLI を使用して復元する場合、項目の制限はありませんが、渡すことができる復元メタデータの長さには 200 KB の制限があります。

これらの項目は、新しいファイルシステムまたは既存のファイルシステムに復元できます。どちらにせよ、 AWS Backup は、項目を含むルートディレクトリの外に新しい Amazon EFS ディレクトリ (`aws-backup-restore_`*`datetime`*) を作成します。復元ディレクトリには、指定した項目の完全な階層構造が保持されます。例えば、ディレクトリ A にサブディレクトリとして B、C、D が含まれている場合、 AWS Backup は A、B、C、D の階層構造を保持して復元します。Amazon EFS の項目レベルの復元を既存のファイルシステムに、または新しいファイルシステムに対して実行するかに関係なく、復元の試行ごとにルートディレクトリから復元されたファイルが含まれる新しい復旧ディレクトリが作成されます。同じパスで複数の復元を試みると、復元先のディレクトリが複数になる場合があります。

> **Note**
>
> 毎週バックアップを 1 つだけ保持している場合、復元できるのは、そのバックアップを実行した時点のファイルシステムの状態に限られます。以前の増分バックアップに復元することはできません。

AWS Backup コンソールを使用して Amazon EFS 復旧ポイントを復元する

Amazon EFS ファイルシステムを作成するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. 作成時に、EFS バックアップボールトがアクセスポリシー Deny backup:StartRestoreJob を受け取ります。バックアップボールトを初めて復元する場合は、次のようにアクセスポリシーを変更する必要があります。

   a. [バックアップボールト] を選択します。

   b. 復元する復旧ポイントを含むバックアップボールトを選択します。

   c. アクセスポリシーボールトまで下にスクロールします。

   d. 存在する場合は、Statement から backup:StartRestoreJob を削除します。これを実行するには [編集] を選択し、backup:StartRestoreJob を削除して、[ポリシーを保存] を選択します。
3. ナビゲーションペインで、[Protected resources (保護されたリソース)] を選択し、復元する EFS ファイルシステム ID を選択します。
4. [Resource details (リソースの詳細)] ページには、選択したファイルシステム ID の回復ポイントのリストが表示されます。ファイルシステムを復元するには、[バックアップ] ペインで、ファイルシステムの復旧ポイント ID の横にあるラジオボタンをクリックします。ペインの右上隅にある [復元] を選択します。
5. ファイルシステムの復元パラメータを指定します。入力する復元パラメータは、選択したリソースタイプに固有です。

   [Full restore (完全復元)] を実行すると、ファイルシステム全体を復元できます。または、[項目レベルの復元] を実行して、特定のファイルやディレクトリを復元することもできます。

   - [完全な復元] オプションを選択すると、すべてのルートレベルのフォルダとファイルを含むファイルシステム全体が復元されます。
   - 特定のファイルまたはディレクトリを復元するには、[項目レベルの復元] オプションを選択します。Amazon EFS 内で最大 5 つの項目を選択して復元できます。

     特定のファイルやディレクトリを復元するには、マウントポイントからの相対パスを指定する必要があります。たとえば、ファイルシステムが /user/home/myname/efs にマウントされていて、ファイルパスが user/home/myname/efs/file1 である場合は、「**/file1**」と入力します。パスの大文字と小文字は区別されますが、特殊文字、ワイルドカードの文字、正規表現文字列を含めることはできません。

1. [項目パス] テキストボックスに、ファイルまたはフォルダのパスを入力します。
2. 追加のファイルまたはディレクトリを追加するには、[項目を追加] を選択します。EFS ファイルシステム内で最大 5 つの項目を選択して復元できます。

6. [復元の場所] の場合

   - ソースファイルシステムに復元する場合、[ソースファイルシステムのディレクトリに復元する] を選択します。
   - 別のファイルシステムに復元する場合、[新しいファイルシステムに復元する] を選択します。

7. ファイルシステムのタイプ

   - （推奨) 複数の AWS アベイラビリティーゾーンにまたがるファイルシステムを復元する場合は、リージョンを選択します。
   - ファイルシステムを単一のアベイラビリティーゾーンに復元する場合、1 ゾーンを選択します。次に、アベイラビリティーゾーンドロップダウンで、復元先を選択します。

   詳細については、Amazon EFS ユーザーガイドの「Amazon EFS ストレージクラスの管理」を参照してください。

8. パフォーマンス

   - リージョン別復元を実行することを選択した場合、[(推奨) 汎用] または [最大I/O] のいずれかを選択します。
   - 1 ゾーンの復元を実行することを選択した場合、[(推奨) 汎用] を選択する必要があります。1 ゾーンの復元では最大I/Oはサポートされません。

9. [暗号化の有効化]

   - ファイルシステムを暗号化する場合、[暗号化を有効にする] を選択します。KMS キー IDs とエイリアスは、 AWS Key Management Service（AWS KMS) コンソールを使用して作成された後、リストに表示されます。
   - [KMS キー] テキストボックスで、使用するキーをリストから選択します。

10. 復元ロール で、この復元のために AWS Backup が引き受ける IAM ロールを選択します。

> **Note**
>
> アカウントに AWS Backup デフォルトのロールが存在しない場合、適切なアクセス許可を持つデフォルトのロールが作成されます。このデフォルトロールを削除するか、使用不能にすることができます。

11. [バックアップを復元] を選択します。

    [復元ジョブ] ペインが表示されます。ページ上部のメッセージには、復元ジョブに関する情報が表示されます。

> **Note**
>
> 毎週バックアップを 1 つだけ保持している場合、復元できるのは、そのバックアップを実行した時点のファイルシステムの状態に限られます。以前の増分バックアップに復元することはできません。

AWS Backup API、CLI、または SDK を使用して Amazon EFS リカバリポイントを復元する

`StartRestoreJob` を使用します。Amazon EFS インスタンスを復元する場合、ファイルシステム全体、または特定のファイルやディレクトリを復元できます。Amazon EFS リソースを復元するには、次の情報が必要です。

- `file-system-id` — によってバックアップされる Amazon EFS ファイルシステムの ID AWS Backup。`GetRecoveryPointRestoreMetadata` で返されます。これは、新しいファイルシステムが復元される場合には必要ありません (パラメータが `newFileSystem` の場合、この値は無視されます`True`)。
- `Encrypted` - true の場合はファイルシステムの暗号化を指定するブール値。`KmsKeyId` が指定される場合、`Encrypted` は `true` である必要があります。
- `KmsKeyId` — 復元されたファイルシステムの暗号化に使用される AWS KMS キーを指定します。
- `PerformanceMode` - ファイルシステムのスループットモードを指定します。
- `CreationToken` - リクエストの一意性 (べき等性) を確認するユーザー指定の値。
- `newFileSystem` - true の場合は復旧ポイントが新しい Amazon EFS ファイルシステムに復元されることを指定するブール値。

- `ItemsToRestore` - 最大 5 つの文字列からなる配列。各文字列はファイルパスです。ファイルシステム全体ではなく、特定のファイルまたはディレクトリを復元するために `ItemsToRestore` を使用します。このパラメータはオプションです。

`aws:backup:request-id` を含めることもできます。

1 ゾーンの復元は、パラメータを含めることで実行できます。

```
"singleAzFilesystem": "true"
"availabilityZoneName": "ap-northeast-3"
```

Amazon EFS 設定値の詳細については、「」を参照してくださいcreate-file-system。

Amazon EFS での自動バックアップの無効化

デフォルトでは、Amazon EFS はデータのバックアップを自動的に作成します。これらのバックアップは、 でリカバリポイントとして表されます AWS Backup。復旧ポイントを削除しようとすると、アクションを実行するための権限が不十分であることを知らせるエラーメッセージが表示されます。

この自動バックアップをアクティブにしておくことがベストプラクティスです。特に、誤ってデータを削除した場合でも、このバックアップにより、ファイルシステムの内容を最後に復旧ポイントが作成された日付に復元できます。

万が一、これらを無効にする場合は、アクセスポリシーを `"Effect": "Deny"` から `"Effect": "Allow"` に変更する必要があります。自動バックアップの有効無効の切り替えの詳細については、「Amazon EFS ユーザーガイド」を参照してください。

Amazon DynamoDB テーブルの復元

AWS Backup コンソールを使用して DynamoDB 復旧ポイントを復元する

DynamoDB テーブルを復元するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[保護されたリソース] を選択し、復元する DynamoDB リソース ID を選択します。

3. [リソースの詳細] ページには、選択したリソース ID の復旧ポイントのリストが表示されます。リソースを復元するには、[バックアップ] ペインで、リソースの復旧ポイント ID の横にあるラジオボタンをクリックします。ペインの右上隅にある [復元] を選択します。
4. [設定] の [New table name (新しいテーブル名)] テキストフィールドに、新しいテーブル名を入力します。
5. 復元ロール で、この復元のために AWS Backup が引き受ける IAM ロールを選択します。
6. 暗号化設定を行うには:

   a. バックアップが DynamoDB によって管理されている場合 (ARN は で始まりますarn:aws:dynamodb)、 は AWSが所有するキーを使用して復元されたテーブルを AWS Backup 暗号化します。

      復元されたテーブルを暗号化する別のキーを選択するには、 AWS Backup StartRestoreJob オペレーションを使用するか、DynamoDB コンソール から復元を実行します。

   b. バックアップがフル AWS Backup 管理をサポートしている場合 (ARN が で始まるarn:aws:backup場合)、次のいずれかの暗号化オプションを選択して、復元されたテーブルを保護できます。

      - (デフォルト) DynamoDB 所有 KMS キー (暗号化に追加料金はかかりません)
      - DynamoDB 管理 KMS キー (KMS 料金が適用されます)
      - カスタマー管理 KMS キー (KMS 料金が適用されます)

      「DynamoDB 所有」キーと「DynamoDB 管理」キーは、それぞれ「AWS所有」キーと「AWS管理」キーと同じものです。詳細については、「Amazon DynamoDB デベロッパーガイド」の「保管中の暗号化: 仕組み」を参照してください。

      フル AWS Backup 管理の詳細については、「」を参照してくださいアドバンスト DynamoDB バックアップ。

> **Note**
>
> 以下のガイダンスは、コピーしたバックアップを復元し、かつ、復元したテーブルを元のテーブルの暗号化に使用したのと同じキーで暗号化する場合にのみ適用されます。クロスリージョンバックアップを復元する場合、元のテーブルの暗号化に使用したのと同じキーを使用して復元されたテーブルを暗号化するには、キーがマルチリージョンキーである必要があります。 AWSが所有するキーと AWSが管理するキーはマルチリー

ジョンキーではありません。詳細については、「AWS Key Management Service デベロッパーガイド」の「マルチリージョンキー」を参照してください。
クロスアカウントバックアップを復元する場合、元のテーブルの暗号化に使用したのと同じキーを使用して復元されたテーブルを暗号化するには、ソースアカウントのキーを送信先アカウントと共有する必要があります。 AWSが所有するキーと AWS管理のキーは、アカウント間で共有できません。詳細については、「AWS Key Management Service デベロッパーガイド」の「他のアカウントのユーザーに KMS キーの使用を許可する」をご参照ください。

7. [バックアップを復元] を選択します。

   [復元ジョブ] ペインが表示されます。ページ上部のメッセージには、復元ジョブに関する情報が表示されます。

AWS Backup API、CLI、または SDK を使用して DynamoDB リカバリポイントを復元する

`StartRestoreJob` を使用します。DynamoDB 復元中に、次のメタデータを指定できます。メタデータでは、大文字と小文字は区別されません。

```
targetTableName
encryptionType
kmsMasterKeyArn
aws:backup:request-id
```

CLI の `StartRestoreJob` オペレーションの `restoreMetadata` 引数の例を次に示します。

```
aws backup start-restore-job \
--recovery-point-arn "arn:aws:backup:us-east-1:123456789012:recovery-point:abcdef12-g3hi-4567-8cjk-012345678901" \
--iam-role-arn "arn:aws:iam::123456789012:role/YourIamRole" \
--metadata
 'TargetTableName=TestRestoreTestTable,EncryptionType=KMS,KMSMasterKeyId=arn:aws:kms:us-east-1:123456789012:key/abcdefg' \
--region us-east-1 \
--endpoint-url https://cell-1.gamma.us-east-1.controller.cryo.aws.a2z.com
```

前の例では、 AWSが所有するキーを使用して復元されたテーブルを暗号化します。 AWS所有キーを使用した暗号化を指定する復元メタデータの一部は、 です`\"encryptionType\":\"Default\",\"kmsMasterKeyArn\":\"Not Applicable\"`。

AWSマネージドキーを使用して復元されたテーブルを暗号化するには、復元メタデータ を指定します`"encryptionType\":\"KMS\",\"kmsMasterKeyArn\":\"Not Applicable\"`。

カスタマーマネージドキーを使用して復元したテーブルを暗号化するには、次の復元メタデータを指定します: `"encryptionType\":\"KMS\",\"kmsMasterKeyArn\":\"`*`arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`*`\"`。

RDS データベースの復元

Amazon RDS データベースを復元するには、複数の復元オプションを指定する必要があります。これらのオプションの詳細については、Amazon RDS ユーザーガイドの「Amazon RDS DB インスタンスのバックアップと復元」を参照してください。

AWS Backup コンソールを使用して Amazon RDS 復旧ポイントを復元する

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[保護されたリソース] を選択し、復元する Amazon RDS リソース ID を選択します。
3. [リソースの詳細] ページには、選択したリソース ID の復旧ポイントのリストが表示されます。リソースを復元するには、[バックアップ] ペインで、リソースの復旧ポイント ID の横にあるラジオボタンをクリックします。ペインの右上隅にある [復元] を選択します。
4. [Instance specifications (インスタンスの仕様)] ペインで、デフォルトを受け入れるか、[DB engine (DB エンジン)]、[License Model (ライセンスモデル)]、[DB instance class (DB インスタンスクラス)]、[Multi AZ (マルチ AZ)]、および [Storage type (ストレージ種別)] 設定のオプションを指定します。たとえば、スタンバイデータベースインスタンスを使用する場合は、マルチ AZ を指定します。
5. 設定ペインで、現在のリージョンで が所有するすべての DB インスタンスとクラスター AWS アカウント に固有の名前を指定します。DB インスタンス識別子は大文字と小文字の区別がありませんが、すべて小文字で保存されます (例: 「`mydbinstance`」)。これは必須のフィールドです。
6. ネットワークとセキュリティペインで、デフォルトを受け入れるか、仮想プライベートクラウド (VPC)、サブネットグループ 、パブリックアクセシビリティ (通常はは い) 、およびアベイラビリティーゾーン設定のオプションを指定します。

7. [Database options (データベースオプション)] ペインで、デフォルトを受け入れるか、[Database port (データベースポート)]、[DB parameter group (DB パラメータグループ)]、[Option Group(オプショングループ)]、[Copy tags to snapshots (スナップショットへのタグのコピー)]、および [IAM DB Authentication Enabled (IAM DB 認証の有効化)] 設定のオプションを指定します。
8. [暗号化] ペインでは、デフォルトの設定を使用します。スナップショットのソースデータベースインスタンスが暗号化されている場合、復元されるデータベースインスタンスも暗号化されます。この暗号化は削除できません。
9. ログエクスポートペインで、Amazon CloudWatch Logs に発行するログタイプを選択します。[IAM ロール] は既に定義されています。
10. [Maintenance (メンテナンス)] ペインで、既定値をそのまま使用するか、[Auto minor version upgrade (マイナーバージョンの自動アップグレード)] のオプションを指定します。
11. [ロールを復元] ペインで、この復元のために AWS Backup が引き受ける IAM ロールを選択します。
12. すべての設定を指定したら、[Restore backup (バックアップを復元)] を選択します。

    [復元ジョブ] ペインが表示されます。ページ上部のメッセージには、復元ジョブに関する情報が表示されます。

AWS Backup API、CLI、または SDK を使用して Amazon RDS リカバリポイントを復元する

`StartRestoreJob` を使用します。受け入れられるメタデータと値については、「Amazon RDS API リファレンス」の「`RestoreDBInstanceFromDBSnapshot`」を参照してください。さらに、は、以下の情報のみの属性 AWS Backup を受け入れます。ただし、これらを含めても復元には影響しません。

```
EngineVersion
KmsKeyId
Encrypted
vpcId
```

Amazon Aurora クラスターの復元

AWS Backup コンソールを使用して Aurora 復旧ポイントを復元する

AWS Backup は Aurora クラスターを復元します。クラスターに Amazon RDS インスタンスを作成またはアタッチすることはありません。次の手順では、CLI を使用して Amazon RDS インスタンスを作成して、復元した Aurora クラスターにアタッチします。

Aurora クラスターを復元するには、複数の復元オプションを指定する必要があります。これらのオプションについては、Amazon Aurora ユーザーガイドの「Aurora DB クラスターのバックアップと復元の概要」を参照してください。復元オプションの仕様については、 の API ガイドを参照してくださいRestoreDBClusterFromSnapshot。

Amazon Aurora クラスターを復元するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[Protected resources (保護されたリソース)] を選択し、復元する Aurora リソース ID を選択します。
3. [リソースの詳細] ページには、選択したリソース ID の復旧ポイントのリストが表示されます。リソースを復元するには、[バックアップ] ペインで、リソースの復旧ポイント ID の横にあるラジオボタンをクリックします。ペインの右上隅にある [復元] を選択します。
4. [Instance specifications (インスタンスの仕様)] ペインで、デフォルトを受け入れるか、[DB engine (DB エンジン)]、[DB engine version (DB エンジンのバージョン)]、[Capacity type (容量タイプ)] 設定のオプションを指定します。

   > **Note**
   >
   > [Serverless (サーバーレス)] キャパシティータイプが選択されている場合は、[Capacity settings (キャパシティー設定)] ペインが表示されます。[Minimum Aurora capacity unit (最小オーロラ容量単位)] と [Maximum Aurora capacity unit (最大オーロラ容量単位)] の設定のオプションを指定するか、[Additional scaling configuration (追加のスケーリング設定)] セクションから別のオプションを選択します。

5. 設定ペインで、現在のリージョンで が所有するすべての DB クラスターインスタンス AWS アカウント に固有の名前を指定します。
6. [Network & Security (ネットワークとセキュリティ)] ペインで、デフォルトを受け入れるか、[仮想プライベートクラウド (VPC)]、[Subnet group (サブネットグループ)]、および [Availability zone (アベイラビリティーゾーン)] 設定のオプションを指定します。

7. [Database options (データベースオプション)] ペインで、デフォルトを受け入れるか、[Database port (データベースポート)]、[DB cluster parameter group (DB クラスターパラメータグループ)]、および [IAM DB Authentication Enabled (IAM DB 認証の有効化)] 設定のオプションを指定します。
8. [Backup (バックアップ)] ペインで、デフォルトを受け入れるか、[Copy tags to snapshots (タグをスナップショットにコピーする)] 設定のオプションを指定します。
9. [Backtrack (バックトラック)] ペインで、既定値をそのまま使用するか、[Enable Backtrack (バックトラックを有効にする)] または [Disable Backtrack (バックトラックを無効にする)] 設定のオプションを指定します。
10. [暗号化] ペインで、デフォルトを使用するか、[暗号化を有効にする] または [[暗号化を無効にする] 設定のオプションを指定します。
11. ログエクスポートペインで、Amazon CloudWatch Logs に発行するログタイプを選択します。[IAM ロール] は既に定義されています。
12. [ロールを復元] ペインで、この復元のために AWS Backup が引き受ける IAM ロールを選択します。
13. すべての設定を指定したら、[バックアップを復元] を選択します。

    [復元ジョブ] ペインが表示されます。ページ上部のメッセージには、復元ジョブに関する情報が表示されます。
14. 復元が完了したら、復元した Aurora クラスターを Amazon RDS インスタンスにアタッチします。

    AWS CLI の使用：

    - Linux、macOS、Unix の場合:

      ```
      aws rds create-db-instance --db-instance-identifier sample-instance \
                  --db-cluster-identifier sample-cluster --engine aurora-mysql --db-
      instance-class db.r4.large
      ```

    - Windows の場合:

      ```
      aws rds create-db-instance --db-instance-identifier sample-instance ^
                  --db-cluster-identifier sample-cluster --engine aurora-mysql --db-
      instance-class db.r4.large
      ```

継続的バックアップと選択した時点への point-in-time 復元については、「継続的バックアップと復元 (PITR)」を参照してください。

AWS Backup API、CLI、または SDK を使用して Aurora リカバリポイントを復元する

StartRestoreJob を使用します。Aurora 復元中に、以下のメタデータを指定できます。

```
List<String> availabilityZones;
Long backtrackWindow;
Boolean copyTagsToSnapshot;
String databaseName;
String dbClusterIdentifier;
String dbClusterParameterGroupName;
String dbSubnetGroupName;
List<String> enableCloudwatchLogsExports;
Boolean enableIAMDatabaseAuthentication;
String engine;
String engineMode;
String engineVersion;
String kmsKeyId;
Integer port;
String optionGroupName;
ScalingConfiguration scalingConfiguration;
List<String> vpcSecurityGroupIds;
```

例：

```
"restoreMetadata":"{\"EngineVersion\":\"5.6.10a\",\"KmsKeyId\":\"arn:aws:kms:us-
east-1:234567890123:key/45678901-ab23-4567-8cd9-012d345e6f7\",\"EngineMode\":
\"serverless\",\"AvailabilityZones\":\"[\\\"us-east-1b\\\",\\\"us-east-1e\\\",\\
\"us-east-1c\\\"]\",\"Port\":\"3306\",\"DatabaseName\":\"\",\"DBSubnetGroupName\":
\"default-vpc-05a3b07cf6e193e1g\",\"VpcSecurityGroupIds\":\"[\\\"sg-012d52c68c6e88f00\
\\"]\",\"ScalingConfiguration\":\"{\\\"MinCapacity\\\":2,\\\"MaxCapacity\\\":64,
\\\"AutoPause\\\":true,\\\"SecondsUntilAutoPause\\\":300,\\\"TimeoutAction\\\":
\\\"RollbackCapacityChange\\\"}\",\"EnableIAMDatabaseAuthentication\":\"false\",
\"DBClusterParameterGroupName\":\"default.aurora5.6\",\"CopyTagsToSnapshot\":\"true\",
\"Engine\":\"aurora\",\"EnableCloudwatchLogsExports\":\"[]\"}"
```

Amazon EC2 インスタンスの復元

EC2 インスタンスを復元すると、 は Amazon マシンイメージ (AMI)、 インスタンス、Amazon EBS ルートボリューム、Amazon EBS データボリューム (保護されたリソースにデータボリュームがあ

る場合）、および Amazon EBS スナップショット AWS Backup を作成します。 AWS Backup コンソールを使用して一部のインスタンス設定をカスタマイズすることも、 AWS CLI または AWS SDK を使用して多数の設定をカスタマイズすることもできます。

EC2 インスタンスの復元には、次の考慮事項が適用されます。

- AWS Backup は、保護されたリソースが最初に使用したものと同じキーペアを使用するように復元されたインスタンスを設定します。復元プロセス中に、復元されたインスタンスのキーペアを別個に指定することはできません。
- AWS Backup は、Amazon EC2 インスタンスの起動中に使用されるユーザーデータをバックアップおよび復元しません。
- 復元されたインスタンスを設定する場合、保護されたリソースが最初に使用したのと同じインスタンスプロファイルを使用するか、インスタンスプロファイルなしで起動するかを選択できます。これは、特権エスカレーションを防ぐためです。Amazon EC2 コンソールを使用して、復元されたインスタンスのインスタンスプロファイルを更新できます。

  元のインスタンスプロファイルを使用する場合は、 AWS Backup 次のアクセス許可を付与する必要があります。リソース ARN は、インスタンスプロファイルに関連付けられた IAM ロールの ARN です。

  ```
  {
        "Effect": "Allow",
        "Action": "iam:PassRole",
        "Resource": "arn:aws:iam::account-id:role/role-name"
  },
  ```

- 復元中に、すべての Amazon EC2 クォータと設定制限が適用されます。
- Amazon EC2 復旧ポイントを含むボールトにボールトロックがある場合は、セキュリティに関するその他の考慮事項「」で詳細を確認してください。

AWS Backup コンソールを使用して Amazon EC2 復旧ポイントを復元する

Amazon EC2 インスタンス全体を、ルートボリューム、データボリューム、インスタンスタイプやキーペアなどのインスタンス設定を含む単一の復旧ポイントから復元できます。

AWS Backup コンソールを使用して Amazon EC2 リソースを復元するには

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

2. ナビゲーションペインで、保護されたリソース を選択し、Amazon EC2 リソースの ID を選択してリソースの詳細ページを開きます。 Amazon EC2
3. 復旧ポイントペインで、復元する復旧ポイントの ID の横にあるラジオボタンを選択します。ペインの右上隅にある [復元] を選択します。
4. ネットワーク設定ペインでは、保護されたインスタンスの設定を使用して、インスタンスタイプ、VPC、サブネット、セキュリティグループ、インスタンス IAM ロールのデフォルト値を選択します。これらのデフォルト値を使用するか、必要に応じて変更できます。
5. ロールの復元ペインで、デフォルトロールを使用するか、IAM ロールの選択を使用して、バックアップを復元する AWS Backup アクセス許可を付与する IAM ロールを指定します。
6. 保護されたリソースタグペインでは、デフォルトで保護されたリソースから復元されたリソースにタグをコピーを選択します。これらのタグをコピーしない場合は、チェックボックスをオフにします。
7. 詳細設定ペインで、インスタンス設定のデフォルト値を受け入れるか、必要に応じて変更します。これらの設定の詳細については、設定の情報を選択してヘルプペインを開きます。
8. インスタンスの設定が完了したら、バックアップの復元 を選択します。

を使用して Amazon EC2 を復元する AWS CLI

コマンドラインインターフェイスでは、 `start-restore-job`は最大 32 個のパラメータ (AWS Backup コンソールではカスタマイズできないパラメータを含む) で復元できます。

以下のリストは、Amazon EC2 復旧ポイントを復元するために受け入れられるメタデータです。

```
InstanceType
KeyName
SubnetId
Architecture
EnaSupport
SecurityGroupIds
IamInstanceProfileName
CpuOptions
InstanceInitiatedShutdownBehavior
HibernationOptions
DisableApiTermination
CreditSpecification
Placement
RootDeviceType
RamdiskId
```

```
KernelId
UserData
Monitoring
NetworkInterfaces
ElasticGpuSpecification
CapacityReservationSpecification
InstanceMarketOptions
LicenseSpecifications
EbsOptimized
VirtualizationType
Platform
RequireIMDSv2
aws:backup:request-id
```

AWS Backup は、以下の情報のみの属性を受け入れます。ただし、これらを含めても復元には影響しません。

```
vpcId
```

また、保存されたパラメータを含めずに Amazon EC2 インスタンスを復元することもできます。このオプションは、 AWS Backup コンソールの [保護されたリソース] タブで利用できます。

Storage Gateway ボリュームの復元

AWS Storage Gateway ボリュームスナップショットを復元する場合は、スナップショットを Storage Gateway ボリュームとして復元するか、Amazon EBS ボリュームとして復元するかを選択できます。これは、 が両方のサービスと AWS Backup 統合され、Storage Gateway スナップショットを Storage Gateway ボリュームまたは Amazon EBS ボリュームのいずれかに復元できるためです。

AWS Backup コンソールから Storage Gateway を復元する

Storage Gateway のボリュームを復元するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[Protected resources (保護されたリソース)] を選択し、復元する Storage Gateway リソース ID を選択します。
3. [リソースの詳細] ページには、選択したリソース ID の復旧ポイントのリストが表示されます。リソースを復元するには、[バックアップ] ペインで、リソースの復旧ポイント ID の横にあるラジオボタンをクリックします。ペインの右上隅にある [復元] を選択します。

4. リソースの復元パラメータを指定します。入力する復元パラメータは、選択したリソースタイプに固有です。

   リソースタイプ で、このバックアップを復元するときに作成する AWS リソースを選択します。

5. Storage Gateway ボリュームを選択すると、到達可能な状態のゲートウェイが選択されます。また、iSCSI ターゲット名も選択してください。

   1. 「ボリューム保管済み」ゲートウェイの場合は、[ディスク ID] を選択します。
   2. 「ボリュームキャッシュ」ゲートウェイの場合は、少なくとも保護されたリソースと同じ容量を選択します。

   [EBS ボリューム] を選択した場合は、[ボリュームタイプ]、[サイズ (GiB)] の値を指定し、[アベイラビリティーゾーン] を選択します。

6. 復元ロール で、この復元のために AWS Backup が引き受ける IAM ロールを選択します。

   > **Note**
   >
   > アカウントに AWS Backup デフォルトのロールが存在しない場合、適切なアクセス許可を持つデフォルトのロールが作成されます。このデフォルトロールを削除するか、使用不能にすることができます。

7. [バックアップを復元] を選択します。

   [復元ジョブ] ペインが表示されます。ページ上部のメッセージには、復元ジョブに関する情報が表示されます。

で Storage Gateway を復元する AWS CLI

コマンドラインインタフェースでは、`start-restore-job` を使用することで Storage Gateway· ボリュームを復元できます。

以下のリストは受け入れられるメタデータです。

```
gatewayArn // The Amazon Resource Name (ARN) of the gateway. Use the ListGateways
 operation to return a list of gateways for your account and AWS #####.
gatewayType // The type of created gateway. Valid value is BACKUP_VM
targetName
```

```
kmsKey
volumeSize
volumeSizeInBytes
diskId
```

Amazon Timestream テーブルを復元する

Amazon Timestream テーブルを復元する場合、新しいテーブル名、送信先データベース、ストレージ割り当て設定 (メモリとマグネティックストレージ)、復元ジョブを完了するために使用するロールなど、いくつかのオプションを設定できます。エラーログを保存する Amazon S3 バケットを選択することもできます。マグネティックストレージへの書き込みは非同期で行われるため、エラーを記録しておくとよいでしょう。

Timestream データストレージには、メモリストアとマグネティックストアの 2 つの階層があります。メモリストアは必須ですが、指定したメモリ時間が経過した後に、復元したテーブルをマグネティックストレージに転送することもできます。メモリストアは、高スループットのデータ書き込みと高速 point-in-time クエリ用に最適化されています。マグネティックストアは、低スループットの遅着データ書き込み、長期間のデータ保存、高速な分析クエリに最適化されています。

Timestream テーブルを復元するときは、そのテーブルを各ストレージ階層に保持する期間を決定します。コンソールまたは API を使用して、両方のストレージ時間を設定できます。ストレージは線形かつシーケンシャルであることに注意してください。Timestream は、復元されたテーブルを最初にメモリストレージに保存し、メモリストレージの時間に達すると自動的にマグネティックストレージに移行します。

> **Note**
>
> マグネティックストアの保持期間は、(コンソールの右上に表示された) 元の保持期間以上でなければなりません。そうでない場合、データは失われます。

例: データを 1 週間保持するようにメモリストア割り当てを設定し、同じデータを 1 年間保持するようにマグネティックストア割り当てを設定したとします。メモリストア内のデータが 1 週間経過すると、そのデータは自動的にマグネティックストアに移動されます。その後、マグネティックストアに 1 年間保存されます。その期間が過ぎると、Timestream と AWS Backupから削除されます。

AWS Backup コンソールを使用して Amazon Timestream テーブルを復元するには

によって AWS Backup 作成された Timestream テーブルは、コンソールで復元できます AWS Backup。

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[保護されたリソース] を選択し、復元する Amazon Timestream リソース ID を選択します。
3. [リソースの詳細] ページには、選択したリソース ID の復旧ポイントのリストが表示されます。リソースを復元するには、[バックアップ] ペインで、リソースの復旧ポイント ID の横にあるラジオボタンをクリックします。ペインの右上隅にある [復元] を選択します。
4. 以下を含む新しいテーブル設定を指定します。
   a. 2～256 文字 (文字、数字、ダッシュ、ピリオド、アンダースコア) で構成される新しいテーブル名。
   b. ドロップダウンメニューから選択した送信先データベース。
5. ストレージ割り当て: 復元されたテーブルが最初にメモリストレージに保存される時間を設定し、復元されたテーブルがその後マグネティックストレージに留まる時間を設定します。メモリストレージは、時間単位、日単位、週単位、または月単位で設定できます。マグネティックストレージは、日単位、週単位、月単位、または年単位に設定できます。
6. (オプション) マグネティックストレージ書き込みを有効にする: マグネティックストレージ書き込みを許可するオプションがあります。このオプションをオンにすると、遅れて到着したデータ、つまりメモリストレージの保持期間外のタイムスタンプが付いたデータが、マグネティックストアに直接書き込まれます。
7. (オプション) Amazon S3 エラーログの場所: エラーログを保存する S3 の場所を指定できます。S3 ファイルを参照するか、S3 ファイルパスをコピーして貼り付けます。

   > **Note**
   >
   > S3 エラーログの場所を指定する場合、この復元に使用するロールには、S3 バケットへの書き込み用のアクセス許可があるか、そのアクセス許可を持つポリシーが含まれている必要があります。

8. 復元を実行するために渡す IAM ロールを選択します。デフォルトの IAM ロールを使用することも、別のロールを指定することもできます。
9. [バックアップを復元] をクリックします。

復元ジョブは、保護されたリソースの下に表示されます。更新ボタンまたは CTRL-R をクリックすると、復元ジョブの現在のステータスを確認できます。

API、CLI、または SDK を使用して Amazon Timestream テーブルを復元するには

API 経由で Timestream テーブルを復元するために StartRestoreJob を使用します。

を使用して Timestream を復元するには AWS CLI、 オペレーションを使用して次のメタデータstart-restore-job.を指定します。

```
TableName: string;
DestinationDatabase: string;
MemoryStoreRetentionPeriodInHours: value: number unit: 'hours' | 'days' | 'weeks' |
 'months'
MagneticStoreRetentionPeriodInDays: value: number unit: 'days' | 'weeks' | 'months' |
 'years'
EnableMagneticStoreWrites?: boolean;
aws:backup:request-id
```

サンプルのテンプレートを次に示します。

```
aws backup start-restore-job \
--recovery-point-arn "arn:aws:backup:us-west-2:accountnumber:recovery-point:1a2b3cde-
f405-6789-012g-3456hi789012_beta" \
--iam-role-arn "arn:aws:iam::accountnumber:role/rolename" \
--metadata
 'TableName=tablename,DatabaseName=databasename,MagneticStoreRetentionPeriodInDays=1,MemoryStor
\":true,\"MagneticStoreRejectedDataLocation\":{\"S3Configuration\":{\"BucketName\":
\"bucketname\",\"EncryptionOption\":\"SSE_S3\"}}}"' \
--region us-west-2 \
--endpoint-url url
```

DescribeRestoreJob を使用して情報を復元するのにも役立ちます。

で AWS CLI、 オペレーションdescribe-restore-jobを使用し、次のメタデータを使用します。

```
TableName: string;
DestinationDatabase: string;
MemoryStoreRetentionPeriodInHours: value: number unit: 'hours' | 'days' | 'weeks' |
 'months'
MagneticStoreRetentionPeriodInDays: value: number unit: 'days' | 'weeks' | 'months' |
 'years'
EnableMagneticStoreWrites?: boolean;
```

サンプルのテンプレートを次に示します。

```
aws backup describe-restore-job \
--restore-job-id restore job ID \
--region awsregion \
--endpoint-url url
```

Amazon Redshift クラスター を復元する

自動スナップショットと手動スナップショットは、 AWS Backup コンソールまたは CLI を使用して復元できます。

Amazon Redshift クラスターを復元すると、元のクラスター設定がデフォルトでコンソールに入力されます。以下の設定には異なる設定を指定できます。テーブルを復元するときは、ソースデータベースとターゲットデータベースを指定する必要があります。これらの設定の詳細については、「Amazon Redshift 管理ガイド」の「スナップショットからのクラスターの復元」を参照してください。

- 単一のテーブルまたはクラスター: クラスター全体を復元するか、1 つのテーブルを復元するかを選択できます。単一のテーブルの復元を選択する場合は、ソースデータベース、ソーススキーマ、ソーステーブル名のほか、ターゲットクラスタ、スキーマ、および新しいテーブル名が必要になります。
- ノードタイプ: 各 Amazon Redshift クラスターは、リーダーノードと少なくとも 1 つのコンピュートノードで構成されます。クラスターを復元するときは、CPU、RAM、ストレージ容量、ドライブタイプの要件を満たすノードタイプを指定する必要があります。
- ノード数: クラスターを復元するときは、必要なノードの数を指定する必要があります。
- 構成の概要
- クラスターのアクセス許可

AWS Backup コンソールを使用して Amazon Redshift クラスターまたはテーブルを復元するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[保護されたリソース] を選択し、復元する Amazon Redshift リソース ID を選択します。
3. [リソースの詳細] ページには、選択したリソース ID の復旧ポイントのリストが表示されます。リソースを復元するには、[復旧ポイント] ペインで、リソースの復旧ポイント ID の横にあるラジオボタンをクリックします。ペインの右上隅にある [復元] を選択します。

4. 復元オプション

   a. スナップショットからクラスターを復元する、または

   b. スナップショット内の 1 つのテーブルを新しいクラスターに復元します。このオプションを選択する場合、以下のとおり設定する必要があります。

      i. 大文字と小文字を区別する名前のオンとオフを切り替えます。

      ii. データベース、スキーマ、テーブルを含むソーステーブルの値を入力します。ソーステーブルの情報は Amazon Redshift コンソールにあります。

      iii. データベース、スキーマ、新しいテーブル名を含むターゲットテーブルの値を入力します。

5. 新しいクラスター設定を指定します。

   a. クラスター復元の場合: クラスター識別子、ノードタイプ、ノード数を選択します。

   b. アベイラビリティーゾーンとメンテナンスウィンドウを指定します。

   c. [IAM ロールを関連付ける] をクリックすると、追加のロールを関連付けることができます。

6. オプション: 追加設定:

   a. [デフォルトを使用] は、デフォルトでオンになっています。

   b. ドロップダウンメニューを使用して、ネットワークとセキュリティ、VPC セキュリティグループ、クラスターサブネットグループ、アベイラビリティーゾーンの設定を選択します。

   c. [拡張 VPC ルーティング] をオンまたはオフに切り替えます。

   d. クラスターエンドポイントをパブリックにアクセス可能にするかどうかを決定します。アクセス可能にする場合は、VPC の外部のインスタンスとデバイスがクラスターエンドポイントを介してデータベースに接続できます。これをオンにする場合は、Elastic IP アドレスを入力します。

7. オプション: データベース設定 以下の入力を選択できます

   a. データベースポート (テキストフィールドへの入力)

   b. パラメータグループ

8. メンテナンス: 次のものを選択できます

   a. メンテナンスウィンドウ

   b. 現在のメンテナンス、トレーリング、プレビューの中からメンテナンストラック。これは、メンテナンスウィンドウ中にどのクラスターバージョンを適用するかを制御します。

9. 自動スナップショットはデフォルトに設定されています。

    a. 自動スナップショットの保持期間。保持期間は 0 ~ 35 日でなければなりません。0 を選択すると、自動スナップショットは作成されません。

    b. 手動スナップショットの保持期間は 1 ~ 3653 日です。

    c. クラスターの再配置にはオプションでチェックボックスがあります。これをオンにすると、クラスターを別のアベイラビリティーゾーンに再配置できるようになります。再配置を有効にすると、VPC エンドポイントを使用できます。

10. モニタリング: クラスターが復元されたら、 CloudWatch または Amazon Redshift を使用してモニタリングを設定できます。

11. 復元を実行するために渡す IAM ロールを選択します。デフォルトのロールを使用することも、別のロールを指定することもできます。

復元ジョブは [ジョブ] に表示されます。更新ボタンまたは CTRL-R をクリックすると、復元ジョブの現在のステータスを確認できます。

API、CLI、または SDK を使用して Amazon Redshift クラスターを復元する

`StartRestoreJob` を使用して Amazon Redshift クラスターを復元します。

を使用して Amazon Redshift を復元するには AWS CLI、 コマンドを使用して次のメタデータ`start-restore-job`を指定します。

```
ClusterIdentifier // required string
AdditionalInfo // optional string
AllowVersionUpgrade // optional Boolean
AquaConfigurationStatus // optional string
AutomatedSnapshotRetentionPeriod // optional integer 0 to 35
AvailabilityZone // optional string
AvailabilityZoneRelocation // optional Boolean
ClusterParameterGroupName // optional string
ClusterSecurityGroups // optional array of strings
ClusterSubnetGroupName // optional strings
DefaultIamRoleArn // optional string
ElasticIp // optional string
Encrypted // Optional TRUE or FALSE
EnhancedVpcRouting // optional Boolean
HsmClientCertificateIdentifier // optional string
HsmConfigurationIdentifier // optional string
```

```
IamRoles // optional array of strings
KmsKeyId // optional string
MaintenanceTrackName // optional string
ManageMasterPassword // optional Boolean
ManualSnapshotRetentionPeriod // optional integer
MasterPasswordSecretKmsKeyId // optional string
NodeType // optional string
NumberOfNodes // optional integer
OwnerAccount // optional string
Port // optional integer
PreferredMaintenanceWindow // optional string
PubliclyAccessible // optional Boolean
ReservedNodeId // optional string
SnapshotClusterIdentifier // optional string
SnapshotScheduleIdentifier // optional string
TargetReservedNodeOfferingId // optional string
VpcSecurityGroupIds // optional array of strings
RestoreType // CLUSTER_RESTORE  or TABLE_RESTORE
```

詳細については、「Amazon Redshift API リファレンス」の「RestoreFromClusterSnapshot」と 「AWS CLI ガイド」の「restore-from-cluster-snapshot」を参照してください。

サンプルのテンプレートを次に示します。

```
aws backup start-restore-job \
-\-recovery-point-arn "arn:aws:backup:region:account:snapshot:name
-\-iam-role-arn "arn:aws:iam:account:role/role-name" \
-\-metadata
-\-resource-type Redshift \
-\-region AWS #####
-\-endpoint-url URL
```

以下がその例です。

```
aws backup start-restore-job \
-\-recovery-point-arn "arn:aws:redshift:us-west-2:123456789012:snapshot:redshift-
cluster-1/awsbackup:job-c40dda3c-fdcc-b1ba-fa56-234d23209a40" \
-\-iam-role-arn "arn:aws:iam::974288443796:role/Backup-Redshift-Role" \
-\-metadata 'RestoreType=CLUSTER_RESTORE,ClusterIdentifier=redshift-cluster-
restore-78,Encrypted=true,KmsKeyId=45e261e4-075a-46c7-9261-dfb91e1c739c' \
-\-resource-type Redshift \
-\-region us-west-2 \
```

DescribeRestoreJob を使用して情報を復元するのにも役立ちます。

で AWS CLI、 オペレーションdescribe-restore-jobを使用し、次のメタデータを使用します。

```
Region
```

サンプルのテンプレートを次に示します。

```
aws backup describe-restore-job –restore-job-id restore job ID
-\-region AWS #####
```

以下がその例です。

```
aws backup describe-restore-job -\-restore-job-id BEA3B353-576C-22C0-9E99-09632F262620
 \
-\-region us-west-2 \
```

Amazon EC2 インスタンスで SAP HANA データベースを復元する

EC2 インスタンスの SAP HANA データベースは、 AWS Backup コンソール、API、または を使用して復元できます AWS CLI。

トピック

- AWS Backup コンソールを使用して Amazon EC2 インスタンスデータベースで SAP HANA を復元する
- EC2 での SAP HANA 用 StartRestoreJob API
- EC2 での SAP HANA 用 CLI
- トラブルシューティング

AWS Backup コンソールを使用して Amazon EC2 インスタンスデータベースで SAP HANA を復元する

同じデータベースに関係するバックアップジョブと復元ジョブは同時に実行できないことに注意してください。SAP HANA データベースの復元ジョブが発生しているときに、同じデータベースをバックアップしようとすると、「データベースが停止している間はバックアップできません」というエラーが表示される可能性があります。

1. 前提条件の認証情報を使用して AWS Backup コンソールにアクセスします。

2. [ターゲットの復元場所] ドロップダウンメニューで、復元に使用している復旧ポイントで上書きするデータベースを選択します (復元ターゲットのデータベースをホストするインスタンスには、前提条件を満たすアクセス許可も必要であることに注意してください)。

> **Important**
>
> SAP HANA データベースの復元は破壊的です。データベースを復元すると、指定されたターゲット復元場所にあるデータベースが上書きされます。

3. このステップは、システムコピーの復元を実行する場合にのみ実行します。それ以外の場合は、ステップ 4 に進みます。

   システムコピーの復元は、復旧ポイントを生成したソースデータベースとは異なるターゲットデータベースに復元する復元ジョブです。システムコピーの復元については、コンソールに表示される `aws ssm-sap put-resource-permission` コマンドに注意してください。このコマンドは、前提条件を満たしたマシンにコピー、貼り付け、実行する必要があります。コマンドを実行するときは、アプリケーションの登録に必要なアクセス許可を設定した前提条件にあるロールの認証情報を使用します。

```
// Example command
aws ssm-sap put-resource-permission \
--region us-east-1 \
--action-type RESTORE \
--source-resource-arn arn:aws:ssm-sap-east-1:112233445566:HANA/Foo/DB/HDB \
--resource-arn arn:aws:ssm-sap:us-east-1:112233445566:HANA/Bar/DB/HDB
```

4. 復元場所を選択すると、ターゲットデータベースのリソース ID、アプリケーション名、データベースタイプ、および EC2 インスタンスが表示されます。
5. オプションで、[詳細復元設定] を開いてカタログ復元オプションを変更できます。デフォルトでは、 AWS Backupから最新のカタログを復元することになっています。
6. [バックアップを復元] をクリックします。
7. ターゲットの場所が復元中に上書き (「破壊復元」) されるので、次のポップアップダイアログボックスで許可するかどうかを確認する必要があります。

   a. 続行するには、復元するデータベースによって既存のデータベースが上書きされることを理解しておく必要があります。

   b. これを理解したら、既存のデータが上書きされることを承認する必要があります。これを承認して次に進むには、テキスト入力フィールドに [上書き] と入力します。

8. [バックアップを復元] をクリックします。

手順が成功すると、コンソールの上部に青いバナーが表示されます。これは、復元ジョブが進行中であることを示します。自動的にジョブページにリダイレクトされ、復元ジョブのリストに復元ジョブが表示されます。この最新のジョブのステータスは Pending になります。復元ジョブ ID を検索してクリックすると、各復元ジョブの詳細が表示されます。[更新] ボタンをクリックすると、復元ジョブリストを更新して、復元ジョブのステータスの変更を確認できます。

EC2 での SAP HANA 用 StartRestoreJob API

このアクションは、Amazon リソースネーム (ARN) で識別された保存されたリソースを回復します。

リクエストの構文

```
PUT /restore-jobs HTTP/1.1
Content-type: application/json
{
   "IdempotencyToken": "string",
   "Metadata": {
      "string" : "string"
   },
   "RecoveryPointArn": "string",
   "ResourceType": "string"
}
```

URI リクエストパラメータ: リクエストでは URI パラメータを使用しません。

リクエスト本文: リクエストは以下の JSON 形式のデータを受け入れます。

IdempotencyTokenへの同じ呼び出しを区別するために使用できる、お客様が選択した文字列StartRestoreJob。同じ冪等性トークンで成功したリクエストを再試行すると、アクションは実行されず、成功メッセージが表示されます。

タイプ: 文字列

必須: いいえ

Metadata

メタデータのキーと値のペアのセット。リカバリポイントの復元に必要なリソース (リソース名など) を含みます。GetRecoveryPointRestoreMetadata を呼び出して、バックアップ時にリソースに

関する構成メタデータを取得できます。ただし、GetRecoveryPointRestoreMetadata によって提供される値に加えて値リソースの復元が必要になる場合があります。たとえば、元のリソースがすでに存在する場合は、新しいリソース名を指定する必要があります。

Amazon EC2 インスタンスで SAP HANA を復元するには、特定のメタデータを含める必要があります。SAP HANA 固有の項目の StartRestoreJob メタデータを参照してください。

関連するメタデータを取得するには、呼び出し GetRecoveryPointRestoreMetadata を使用できます。

SAP HANA データベースの標準復旧ポイントの例:

```
"RestoreMetadata": {
        "BackupSize": "1660948480",
        "DatabaseName": "DATABASENAME",
        "DatabaseType": "SYSTEM",
        "HanaBackupEndTime": "1674838362",
        "HanaBackupId": "1234567890123",
        "HanaBackupPrefix": "1234567890123_SYSTEMDB_FULL",
        "HanaBackupStartTime": "1674838349",
        "HanaVersion": "2.00.040.00.1553674765",
        "IsCompressedBySap": "FALSE",
        "IsEncryptedBySap": "FALSE",
        "SourceDatabaseArn": "arn:aws:ssm-sap:region:accountID:HANA/applicationID/
DB/DATABASENAME",
        "SystemDatabaseSid": "HDB",
        "aws:backup:request-id": "46bbtt4q-7unr-2897-m486-yn378k2mrw9c"
    }
```

SAP HANA データベースの継続的復旧ポイントの例:

```
"RestoreMetadata": {
        "AvailableRestoreBases":
 "[1234567890123,9876543210987,1472583691472,7418529637418,1678942598761]",
        "BackupSize": "1711284224",
        "DatabaseName": "DATABASENAME",
        "DatabaseType": "TENANT",
        "EarliestRestorablePitrTimestamp": "1674764799789",
        "HanaBackupEndTime": "1668032687",
        "HanaBackupId": "1234567890123",
        "HanaBackupPrefix": "1234567890123_HDB_FULL",
        "HanaBackupStartTime": "1668032667",
```

```
        "HanaVersion": "2.00.040.00.1553674765",
        "IsCompressedBySap": "FALSE",
        "IsEncryptedBySap": "FALSE",
        "LatestRestorablePitrTimestamp": "1674850299789",
        "SourceDatabaseArn": "arn:aws:ssm-sap:region:accountID:HANA/applicationID/
DB/SystemDatabaseSid",
        "SystemDatabaseSid": "HDB",
        "aws:backup:request-id": "46bbtt4q-7unr-2897-m486-yn378k2mrw9d"
    }
```

EC2 での SAP HANA 用 CLI

コマンド `start-restore-job` は、Amazon リソースネーム (ARN) で識別された保存されたリソースを回復します。CLI は上記の API ガイドラインに従います。

概要:

```
start-restore-job
--recovery-point-arn value
--metadata value
--aws:backup:request-id value
[--idempotency-token value]
[--resource-type value]
[--cli-input-json value]
[--generate-cli-skeleton value]
[--debug]
[--endpoint-url value]
[--no-verify-ssl]
[--no-paginate]
[--output value]
[--query value]
[--profile value]
[--region value]
[--version value]
[--color value]
[--no-sign-request]
[--ca-bundle value]
[--cli-read-timeout value]
[--cli-connect-timeout value]
```

オプション

--recovery-point-arn (文字列) は、復旧ポイントを一意に識別する Amazon リソース番号 (ARN) 形式の文字列 (例: arn:aws:backup:*region*:123456789012:recovery-point:46bbtt4q-7unr-2897-m486-yn378k2mrw9d) です。

--metadata (マップ): メタデータのキーと値のペアのセット。リカバリポイントの復元に必要なリソース (リソース名など) を含みます。GetRecoveryPointRestoreMetadata を呼び出して、バックアップ時にリソースに関する構成メタデータを取得できます。ただし、GetRecoveryPointRestoreMetadata によって提供される値に加えて値リソースの復元が必要になる場合があります。Amazon EC2 インスタンスで SAP HANA を復元するには、特定のメタデータを指定する必要があります。

- aws:backup:request-id: これは同一性を保つために使用される任意の UUID 文字列です。これによって復元方法が変わることは一切ありません。
- aws:backup:TargetDatabaseArn: 復元先のデータベースを指定します。これが、Amazon EC2 での SAP HANA のデータベース ARN です。
- CatalogRestoreOption: カタログの復元元を指定します。NO_CATALOG、LATEST_CATALOG_FROM_AWS_BACKUP、CATALOG_FROM_LOCAL_PATH のうちのいずれか
- LocalCatalogPath: CatalogRestoreOption メタデータ値が の場合CATALOG_FROM_LOCAL_PATH、EC2 インスタンスのローカルカタログへのパスを指定します。これは、EC2 インスタンス内の有効なファイルパスである必要があります。
- RecoveryType: 現在、FULL_DATA_BACKUP_RECOVERY、POINT_IN_TIME_RECOVERY、および MOST_RECENT_TIME_RECOVERY のリカバリタイプがサポートされています。

キー = (文字列); 値 = (文字列)。短縮構文:

```
KeyName1=string,KeyName2=string
```

JSON 構文:

```
{"string": "string"
  ...}
```

--idempotency-token は、別の StartRestoreJob への同じコール間を区別するために使用できる顧客が選択した文字列です。同じ冪等性トークンで成功したリクエストを再試行すると、アクションは実行されず、成功メッセージが表示されます。

`--resource-type` は、次のいずれかのリソースの復旧ポイントを復元するジョブを開始する文字列です: Amazon EC2 上の SAP HANA 用 の SAP HANA on Amazon EC2。オプションで、コマンド `aws ssm-sap tag-resource` を使用して SAP HANA リソースにタグを付けることができます。

出力: `RestoreJobId` は、リカバリーポイントを復元するジョブを一意に識別する文字列です。

トラブルシューティング

バックアップオペレーションを試みているときに以下のエラーのいずれかが発生した場合は、関連する解決策を参照してください。

- エラー: 継続的バックアップログエラー

  継続的バックアップの復旧ポイントを維持するために、SAP HANA はすべての変更について ログを作成します。ログが利用できなくなると、これらの継続的復旧ポイントそれぞれのステータスは `STOPPED` になります。復元に使用できる最後の実行可能な復旧ポイントは、ステータスが `AVAILABLE` の復旧ポイントです。ステータスが `STOPPED` である復旧ポイントと、ステータスが `AVAILABLE` である復旧ポイントとの間でログデータが欠落している場合、その期間での復元が成功する保証はありません。この範囲内の日付と時刻を入力すると、 はバックアップ AWS Backup を試みますが、最も近い復元可能な時刻が使用されます。このエラーはメッセージ “`Encountered an issue with log backups. Please check SAP HANA for details.`" に表示されます

  解決策: コンソールには、ログに基づいて復元可能な最新の時刻が表示されます。表示されている時刻よりも新しい時刻を入力できます。ただし、この時刻のデータがログから利用できない場合、AWS Backup は復元可能な最新の時刻を使用します。

- エラー: `Internal error`

  解決策 : コンソールからサポートケースを作成するか、復元ジョブ ID などの復元の詳細 AWS Support について にお問い合わせください。

- エラー: `The provided role arn:aws:iam::`*`ACCOUNT_ID`*`:role/ServiceLinkedRole cannot be assumed by AWS Backup`

  解決策: 復元を呼び出す際に引き受けたロールに、サービスにリンクされたロールを作成するのに必要なアクセス許可があることを確認します。

- エラー: `User: arn:aws:sts::`*`ACCOUNT_ID`*`:assumed-role/ServiceLinkedRole/AWSBackup-ServiceLinkedRole is not authorized to perform: ssm-sap:GetOperation on resource: arn:aws:ssm-sap:us-east-1:`*`ACCOUNT_ID`*`:...`

解決策: 前提条件に記載されている復元用のアクセス許可を呼び出すときに引き受けるロールが正しく入力されていることを確認します。

- エラー: `b* 449: recovery strategy could not be determined: [111014] The backup with backup id '1660627536506' cannot be used for recovery SQLSTATE: HY000\n`

  解決策: Backint agent が正しくインストールされていることを確認します。すべての前提条件、特に SAP アプリケーションサーバーに AWS BackInt エージェントと AWS Systems Manager for SAP をインストールしてから、 BackInt エージェントのインストールを再試行してください。

- エラー: `IllegalArgumentException: Restore job provided is not ready to return chunks, current restore job status is: CANCELLED`

  解決策: 復元ジョブがサービスワークフローによってキャンセルされました。復元ジョブを再試行します。

- エラー: `RequestError: send request failed\ncaused by: read tcp 10.0.131.4:40482->35.84.99.47:443: read: connection timed out"`

  解決策: インスタンスで一時的にネットワークが不安定になっています。復元を再試行します。この問題が常に発生する場合は、`/hana/shared/aws-backint-agent/aws-backint-agent-config.yaml` のエージェント設定ファイルに `ForceRetry: "true"` を追加してみます。

その他の AWS Backint エージェント関連の問題については、「SAP HANA 用 AWS Backint Agent のトラブルシューティング」を参照してください。

DocumentDB クラスターの復元

AWS Backup コンソールを使用して Amazon DocumentDB 復旧ポイントを復元する

Amazon DocumentDB クラスターを復元するには、複数の復元オプションを指定する必要があります。これらのオプションについては、Amazon DocumentDB 開発者ガイドの「クラスタースナップショットからの復元」を参照してください。

Amazon DocumentDB クラスターを復元するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[Protected resources (保護されたリソース)] を選択し、復元する Amazon DocumentDB リソース ID を選択します。

3. [リソースの詳細] ページには、選択したリソース ID の復旧ポイントのリストが表示されます。リソースを復元するには、[バックアップ] ペインで、リソースの復旧ポイント ID の横にあるラジオボタンをクリックします。ペインの右上隅にある [復元] を選択します。
4. [設定] ペインで、デフォルトを受け入れるか、[クラスター識別子]、[エンジンバージョン]、[インスタンスクラス] および [インスタンス数] オプションを指定します。

   - 注: 復元時にデフォルト VPC が存在しない場合は、別の VPC のサブネットを指定する必要があります。
5. [ネットワークとセキュリティ] ペインには「設定なし」と表示されます。
6. Encryption-at-rest ペインで、デフォルトの を受け入れるか、暗号化を有効にするまたは暗号化を無効にする のオプションを指定します。
7. [クラスターオプション] ペインで、[ポート] に入力し、[クラスターパラメータグループ] を選択します。
8. Backup ペインで、 point-in-time 継続的バックアップリカバリ (PITR)、スケジュールされたスナップショットバックアップ、またはその両方を選択します。
9. ログエクスポートペインで、Amazon CloudWatch Logs に発行するログタイプを選択します。[IAM ロール] は既に定義されています。
10. [メンテナンス] ペインで、[メンテナンスウィンドウ] を指定するか、[優先設定なし] を指定します。
11. [タグ] ペインでは、[タグの追加] を選択できます。
12. [削除保護] ペインでは、[削除保護の有効化] を選択できます。
13. すべての設定を指定したら、[バックアップを復元] を選択します。

    [復元ジョブ] ペインが表示されます。ページ上部のメッセージには、復元ジョブに関する情報が表示されます。
14. 復元が完了したら、復元した Amazon DocumentDB クラスターを Amazon RDS インスタンスにアタッチします。

AWS Backup API、CLI、または SDK を使用して Amazon DocumentDB リカバリポイントを復元する

まず、クラスターを復元します。`StartRestoreJob` を使用します。Amazon DocumentDB 復元中に、以下のメタデータを指定できます。

```
availabilityZones
```

```
backtrackWindow
copyTagsToSnapshot // Boolean
databaseName // string
dbClusterIdentifier // string
dbClusterParameterGroupName // string
dbSubnetGroupName // string
enableCloudwatchLogsExports // string
enableIAMDatabaseAuthentication // Boolean
engine // string
engineMode // string
engineVersion // string
kmsKeyId // string
port // integer
optionGroupName // string
ScalingConfiguration
pcSecurityGroupIds // string
```

次に、`create-db-instance` を使用して、復元した Amazon DocumentDB クラスターを Amazon RDS インスタンスにアタッチします。

- Linux、macOS、Unix の場合:

```
aws docdb create-db-instance --db-instance-identifier sample-instance /
                  --db-cluster-identifier sample-cluster --engine docdb --db-
instance-class db.r5.large
```

- Windows の場合:

```
aws docdb create-db-instance --db-instance-identifier sample-instance ^
                  --db-cluster-identifier sample-cluster --engine docdb --db-
instance-class db.r5.large
```

Neptune クラスターの復元

AWS Backup コンソールを使用して Amazon Neptune 復旧ポイントを復元する

Amazon Neptune データベースを復元するには、複数の復元オプションを指定する必要があります。これらのオプションについては、Neptune ユーザーガイドの「DB クラスタースナップショットからの復元」を参照してください。

Neptune データベースを復元するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[Protected resources (保護されたリソース)] を選択し、復元する Neptune リソース ID を選択します。
3. [リソースの詳細] ページには、選択したリソース ID の復旧ポイントのリストが表示されます。リソースを復元するには、[バックアップ] ペインで、リソースの復旧ポイント ID の横にあるラジオボタンをクリックします。ペインの右上隅にある [復元] を選択します。
4. [インスタンスの仕様] ペインで、デフォルトを受け入れるか、[DB エンジン] および [バージョン] を指定します。
5. 設定ペインで、現在のリージョンで が所有するすべての DB クラスターインスタンス AWS アカウント に固有の名前を指定します。DB クラスター識別子は大文字と小文字の区別がありませんが、すべて小文字で保存されます (例: 「`mydbclusterinstance`」)。これは必須のフィールドです。
6. [Database options (データベースオプション)] ペインで、デフォルトを受け入れるか、[Database port (データベースポート)]、および [DB cluster parameter group (DB クラスターパラメータグループ)] 設定のオプションを指定します。
7. [暗号化] ペインで、デフォルトを使用するか、[暗号化を有効にする] または [[暗号化を無効にする] 設定のオプションを指定します。
8. ログエクスポートペインで、Amazon CloudWatch Logs に発行するログタイプを選択します。[IAM ロール] は既に定義されています。
9. [ロールを復元] ペインで、この復元のために AWS Backup が引き受ける IAM ロールを選択します。
10. すべての設定を指定したら、[バックアップを復元] を選択します。

    [復元ジョブ] ペインが表示されます。ページ上部のメッセージには、復元ジョブに関する情報が表示されます。
11. 復元が完了したら、復元した Neptune クラスターを Amazon RDS インスタンスにアタッチします。

AWS Backup API、CLI、または SDK を使用して Neptune リカバリポイントを復元する

まず、クラスターを復元します。`StartRestoreJob` を使用します。Amazon DocumentDB 復元中に、以下のメタデータを指定できます。

```
availabilityZones
backtrackWindow
copyTagsToSnapshot // Boolean
databaseName // string
dbClusterIdentifier // string
dbClusterParameterGroupName // string
dbSubnetGroupName // string
enableCloudwatchLogsExports // string
enableIAMDatabaseAuthentication // Boolean
engine // string
engineMode // string
engineVersion // string
kmsKeyId // string
port // integer
optionGroupName // string
ScalingConfiguration
pcSecurityGroupIds // string
```

次に、create-db-instance を使用して、復元した Neptune クラスターを Amazon RDS インスタンスにアタッチします。

- Linux、macOS、Unix の場合:

```
aws neptune create-db-instance --db-instance-identifier sample-instance \
                  --db-instance-class db.r5.large --engine neptune --engine-
version 1.0.5.0 --db-cluster-identifier sample-cluster --region us-east-1
```

- Windows の場合:

```
aws neptune create-db-instance --db-instance-identifier sample-instance ^
                  --db-instance-class db.r5.large --engine neptune --engine-
version 1.0.5.0 --db-cluster-identifier sample-cluster --region us-east-1
```

詳細については、「Neptune 管理 API リファレンス」の「RestoreDBClusterFromSnapshot」と「Neptune CLI ガイド」の「restore-db-cluster-from-snapshot」を参照してください。

CloudFormation スタックバックアップの復元

CloudFormation 複合バックアップは、 CloudFormation テンプレートと関連するすべてのネストされた復旧ポイントの組み合わせです。ネストされた復旧ポイントはいくつでも復元できますが、複合復旧ポイント (最上位の復旧ポイント) は復元できません。

CloudFormation テンプレート復旧ポイントを復元するときは、バックアップを表すように変更が設定された新しいスタックを作成します。

AWS Backup コンソール CloudFormation を使用して復元します。

CloudFormation コンソールから、新しいスタックと変更セットを確認できます。変更セットの詳細は、「AWS CloudFormation ユーザーガイド」の「変更セットを使用してスタックを更新する」を参照してください。

スタックで CloudFormation復元するネストされた復旧ポイントを特定し、 AWS Backup コンソールを使用して復元します。

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. [バックアップボールト] に移動し、目的の復旧ポイントを含むバックアップボールトを選択して、[復旧ポイント] をクリックします。
3. AWS CloudFormation テンプレート復旧ポイントを復元します。

    a. 復元するネストされた復旧ポイントを含む複合復旧ポイントをクリックすると、その複合復旧ポイントの詳細ページが表示されます。

    b. ネストされた復旧ポイントには、ネストされた復旧ポイントが表示されます。各復旧ポイントには、復旧ポイント ID、ステータス、リソース ID、リソースタイプ、バックアップタイプ、および復旧ポイントが作成された時刻があります。 AWS CloudFormation 復旧ポイントの横にあるラジオボタンをクリックし、復元 をクリックします。リソースタイプが AWS CloudFormation で、バックアップタイプがバックアップである復旧ポイントを選択していることを確認します。
4. CloudFormation テンプレートの復元ジョブが完了すると、復元された AWS CloudFormation テンプレートが AWS CloudFormationスタックの コンソールに表示されます。
5. [スタック名] の下に、ステータスが `REVIEW_IN_PROGRESS` の復元されたテンプレートが表示されます。
6. スタックの名前をクリックすると、スタックの詳細が表示されます。
7. スタックの名前の下にタブがあります。[セットを変更] をクリックします。

8. 変更セットを実行します。
9. この処理が完了すると、元のスタックのリソースが新しいスタックに再作成されます。ステートフルリソースは空の状態で再作成されます。ステートフルリソースを復旧するには、 AWS Backup コンソールの復旧ポイントのリストに戻り、必要な復旧ポイントを選択して復元を開始します。

CloudFormation で復元する AWS CLI

コマンドラインインターフェイスでは、 `start-restore-job`を使用してスタックを CloudFormation復元できます。

次のリストは、 CloudFormation リソースを復元するために受け入れられるメタデータです。

```
// Mandatory metadata:
ChangeSetName // This is the name of the change set which will be created
StackName // This is the name of the stack that will be created by the new change set

// Optional metadata:
ChangeSetDescription // This is the description of the new change set
StackParameters // This is the JSON of the stack parameters required by the stack
aws:backup:request-id
```

復元テスト

トピック

- 概要
- 復元テストと復元プロセスの比較
- 復元テストの管理
- 復元テストプランの作成
- 復元テストプランの更新
- 既存の復元テストプランの表示
- 復元テストジョブの表示
- 復元テストプランの削除
- 復元テストの監査

- 復元テストのクォータとパラメータ
- 復元テストの失敗のトラブルシューティング
- 復元テストの推定メタデータ
- 復元テストの検証

概要

が提供する機能である復元テスト は AWS Backup、復元の実行可能性を自動的かつ定期的に評価し、復元ジョブの継続時間をモニタリングする機能を提供します。

まず、復元テストプランを作成します。復元テストプランには、プランの名前、復元テストの頻度、目標開始時間を指定します。次に、プランに含めるリソースを割り当てます。次に、test. AWS Backup backup に特定の復旧ポイントまたはランダムな復旧ポイントを含めることを選択します。バックアップは、復元ジョブを成功させるために必要なメタデータをインテリジェントに推測します。

プランのスケジュールされた時刻が到着すると、 はプランに基づいて復元ジョブ AWS Backup を開始し、復元の完了にかかる時間をモニタリングします。

復元テストプランの実行が完了したら、その結果を使用して、復元テストのシナリオの正常な完了や復元ジョブの完了時間など、組織またはガバナンス上の要件に準拠しているかどうかを確認できます。

オプションで、 復元テストの検証を使用して復元テスト結果を確認できます。

オプションの検証が完了するか、検証ウィンドウが閉じると、 は復元テストに関連するリソース AWS Backup を削除し、リソースはサービス SLAs に従って削除されます。

テストプロセスが終了すると、テストの結果と完了時間を確認できます。

復元テストと復元プロセスの比較

復元テストでは、オンデマンド復元と同じ方法で復元ジョブを実行し、オンデマンド復元と同じ復旧ポイント (バックアップ) を使用します。復元テストによって開始されたジョブごとに CloudTrail 、(オプトインされている場合) `StartRestoreJob`で への呼び出しが表示されます。

ただし、スケジュールされた復元テストとオンデマンドの復元のオペレーションには、いくつかの違いがあります。

	復元テスト	復元
アカウント	推奨されるベストプラクティスは、復元テストに使用するアカウントを指定することです。	特定のアカウントのリソースを復元できます。
AWS Backup Audit Manager	コントロールを有効にして、復元テストが指定された復元目標を満たしているかどうかを確認できます。	
頻度	スケジュール設定されているプランの一環として定期的に実行されます。	オンデマンド
リージョナリティー	イスラエル (テルアビブ) を除く、 が AWS Backup 運営するすべての商用リージョンで利用可能 利用不可 AWS GovCloud （米国東部）、 AWS GovCloud （米国西部）、中国 (北京）、中国 (寧夏）。	AWS Backup が運営されているすべての商用リージョンで利用可能
リソース	テストプランに割り当てることができるリソースタイプには、Aurora、Amazon DocumentDB、Amazon DynamoDB、Amazon EBS、Amazon EC2、Amazon EFS、Amazon FSx (Lustre、ONTAP、OpenZFS、Windows)、Amazon Neptune、Amazon	すべてのリソースを復元できます。

	復元テスト	復元
	RDS、Amazon S3 があります。	
結果	復元テストジョブが完了すると、復元されたリソースは復元テストの検証ウィンドウの終了後に削除されます。	復元ジョブが完了すると、復元されたバージョンのリソースはそのまま残ります。
タグ	復元時にタグをサポートするリソースタイプでは、テストに際して復元時にタグが適用されます。	サポートされているリソースでは、タグは省略可能です。

復元テストの管理

復元テストプランは AWS Backup コンソールで作成、表示、更新、削除できます。

AWS CLI を使用すると、復元テストプランの操作をプログラムによって実行できます。各 CLI は、その CLI が発信される AWS サービスに固有です。コマンドの先頭には `aws backup` を付ける必要があります。

データの削除

復元テストが完了すると、 はテストに関係するリソースの削除 AWS Backup を開始します。この削除は即時には行われません。各リソースには、それらのリソースの保存方法とライフサイクル方法を決定する基盤となる設定があります。例えば、Amazon S3 バケットが復元テストに含まれている場合、ライフサイクルルールがバケットに追加されます。ルールが実行され、バケットとそのオブジェクトが完全に削除されるまでに数日かかることがありますが、これらのリソースに対して課金されるのは、このライフサイクルルールが開始される日 (デフォルトでは 1 日) までです。削除の速さはリソースタイプによって異なります。

復元テストプランに含まれるリソースには、`awsbackup-restore-test` というタグが含まれています。ユーザーがこのタグを削除した場合、テスト期間の終了時にリソースを削除 AWS Backup することはできません。代わりに手動で削除する必要があります。

リソースが想定どおりに削除されなかった理由を確認するには、コンソールで失敗したジョブを検索するか、コマンドラインインターフェイスを使用して API リクエスト DescribeRestoreJob を呼び出し、削除ステータスメッセージを取得します。

バックアッププラン (非復元テストプラン) は、復元テストによって作成されたリソース (で始まるタグawsbackup-restore-testまたは名前を持つもの) を無視しますawsbackup-restore-test。

コスト管理

復元テストでは復元テスト 1 回ごとにコストがかかります。復元テストプランに含まれるリソースによっては、プランに含まれる復元ジョブにもコストがかかる場合があります。詳細については、「AWS Backup の料金」を参照してください。

復元テストプランを初めて設定するときは、機能、プロセス、および関連する平均コストについて理解するために、最小限のリソースタイプと保護対象リソースを含めることをお勧めします。プランの作成後に、リソースタイプや保護対象リソースをさらに追加してプランを更新できます。

復元テストプランの作成

復元テストプランには、プランの作成とリソースの割り当ての 2 つのステップがあります。

コンソールを使用する場合、これらのステップは順番に行われます。最初の部分では、名前、頻度、開始時間を設定します。2 番目の部分では、テストプランにリソースを割り当てます。

AWS CLI と API を使用する場合は、まず を使用しますcreate-restore-testing-plan。成功のレスポンスを受け取り、プランが作成されたら、プランに含めるリソースタイプごとに create-restore-testing-selection を使用します。

Console

パート I: コンソールを使用して復元テストプランを作成する

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. 左側のナビゲーションで、[復元テスト] を選択します。
3. [復元テストプランを作成] を選択します。
4. 全般

    a. 名前: 新しい復元テストプランの名前を入力します。作成後にこの名前を変更することはできません。名前には英数字とアンダースコアのみを使用できます。

b. テスト頻度: 復元テストを実行する頻度を選択します。

c. 開始時間: テストを開始する時間 (時間と分) を設定します。復元テストプランを実行するローカルタイムゾーンを設定することもできます。

d. 開始時間： この値 (時間単位) は、復元テストの開始が指定されている期間です。 は AWS Backup 、指定されたすべての復元ジョブを開始時間内に開始し、この期間内の開始時間をランダム化するために最善を尽くします。

5. 回復ポイントの選択: ここでは、ソースボールト、復旧ポイントの範囲、およびプランに含める復旧ポイント (バックアップ) の選択基準を設定します。

a. ソースボールト: 使用可能なすべてのボールトを含めるか、プランに追加する復旧ポイントを絞り込むために特定のボールトのみを含めるかを選択します。[特定のボールト] を選択した場合は、ドロップダウンメニューから目的のボールトを選択します。

b. 対象となる復旧ポイント: 復旧ポイントを選択する期間を指定します。1～365 日、1 ～ 52 週間、1 ～ 12 か月、または 1 年を選択できます。

c. 選択基準: 復旧ポイントの日付範囲を指定したら、直近の復旧ポイントをプランに含めるか、ランダムに 1 つの復旧ポイントを含めるかを選択できます。古いバージョンへの復元が必要になった場合に備えて、ランダムな選択によって復旧ポイントの全般的な状態をより定期的に測定することをお勧めします。

d. P oint-in-time リカバリポイント： プランに継続的バックアップ (point-in-time-restore/PITR) ポイントを持つリソースが含まれている場合は、このチェックボックスをオンにして、テストプランに適格なリカバリポイントとして継続的バックアップを含めることができます (リソースタイプにこの機能があるリソース別の機能の可用性を参照) 。

6. (オプション) 復元テストプランに追加されたタグ: 復元テストプランには最大 50 個のタグを追加できます。各タグは個別に追加する必要があります。タグを追加するには、[新しいタグを追加] を選択します。

パート II: コンソールを使用してプランにリソースを割り当てる

このセクションでは、復元テストプランに含めるバックアップ済みのリソースを選択します。リソース割り当ての名前を選択し、復元テストに使用するロールを選択して、クリーンアップまでの保持期間を設定します。次に、リソースタイプと範囲を選択し、必要に応じてタグを使用して選択内容を絞り込みます。

> **Tip**
>
> リソースを追加する復元テストプランに戻るには、AWS Backup コンソールに移動して [復元テスト] を選択し、目的のテストプランを見つけて選択します。

1. 全般

   a. リソース割り当て名: このリソース割り当ての名前を、英数字とアンダースコアを使用して入力します。スペースは使用できません。

   b. IAM ロールを復元: テストでは、指定した Identity and Access Management (IAM) ロールを使用する必要があります。 AWS Backup デフォルトのロールまたは別のロールを選択できます。このプロセスの完了時に AWS Backup デフォルトがまだ存在しない場合、AWS Backup は必要なアクセス許可でデフォルトを自動的に作成します。復元テスト用に選択する IAM ロールには、「AWSBackupServicePolicyForRestores」に記載されているアクセス許可が付与されている必要があります。

   c. クリーンアップ前の保持期間: 復元テストにおいて、バックアップデータは一時的に復元されます。デフォルトでは、このデータはテスト完了後に削除されます。復元に関する検証を実行する場合は、このデータの削除を遅らせることもできます。

      検証の実行を予定している場合は、[特定の時間数について保持] を選択し、1 ~ 168 時間の値を入力します。検証はプログラムで実行できますが、 AWS Backup コンソールでは実行できないことに注意してください。

2. 保護されたリソース

   a. リソースタイプを選択: 復元テストプランに含めるリソースタイプとそのタイプのバックアップの範囲を選択します。各プランには複数のリソースタイプを含めることができますが、各タイプのリソースを個別にプランに割り当てる必要があります。

   b. リソースの選択の範囲: タイプを選択したら、そのタイプの保護対象リソースをすべて含めるか、特定の保護対象リソースのみを含めるかを選択します。

   c. (オプション) タグを使用してリソースの選択を絞り込む: バックアップにタグが付いている場合は、タグでフィルタリングして特定の保護対象リソースを選択できます。タグキー、このキーを含めるか含めないかの条件、およびキーの値を入力します。次に、[タグを追加] ボタンを選択します。

      保護対象リソースが含まれるバックアップボールト内の直近の復旧ポイントのタグをチェックすることで、保護対象リソースのタグが評価されます。

3. 復元パラメータ: 一部のリソースでは、復元ジョブの準備としてパラメータを指定する必要があります。ほとんどの場合、 AWS Backup は保存されたバックアップに基づいて値を推測します。

   通常、これらのパラメータはそのままにしておくことをお勧めしますが、ドロップダウンメニューから別のパラメータを選択して値を変更することもできます。値の変更が適している例としては、暗号化キーの上書き、データを推定できない Amazon FSx 設定、サブネットの作成などがあります。

   例えば、復元テストプランに割り当てるリソースタイプの 1 つが RDS データベースである場合、アベイラビリティーゾーン、データベース名、データベースインスタンスクラス、VPC セキュリティグループなどのパラメータが推定値とともに表示され、必要に応じて値を変更できます。

AWS CLI

復元テストプランの作成には CLI コマンド `CreateRestoreTestingPlan` を使用します。

テストプランには以下が含まれている必要があります。

- `RestoreTestingPlan` (固有の `RestoreTestingPlanName` が含まれている必要があります)
- `ScheduleExpression` Cron 式
- `RecoveryPointSelection`

  名前は似ていますが、これは と同じではありません`RestoreTestingSelection`。

  `RecoveryPointSelection` には 5 つのパラメータがあります (3 つは必須、2 つはオプション) 。指定した値によって、復元テストに含まれる復旧ポイントが決まります。内で最新の復旧ポイントが必要`Algorithm`かどうか`SelectionWindowDays`、またはランダムな復旧ポイントが必要かどうかを示す必要があります。また、どのボールト`IncludeVaults`から復旧ポイントを選択できるかを示す必要があります。

選択には 1 つ以上の保護リソース ARN を含めることも、1 つ以上の条件を含めることもできますが、両方を含めることはできません。

以下を含めることもできます。

- `ScheduleExpressionTimezone`
- `Tags`

- CreatorRequestId
- StartWindowHours

CLI コマンド create-restore-testing-plan を使用します。

プランが正常に作成されたら、create-restore-testing-selection を使用してプランにリソースを割り当てる必要があります

これは、RestoreTestingSelectionName、ProtectedResourceType と、以下のいずれかで構成されます。

- ProtectedResourceArns

- ProtectedResourceConditions

保護対象リソースのタイプごとに値を 1 つ設定できます。復元テスト選択には、ProtectedResourceArns のワイルドカード値 (「*」) を ProtectedResourceConditions と併せて含めることができます。または、ProtectedResourceArns に保護対象リソースの ARN を最大 30 個まで含めることもできます。

復旧ポイントの決定

テストプランが実行されるたびに (指定した頻度と開始時刻に従って)、選択した保護されたリソースごとに 1 つの適格な復旧ポイントが復元テストによって復元されます。リソースのリカバリポイントがリカバリポイントの選択基準を満たしていない場合、そのリソースはテストに含まれません。

テスト選択内の保護されたリソースの復旧ポイントは、 が指定された時間枠の基準を満たし、復元テストプランにボールトが含まれている場合に適格です。

リソーステストの選択にリソースタイプが含まれ、次のいずれかの条件が満たされた場合、保護されたリソースが選択されます。

- リソース ARN はその選択で指定されます。または、
- その選択のタグ条件は、リソースの最新の復旧ポイントのタグと一致します。

復元テストプランの更新

コンソールまたは AWS CLIを使用して、復元テストプランの一部と、プランで指定されたリソースの選択内容を更新できます。

Console

コンソールで復元テストプランと選択内容を更新する

コンソールで復元テストプランの詳細ページを表示すると、プランの設定の多くを編集 (更新) できます。以下の手順に従ってください。

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. 左側のナビゲーションで、[復元テスト] を選択します。
3. [編集] ボタンを選択します。
4. 頻度、開始時間、選択した開始時間からテストを開始するまでの時間範囲を調整します。
5. 変更を保存します。

AWS CLI

による復元テストプランと選択の更新 AWS CLI

リクエストUpdateRestoreTestingPlanと UpdateRestoreTestingSelection は、指定されたプランまたは選択に部分的な更新を送信するために使用できます。名前は変更できませんが、他のパラメーターは更新できます。各リクエストには変更するパラメータのみを含めてください。

更新リクエストを送信する前に、 GetRestoreTestingPlanと を使用して、 に RestoreTestingSelection特定の ARNs、ワイルドカードと条件を使用しているかGetRestoreTestingSelectionを判断します。

復元テストの選択で (ワイルドカードではなく) ARN が指定されていて、それを条件付きのワイルドカードに変更する場合は、更新リクエストに ARN のワイルドカードと条件の両方を含める必要があります。選択内容には、保護対象リソースの ARN を含めることも、条件付きのワイルドカードを使用することもできますが、両方を含めることはできません。

- `get-restore-testing-plan`
- `get-restore-testing-selection`
- `update-restore-testing-plan`

- update-restore-testing-selection

既存の復元テストプランの表示

Console

コンソールで既存の復元テストプランと割り当てられたリソースに関する詳細を表示する

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. 左側のナビゲーションで、[復元テスト] を選択します。ディスプレイに復元テストプランが表示されます。デフォルトでは、最後に実行されたプランから順に表示されます。
3. プランからリンクを選択すると、プランの概要、名前、頻度、開始時間、開始までの時間範囲などの詳細が表示されます。

また、このプランに割り当てられている保護対象リソース、このプランに含まれる直近の 30 日間の復元テストジョブ、このテストプランの一部として作成されたタグも表示できます。

AWS CLI

コマンドラインを使用して、既存の復元テストプランとテストの選択内容に関する詳細を取得する

- list-restore-testing-plan
- list-restore-testing-selections
- get-restore-testing-plan
- get-restore-testing-selection

復元テストジョブの表示

Console

コンソールで既存の復元テストジョブを表示する

復元テストジョブは復元ジョブページに表示されます。

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. [ジョブ] ページに移動します。

または、[復元テスト] を選択し、復元テストプランを選択すると、その詳細とプランに関連するジョブを確認できます。

3. [復元ジョブ] タブを選択します。

   このページでは、復元ジョブのステータス、復元時間、復元タイプ、リソース ID、リソースタイプ、ジョブが属する復元テストプラン、作成時間、復旧ポイント ID を確認できます。

   復元テストプランに含まれるジョブは、復元タイプが [テスト] と表示されます。

復元テストジョブには複数のステータスカテゴリがあります。

- 注意が必要なステータスタイプには下線が表示されており、ステータスにカーソルを合わせると、追加の詳細情報が表示されます (ある場合)。
- テストで 復元テストの検証が開始された場合 (コンソールでは使用不可)、検証ステータスが表示されます。
- [削除ステータス] には、復元テストで生成されたデータのステータスが表示されます。削除ステータスには、[成功]、[削除中]、[失敗] の 3 つがあります。

  復元テストジョブの削除が失敗の場合、復元テストのフローでリソースが自動的に削除されていないないため、リソースを手動で削除する必要があります。多くの場合、`awsbackup-restore-test` のタグがリソースから削除されると、削除の失敗が起きる原因となります。

AWS CLI

コマンドラインから既存の復元テストジョブを表示する

- `list-restore-jobs-by-protected-resource`

復元テストプランの削除

Console

コンソールで復元テストプランを削除する

1. 「既存の復元テストプランの表示」に従って、既存の復元テストプランを確認します。
2. 復元テストプランの詳細ページで、[削除] を選択してプランを削除します。

3. [削除] を選択すると、プランを削除するかどうかを確認するポップアップ画面が表示されます。この画面には、特定の復元テストプランの名前が太字で表示されます。続行するには、このテストプランの正確な名前を、アンダースコア、ダッシュ、ピリオドをすべて含め、大文字と小文字を区別して入力します。

   [復元テストプランを削除] オプションが選択できない場合は、表示された名前と一致するまで名前を再入力します。名前が完全に一致すると、[復元テストプランを削除] オプションが選択可能になります。

AWS CLI

コマンドラインで復元テストプランを削除する

CLI コマンドを使用して、復元テストの選択を削除DeleteRestoreTestingSelectionできます。リクエストには `RestoreTestingPlanName` と `RestoreTestingSelectionName` 含めます。

テストプランを削除する前に、テストプランに関連付けられているすべてのテスト選択を削除する必要があります。すべてのテスト選択が削除されたら、 API リクエストを使用して復元テストプランDeleteRestoreTestingPlanを削除できます。`RestoreTestingPlanName` を含める必要があります。

- `delete-restore-testing-selection`
- `delete-restore-testing-plan`

復元テストの監査

復元テストと AWS Backup Audit Manager の統合は、復元されたリソースがターゲット復元時間内に完了したかどうかを評価するのに役立ちます。

詳細については、「AWS Backup Audit Manager のコントロールと修正」の「リソースが目標に達するまでの復元時間」を参照してください。

復元テストのクォータとパラメータ

- 復元テストプラン 100 個
- 復元テストプランごとに 50 個のタグを追加可能
- プランあたり 30 件の選択

- 選択ごとに 30 個の保護対象リソース ARN
- 選択ごとに 30 個の保護対象リソース条件 (StringEquals と StringNotEquals の両方に含まれるものを含む)
- 選択ごとに 30 のボールト選択項目
- 選択期間の最大日数: 365 日
- 開始期間の時間範囲: 最小: 1 時間、最大: 168 時間 (7 日間)
- プラン名の最大長: 50 文字
- 選択名の最大長: 50 文字

制限に関する追加情報については、「AWS Backup クォータ」を参照してください。

復元テストの失敗のトラブルシューティング

復元ステータスが の復元テストジョブがある場合Failed、次の理由が原因と修復方法を決定するのに役立ちます。

エラーメッセージは、コンソールのジョブステータスの詳細ページ、または CLI コマンドlist-restore-jobs-by-protected-resourceまたは を使用して表示できますlist-restore-jobs。 AWS Backup

1. エラー: *No default VPC for this user. GroupName is only supported for EC2-Classic and default VPC.*

   解決策 1: 復元テストの選択内容を更新し、パラメータ を上書きしますSubnetId。 AWS Backup コンソールには、このパラメータが「サブネット」と表示されます。

   解決策 2: デフォルトの VPC を再作成します。

   影響を受けるリソースタイプ： Amazon EC2

2. エラー: *No subnets found for the default VPC [vpc]. Please specify a subnet.*

   解決策 1: 復元テストの選択内容を更新し、SubnetId復元パラメータを上書きします。 AWS Backup コンソールには、このパラメータが「サブネット」と表示されます。

   解決策 2: デフォルト VPC にデフォルトサブネットを作成します。

影響を受けるリソースタイプ： Amazon EC2

3. エラー: *No default subnet detected in VPC. Please contact AWS Support to recreate default Subnets.*

   解決策 1: 復元テストの選択内容を更新し、DBSubnetGroupName復元パラメータを上書きします。コンソールには AWS Backup 、このパラメータがサブネットグループとして表示されます。

   解決策 2: デフォルト VPC にデフォルトサブネットを作成します。

   影響を受けるリソースタイプ： Amazon Aurora、Amazon DocumentDB、Amazon RDS、Neptune

4. エラー： *IAM Role cannot be assumed by AWS Backup*。

   解決策： 復元ロールは によって引き受け可能である必要があります AWS Backup。IAM でロールの信頼ポリシーを更新して による引き受けを許可するか、復元テストの選択"backup.amazonaws.com"を更新して が引き受けることができるロールを使用します AWS Backup。

   影響を受けるリソースタイプ： すべて

5. エラー： *Access denied to KMS key.*または *The specified AWS KMS key* ARN *does not exist, is not enabled or you do not have permissions to access it.*

   解決策： 以下を確認します。

   a. 復元ロールは、バックアップの暗号化に使用される AWS KMS キーと、該当する場合は、復元されたリソースの暗号化に使用される KMS キーにアクセスできます。
   b. 上記の KMS キーのリソースポリシー (複数可) により、復元ロールはそれらにアクセスできます。

   上記の条件がまだ満たされていない場合は、適切なアクセスのために復元ロールとリソースポリシーを設定します。次に、復元テストジョブを再度実行します。

   影響を受けるリソースタイプ： すべて

6. エラー： *User ARN is not authorized to perform action on resource because no identity based policy allows the action.*または *Access denied performing s3:CreateBucket on awsbackup-restore-test-xxxxxx*。

解決策： 復元ロールに適切なアクセス許可がありません。復元ロールの IAM のアクセス許可を更新します。

影響を受けるリソースタイプ： すべて

7. エラー: *User ARN is not authorized to perform action on resource because no resource-based policy allows the action.* または *User ARN is not authorized to perform action on resource with an explicit deny in a resource based policy.*

   解決策： 復元ロールに、メッセージで指定されたリソースへの適切なアクセス権がありません。前述のリソースのリソースポリシーを更新します。

   影響を受けるリソースタイプ： すべて

復元テストの推定メタデータ

復旧ポイントを復元するには、復元メタデータが必要です。復元テストを実行する場合、復元が成功する可能性が高いメタデータが、 AWS Backup によって自動的に推定されます。コマンドを使用して、 AWS Backup が推測する内容をプレビューget-restore-testing-inferred-metadataできます。コマンドは、 によって推測されたメタデータのセットget-restore-job-metadataを返します AWS Backup。一部のリソースタイプ (Amazon FSx) では、 AWS Backup はメタデータの完全なセットを推測できないことに注意してください。

推定の復元メタデータは、復元テストプロセス中に決定されます。RestoreTestingSelection の本文にパラメータ RestoreMetadataOverrides を含めることで、特定の復元メタデータのキーを上書きできます。一部のメタデータオーバーライドは AWS Backup コンソールでは使用できません。

サポートされている各リソースには、推定される復元メタデータのキーと値のペアと、上書き可能な復元メタデータのキーの両方があります。含める必要があるのは、RestoreMetadataOverrides のキーと値のペア、または「*##########*」とマークされているネストされたキーと値のペアのみで、それ以外のものはオプションです。キーの値では、大文字と小文字が区別されないことに注意してください。

> **Important**
>
> AWS Backup は、Amazon EC2 インスタンスや Amazon RDS クラスターがデフォルト VPC に復元されるなど、リソースをデフォルト設定に復元する必要があると推測できます。ただし、デフォルトの VPC やサブネットが削除され、メタデータの上書きが入力されていない場合など、デフォルトが存在しない場合、復元は成功しません。

リソースタイプ	推定される復元メタデータのキーと値	上書き可能なメタデータ

DynamoDB	`deletionProtection` 、値は `false` に設定されます。
	
	`encryptionType` は、`Default` に設定されます。
	
	`targetTableName` 、値は `awsbackup-restore-test-` で始まるランダム値に設定されます。
		`encryptionType`
		
		`kmsMasterKeyArn`

Amazon EBS	`availabilityZone` 、値はランダムなアベイラビリティーゾーンに設定されます。
	
	`encrypted` 、値は `true` に設定されます。
		`availabilityZone`
		
		`kmsKeyId`

「Amazon EC2」	`disableApiTermination` 値は `false` に設定されます。
	
	`instanceType` 値は復元される復旧ポイントのインスタンスタイプに設定されます。
		`iamInstanceProfileName` 値は null または `UseBackedUpValue`
		
		`instanceType`
		
		`requireImdsV2`

リソースタイプ	推定される復元メタデータのキーと値	上書き可能なメタデータ
	requiredImdsV2 値は true に設定されます。	securityGroupIds subnetId
Amazon EFS	encrypted 値は true に設定されます。 file-system-id 値は復元される復旧ポイントのファイルシステム ID に設定されます。 kmsKeyId value は、alias/aws/elasticfilesystem に設定されます。 newFileSystem 値は true に設定されます。 performanceMode 値は generalPurpose に設定されます。	kmsKeyId
Amazon FSx for Lustre	lustreConfiguration にはネストされたキーがあります。ネストされたキーの 1 つは automaticBackupRetentionDays で、値は 0 に設定されます。	kmsKeyId lustreConfiguration にはネストされたキー logConfiguration があります。 securityGroupIds subnetIds 、##########

リソースタイプ	推定される復元メタデータのキーと値	上書き可能なメタデータ
Amazon FSx for NetApp ONTAP	name は awsbackup _restore_test_ で始まるランダム値に設定されます。 ontapConfiguration には次のようなネストされたキーがあります。 • junctionPath 、/name は復元するボリュームの名前です。 • sizeInMegabytes 、値は復元する復旧ポイントのサイズ (MB 単位) に設定されます。 • snapshotPolicy 、値は none に設定されます。	ontapConfiguration には、次のような特定の上書き可能なネストされたキーがあります。 • junctionPath • ontapVolumeType • securityStyle • sizeInMegabytes • storageEfficiencyEnabled • storageVirtualMachineId 、########## • tieringPolicy

リソースタイプ	推定される復元メタデータのキーと値	上書き可能なメタデータ
Amazon FSx for OpenZFS	openZfzConfiguration 、次のようなネストされたキーがあります。 • automaticBackupRetentionDays 、値は 0 に設定されます。 • deploymentType 、値は復元する復旧ポイントのデプロイタイプに設定されます。 • throughputCapacity 、値は deploymentType に基づいて決まります。deploymentType が SINGLE_AZ_1 の場合、値は 64 に設定され、deploymentType が SINGLE_AZ_2 or MULTI_AZ_1 の場合、値は 160 に設定されます。	kmsKeyId openZfsConfiguration には、次のような特定の上書き可能なネストされたキーがあります。 • deploymentType • throughputCapacity • diskiopsConfiguration securityGroupIds subnetIds

リソースタイプ	推定される復元メタデータのキーと値	上書き可能なメタデータ
Amazon FSx for Windows File Server	windowsConfiguration 、次のようなネストされたキーがあります。 • automaticBackupRetentionDays 、値は 0 に設定されます。 • deploymentType 、値は復元する復旧ポイントのデプロイタイプに設定されます。 • throughputCapacity 、値は 8 に設定されます。	kmsKeyId securityGroupIds subnetIds 、*##########* windowsConfiguration 、特定の上書き可能なネストされたキーがあります。 • throughputCapacity • activeDirectoryId *########## selfManagedActiveDirectoryConfiguration ######## ###* • selfManagedActiveDirectoryConfiguration *########## #activeDirectoryId ###### ###* • preferredSubnetId

リソースタイプ	推定される復元メタデータのキーと値	上書き可能なメタデータ
Amazon RDS、Aurora、Amazon DocumentDB、Amazon Neptune クラスター	availabilityZones 、値は最大 3 つのランダムなアベイラビリティーゾーンのリストに設定されます。 dbClusterIdentifier 、awsbackup-restore-test で始まるランダム値 engine、値は復元する復旧ポイントのエンジンに設定されます。	availabilityZones databaseName dbClusterParameterGroupName dbSubnetGroupName enableCloudwatchLogsExports enableIamDatabaseAuthentication engine engineMode engineVersion kmskeyId port optionGroupName scalingConfiguration vpcSecurityGroupIds

リソースタイプ	推定される復元メタデータのキーと値	上書き可能なメタデータ
Amazon RDS インスタンス	dbInstanceIdentifier 、awsbackup-restore-test- で始まるランダム値 deletionProtection 、値は false に設定されます。 multiAz、値は false に設定されます。 publiclyAccessible 、値は false に設定されます。	allocatedStorage availabilityZones dbInstanceClass dbName dbParameterGroupName dbSubnetGroupName domain domainIamRoleName enableCloudwatchLogsExports enableIamDatabaseAuthentication iops licensemodel multiAz optionGroupName port processorFeatures publiclyAccessible storageType vpcSecurityGroupIds

リソースタイプ	推定される復元メタデータのキーと値	上書き可能なメタデータ
Amazon Simple Storage Service (Amazon S3)	destinationBucketName 、awsbackup-restore-test- で始まるランダム値 encrypted 、値は true に設定されます。 encryptionType 、値は SSE-S3 に設定されます。 newBucket 、値は true に設定されます。	encryptionType kmsKey

復元テストの検証

復元テストジョブの完了時に実行されるイベント駆動型検証を作成するオプションがあります。

まず、 など EventBridge、Amazon でサポートされているターゲットを使用して検証ワークフローを作成します AWS Lambda。次に、復元ジョブがステータス に達するのをリッスンする EventBridge ルールを追加しますCOMPLETED。3 つ目は、復元テストプランを作成する (または既存のプランをスケジュールどおりに実行させる) ことです。最後に、復元テストが完了したら、検証ワークフローのログをモニタリングして、期待どおりに実行されたことを確認します (検証が実行されると、検証ステータスがAWS Backup コンソール に表示されます)。

1. 検証ワークフローを設定する

   Lambda または でサポートされている他のターゲットを使用して、検証ワークフローを設定できます EventBridge。例えば、Amazon EC2 インスタンスを含む復元テストを検証する場合、ヘルスチェックエンドポイントに ping を実行するコードを含めることができます。

   イベントの詳細を使用して、検証するリソースを決定できます (複数可)。

   カスタム Lambda レイヤーを使用して最新の SDK を使用できます (Lambda SDK 経由でPutRestoreValidationResultはまだ利用できないため)。

サンプルは次のとおりです。

```
import { Backup } from "@aws-sdk/client-backup";

export const handler = async (event) => {
  console.log("Handling event: ", event);

  const restoreTestingPlanArn = event.detail.restoreTestingPlanArn;
  const resourceType = event.detail.resourceType;
  const createdResourceArn = event.detail.createdResourceArn;

  // TODO: Validate the resource

  const backup = new Backup();
  const response = await backup.putRestoreValidationResult({
    RestoreJobId: event.detail.restoreJobId,
    ValidationStatus: "SUCCESSFUL", // TODO
    ValidationStatusMessage: "" // TODO
  });

  console.log("PutRestoreValidationResult: ", response);
  console.log("Finished");
};
```

2. EventBridge ルールを追加する

復元ジョブ[COMPLETEDイベント をリッスンする EventBridge ルールを作成します](#)。

オプションで、リソースタイプまたは復元テストプラン ARN でイベントをフィルタリングできます。このルールのターゲットを設定して、ステップ 1 で定義した検証ワークフローを呼び出します。以下がその例です。

```
{
  "source":[
    "aws.backup"
  ],
  "detail-type":[
    "Restore Job State Change"
  ],
  "detail":{
    "resourceType":[
      "..."
```

```
    ],
    "restoreTestingPlanArn":[
      "..."
    ],
    "status":[
      "COMPLETED"
    ]
  }
}
```

3. 復元テストプランを実行して完了させる

   復元テストプランは、設定したスケジュールに従って実行されます。

   復元テストプランがまだない場合は「復元テストプランを作成する」、設定を変更する場合は「復元テストプランを更新する」を参照してください。

4. 結果をモニタリングする

   復元テストプランがスケジュールどおりに実行されたら、検証ワークフローのログをチェックして、正しく実行されたことを確認できます。

   API を呼び出しPutRestoreValidationResultて結果を投稿できます。その結果は、AWS Backup コンソールで表示でき、 DescribeRestoreJob や などの復元ジョブを記述および一覧表示する AWS Backup API コールを通じて表示できますListRestoreJob。

   検証ステータスが設定されると、変更することはできません。

バックアップのリストの表示

バックアップのリストは、AWS Backup コンソールまたはプログラムで表示できます。

トピック

- コンソール内で、保護されたリソースごとにバックアップをリストする
- コンソール内で、バックアップボールトごとにバックアップをリストする
- バックアップをプログラムでリストする

コンソール内で、保護されたリソースごとにバックアップをリストする

AWS Backup コンソールで特定のリソースのバックアップのリストを表示するには、次のステップに従います。

1. にサインインし AWS Management Console、https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[保護されたリソース] を選択します。
3. リスト内の保護されたリソースを選択して、バックアップのリストを表示します。によってバックアップされたリソースのみが AWS Backup 、保護されたリソース にリストされます。

リソースのバックアップを表示できます。このビューから、バックアップを選択して復元することもできます。

コンソール内で、バックアップボールトごとにバックアップをリストする

バックアップボールトに整理されたバックアップのリストを表示するには、以下のステップに従います。

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[バックアップボールト] を選択します。
3. [Backups (バックアップ)] セクションで、このバックアップボールトに整理されたすべてのバックアップのリストを表示します。このビューでは、任意の列ヘッダー (ステータスを含む) でバックアップをソートできるほか、バックアップを選択して復元、編集、または削除できます。

バックアップをプログラムでリストする

`ListRecoveryPoint` API オペレーションを使用してプログラムでバックアップをリストできます。

- `ListRecoveryPointsByBackupVault`
- `ListRecoveryPointsByResource`

例えば、次の AWS Command Line Interface （ AWS CLI) コマンドは、すべてのバックアップを `EXPIRED`ステータスで一覧表示します。

```
aws backup list-recovery-points-by-backup-vault \
```

```
  --backup-vault-name sample-vault \
  --query 'RecoveryPoints[?Status == `EXPIRED`]'
```

AWS Backup Audit Manager

AWS Backup Audit Manager を使用して、定義したコントロールに対する AWS Backup ポリシーのコンプライアンスを監査できます。コントロールは、バックアップの頻度もしくはバックアップ保持期間など、バックアップ要件のコンプライアンスを監査するために設計された手順です。

AWS Backup Audit Manager は、次のような質問に答えるのに役立ちます。

- 「すべてのリソースをバックアップしていますか？」
- 「私のバックアップはすべて暗号化されていますか？」
- 「バックアップは毎日行われていますか？」

AWS Backup Audit Manager を使用して、定義したコントロールにまだ準拠していないバックアップアクティビティとリソースを検索できます。コントロールがリソースのコンプライアンスを評価するときには、アクティブなリソースのみが含まれることに注意してください。例えば、実行状態の Amazon EC2 インスタンスは評価されます。停止状態の EC2 インスタンスはコンプライアンス評価には含まれません。

また、バックアップガバナンスのために、日次レポートとオンデマンドレポートの監査証跡を自動的に生成するために、それれも使用できます。

次の手順では、 AWS Backup Audit Manager の使用方法の概要を示します。詳細なウォークスルーについては、このページの最後にあるトピックのいずれかを選択します。

1. 1 つ以上のガバナンス制御テンプレートを含むフレームワークを作成します。前述の質問は、3 つのガバナンス管理テンプレートの例です。一部のガバナンス制御テンプレートのパラメータをカスタマイズできます。たとえば、最後のコントロールをカスタマイズして、「バックアップは毎週行われていますか」と尋ねることができます。毎日の代わりに。
2. フレームワークを表示して、そのフレームワークで定義したコントロールに準拠している (または非準拠) のリソースの数を確認します。
3. バックアップおよびコンプライアンスステータスのレポートを作成します。これらのレポートは、コンプライアンス· プラクティスの実証可能な証拠として保存するか、またはまだコンプライアンスに準拠していない個々のバックアップ· アクティビティおよびリソースを特定します。

   AWS Backup Audit Manager は 24 時間ごとに新しいレポートを自動的に生成し、Amazon S3 に発行します。オンデマンドレポートを生成することもできます。

> **Note**
>
> 最初のコンプライアンス関連フレームワークを作成する前に、リソーストラッキングを有効にする必要があります。これにより、 AWS Config は AWS Backup リソースを追跡できます。リソース追跡の管理方法に関する技術ドキュメントについては、「 AWS Config デベロッパーガイドAWS Config 」の「 コンソールでのセットアップ」を参照してください。リソーストラッキングを有効にすると、料金が適用されます。 AWS Backup Audit Manager のリソース追跡の料金と請求については、「計測、コスト、請求」を参照してください。

トピック

監査フレームワークの操作

フレームワークは、バックアッププラクティスの評価に役立つコントロールのコレクションです。事前に構築されたカスタマイズ可能なコントロールを使用して、ポリシーを定義し、バックアッププラクティスがポリシーに準拠しているかどうかを評価できます。また、自動日報を設定して、フレームワークのコンプライアンスステータスに関する洞察を得ることもできます。

各フレームワークは 1 つの アカウントと に適用されます AWS リージョン。リージョンごとに、アカウントごとに最大 15 のフレームワークをデプロイできます。重複フレームワーク (同じコントロールとパラメーターを含むフレームワーク) をデプロイすることはできません。

2 つの異なるタイプのフレームワークがあります。

- -AWS Backup フレームワーク(推奨) — AWS Backup フレームワークを使用して、バックアップアクティビティ、カバレッジ、リソースを推奨するベスト· プラクティスに照らして監視するために、使用可能なすべてのコントロールを展開します。
- 定義するカスタムフレームワーク — カスタムフレームワークを使用して、1 つまたは複数の特定のコントロールを選択し、コントロールパラメーターをカスタマイズします。

トピック

コントロールを選択する

次の表に、 AWS Backup Audit Manager のコントロール、カスタマイズ可能なパラメータ、および AWS Config 記録リソースタイプを示します。すべてのコントロールには、記録リソースタイプが必要です。`AWS Config: resource compliance`これは、このタイプがコンプライアンスステータスを記録するためです。

使用可能なコントロール

コントロール名	コントロールの記述	カスタマイズ可能なパラメータ	AWS Config 記録リソースタイプ
リソースはバックアッププランによって保護されています	リソースがバックアッププランによって保護されているかどうかを評価します。	なし	`AWS Backup: backup selection`
バックアッププランに最小頻度および最小保持期間があります	バックアップの頻度が [1日] 以上で、保存期間が少なくとも [35日] であるかどうかを評価します。	Backup の頻度、保存期間	`AWS Backup: backup plans`

コントロール名	コントロールの記述	カスタマイズ可能なパラメータ	AWS Config 記録リソースタイプ
復旧ポイントの手動削除をボールトによって防止します	バックアップボールトが、特定の AWS Identity and Access Management (IAM) ロールによる場合を除き、リカバリポイントの手動削除を許可していないかどうかを評価します。デフォルトでは、IAM ロールの例外はありません。このコントロールを AWS Backup フレームワークでデプロイする場合も、IAM ロールの例外はありません。	リカバリポイントを手動で削除できる最大 5 つの IAM ロール	`AWS Backup: backup vaults`
復旧ポイントが暗号化されています	リカバリポイントが暗号化されているかどうかを評価します。	なし	`AWS Backup: recovery points`
復旧ポイントに設定された最小保持期間	リカバリポイントの保存期間が少なくとも [35 日] であるかどうかを評価します。	復旧ポイント保持期間	`AWS Backup: recovery points`
クロスリージョンバックアップコピーが予定されています	リソースが別の AWS リージョンへのバックアップのコピーを作成するように設定されているかどうかを評価します。	AWS リージョン	`AWS Backup: backup selection`

コントロール名	コントロールの記述	カスタマイズ可能なパラメータ	AWS Config 記録リソースタイプ
クロスアカウントバックアップコピーがスケジュールされています	リソースにクロスアカウントバックアップコピーが設定されているかどうかを評価します。	AWS アカウント ID	`AWS Backup: backup selection`
バックアップは AWS Backup ボールトロックで保護されています	リソースが、ロックされたバックアップボールトにバックアップを保存するように設定されているかどうかを評価します。	最小保持日数、最大保持日数	`AWS Backup: backup selection`
最後の復旧ポイントが作成されました	復旧ポイントが、指定した時間枠内に作成されたかどうかを評価します。	時間単位 [1 から 744] または日数単位 [1 から 31] の値。	`AWS Backup recovery points`
リソースが目標に達するまでの復元時間	復元テストジョブが目標復元時間内に完了したかどうかを評価します。	値 (分)	なし

これら制御の詳細については、コントロールと修正を参照してください

すべてのコントロールをサポートしていない が AWS Backupサポートするリソースのリストについては、リソース別の機能の可用性表の Audit Manager セクションを参照してください AWS Backup 。

> **Note**
>
> 上記のコントロールを使用しない場合でも、 AWS Backup Audit Manager を使用してバックアップ、コピー、復元ジョブの日次レポートを作成できます。監査レポートの操作を参照してください。

リソーストラッキングの有効化

最初のコンプライアンス関連フレームワークを作成する前に、リソーストラッキングを有効にする必要があります。これにより、 AWS Config は AWS Backup リソースを追跡できます。リソース追跡の管理方法に関する技術ドキュメントについては、「 AWS Config デベロッパーガイドAWS Config 」の「 コンソールでのセットアップ」を参照してください。

リソーストラッキングを有効にすると、料金が適用されます。 AWS Backup Audit Manager のリソース追跡の料金と請求については、「計測、コスト、請求」を参照してください。

トピック

- コンソールを使用したリソーストラッキングを有効にする
- AWS Command Line Interface (AWS CLI)を使用して、リソーストラッキングを有効にします。
- AWS CloudFormation テンプレートを使用して、リソーストラッキングを有効にします。

コンソールを使用したリソーストラッキングを有効にする

コンソールを使用してリソーストラッキングを有効にするには:

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. Audit Managerの下にある左のナビゲーションペインでAフレームワークを選択します。
3. リソーストラッキングの管理を選択して、リソーストラッキングを有効にします。
4. AWS Config 「設定に移動」を選択します。
5. 選択録画を有効または無効にする。
6. 選択有効化次のすべてのリソースタイプについて記録するか、一部のリソースタイプで記録を有効にすることを選択します。コントロールに必要なリソースタイプを指定するには、AWS Backup Audit Manager の制御と修正を参照にしてください。

    - `AWS Backup: backup plans`

- `AWS Backup: backup vaults`
- `AWS Backup: recovery points`
- `AWS Backup: backup selection`

> **Note**
>
> AWS Backup Audit Manager では、すべてのコントロール`AWS Config: resource compliance`に が必要です。

7. [閉じる] を選びます。
8. テキスト付きの青いバナーを待ってください。テキストで緑のバナーに移行するにはリソーストラッキングの有効化にしてください。リソーストラッキングはオンです。

リソース追跡を有効にしているかどうか、有効になっている場合は、 AWS Backup コンソールの 2 つの場所で記録するリソースタイプを確認できます。左のナビゲーションペインで、次のいずれかの操作を行います。

- フレームワークを選択し、AWS Config レコーダーのステータス下に次の出来ストを選択します。
- 設定を選択し、AWS Config レコーダーのステータス下に次のテキストを選択します。

AWS Command Line Interface (AWS CLI)を使用して、リソーストラッキングを有効にします。

まだ にオンボードしていない場合は AWS Config、 を使用してオンボードする方が速い場合があります AWS CLI。

AWS CLIを使用してリソーストラッキングを有効にするには:

1. 次のコマンドを入力して、 AWS Config レコーダーがすでに有効かどうかを確認します。

```
$ aws configservice describe-configuration-recorders
```

   a. `ConfigurationRecorders`リストは次のように空の場合。

```
{
  "ConfigurationRecorders": []
```

```
}
```

レコーダーが有効になっていません。ステップ 2 に進み、レコーダーを作成します。

b. すべてのリソースで録音をすでに有効にした場合は、ConfigurationRecorders出力は次のようになります。

```
{
  "ConfigurationRecorders":[
    {
      "recordingGroup":{
        "allSupported":true,
        "resourceTypes":[

        ],
        "includeGlobalResourceTypes":true
      },
      "roleARN":"arn:aws:iam::[account]:role/[roleName]",
      "name":"default"
    }
  ]
}
```

すべてのリソースを有効にしたので、リソーストラッキングはすでに有効になっています。AWS Backup Audit Manager を使用するには、この手順の残りの部分を完了する必要はありません。

c. ConfigurationRecordersは空ではなかったら、すべてのリソースで録音を有効にしていません。次のコマンドを使用して、既存のレコーダーにバックアップリソースを追加します。ステップ 3 に進みます。

```
$ aws configservice describe-configuration-recorders
{
  "ConfigurationRecorders":[
    {
      "name":"default",
      "roleARN":"arn:aws:iam::accountId:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig",
      "recordingGroup":{
        "allSupported":false,
        "includeGlobalResourceTypes":false,
        "resourceTypes":[
```

```
            "AWS::Backup::BackupPlan",
            "AWS::Backup::BackupSelection",
            "AWS::Backup::BackupVault",
            "AWS::Backup::RecoveryPoint",
            "AWS::Config::ResourceCompliance"
          ]
        }
      }
    ]
}
```

2. AWS Backup Audit Manager リソースタイプを使用して AWS Config レコーダーを作成する

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=default, \
roleARN=arn:aws:iam::accountId:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig \
--recording-group
 resourceTypes="['AWS::Backup::BackupPlan','AWS::Backup::BackupSelection', \
'AWS::Backup::BackupVault','AWS::Backup::RecoveryPoint','AWS::Config::ResourceCompliance']"
```

3. AWS Config レコーダーを記述します。

```
$ aws configservice describe-configuration-recorders
```

出力を次の想定出力と比較することで、 AWS Backup Audit Manager のリソースタイプがあることを確認します。

```
{
  "ConfigurationRecorders":[
    {
      "name":"default",
      "roleARN":"arn:aws:iam::accountId:role/AWSServiceRoleForConfig",
      "recordingGroup":{
        "allSupported":false,
        "includeGlobalResourceTypes":false,
        "resourceTypes":[
          "AWS::Backup::BackupPlan",
          "AWS::Backup::BackupSelection",
          "AWS::Backup::BackupVault",
          "AWS::Backup::RecoveryPoint",
          "AWS::Config::ResourceCompliance"
```

```
        ]
      }
    }
  ]
}
```

4. AWS Config 設定ファイルを保存する送信先として Amazon S3 バケットを作成します。

```
$ aws s3api create-bucket --bucket my-bucket –region us-east-1
```

5. *policy.json* を使用して、バケットへのアクセス AWS Config 許可を付与します。次のサンプル。*policy.json*を参照してください。

```
$ aws s3api put-bucket-policy --bucket MyBucket --policy file://policy.json
```

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AWSConfigBucketPermissionsCheck",
      "Effect":"Allow",
      "Principal":{
        "Service":"config.amazonaws.com"
      },
      "Action":"s3:GetBucketAcl",
      "Resource":"arn:aws:s3:::my-bucket"
    },
    {
      "Sid":"AWSConfigBucketExistenceCheck",
      "Effect":"Allow",
      "Principal":{
        "Service":"config.amazonaws.com"
      },
      "Action":"s3:ListBucket",
      "Resource":"arn:aws:s3:::my-bucket"
    },
    {
      "Sid":"AWSConfigBucketDelivery",
      "Effect":"Allow",
      "Principal":{
        "Service":"config.amazonaws.com"
      },
```

```
      "Action":"s3:PutObject",
      "Resource":"arn:aws:s3:::my-bucket/*"
    }
  ]
}
```

6. バケットを AWS Config 配信チャネルとして設定する

```
$ aws configservice put-delivery-channel --delivery-channel
 name=default,s3BucketName=my-bucket
```

7. AWS Config 録音を有効にする

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name default
```

8. DescribeFramework次のように出力が"FrameworkStatus":"ACTIVE"あなたの最後の行になっていることを確認します。

```
$ aws backup describe-framework --framework-name test --region us-east-1
```

```
{
  "FrameworkName":"test",
 "FrameworkArn":"arn:aws:backup:us-east-1:accountId:framework:test-
f0001b0a-0000-1111-ad3d-4444f5cc6666",
  "FrameworkDescription":"",
  "FrameworkControls":[
    {
      "ControlName":"BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK",
      "ControlInputParameters":[
        {
          "ParameterName":"requiredRetentionDays",
          "ParameterValue":"1"
        }
      ],
      "ControlScope":{

      }
    },
    {
      "ControlName":"BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK",
      "ControlInputParameters":[
```

```
        {
          "ParameterName":"requiredFrequencyUnit",
          "ParameterValue":"hours"
        },
        {
          "ParameterName":"requiredRetentionDays",
          "ParameterValue":"35"
        },
        {
          "ParameterName":"requiredFrequencyValue",
          "ParameterValue":"1"
        }
      ],
      "ControlScope":{

      }
    },
    {
      "ControlName":"BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN",
      "ControlInputParameters":[

      ],
      "ControlScope":{

      }
    },
    {
      "ControlName":"BACKUP_RECOVERY_POINT_ENCRYPTED",
      "ControlInputParameters":[

      ],
      "ControlScope":{

      }
    },
    {
      "ControlName":"BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED",
      "ControlInputParameters":[

      ],
      "ControlScope":{

      }
    }
```

```
  ],
  "CreationTime":1633463605.233,
  "DeploymentStatus":"COMPLETED",
  "FrameworkStatus":"ACTIVE"
}
```

AWS CloudFormation テンプレートを使用して、リソーストラッキングを有効にします。

リソース追跡を有効にする AWS CloudFormation テンプレートについては、「 での AWS Backup Audit Manager の使用 AWS CloudFormation」を参照してください。

を使用してフレームワークを作成する AWS Backup コンソールを使用してフレームワークを作成します。

リソーストラッキングを有効にした後、次の手順を使用してフレームワークを作成します。

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. 左のナビゲーションペインで フレームワークを選択します。
3. フレームワークの作成を選択します。
4. [フレームワークネーム] に、一意のワークフロー名を入力します。フレームワーク名は、1 ~ 256 文字で、文字 (a~z)、数字 (0~9)、アンダースコア (_) で構成されます。
5. (任意) フレームワークの説明を入力します。
6. [コントロール] には、アクティブなコントロールが表示されます。デフォルトでは、リソースの対象となるすべてのコントロールが一覧表示されます。

   アクティブにするコントロールを変更するには、[コントロールを編集] をクリックします。

   a. 最初のチェックボックスは、コントロールがオンになっているかどうかを示します。コントロールをオフにするには、このボックスのチェックを外します。

   b. [評価するリソースを選択] で、リソースを選択する方法を、タイプ、タグ、または単一リソースから選択できます。

   AWS Backup Audit Manager のコントロールリストでは、各コントロールのカスタマイズオプションについて記述しています。

7. (任意の) [] を選択して新しいタグを追加を選択して、フレームワークにタグを付けます。タグを使用して、フレームワークを検索してフィルタリングしたり、コストを追跡したりできます。
8. フレームワークの作成を選択します。

AWS Backup Audit Manager は、フレームワークの作成に数分かかる場合があります。

エラー `AlreadyExists` が発生した場合、同じコントロールとパラメーターを備えたフレームワークが既に存在しています。新しいフレームワークを正常に作成するには、少なくとも 1 つのコントロールまたはパラメーターが既存のフレームワークと異なる必要があります。

AWS Backup API を使用したフレームワークの作成

次の表は、対応する DescribeFrameworkリクエストに対するサンプルAPI対応と共に、CreateFramework各コントロールについサンプルAPIリクエストを含みます。 AWS Backup Audit Manager をプログラムで操作するには、これらのコードスニペットを参照してください。

コントロール	**CreateFramework** リクエスト	**DescribeFramework** レスポンス
`Backup resources are protected by a backup plan`	`{"FrameworkName": "Control1", "FrameworkDescription": "This is a test framework", "FrameworkControls": [ {"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["RDS"] // Evaluate only RDS instances } }`	`{"FrameworkName": "Control1", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control1-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN", "ControlInputParameters":[], "ControlScope":`

コントロール	**CreateFramework** リクエスト	**DescribeFramework** レスポンス
	] "IdempotencyToken": "Control1", "FrameworkTags": {"key1": "foo"} }	{"Complia nceResourceTypes": ["RDS"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control1", "FrameworkTags": {"key1": "foo"} }

コントロール	**CreateFramework** リクエスト	**DescribeFramework** レスポンス
Backup plan minimum frequency and minimum retention	{"FrameworkName": "Control2", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK", "ControlInputParameters": [{"ParameterName": "requiredRetentionDays", "ParameterValue": "35"}, {"ParameterName": "requiredFrequencyUnit", "ParameterValue": "hours"}, {"ParameterName": "requiredFrequencyValue", "ParameterValue": "24"}], "ControlScope": { "Tags": {"key1": "prod"} // Evaluate backup plans that tagged with "key1": "prod". } }],	{"FrameworkName": "Control2", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control2-de7655ae-1e31-45cb-96a0-4f43d8c1969d", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK", "ControlInputParameters": [{"ParameterName": "requiredRetentionDays", "ParameterValue": "35"}, {"ParameterName": "requiredFrequencyUnit", "ParameterValue": "hours"}, {"ParameterName": "requiredFrequencyValue", "ParameterValue": "24"}], "ControlScope": {

コントロール	**CreateFramework** リクエスト	**DescribeFramework** レスポンス
	"IdempotencyToken": "Control2", "FrameworkTags": {"key1": "foo"} }	"Tags": {"key1": "prod"} } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control2", "FrameworkTags": {"key1": "foo"} }

コントロール	**CreateFramework** リクエスト	**DescribeFramework** レスポンス
Vaults prevent manual deletion of recovery points	{"FrameworkName": "Control3", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED", "ControlInputParameters": [{"ParameterName": "principalArnList", "ParameterValue": "arn:aws:iam::123456789012:role/application_abc/component_xyz/RDSAccess, arn:aws:iam::123456789012:role/aws-service-role/access-analyzer.amazonaws.com/AWSServiceRoleForAccessAnalyzer, arn:aws:iam::123456789012:role/service-role/QuickSightAction"}], "ControlScope": {"ComplianceResourceIds":["default"],	{"FrameworkName": "Control3", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control2-de7655ae-1e31-45cb-96a0-4f43d8c1969d", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED", "ControlInputParameters": [{"ParameterName": "principalArnList", "ParameterValue": "arn:aws:iam::123456789012:role/application_abc/component_xyz/RDSAccess, arn:aws:iam::123456789012:role/aws-service-role/access-analyzer.amazonaws.com/AWSServiceRoleForAccessAnalyzer, arn:aws:iam::123456789012:r

コントロール	**CreateFramework** リクエスト	**DescribeFramework** レスポンス
	"Complian ceResourceTypes": ["AWS::Backup::Bac kupVault"] } }], "IdempotencyToken": "Control3", "FrameworkTags": {"key1": "foo"} }	ole/service-role/Q uickSightAction"}], "ControlScope": {"Complia nceResourceIds":[" default"], "Complian ceResourceTypes": ["AWS::Backup::Bac kupVault"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control3", "FrameworkTags": {"key1": "foo"} }

コントロール	**CreateFramework** リクエスト	**DescribeFramework** レスポンス
Minimum retention established for recovery point	{"FrameworkName": "Control4", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK", "ControlInputParameters": [{"ParameterName": "requiredRetentionDays", "ParameterValue": "35"}], "ControlScope": {} // Default scope (no scope input) sets scope to all recovery points. }], "IdempotencyToken": "Control4", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control4", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control6-6e7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK", "ControlInputParameters": [{"ParameterName": "requiredRetentionDays", "ParameterValue": "35"}], "ControlScope": {} }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control4", "FrameworkTags":

コントロール	**CreateFramework** リクエスト	**DescribeFramework** レスポンス
		<pre> {"key1": "foo"} }</pre>

Backup recovery points are encrypted	<pre>{"FrameworkName":
	 "Control5",
	 "FrameworkDescript
	ion": "This is a test
	 framework",
	 "FrameworkControls":
	  [
	  {"ControlName":
	 "BACKUP_RECOVERY_P
	OINT_ENCRYPTED",
	  "ControlInputParam
	eters":
	  [],
	  "ControlScope":
	 {} // Default scope
	 (no scope input) is all
	 recovery points
	  }
	],
	 "IdempotencyToken":
	 "Control5",
	 "FrameworkTags":
	  {"key1": "foo"}
	}</pre>
		<pre>{"FrameworkName":
		 "Control5",
		"FrameworkArn":
		 "arn:aws:backup:us
		-east-1:1234567890
		12:framework/Contr
		ol7-7e7655ae-1e31-
		45cb-96a0-4f43d8c1
		9642",
		 "FrameworkDescript
		ion": "This is a test
		 framework",
		  "FrameworkControls
		":
		  [
		  {"ControlName":
		 "BACKUP_RECOVERY_P
		OINT_ENCRYPTED",
		  "ControlInputParam
		eters":
		  [],
		  "ControlScope": {}
		  }
		  ],
		 "CreationTime":
		 1516925490,
		 "DeploymentStatus":
		 "Active",
		 "FrameworkStatus":
		 "Completed",
		 "IdempotencyToken":
		 "Control5",
		 "FrameworkTags":
		  {"key1": "foo"}
		}</pre>

コントロール	**CreateFramework** リクエスト	**DescribeFramework** レスポンス
Cross-Region backup copy is scheduled	{"FrameworkName": "Control6", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_REGION", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control6", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control6", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control6-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_REGION", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control6", "FrameworkTags": {"key1": "foo"} }

コントロール	**CreateFramework** リクエスト	**DescribeFramework** レスポンス
Cross-account backup copy is scheduled	{"FrameworkName": "Control7", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_ACCOUNT", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control7", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control7", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control7-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_ACCOUNT", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control7", "FrameworkTags": {"key1": "foo"} }

コントロール	**CreateFramework** リクエスト	**DescribeFramework** レスポンス
Backups are protected by AWS Backup Vault Lock	{"FrameworkName": "Control8", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_VAULT_LOCK", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control8", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control8", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control8-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_VAULT_LOCK", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control8", "FrameworkTags": {"key1": "foo"} }

コントロール	**CreateFramework** リクエスト	**DescribeFramework** レスポンス
Last recovery point was created	{"FrameworkName": "Control9", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_LAST_RECOVERY_POINT_CREATED", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control9", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control9", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control9-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_LAST_RECOVERY_POINT_CREATED", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control9", "FrameworkTags": {"key1": "foo"} }

コントロール	**CreateFramework** リクエスト	**DescribeFramework** レスポンス
Restore time for resources meet target	{"FrameworkName":"Control10", "FrameworkDescription":"This is a test framework", "FrameworkControls":[{ "ControlName":"RESTORE_TIME_FOR_RESOURCES_MEET_TARGET", "ControlInputParameters":[{ "ParameterName":"maxRestoreTime", "ParameterValue":"720" }], "ControlScope":{ "ComplianceResourceIds":[ ], "ComplianceResourceTypes":["DynamoDB" // Evaluates only DynamoDB databases] } }]"IdempotencyToken":"Control10", "FrameworkTags":{ "key1":"foo" }	{"FrameworkName": "Control10", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control9-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "RESTORE_TIME_FOR_RESOURCES_MEET_TARGET", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control10", "FrameworkTags": {"key1": "foo"} }

コントロール	**CreateFramework** リクエスト	**DescribeFramework** レスポンス
	} 	

フレームワークのコンプライアンスステータスの表示

監査フレームワークを作成すると、フレームワーク表に表示さえます。このテーブルを表示するには、 AWS Backup コンソールの左側のナビゲーションペインでフレームワークを選択します。フレームワークの監査結果を表示するには、フレームワーク名を選択します。そうすることで、概要およびコントロールという 2 つのセクションがあるフレームワークの詳細ページに行くことができます。

-概要セクションには、次のステータスが左から右に一覧表示さえれます。

- コンプライアンス状況は、各コントロールのコンプライアンスステータスによって決定される監査フレームワークの全体的なコンプライアンスステータスです。各コントロールのコンプライアンスステータスは、評価する各リソースのコンプライアンスステータスによって決まります。

  フレームワークコンプライアンス状況は、Compliantコントロール評価のスコープ内のすべてのリソースがそれらの評価に合格した場合に限ります。1 つ以上のリソースが制御評価に失敗した場合、コンプライアンスステータスはNon-Compliantになります。非準拠のリソースを見つける方法については、非準拠リソースの検索を参照してください。リソースをコンプライアンスに組み込む方法については、AWS Backup Audit Manager の制御と修正の「是正」セクションを参照してください。
- フレームワークのステータスは、すべてのリソースのリソーストラッキングを有効にしているかどうかを示します。次のようなステータスがあります。
  - Activeフレームワークが評価するすべてのリソースで記録が有効になっている場合。
  - Partially active少なくとも 1 つのリソースについて記録がオフになっている場合、フレームワークが評価します。
  - Inactiveフレームワークが評価するすべてのリソースについて記録がオフになっている場合。
  - Unavailable AWS Backup Audit Manager が現時点で記録ステータスを検証できない場合。

  Partially activeもしくは**Inactive**状態を修正するには

  1. 左のナビゲーションペインの [フレームワーク] を選択します。

2. リソーストラッキングの管理を選択します。
3. ポップアップの指示に従って、リソースタイプで以前に無効になっていた録音を有効にします。

フレームワークに含まれるコントロールに基づいて、リソーストラッキングが必要なリソースタイプの詳細については、AWS Backup Audit Manager の制御と修正のリソースコンポーネントを参照してください。

- デプロイのステータスは、フレームワークのデプロイステータスを示します。このステータスは、ほとんどの場合Completedとすることができますが、。Create in progress,Update in progress,Delete in progress, およびFailedも可能です。
  - ステータスが Failed の場合、フレームワークが正しくデプロイされなかったことを意味します。フレームワークを削除し、AWS Backup コンソールを用いて、または AWS Backup API を使用してフレームワークを再作成します。
- 準拠のコントロールは、すべての評価が渡されたフレームワークコントロールの数を表示します。
- 非準拠のコントロールは、少なくとも 1 つの評価が合格していないフレームワークコントロールの数を表示します。

-コントロールセクションには、次の情報が表示されます。

- コントロールステータスは、各コントロールのコンプライアンスステータスを示します。コントロールはCompliantつまり、すべてのリソースがその評価に合格することを意味します。Non-compliant、少なくとも1つのリソースがその評価に合格しなかったことを意味するか、もしくはInsufficient data。つまり、コントロールが評価スコープ内に評価するリソースが見つからなかったことを意味します。
- 評価スコープは、各コントロールを 1 つもしくは複数リソースタイプに制限する必要があります。1 つのリソース ID、もしくは1つタグキーおよび監査フレームワークの作成時にコントロールをカスタマイズした方法に基づたタグ値です。すべてのフィールドが空の場合 (ダッシュ「-」で表示)、コントロールは適用可能なすべてのリソースを評価します。

アカウントの非準拠リソースの検索

AWS Backup Audit Manager は、2 つの方法で準拠していないリソースを見つけるのに役立ちます。

- フレームワークのコンプライアンスステータスを表示する際は、で、コントロール名を詳細セクションでコントロール名を選択してください。これにより、 AWS Config コンソールに移動し、Non-Compliantリソースのリストを表示できます。
- https://docs.aws.amazon.com/aws-backup/latest/devguide/create-report-plan-console.htmlフレームワークが含まれているリソースコンプライアンステンプレートを使用してレポートを作成した後で、Non-Compliantすべてのコントロールにまたがるリソースを特定するレポートを見ることができます。

  さらに、Resource compliance report AWS Backup Audit Manager が、最後に各コントロールを評価した最後の時間を表示します。

監査フレームワークを更新する

既存の監査フレームワークの説明、コントロール、およびパラメータを更新できます。

既存のフレームワークを更新するには

1. AWS Backup コンソールの左側のナビゲーションペインで、フレームワーク を選択します。
2. フレームワーク名で編集したいフレームワークを選択します。
3. [編集] を選択します。

監査フレームワークを削除する

既存のフレームワークを削除するには

1. AWS Backup コンソールの左側のナビゲーションペインで、フレームワーク を選択します。
2. フレームワーク名で削除したいフレームワークを選択します。
3. [削除] を選択します。
4. フレームワークの名前を入力して、フレームワークの削除を選択します。

Working with audit reports (レポートの操作)

AWS Backup Audit Manager レポートは、次のような AWS Backup アクティビティの証拠を自動的に生成します。

- どのバックアップジョブが終了し、いつ

- どのリソースをバックアップしましたか

レポートには 2 つのタイプがあります。レポートを作成するときに、どちらのタイプを作成するかを選択します。

1 つ目のタイプは、ジョブレポートで、過去 24 時間以内に完了したジョブとすべてのアクティブなジョブが表示されます。ジョブレポートに `completed with issues` のステータスは表示されません。このステータスを見つけるには、1 つ以上のステータスメッセージを含むCompletedジョブをフィルタリングできます。メッセージに注意またはアクションが必要な場合にのみ、Completedジョブのステータスの一部としてステータスメッセージ AWS Backup が含まれます。

2 つ目のタイプのレポートはコンプライアンスレポートです。コンプライアンスレポートでは、リソースレベルや実施されているさまざまなコントロールをモニタリングできます。

AWS Backup Audit Manager は、毎日のレポートを Amazon S3 バケットに配信します。レポートが現在のリージョンと現在のアカウントに関するものである場合は、レポートを CSV 形式と JSON 形式のどちらで受け取るかを選択できます。それ以外の場合は、レポートを CSV 形式で利用できます。 AWS Backup Audit Manager は、パフォーマンスを維持するためにランダム化を実行するため、日次レポートのタイミングは数時間にわたって変動する可能性があります。オンデマンドレポートはいつでも実行できます。

すべてのアカウントホルダーがクロスリージョンレポートを作成できます。管理アカウントホルダーと委任された管理者アカウントホルダーもクロスアカウントレポートを作成できます。

ごとに最大 20 個のレポートプランを設定できます AWS アカウント。

> **Note**
>
> RDS のように、特定のバックアップのデータを増分バイト単位で表示できないリソースでは、値 `backupSizeInBytes` は 0 と表示されます。

AWS Backup Audit Manager が日次レポートまたはオンデマンドレポートを作成できるようにするには、まずレポートテンプレート からレポートプランを作成する必要があります。

トピック

- レポートテンプレートの選択
- AWS Backup コンソールを使用したレポートプランの作成

- AWS Backup API を使用したレポートプランの作成
- オンデマンドレポートの作成
- 監査レポートの表示
- レポートプランの更新
- レポートプランの削除

レポートテンプレートの選択

レポートテンプレートは、レポートプランがレポートに含まれる情報を定義します。レポートプランを使用してレポートを自動化すると、 AWS Backup Audit Manager は過去 24 時間のレポートを提供します。 AWS Backup Audit Manager は、UTC の午前 1 時から午前 5 時の間にこれらのレポートを作成します。これには、次のレポートテンプレートが用意されています。

レポートテンプレートをBackup する

レポートテンプレートをBackup する。これらのテンプレートを使用すると、バックアップ、リストア、またはコピージョブの毎日の更新が提供されます。これらのレポートを使用して、運用ポスチャを監視し、さらにアクションが必要になる可能性のある障害を特定できます。次の表に、各バックアップレポートテンプレート名およびその出力例を一覧表示します。

Backup レポートテンプレート	JSON 形式のサンプルレポート
BACKUP_JOB_REPORT	{ "reportItems": [{ "reportTimePeriod": "2021-07-14T00:00:00Z - 2021-07-15T00:00:00Z", "accountId": "112233445566", "region": "us-west-2", "backupJobId": "FCCB040A-9426-2A49-2EA9-5EAFFAC656AC", "jobStatus": "COMPLETED", "resourceType": "EC2", "resourceArn": "arn:aws:ec2:us-west-2:112233445566:instance/i-0bc877aee7782ba75", "backupPlanArn": "arn:aws:backup:us-west-2:1122334455

Backup レポートテンプレート	JSON 形式のサンプルレポート


```
66:backup-plan:349f2247-b48
9-4301-83ac-4b7dd724db9a",
      "backupRuleId": "ab88bbf8-
ff4e-4f1b-92e7-e13d3e65dcfb",
      "creationDate": "2021-07-
14T23:53:47.229Z",
      "completionDate": "2021-07-
15T00:16:07.282Z",
      "recoveryPointArn": "arn:aws:
ec2:us-west-2::image/ami-03
0cafb98e5a6dcdf",
      "jobRunTime": "00:22:20",
      "backupSizeInBytes": 858993459
2,
      "backupVaultName": "Default",
      "backupVaultArn": "arn:aws:
backup:us-west-2:1122334455
66:backup-vault:Default",
      "iamRoleArn": "arn:aws:
iam::112233445566:role/service-
role/AWSBackupDefaultServiceRole"
    }
  ]
}
```

Backup レポートテンプレート	JSON 形式のサンプルレポート

COPY_JOB_REPORT	{
	  "reportItems": [
	    {
	      "reportTimePeriod": "2021-07-14T15:48:31Z - 2021-07-15T15:48:31Z",
	      "accountId": "112233445566",
	      "region": "us-west-2",
	      "copyJobId": "E0AD48A9-0560-B668-3EF0-941FDC0AD6B1",
	      "jobStatus": "RUNNING",
	      "resourceType": "EC2",
	      "resourceArn": "arn:aws:ec2:us-west-2:112233445566:instance/i-0bc877aee7782ba75",
	      "backupPlanArn": "arn:aws:backup:us-west-2:112233445566:backup-plan:349f2247-b489-4301-83ac-4b7dd724db9a",
	      "backupRuleId": "ab88bbf8-ff4e-4f1b-92e7-e13d3e65dcfb",
	      "creationDate": "2021-07-15T15:42:04.771Z",
	      "backupSizeInBytes": 8589934592,
	      "sourceRecoveryPointArn": "arn:aws:ec2:us-west-2::image/ami-007b3819f25697299",
	      "sourceBackupVaultArn": "arn:aws:backup:us-west-2:112233445566:backup-vault:Default",
	      "destinationRecoveryPointArn": "arn:aws:ec2:us-east-2::image/ami-0eba2199a0bcece3c",
	      "destinationBackupVaultArn": "arn:aws:backup:us-east-2:112233445566:backup-vault:Default",
	      "iamRoleArn": "arn:aws:iam::112233445566:role/service-role/AWSBackupDefaultServiceRole"
	    }

Backup レポートテンプレート	JSON 形式のサンプルレポート
	<pre>] }</pre>

RESTORE_JOB_REPORT	<pre>{
	  "reportItems": [
	    {
	      "reportTimePeriod": "2021-07-
	14T15:53:30Z - 2021-07-15T15:53:3
	0Z",
	      "accountId": "112233445566",
	      "region": "us-west-2",
	      "restoreJobId": "4CACA67D-4E12-
	DC05-6C2B-0E97D01FA41E",
	      "jobStatus": "RUNNING",
	      "recoveryPointArn": "arn:aws:
	ec2:us-west-2::image/ami-00
	201ecb57a5271ae",
	      "creationDate": "2021-07-
	15T15:52:49.797Z",
	      "backupSizeInBytes": 858993459
	2,
	      "percentDone": "0.00%",
	      "iamRoleArn": "arn:aws:
	iam::112233445566:role/service-
	role/AWSBackupDefaultServiceRole"
	    }
	  ]
	}</pre>

コンプライアンスレポートテンプレート

コンプライアンスレポートテンプレートは、1つ以上のフレームワークで定義したコントロールに対するバックアップ・アクティビティおよびリソースのコンプライアンスに関する日次レポートを提供します。いずれかのフレームワークのコンプライアンスステータスがNon-compliantなら、コンプライアンスレポートを確認して、非準拠のリソースを特定します。

コンプライアンスレポートテンプレートのタイプ

- Control compliance reportは、フレームワークで定義したコントロールのコンプライアンスステータスを追跡するのに役立ちます。
- Resource compliance reportは、フレームワークで定義したコントロールに対して、リソースのコンプライアンスステータスを追跡するのに役立ちます。これらのレポートには、詳細な評価結果が含まれます。これには、これらのリソースを特定して修正するために使用できる非準拠リソースに関する情報が含まれます。

次の表は、コンプライアンスレポートからの出力例を示します。

コンプライアンスレポートテンプレート	JSON 形式のサンプルレポート
CONTROL_COMPLIANCE_REPORT	{ "reportItems": [{ "accountId": "112233445566", "region": "me-south-1", "frameworkName": "TestFram ework7", "frameworkDescription": "A test framework", "controlName": "BACKUP_R ESOURCES_PROTECTED_BY_BACKUP_PLAN", "controlComplianceStatus": "NON_COMPLIANT", "lastEvaluationTime": "2021-08- 17T03:21:56.002Z", "numResourcesCompliant": 91, "numResourcesNonCompliant": 205, "controlFrequency": "Twelve_H ours", "controlScope": "", "controlParameters": "" }, { "accountId": "112233445566", "region": "me-south-1", "frameworkName": "TestFram ework7",

コンプライアンスレポートテンプレート	JSON 形式のサンプルレポート


```
      "frameworkDescription": "A test
 framework",
      "controlName": "BACKUP_P
LAN_MIN_FREQUENCY_AND_MIN_R
ETENTION_CHECK",
      "controlComplianceStatus":
 "NON_COMPLIANT",
      "lastEvaluationTime": "2021-08-
17T03:21:19.995Z",
      "numResourcesCompliant": 0,
      "numResourcesNonCompliant": 25,
      "controlScope": "{Complia
nceResourceTypes: [],}",
      "controlParameters": "{\"requi
redFrequencyValue\":\"1\",\
"requiredRetentionDays\":\"35\",
\"requiredFrequencyUnit\":\"hours
\"}"
    }
  ]
}
```

コンプライアンスレポートテンプレート	JSON 形式のサンプルレポート

RESOURCE_COMPLIANCE_REPORT	{
	  "reportItems": [
	    {
	      "accountId": "112233445566",
	      "region": "us-west-2",
	      "frameworkName": "MyTestFr
	amework",
	      "frameworkDescription": "",
	      "controlName": "BACKUP_L
	AST_RECOVERY_POINT_CREATED",
	      "resourceName": "",
	      "resourceId": "AWS::EFS
	::FileSystem/fs-63c74e66",
	      "resourceType": "AWS::EFS
	::FileSystem",
	      "resourceComplianceStatus":
	 "NON_COMPLIANT",
	      "lastEvaluationTime": "2021-07-
	07T18:55:40.963Z"
	    },
	    {
	      "accountId": "112233445566",
	      "region": "us-west-2",
	      "frameworkName": "MyTestFr
	amework",
	      "frameworkDescription": "",
	      "controlName": "BACKUP_L
	AST_RECOVERY_POINT_CREATED",
	      "resourceName": "",
	      "resourceId": "AWS::EFS
	::FileSystem/fs-b3d7c218",
	      "resourceType": "AWS::EFS
	::FileSystem",
	      "resourceComplianceStatus":
	 "NON_COMPLIANT",
	      "lastEvaluationTime": "2021-07-
	07T18:55:40.961Z"
	    }
	  ]
	}

AWS Backup コンソールを使用したレポートプランの作成

レポートには 2 つのタイプがあります。1 つ目のタイプは、ジョブレポートで、過去 24 時間以内に完了したジョブとすべてのアクティブなジョブが表示されます。2 つ目のタイプのレポートはコンプライアンスレポートです。コンプライアンスレポートでは、リソースレベルや実施されているさまざまなコントロールをモニタリングできます。レポートを作成するときは、作成するレポートのタイプを選択します。

注: アカウントのタイプによって、コンソールの表示は異なる場合があります。マルチアカウント機能を利用できるのは管理アカウントだけです。

バックアッププランと同様に、レポートプランを作成し、レポートの作成を自動化して、送信先の Amazon S3 バケットを定義します。レポートプランでは、レポートを受け取る S3 バケットが必要です。新しい S3 バケットを設定する手順については、Amazon Simple Storage Service ユーザーガイドのステップ 1: 最初の S3 バケットを作成するを参照してください。

AWS Backup コンソールでレポートプランを作成するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. 左のナビゲーションペインの [レポート] を選択します。
3. [Create report group (レポートグループを作成)] を選択します。
4. ドロップダウンリストからレポートテンプレートの 1 つを選択します。
5. 唯一のレポートプラン名を入力します。名前は、1 ~ 256 文字で、英字 (a~z)、数字 (0~9)、およびアンダースコア (_) で構成されます。
6. (任意) レポートプランの記述を入力します。
7. 1 アカウント用のコンプライアンスレポートテンプレートのみ。レポートするフレームワークを 1 つ以上選択します。レポートプランには最大 1,000 のフレームワークを追加できます。

    1. ドロップダウンを使用して AWS リージョンを選択します。
    2. ドロップダウンを使用して、そのリージョンからフレームワークを選択します。
    3. フレームワークの追加を選択します。
8. (任意) レポートプランにタグを追加するには、レポートプランにタグを追加するを選択します。
9. 管理アカウントを使用している場合は、このレポートプランに含めるアカウントを指定できます。[自分のアカウントのみ] を選択すると、現在ログインしているアカウントのみに関するレポートが生成されます。または、組織内の 1 つ以上のアカウント (管理アカウントと委任された管理者アカウントで使用可能) を選択できます。

10. (1 つのリージョンのみのコンプライアンスレポートを作成する場合は、この手順を省略します)。レポートに含めるリージョンを選択できます。ドロップダウンメニューをクリックして、利用可能なリージョンを表示します。[利用可能なすべてのリージョン] または希望するリージョンを選択します。

    - [Backup Audit Manager に組み込まれるときに新しいリージョンを含める] チェックボックスをオンにすると、新しいリージョンが利用可能になった時点でレポートに含まれるようになります。

11. あなたのレポートのファイル形式を選択します。すべてのレポートは CSV 形式でエクスポートできます。また、1 つのリージョンのレポートを JSON 形式でエクスポートできます。
12. ドロップダウンリストを使用して、[S3 バケット名] を選択します。
13. (オプション) バケットプレフィックスを入力します。

    AWS Backup は、現在のアカウント、現在のリージョンレポートを に配信しますs3://*your-bucket-name*/prefix/Backup/*accountID*/*Region*/year/month/day/report-name。

    AWS Backup は、クロスアカウントレポートを に配信します。 s3://*your-bucket-name*/prefix/Backup/crossaccount/*Region*/year/month/day/report-name

    AWS Backup は、クロスリージョンレポートを に配信します。 s3://*your-bucket-name*/prefix/Backup/*accountID*/crossregion/year/month/day/report-name
14. [レポートプランの作成] を選択します。

次に、S3 バケットが からレポートを受信することを許可する必要があります AWS Backup。レポートプランを作成すると、 AWS Backup Audit Manager は適用する S3 バケットアクセスポリシーを自動的に生成します。

カスタム KMS キーを使用してバケットを暗号化する場合、KMS キーポリシーは次の要件を満たしている必要があります。

- Principal 属性には、Backup Audit Manager のサービスにリンクされたロール AWSServiceRolePolicyForBackupReports ARN が含まれている必要があります。

- Action 属性には、kms:Decrypt少なくとも kms:GenerateDataKeyと を含める必要があります。

ポリシーAWSServiceRolePolicyForBackupReportsにはこれらのアクセス許可があります。

このアクセスポリシーを S3 バケットに表示して適用するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. 左のナビゲーションペインの [Reports] を選択します。
3. レポートプラン名の下で、レポートプランの名前を選択して、レポートプランを選択します。
4. [編集] を選択します。
5. 選択S3 バケットのアクセスポリシーを表示します。この手順の最後にポリシーを使用することもできます。
6. 選択権限をコピーする。
7. [Edit Bucket Policy] を選択します。バックアップレポートが初めて作成されるまで、S3 バケットポリシーで参照されるサービスにリンクされたロールはまだ存在せず、「無効なプリンシパル」というエラーが発生することに注意してください。
8. パーミッションをポリシーにコピーします。

サンプルバケットポリシー

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":{
        "AWS":"arn:aws:iam::123456789012:role/aws-service-role/
reports.backup.amazonaws.com/AWSServiceRoleForBackupReports"
      },
      "Action":"s3:PutObject",
      "Resource":[
        "arn:aws:s3:::BucketName/*"
      ],
      "Condition":{
        "StringEquals":{
          "s3:x-amz-acl":"bucket-owner-full-control"
        }
      }
    }
  ]
}
```

カスタム を使用してレポートを保存するターゲット AWS Key Management Service S3 バケットを暗号化する場合は、ポリシーに次のアクションを含めます。

```
"Action":[
  "kms:GenerateDataKey",
  "kms:Encrypt"
],
"Resource":[
  "*"
],
```

AWS Backup API を使用したレポートプランの作成

レポート計画は、プログラムで操作することもできます。

レポートには 2 つのタイプがあります。1 つ目のタイプは、ジョブレポートで、過去 24 時間以内に完了したジョブとすべてのアクティブなジョブが表示されます。2 つ目のタイプのレポートはコンプライアンスレポートです。コンプライアンスレポートでは、リソースレベルや実施されているさまざまなコントロールをモニタリングできます。レポートを作成するときは、作成するレポートのタイプを選択します。

バックアッププランと同様に、レポートプランを作成し、レポートの作成を自動化して、送信先の Amazon S3 バケットを定義します。レポートプランでは、レポートを受け取る S3 バケットが必要です。新しい S3 バケットを設定する手順については、Amazon Simple Storage Service ユーザーガイドのステップ 1: 最初の S3 バケットを作成するを参照してください。

カスタム KMS キーを使用してバケットを暗号化する場合、KMS キーポリシーは次の要件を満たしている必要があります。

- `Principal` 属性には、Backup Audit Manager のサービスにリンクされたロール `AWSServiceRolePolicyForBackupReports` ARN が含まれている必要があります。

- `Action` 属性には、`kms:Decrypt`少なくとも `kms:GenerateDataKey`と を含める必要があります。

ポリシーAWSServiceRolePolicyForBackupReportsにはこれらのアクセス許可があります。

単一アカウント、単一リージョンのレポートの場合は、次の構文を使用して CreateReportPlan を呼び出します。

```
{
   "ReportPlanName": "string",
   "ReportPlanDescription": "string",
   "ReportSetting": {
        "ReportTemplate": enum, // Can be RESOURCE_COMPLIANCE_REPORT,
 CONTROL_COMPLIANCE_REPORT, BACKUP_JOB_REPORT, COPY_JOB_REPORT, or RESTORE_JOB_REPORT.
 Only include "ReportCoverageList" if your report is a COMPLIANCE_REPORT.
   "ReportDeliveryChannel": {
       "S3BucketName": "string",
       "S3KeyPrefix": "string",
       "Formats": [ enum ] // Optional. Can be either CSV, JSON, or both. Default is
 CSV if left blank.
   },
   "ReportPlanTags": {
       "string" : "string" // Optional.
   },
   "IdempotencyToken": "string"
}
```

DescribeReportPlanレポートプランの一意の名前で電話すると、 AWS Backup API は以下の情報を応答します。

```
{
    "ReportPlanArn": "string",
    "ReportPlanName": "string",
    "ReportPlanDescription": "string",
    "ReportSetting": {
        "ReportTemplate": enum,
    },
    "ReportDeliveryChannel": {
        "S3BucketName": "string",
        "S3KeyPrefix": "string",
        "Formats": [ enum ]
    },
    "DeploymentStatus": enum
    "CreationTime": timestamp,
    "LastAttemptExecutionTime": timestamp,
    "LastSuccessfulExecutionTime": timestamp
}
```

マルチアカウント、マルチリージョンのレポートでは、次の構文を使用して CreateReportPlan を呼び出します。

```
{
   "IdempotencyToken": "string",
   "ReportDeliveryChannel": {
      "Formats": [ "string" ], *//Organization report only support CSV file*
      "S3BucketName": "string",
      "S3KeyPrefix": "string"
   },
   "ReportPlanDescription": "string",
   "ReportPlanName": "string",
   "ReportPlanTags": {
      "string" : "string"
   },
   "ReportSetting": {
      "Accounts": [ "string" ], // Use string value of "ROOT" to include all
 organizational units
      "OrganizationUnits": [ "string" ],
      "Regions": ["string"], // Use wildcard value in string to include all Regions
      "FrameworkArns": [ "string" ],
      "NumberOfFrameworks": number,
      "ReportTemplate": "string"
   }
}
```

レポートプランの一意の名前で DescribeReportPlan を呼び出すと、 AWS Backup API は、マルチアカウント、マルチリージョンのプランに関して、以下の情報を応答します。

```
{
   "ReportPlan": {
      "CreationTime": number,
      "DeploymentStatus": "string",
      "LastAttemptedExecutionTime": number,
      "LastSuccessfulExecutionTime": number,
      "ReportDeliveryChannel": {
         "Formats": [ "string" ],
         "S3BucketName": "string",
         "S3KeyPrefix": "string"
      },
      "ReportPlanArn": "string",
      "ReportPlanDescription": "string",
      "ReportPlanName": "string",
      "ReportSetting": {
         "Accounts":[ "string" ],
         "OrganizationUnits":[ "string" ],
```

```
            "Regions": [ "string" ],
            "FrameworkArns": [ "string" ],
            "NumberOfFrameworks": number,
            "ReportTemplate": "string"
        }
    }
}
```

オンデマンドレポートの作成

次の手順でオンデマンドレポートを作成することで、新しいレポートをいつでも生成できます。AWS Backup Audit Manager は、レポートプランで指定した Amazon S3 バケットにオンデマンドレポートを配信します。

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. 左のナビゲーションペインの [Reports] を選択します。
3. レポートプラン名の下で、レポートプランの名前を選択して、レポートプランを選択します。
4. [Create on-demand report] を選択します。

既存のレポートプランのオンデマンドレポートを生成できます。

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. 左のナビゲーションペインの [レポート] を選択します。
3. [レポートプラン]で、レポートプラン名の横にあるラジオボタンをクリックしてレポートプランを選択します。
4. [アクション] をクリックし、[オンデマンドレポートを作成] をクリックします。

レポートの生成中であっても、複数のレポートに対してこの操作を行うことができます。

監査レポートの表示

CSV ファイルまたは JSON ファイルの操作に通常使用するプログラムを使用して、 AWS Backup Audit Manager レポートを開く、表示、分析できます。複数のリージョンまたは複数のアカウントのレポートは CSV 形式でのみ利用できることに注意してください。

ファイルの合計サイズが 50 MB を超えると、サイズの大きいファイルは複数のレポートに分割されます。結果のファイルが 50 MB を超える場合、 AWS Backup Audit Manager はレポートの残りの部分を含む追加の CSV ファイルを作成します。

レポートを表示するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. 左のナビゲーションペインの [Reports] を選択します。
3. レポートプラン名の下で、レポートプランの名前を選択して、レポートプランを選択します。
4. [レポートジョブ] で、レポートリンクをクリックしてレポートを表示します。
5. レポートのステータスの報告に点線の下線が付いていたら、レポートに関する情報については、これを選択してください。
6. る完了時間で、表示するレポートを選択します。
7. S3link を選択します。これにより、送信先 S3 バケットが開きます。
8. 名前の下に、表示するレポートの名前を選択します。
9. レポートをコンピュータに保存するには、ダウンロードを選択します。

レポートプランの更新

既存のレポートプランの記述、配信先、および形式を更新できます。該当する場合は、レポートプランにフレームワークを追加または削除することもできます。

既存のレポートプランを更新するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. 左のナビゲーションペインの [Reports] を選択します。
3. レポートプラン名の下で、レポートプランの名前を選択して、レポートプランを選択します。
4. [編集] を選択します。
5. レポート名や説明、レポートに含まれるアカウントやリージョンなど、レポートプランの詳細を編集できます。

レポートプランの削除

既存のレポートプランを削除できます。レポートプランを削除すると、そのレポートプランによって既に作成されたレポートは、送信先の Amazon S3 バケットに残ります。

既存のレポートプランを削除するには

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

2. 左のナビゲーションペインの [Reports] を選択します。
3. レポートプラン名の下で、レポートプランの名前を選択して、レポートプランを選択します。
4. [削除] を選択します。
5. レポート計画の名前を入力し、[レポートプランの削除を選択します。

での AWS Backup Audit Manager の使用 AWS CloudFormation

参考までに、以下のサンプル AWS CloudFormation テンプレートを提供しています。

トピック

- リソーストラッキングを有効にする
- 既定のコントロールをデプロイする
- IAM ロールをコントロール評価から除外する
- レポートプランを作成します。

リソーストラッキングを有効にする

次のテンプレートでは、リソーストラッキングの有効化に記述するようにリソーストラッキングが有効になります。

```
AWSTemplateFormatVersion: 2010-09-09
Description: Enable AWS Config

Metadata:
  AWS::CloudFormation::Interface:
    ParameterGroups:
      - Label:
          default: Recorder Configuration
        Parameters:
          - AllSupported
          - IncludeGlobalResourceTypes
          - ResourceTypes
      - Label:
          default: Delivery Channel Configuration
        Parameters:
          - DeliveryChannelName
          - Frequency
      - Label:
```

```
          default: Delivery Notifications
        Parameters:
          - TopicArn
          - NotificationEmail
    ParameterLabels:
      AllSupported:
        default: Support all resource types
      IncludeGlobalResourceTypes:
        default: Include global resource types
      ResourceTypes:
        default: List of resource types if not all supported
      DeliveryChannelName:
        default: Configuration delivery channel name
      Frequency:
        default: Snapshot delivery frequency
      TopicArn:
        default: SNS topic name
      NotificationEmail:
        default: Notification Email (optional)

Parameters:
  AllSupported:
    Type: String
    Default: True
    Description: Indicates whether to record all supported resource types.
    AllowedValues:
      - True
      - False

  IncludeGlobalResourceTypes:
    Type: String
    Default: True
    Description: Indicates whether AWS Config records all supported global resource
 types.
    AllowedValues:
      - True
      - False

  ResourceTypes:
    Type: List<String>
    Description: A list of valid AWS resource types to include in this recording group,
 such as AWS::EC2::Instance or AWS::CloudTrail::Trail.
    Default: <All>
```

```
  DeliveryChannelName:
    Type: String
    Default: <Generated>
    Description: The name of the delivery channel.

  Frequency:
    Type: String
    Default: 24hours
    Description: The frequency with which AWS Config delivers configuration snapshots.
    AllowedValues:
      - 1hour
      - 3hours
      - 6hours
      - 12hours
      - 24hours

  TopicArn:
    Type: String
    Default: <New Topic>
    Description: The Amazon Resource Name (ARN) of the Amazon Simple Notification
 Service (Amazon SNS) topic that AWS Config delivers notifications to.

  NotificationEmail:
    Type: String
    Default: <None>
    Description: Email address for AWS Config notifications (for new topics).

Conditions:
  IsAllSupported: !Equals
    - !Ref AllSupported
    - True
  IsGeneratedDeliveryChannelName: !Equals
    - !Ref DeliveryChannelName
    - <Generated>
  CreateTopic: !Equals
    - !Ref TopicArn
    - <New Topic>
  CreateSubscription: !And
    - !Condition CreateTopic
    - !Not
      - !Equals
        - !Ref NotificationEmail
        - <None>
```

```
Mappings:
  Settings:
    FrequencyMap:
      1hour   : One_Hour
      3hours  : Three_Hours
      6hours  : Six_Hours
      12hours : Twelve_Hours
      24hours : TwentyFour_Hours

Resources:

  ConfigBucket:
    DeletionPolicy: Retain
    Type: AWS::S3::Bucket
    Properties:
      BucketEncryption:
          ServerSideEncryptionConfiguration:
            - ServerSideEncryptionByDefault:
                SSEAlgorithm: AES256

  ConfigBucketPolicy:
    Type: AWS::S3::BucketPolicy
    Properties:
      Bucket: !Ref ConfigBucket
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Sid: AWSConfigBucketPermissionsCheck
            Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action: s3:GetBucketAcl
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}"
          - Sid: AWSConfigBucketDelivery
            Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action: s3:PutObject
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}/AWSLogs/
${AWS::AccountId}/*"
```

```
          - Sid: AWSConfigBucketSecureTransport
            Action:
              - s3:*
            Effect: Deny
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}"
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}/*"
            Principal: "*"
            Condition:
              Bool:
                aws:SecureTransport:
                  false

  ConfigTopic:
    Condition: CreateTopic
    Type: AWS::SNS::Topic
    Properties:
      TopicName: !Sub "config-topic-${AWS::AccountId}"
      DisplayName: AWS Config Notification Topic
      KmsMasterKeyId: "alias/aws/sns"

  ConfigTopicPolicy:
    Condition: CreateTopic
    Type: AWS::SNS::TopicPolicy
    Properties:
      Topics:
        - !Ref ConfigTopic
      PolicyDocument:
        Statement:
          - Sid: AWSConfigSNSPolicy
            Action:
              - sns:Publish
            Effect: Allow
            Resource: !Ref ConfigTopic
            Principal:
              Service:
                - config.amazonaws.com

  EmailNotification:
    Condition: CreateSubscription
    Type: AWS::SNS::Subscription
    Properties:
      Endpoint: !Ref NotificationEmail
      Protocol: email
```

```
      TopicArn: !Ref ConfigTopic

  ConfigRecorderServiceRole:
    Type: AWS::IAM::ServiceLinkedRole
    Properties:
      AWSServiceName: config.amazonaws.com
      Description: Service Role for AWS Config

  ConfigRecorder:
    Type: AWS::Config::ConfigurationRecorder
    DependsOn:
      - ConfigBucketPolicy
      - ConfigRecorderServiceRole
    Properties:
      RoleARN: !Sub arn:${AWS::Partition}:iam::${AWS::AccountId}:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig
      RecordingGroup:
        AllSupported: !Ref AllSupported
        IncludeGlobalResourceTypes: !Ref IncludeGlobalResourceTypes
        ResourceTypes: !If
          - IsAllSupported
          - !Ref AWS::NoValue
          - !Ref ResourceTypes

  ConfigDeliveryChannel:
    Type: AWS::Config::DeliveryChannel
    DependsOn:
      - ConfigBucketPolicy
    Properties:
      Name: !If
        - IsGeneratedDeliveryChannelName
        - !Ref AWS::NoValue
        - !Ref DeliveryChannelName
      ConfigSnapshotDeliveryProperties:
        DeliveryFrequency: !FindInMap
          - Settings
          - FrequencyMap
          - !Ref Frequency
      S3BucketName: !Ref ConfigBucket
      SnsTopicARN: !If
        - CreateTopic
        - !Ref ConfigTopic
        - !Ref TopicArn
```

既定のコントロールをデプロイする

次のテンプレートは、「AWS Backup Audit Manager の制御と修正」に記述されたデフォルトコントロールを持つフレームワークを作成します。

```
AWSTemplateFormatVersion: '2010-09-09'
Resources:
  TestFramework:
    Type: AWS::Backup::Framework
    Properties:
      FrameworkControls:
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN
        - ControlName: BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK
          ControlInputParameters:
            - ParameterName: requiredRetentionDays
              ParameterValue: '35'
        - ControlName: BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
        - ControlName: BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK
          ControlInputParameters:
            - ParameterName: requiredRetentionDays
              ParameterValue: '35'
            - ParameterName: requiredFrequencyUnit
              ParameterValue: 'hours'
            - ParameterName: requiredFrequencyValue
              ParameterValue: '24'
          ControlScope:
            Tags:
              - Key: customizedKey
                Value: customizedValue
        - ControlName: BACKUP_RECOVERY_POINT_ENCRYPTED
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_CROSS_REGION
          ControlInputParameters:
            - ParameterName: crossRegionList
              ParameterValue: 'eu-west-2'
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_CROSS_ACCOUNT
          ControlInputParameters:
            - ParameterName: crossAccountList
              ParameterValue: '111122223333'
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_BACKUP_VAULT_LOCK
        - ControlName: BACKUP_LAST_RECOVERY_POINT_CREATED
        - ControlName: RESTORE_TIME_FOR_RESOURCES_MEET_TARGET
          ControlInputParameters:
            - ParameterName: maxRestoreTime
```

```
              ParameterValue: '720'

Outputs:
  FrameworkArn:
    Value: !GetAtt TestFramework.FrameworkArn
```

IAM ロールをコントロール評価から除外する

コントロールBACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLEDでは、リカバリポイントを手動で削除できる IAM ロールを最大 5 つまで免除できます。次のテンプレートでは、このコントロールがデプロイされ、2 つの IAM ロールも免除されます。

```
AWSTemplateFormatVersion: '2010-09-09'
Resources:
  TestFramework:
    Type: AWS::Backup::Framework
    Properties:
      FrameworkControls:
        - ControlName: BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
          ControlInputParameters:
            - ParameterName: "principalArnList"
              ParameterValue: !Sub
 "arn:aws:iam::${AWS::AccountId}:role/AccAdminRole,arn:aws:iam::${AWS::AccountId}:role/
ConfigRole"

Outputs:
  FrameworkArn:
    Value: !GetAtt TestFramework.FrameworkArn
```

レポートプランを作成します。

次のテンプレートでは、レポートプランが作成されます。

```
Description: "Basic AWS::Backup::ReportPlan template"

Parameters:
  ReportPlanDescription:
    Type: String
    Default: "SomeReportPlanDescription"
  S3BucketName:
    Type: String
    Default: "some-s3-bucket-name"
```

```
  S3KeyPrefix:
    Type: String
    Default: "some-s3-key-prefix"
  ReportTemplate:
    Type: String
    Default: "BACKUP_JOB_REPORT"

Resources:
  TestReportPlan:
    Type: "AWS::Backup::ReportPlan"
    Properties:
      ReportPlanDescription: !Ref ReportPlanDescription
      ReportDeliveryChannel:
        Formats:
          - "CSV"
        S3BucketName: !Ref S3BucketName
        S3KeyPrefix: !Ref S3KeyPrefix
      ReportSetting:
        ReportTemplate: !Ref ReportTemplate
        Regions: ['us-west-2', 'eu-west-1', 'us-east-1']
        Accounts: ['123456789098']
        OrganizationUnits: ['ou-abcd-1234wxyz']
      ReportPlanTags:
        - Key: "a"
          Value: "1"
        - Key: "b"
          Value: "2"

Outputs:
  ReportPlanArn:
    Value: !GetAtt TestReportPlan.ReportPlanArn
```

での AWS Backup Audit Manager の使用 AWS Audit Manager

AWS Backup Audit Manager のコントロールは、 で構築済みの標準コントロールにマッピングされるため AWS Audit Manager、 AWS Backup Audit Manager のコンプライアンス結果を AWS Audit Manager レポートにインポートできます。これは、組織の全体的なコンプライアンス体制の一部としてバックアップアクティビティについて報告するコンプライアンス担当者、監査マネージャ、もしくはその他の同僚を支援するために必要です。

AWS Backup Audit Manager コントロールのコンプライアンス結果を AWS Audit Manager フレームワークにインポートできます。 AWS Audit Manager が AWS Backup Audit Manager コントロールか

ら自動的にデータを収集できるようにするには、 AWS Audit Manager ユーザーガイドの「既存のコントロールをカスタマイズする」の手順 AWS Audit Manager を使用して、 でカスタムコントロールを作成します。 https://docs.aws.amazon.com/audit-manager/latest/userguide/customize-control-from-existing.htmlこれらの指示に従うときは、 AWS Backup コントロールのデータソースが であることに注意してくださいAWS Config。

AWS Backup コントロールのリストについては、「コントロールの選択」を参照してください。

コントロールと修正

このページには、 AWS Backup Audit Manager で使用できるコントロールが一覧表示されます。右側の情報ペインを選択すると、コントロールのリストが表示され、特定のコントロールにジャンプできます。コントロールをすばやく比較するには、コントロールを選択するの表を参照してください。プログラムでコントロールを定義するには、 AWS Backup APIを使用して、フレームワークを作成する中にあるコードスニペックを参照してください。

リージョンごとにアカウントごとに最大 50 個のコントロールを使用できます。2 つの異なるフレームワークで同じコントロールを使用すると、50 制御限界の 2 つのコントロールを使用する場合とカウントされます。

このページには、次の情報を含む各コントロールの一覧が表示されます。

- 説明。角カッコ (「[]」) 内の値は、デフォルトのパラメータ値です。
- コントロールが評価するリソース (複数可) 。
- コントロールのパラメータ。
- コントロールの実行時に が発生することがあります。
- コントロールの範囲は次のとおりです。
  - 1 つ、または複数の項目 AWS Backup-でサポートされるサービスを選択して、タイプ別のリソースを指定できます。
  - タグ付きリソーススコープは、1 つのタグキーとオプションの値を持つと指定してください。
  - [単一リソース] ドロップダウンリストを使用して、単一リソースを指定できます。
- 該当するリソースをコンプライアンスに組み込むための修復手順。

コントロールがリソースのコンプライアンスを評価するときには、アクティブなリソースのみが含まれることに注意してください。例えば、実行中状態の Amazon EC2 インスタンスは、[最後の復旧ポ

イントが作成されました] というコントロールによって評価されます。停止状態の EC2 インスタンスはコンプライアンス評価には含まれません。

リソースはバックアッププランによって保護されています

記述：リソースがバックアッププランによって保護されているかどうかを評価します。

リソース: `AWS Backup: backup selection`

パラメータ: なし

発生: 24 時間ごとに自動的に

スコープ:

- タグ付きリソース
- タイプ別のリソースタイプ (デフォルト)
- 単一リソース

修復: バックアッププランにリソースを割り当てます。 AWS Backup バックアッププランに割り当てた後で、自動的にリソースを保護します。詳細については、 デベロッパーガイドのバックアッププランへのリソースの割り当てを参照してください。

Backup プランの最小頻度と最小保存期間

記述：バックアッププランにバックアップ頻度が [1日] 以上で、保存期間が少なくとも [35 日] であるバックアップルールが少なくとも1つ含まれているかどうかを評価します。

リソース: `AWS Backup: backup plans`

パラメータ:

- 必要なバックアップの頻度 (時間または日数) 。
- 必要な保持期間は日、週、月、または年の数です。可能な場合は、 が増分バックアップ AWS Backup を取ることができるように、少なくとも 1 週間のウォームストレージの保持をお勧めします。追加料金は発生しません。

発生： 設定の変更

スコープ:

- タグ付きリソース
- 単一リソース

修復:バックアッププランの更新をクリックして、バックアップの頻度、保存期間、またはその両方を変更します。バックアッププランを更新すると、更新後にプランが作成するリカバリポイントの保持期間が変更されます。

復旧ポイントの手動削除をボールトによって防止します

記述: 特定の IAM ロールを除き、バックアップボールトで復旧ポイントを手動で削除できないかどうかを評価します。

リソース: `AWS Backup: backup vaults`

パラメータ: 最大 5 つの IAM ロールの Amazon リソースネーム (ARN) で、リカバリポイントを手動で削除できます。

発生： 設定の変更

スコープ:

- タグ付きリソース
- 単一リソース

修復 : バックアップボールトのリソースベースのアクセスポリシーを作成もしくは修正します。バックアップボールトアクセスポリシーを設定するポリシーの例と手順については、バックアップボールト内のリカバリポイントを削除するためのアクセスを拒否するを参照してください。

復旧ポイントが暗号化されています

記述: リカバリポイントが暗号化されているかどうかを評価します。

リソース: `AWS Backup: recovery points`

パラメータ: なし

発生： 設定の変更

スコープ:

- タグ付きリソース

修復: リカバリポイントの暗号化を構成します。 AWS Backup リカバリポイントの暗号化を設定する方法は、リソースタイプによって異なります。

を使用して、 でのフル AWS Backup 管理をサポートするリソースタイプの暗号化を設定できます AWS Backup。リソースタイプがフル AWS Backup 管理をサポートしていない場合は、Amazon Elastic Compute Cloud ユーザーガイドの「Amazon EBS 暗号化」など、そのサービスの指示に従ってバックアップ暗号化を設定する必要があります。フル AWS Backup 管理をサポートするリソースタイプのリストを確認するには、リソース別の機能の可用性表の「フル AWS Backup 管理」セクションを参照してください。

復旧ポイントに設定された最小保持期間

記述: リカバリポイントの保存期間が少なくとも [35 日] であるかどうかを評価します。

リソース: `AWS Backup: recovery points`

パラメータ: 必要なリカバリポイントの保持期間は、日、週、月、または年数で表されます。可能な場合は、 が増分バックアップ AWS Backup を取ることができるように、少なくとも 1 週間のウォームストレージの保持をお勧めします。追加料金は発生しません。

発生: 設定の変更

スコープ:

- タグ付きリソース

修復: リカバリポイントの保持期間を変更します。詳細については、「Editing a backup」を参照してください。

クロスリージョンバックアップコピーが予定されています

説明： リソースが別の AWS リージョンへのバックアップのコピーを作成するように設定されているかどうかを評価します。

リソース: `AWS Backup: backup selection`

パラメータ:

- バックアップコピーが存在する (AWS リージョン複数可) を選択します (オプション)
- リージョン

発生: 24 時間ごとに自動的に

スコープ:

- タグ付きリソース
- タイプ別のリソース
- 単一リソース

修正: バックアッププランを更新して、 AWS リージョン バックアップコピーが存在する を変更します。

クロスアカウントバックアップコピーがスケジュールされています

説明: リソースが別のアカウントにバックアップのコピーを作成するように設定されているかどうかを評価します。コントロールが評価するアカウントは 5 つまで追加できます。コピー先アカウントは、 AWS Organizationsのソースアカウントと同じ組織にある必要があります。

リソース: `AWS Backup: backup selection`

パラメータ:

- バックアップコピーが存在する AWS アカウント ID (オプション) を選択します。
- アカウント ID

発生: 24 時間ごとに自動的に

スコープ:

- タグ付きリソース
- タイプ別のリソース
- 単一リソース

修正: バックアッププランを更新して、コピーが存在するアカウント AWS ID を変更または追加します (複数可) 。

バックアップは AWS Backup ボールトロックで保護されています

説明: ロックされたバックアップボールトに保存されているイミュータブルバックアップがリソースにあるかどうかを評価します。

リソース: `AWS Backup: backup selection`

パラメータ:

- AWS Backup ボールトロックの最小保持日数と最大保持日数を入力します (オプション)
- 最小保持日数
- 最大保持日数

発生: 24 時間ごとに自動的に

スコープ:

- タグ付きリソース
- タイプ別のリソース
- 単一リソース

修正: バックアップホールドをロックして名前を設定したり、最小保持日数、最大保持日数、あるいはその両方を変更したりします。コンプライアンスモードでボールトロックに `ChangeableForDays` を含めることもできます。

最後の復旧ポイントが作成されました

説明: このコントロールは、指定された時間枠 (日単位または時間単位) 内に復旧ポイントが作成されたかどうかを評価します。

指定された時間枠内にリソースに復旧ポイントが作成されていれば、コントロールは準拠になります。指定された日数内または時間内に復旧ポイントが作成されなかった場合、コントロールは非準拠になります。

リソース: `AWS Backup: recovery points`

パラメータ:

- 指定された時間枠を時間単位または日単位の整数で入力します。
- hours の値の範囲は 1 ~ 744 です。
- days の値の範囲は 1 ~ 31 です。

発生: 24 時間ごとに自動

スコープ:

- タグ付きリソース
- タイプ別のリソース
- 単一リソース

修正:

- バックアッププランを更新して、指定された復旧ポイント作成枠を変更します。
- さらに、オンデマンドバックアップを作成できます。

リソースが目標に達するまでの復元時間

説明 : 保護対象リソースの復元が目標の復元時間内に完了したかどうかを評価します。

このコントロールは、特定のリソースの復元時間が目標を満たしているかどうかをチェックします。リソースタイプの LatestRestoreExecutionTimeMinutes が maxRestoreTime (分) より大きい場合、ルールは NON_COMPLIANT です。

パラメータ:

- maxRestoreTime (分)

発生: 24 時間ごとに自動

スコープ:

- タグ付きリソース
- タイプ別のリソース

- 単一リソース

> **Note**
>
> AWS Backup は、復元時間に関するサービスレベルアグリーメント (SLAsを提供しません。復元にかかる時間は、同じリソースを含む復元であっても、システムの負荷と容量によって異なる場合があります。

複数の にわたる AWS Backup リソースの管理 AWS アカウント

> **Note**
>
> AWS アカウント の複数の にまたがるリソースを管理する前に AWS Backup、アカウントは AWS Organizations サービス内の同じ組織に属している必要があります。

のクロスアカウント管理機能を使用して、 で AWS アカウント 設定した 全体のバックアップ、復元、コピージョブ AWS Backup を管理およびモニタリングできます AWS Organizations。 AWS Organizationsは、単一の管理アカウント AWS アカウント から複数の のポリシーベースの管理を提供するサービスです。これにより、バックアップポリシーの実装方法を標準化し、手作業による エラーと労力を同時に最小化することができます。一元的なビューから、関心のある条件を満たす、すべてのアカウントのリソースを簡単に識別できます。

をセットアップすると AWS Organizations、すべてのアカウントのアクティビティを 1 か所でモニタリング AWS Backup するように を設定できます。バックアップポリシーを作成して、組織の一部である選択したアカウントに適用し、 AWS Backup コンソールから直接集計バックアップジョブアクティビティを表示することもできます。この機能により、バックアップ管理者は、単一の管理アカウントから、企業全体の何百ものアカウントのバックアップジョブのステータスを効果的にモニタリングできます。AWS Organizations クォータが適用されます。

たとえば、特定のリソースのバックアップを毎日作成し、そのバックアップを 7 日間保持するバックアップポリシー A を定義するとします。バックアップポリシー A は組織全体に適用することを選択します。これにより、組織内の各アカウントにそのバックアッププランが適用され、そのアカウントに表示される、対応するバックアッププランが作成されます。次に、Finance という名前の OU を作成し、バックアップを 30 日間だけ保持することにしました。この場合、ライフサイクル値を上書きするバックアップポリシー B を定義し、その Finance OU にアタッチします。これにより、指定されたすべてのリソースのバックアップを毎日作成し、それを 30 日間保持する新しい有効なバックアッププランが、Finance OU のすべてのアカウントに適用されます。

この例では、バックアップポリシー A とバックアップポリシー B が単一のバックアップポリシーにマージされ、これにより Finance という名前の OU の下にあるすべてのアカウントの保護戦略が定義されます。組織内の他のすべてのアカウントは、バックアップポリシー A によってそのまま保護されます。マージは、同じバックアップ名を共有するバックアップポリシーに対してのみ

行われます。また、ポリシー A とポリシー B をマージせずにそのアカウントに共存させることができます。高度なマージ演算子は、コンソールの JSON ビューでのみ使用できます。マージポリシーの詳細については、ポリシー、ポリシーの構文、およびポリシー継承の定義 ユーザーガイドの「AWS Organizations 」を参照してください。その他のリファレンスとユースケースについては、ブログ「 AWS Organizations を使用した での大規模なバックアップの管理 AWS Backup」およびビデオチュートリアル「 AWS Organizations を使用した での大規模なバックアップの管理 AWS Backup」を参照してください。

クロスアカウント管理機能が利用できる場所については、AWS 「リージョン別の機能の可用性」を参照してください。

クロスアカウント管理を使用するには、次のステップを実行する必要があります。

1. で管理アカウントを作成し AWS Organizations 、管理アカウントの下にアカウントを追加します。
2. でクロスアカウント管理機能を有効にします AWS Backup。
3. AWS アカウント 管理アカウントのすべての に適用するバックアップポリシーを作成します。

> **Note**
>
> 組織によって管理されるバックアッププランの場合、委任された管理者アカウントが 1 つ以上設定されていたとしても、管理アカウントでのリソースオプトイン設定がメンバーアカウントでの設定よりも優先されます。委任された管理者アカウントは、機能が強化されたメンバーアカウントであり、管理アカウントのように設定を上書きすることはできません。

4. すべての でバックアップ、復元、コピージョブを管理します AWS アカウント。

トピック

- Organizations での管理アカウントの作成
- クロスアカウント管理の有効化
- 委任管理者
- バックアップポリシーの作成
- 複数の AWS アカウントでのアクティビティのモニタリング

- リソースのオプトインルール
- ポリシー、ポリシーの構文、およびポリシー継承の定義

Organizations での管理アカウントの作成

まず、組織を作成し、 AWS のメンバーアカウントで設定する必要があります AWS Organizations。

で管理アカウントを作成し AWS Organizations 、アカウントを追加するには

- 手順については、AWS Organizations ユーザーガイドの「チュートリアル: 組織の作成と設定」を参照してください。

クロスアカウント管理の有効化

でクロスアカウント管理を使用する前に AWS Backup、この機能を有効にする (つまり、オプトインする) 必要があります。この機能を有効にすると、複数のアカウントの同時管理を自動化できるバックアップポリシーを作成できます。

クロスアカウント管理を有効にするには

1. https://console.aws.amazon.com/backup/ AWS Backup コンソール で を開きます。管理アカウントの認証情報を使用してサインインします。
2. 左側のナビゲーションペインで [設定] を選択して、クロスアカウント管理ページを開きます。
3. [バックアップポリシー] セクションで [有効] を選択します。

   これにより、すべてのアカウントにアクセスでき、組織内の複数のアカウントの同時管理を自動化するためのポリシーを作成できます。
4. [クロスアカウントモニタリング] セクションで、[有効にする] を選択します。

   これにより、組織内のすべてのアカウントのバックアップ、コピー、および復元アクティビティを管理アカウントからモニタリングできます。

委任管理者

委任管理は、登録されたメンバーアカウントの割り当てられたユーザーがほとんどの AWS Backup 管理タスクを実行するのに便利な方法を提供します。の管理を AWS Backup のメンバーアカウン

トに委任することを選択できます。これにより AWS Organizations、管理アカウントの外部 AWS Backup から組織全体で を管理する機能を拡張できます。

デフォルトでは、管理アカウントはポリシーの編集と管理に使用されるアカウントになっています。委任された管理者機能を使用すると、これらの管理機能を、指定したメンバーアカウントに委任できます。また、これらのアカウントは、管理アカウントに加えてポリシーも管理できます。

メンバーアカウントが委任された管理用に正常に登録されると、そのメンバーアカウントは委任された管理者アカウントになります。委任された管理者として指定されるのはユーザーではなくアカウントであることに注意してください。

委任された管理者アカウントを有効にすると、バックアップポリシーを管理できるようになり、管理アカウントにアクセスできるユーザーの数が最小限に抑えられ、ジョブのクロスアカウントモニタリングができるようになります。

以下は、管理アカウント、バックアップ管理者として委任されたアカウント、および AWS 組織内のメンバーであるアカウントの機能を示す表です。

> **Note**
>
> 委任された管理者アカウントは機能が強化されたメンバーアカウントですが、管理アカウントのように他のメンバーアカウントのサービスのオプトイン設定を上書きすることはできません。

権限	管理アカウント	委任された管理者	メンバーアカウント
委任された管理者アカウントの登録/登録解除	はい	いいえ	いいえ
のアカウント間でバックアップポリシーを管理する AWS Organizations	はい	はい	いいえ
ジョブのクロスアカウントモニタリング	はい	はい	いいえ

前提条件

バックアップ管理を委任する前に、まず AWS 組織内の少なくとも 1 つのメンバーアカウントを委任管理者 として登録する必要があります。アカウントを委任された管理者として登録するには、まず、以下を設定する必要があります。

- AWS Organizations は、デフォルトの管理アカウントに加えて、少なくとも 1 つのメンバーアカウントで有効化および設定する必要があります。
- AWS Backup コンソールで、バックアップポリシー 、クロスアカウントモニタリング 、およびクロスアカウントバックアップ機能が有効になっていることを確認します。これらは、 AWS Backup コンソールの委任管理者ペインの下にあります。
  - クロスアカウントモニタリングでは、管理アカウントと委任された管理者アカウントの両方から、組織内のすべてのアカウントのバックアップアクティビティをモニタリングできます。
  - オプション： クロスアカウントバックアップ。組織内のアカウントがバックアップを他のアカウント (バックアップがサポートするクロスアカウントリソース用) にコピーできるようにします。
  - でサービスアクセスを有効にします AWS Backup。

委任された管理の設定には 2 つのステップがあります。最初のステップは、ジョブのクロスアカウントモニタリングを委任することです。2 つ目のステップは、バックアップポリシー管理を委任することです。

委任された管理者のアカウントとしてのメンバーアカウントの登録

これは最初のセクションです。 AWS Backup コンソールを使用して委任管理者アカウントを登録し、クロスアカウントジョブをモニタリングします。 AWS Backup ポリシーを委任するには、次のセクションで Organizations コンソールを使用します。

AWS Backup コンソールを使用してメンバーアカウントを登録するには：

1. https://console.aws.amazon.com/backup/ AWS Backup コンソール で を開きます。管理アカウントの認証情報を使用してサインインします。
2. コンソールの左側のナビゲーションにある [マイアカウント] で [設定] を選択します。
3. [委任された管理者] ペインで、[委任された管理者を登録] または [委任された管理者を追加] をクリックします。
4. [委任された管理者を登録] ページで、登録するアカウントを選択し、[アカウントを登録] を選択します。

これで、この指定されたアカウントが、委任された管理者として登録され、組織内のアカウント全体のジョブのモニタリングと、ポリシーの表示および編集 (ポリシー委任) を行うことができる管理者権限が付与されます。このメンバーアカウントは、他の委任された管理者のアカウントの登録や登録解除はできません。コンソールを使用して、委任された管理者として最大 5 つのアカウントを登録できます。

メンバーアカウントをプログラムで登録するには:

`register-delegated-administrator` CLI コマンドを使用します。CLI リクエストでは、次のパラメータを指定できます。

- `service-principal`
- `account-id`

以下は、メンバーアカウントをプログラムで登録する CLI リクエストの例です。

```
aws organizations register-delegated-administrator \
--account-id 012345678912 \
--service-principal "backup.amazonaws.com"
```

メンバーアカウントの登録解除

委任された管理者として以前に指定された AWS 組織内のメンバーアカウントを登録解除 AWS Backup して、 から管理アクセスを削除するには、次の手順に従います。

コンソールを使用してメンバーの登録を解除するには

1. https://console.aws.amazon.com/backup/ AWS Backup コンソール で を開きます。管理アカウントの認証情報を使用してサインインします。
2. コンソールの左側のナビゲーションにある [マイアカウント] で [設定] を選択します。
3. [委任された管理者] セクションで、[アカウントの登録を解除] をクリックします。
4. 登録解除するアカウントを選択します。
5. [アカウントの登録を解除] ダイアログボックスで、セキュリティ上の影響を確認し、「`confirm`」と入力して登録解除を完了します。
6. [`Deregister account`] を選択します。

メンバーアカウントをプログラムで登録解除するには:

`deregister-delegated-administrator` CLI コマンドを使用して、委任された管理者のアカウントの登録を解除します。API リクエストでは、次のパラメータを指定できます。

- `service-principal`
- `account-id`

以下は、メンバーアカウントをプログラムで登録解除する CLI リクエストの例です。

```
aws organizations deregister-delegated-administrator \
--account-id 012345678912 \
--service-principal "backup.amazonaws.com"
```

による AWS Backup ポリシーの委任 AWS Organizations

AWS Organizations コンソール内では、バックアップポリシーを含む複数のポリシーの管理を委任できます。

AWS Organizations コンソールにログインした管理アカウントから、組織のリソースベースの委任ポリシーを作成、表示、または削除できます。ポリシーを委任する手順については、「AWS Organizations ユーザーガイド」の「リソースベースの委任ポリシーの作成」を参照してください。

バックアップポリシーの作成

クロスアカウント管理を有効にした後で、管理アカウントからクロスアカウントのバックアップポリシーを作成します。

> **Warning**
>
> JSON を使用してポリシーを作成すると、重複するキー名は拒否されます。複数のプラン、ルール、または選択が 1 つのポリシーに含まれている場合、各キーの名前は一意である必要があります。

AWS Backup コンソールからバックアップポリシーを作成する

1. 左のナビゲーションペインで、[バックアップポリシー] を選択します。[バックアップポリシー] ページで、[バックアップポリシーの作成] を選択します。

2. [詳細] セクションで、バックアップポリシー名を入力し、説明を入力します。
3. [バックアッププランの詳細] セクションで、[ビジュアルエディタ] タブを選択し、次の操作を行います。

   a. [バックアッププラン名] に名前を入力します。

   b. [リージョン] でリストからリージョンを選択します。
4. [バックアップルールの設定] セクションで、[バックアップルールの追加] を選択します。

   バックアッププランあたりのルールの最大数は 10 です。プランに 10 を超えるルールが含まれている場合、バックアッププランは無視され、バックアップは作成されません。

   a. [ルール名] にルールの名前を入力します。ルール名では大文字と小文字が区別され、英数字またはハイフンのみを使用できます。

   b. [スケジュール] の [頻度] リストでバックアップ頻度を選択し、[バックアップウィンドウ] のいずれかのオプションを選択します。[バックアップウィンドウのデフォルトを使用 — 推奨] を選択することをお勧めします。
5. [ライフサイクル] で、必要なライフサイクル設定を選択します。
6. [バックアップボールト名] に名前を入力します。これは、バックアップによって作成されたリカバリポイントが保存されるバックアップボールトです。

   バックアップボールトがすべての accounts. AWS Backup doesn't check for this に存在することを確認してください。
7. （オプション) バックアップを別の にコピーする場合は、リストから送信先リージョンを選択し AWS リージョン、タグを追加します。クロスリージョンコピーの設定に関係なく、作成されるリカバリポイントのタグを選択できます。ルールを追加することもできます。
8. 「リソース割り当て」セクションで、 AWS Identity and Access Management (IAM) ロールの名前を指定します。 AWS Backup サービスロールを使用するには、 を指定しますservice-role/AWSBackupDefaultServiceRole。

   AWS Backup は、各アカウントでこのロールを引き受け、必要に応じて暗号化キーのアクセス許可を含むバックアップジョブとコピージョブを実行するアクセス許可を取得します。 AWS Backup は、このロールを使用してライフサイクルの削除も実行します。

   > **Note**
   >
   > AWS Backup は、ロールが存在するかどうか、またはロールを引き受けることができるかどうかを検証しません。

クロスアカウント管理によって作成されたバックアッププランの場合、 AWS Backup は管理アカウントのオプトイン設定を使用し、特定のアカウントの設定を上書きします。バックアップポリシーを追加するアカウントごとに、ボールトと IAM ロールを自分で作成する必要があります。

9. タグを追加して、バックアップするリソースを選択します。許可されるタグの最大数は 30 です。

   AWS Organizations ポリシーでは、バックアッププランが Organizations ポリシーを介して作成されている場合、最大 30 個のタグを指定できます。複数のリソース割り当てを利用するか、複数のバックアッププランをエンゲージすることで、追加のタグを含めることができます。

   既存の選択を変更するか、 を使用して、同じバックアップ選択でタグの数が 30 を超える場合@@append、バックアッププランは無効になり、ローカルアカウントから削除されます。

10. バックアップするリソースが、Amazon EC2 インスタンスで Microsoft Windows を実行している場合は、[詳細設定] セクションで [Windows VSS] を選択します。これにより、アプリケーション整合性のある Windows VSS バックアップを実行できます。

    > **Note**
    >
    > AWS Backup は現在、Amazon EC2 でのみ実行されているリソースのアプリケーション整合性のあるバックアップをサポートしています。Windows VSS バックアップでは、すべてのインスタンスタイプまたはアプリケーションがサポートされているわけではありません。詳細については、「Windows VSS バックアップの作成」を参照してください。

11. [バックアッププランの追加] を選択してポリシーに追加し、[バックアップポリシーの作成] を選択します。

    バックアップポリシーを作成しても、アカウントにアタッチするまでリソースは保護されません。ポリシー名を選択し、詳細を確認できます。

    バックアッププランを作成する AWS Organizations ポリシーの例を次に示します。Windows VSS バックアップを有効にする場合は、`advanced_backup_settings` ポリシーセクションで示しているように、アプリケーション整合性のとれたバックアップを実行できるアクセス権限を追加する必要があります。

```
{
```

```
 "plans": {
   "PiiBackupPlan": {
     "regions": {
       "@@append":[
         "us-east-1",
         "eu-north-1"
       ]
     },
     "rules": {
       "Hourly": {
         "schedule_expression": {
           "@@assign": "cron(0 0/1 ? * * *)"
         },
         "start_backup_window_minutes": {
           "@@assign": "60"
         },
         "complete_backup_window_minutes": {
           "@@assign": "604800"
         },
         "target_backup_vault_name": {
           "@@assign": "FortKnox"
         },
         "recovery_point_tags": {
           "owner": {
             "tag_key": {
               "@@assign": "Owner"
             },
             "tag_value": {
               "@@assign": "Backup"
             }
           }
         },
         "lifecycle": {
           "delete_after_days": {
             "@@assign": "365"
           },
           "move_to_cold_storage_after_days": {
             "@@assign": "180"
           }
         },
         "copy_actions": {
           "arn:aws:backup:eu-north-1:$account:backup-vault:myTargetBackupVault" :
{
           "target_backup_vault_arn" : {
```

```
            "@@assign" : "arn:aws:backup:eu-north-1:$account:backup-
vault:myTargetBackupVault"  },
              "lifecycle": {
                "delete_after_days": {
                  "@@assign": "365"
                },
                "move_to_cold_storage_after_days": {
                  "@@assign": "180"
                }
              }
            }
          }
        }
      },
      "selections": {
        "tags": {
          "SelectionDataType": {
            "iam_role_arn": {
              "@@assign": "arn:aws:iam::$account:role/MyIamRole"
            },
            "tag_key": {
              "@@assign": "dataType"
            },
            "tag_value": {
              "@@assign": [
                "PII",
                "RED"
              ]
            }
          }
        }
      },
      "backup_plan_tags": {
        "stage": {
          "tag_key": {
            "@@assign": "Stage"
          },
          "tag_value": {
            "@@assign": "Beta"
          }
        }
      }
    }
  }
```

```
}
```

12. [ターゲット] セクションで、ポリシーをアタッチする組織単位またはアカウントを選択し、[アタッチ] を選択します。ポリシーは、個々の組織単位またはアカウントに追加することもできます。

> **Note**
>
> ポリシーを検証し、必ずすべての必須フィールドをポリシーに含めるようにしてください。ポリシーの一部が有効でない場合、 AWS Backup はそれらの部分を無視しますが、ポリシーの有効な部分は想定どおりに機能します。現在、 AWS Backup は AWS Organizations ポリシーの正確性を検証しません。
> 管理アカウントに 1 つのポリシーを、メンバーアカウントに 1 つのポリシーを適用し、それらのポリシーが競合する場合 (たとえば、バックアップ保持期間が異なる) 場合、両方のポリシーは問題なく実行されます (つまり、ポリシーは各アカウントに対して個別に実行されます)。たとえば、管理アカウントポリシーが 1 日に 1 回 Amazon EBS ボリュームをバックアップし、ローカルポリシーが EBS ボリュームを週に 1 回バックアップする場合、両方のポリシーが実行されます。
> (異なるポリシー間のマージなどの理由で) アカウントに適用される有効なポリシーに必須フィールドがない場合、 AWS Backup ポリシーはアカウントに適用されません。一部の設定が有効でない場合は、 によって AWS Backup 調整されます。

バックアップポリシーから作成されたバックアッププランのメンバーアカウントのオプトイン設定にかかわらず、 AWS Backup は組織の管理アカウントで指定されたオプトイン設定を使用します。

組織単位にポリシーをアタッチすると、この組織単位に参加するすべてのアカウントがこのポリシーを自動的に取得し、組織単位から削除されたすべてのアカウントはこのポリシーを失います。対応するバックアッププランは、そのアカウントから自動的に削除されます。

複数の AWS アカウントでのアクティビティのモニタリング

アカウント間でバックアップ、コピー、および復元ジョブをモニタリングするには、クロスアカウントのモニタリングを有効にする必要があります。これにより、組織の管理アカウントからすべてのアカウントのバックアップアクティビティをモニタリングできます。オプトイン後は、オプトイン後に作成された組織全体のすべてのジョブが表示されます。オプトアウトすると、 AWS Backup はジョ

ブを集約ビューに (終了状態に達してから) 30 日間保持します。オプトアウト後に作成されたジョブは表示されず、新しく作成されたバックアップジョブも表示されません。オプトイン手順については、「クロスアカウント管理の有効化」を参照してください。

複数のアカウントをモニタリングするには

1. https://console.aws.amazon.com/backup/ AWS Backup コンソール で を開きます。管理アカウントの認証情報を使用してサインインします。
2. 左側のナビゲーションペインで [設定] を選択して、クロスアカウント管理ページを開きます。
3. [クロスアカウントモニタリング] セクションで、[有効にする] を選択します。

   これにより、組織内のすべてのアカウントのバックアップおよび復元アクティビティを管理アカウントからモニタリングできます。
4. 左のナビゲーションペインで、[クロスアカウントのモニタリング] を選択します。

5. [クロスアカウントのモニタリング] ページで、[バックアップジョブ]、[復元ジョブ]、または [コピージョブ] タブを選択して、すべてのアカウントで作成されたすべてのジョブを表示します。これらの各ジョブは AWS アカウント ID ごとに表示でき、特定のアカウントのすべてのジョブを表示できます。
6. 検索ボックスでは、アカウント ID、ステータス、またはジョブ ID でジョブをフィルタリングできます。

   たとえば、[バックアップジョブ] タブを選択すると、すべてのアカウントで作成されたすべてのバックアップジョブを表示できます。アカウント ID でリストをフィルタリングし、そのアカウントで作成されたすべてのバックアップジョブを表示できます。

リソースのオプトインルール

メンバーアカウントのバックアッププランが Organizations レベルのバックアップポリシーによって作成された場合、Organizations 管理アカウントの AWS Backup オプトイン設定は、そのメンバーアカウントのオプトイン設定を上書きしますが、そのバックアッププランに対してのみ上書きされます。

メンバーアカウントにユーザーが作成したローカルレベルのバックアッププランがある場合、これらのバックアッププランは Organizations 管理アカウントのオプトイン設定を参照せずに、メンバーアカウントのオプトイン設定に従います。

ポリシー、ポリシーの構文、およびポリシー継承の定義

以下のトピックは、 AWS Organizations ユーザーガイド に記載されています。

- バックアップポリシー – 「バックアップポリシー」を参照してください。
- ポリシーの構文 – 「バックアップポリシーの構文と例」を参照してください。
- 管理ポリシータイプの継承 – 「管理ポリシータイプの継承」を参照してください。

AWS Backup および AWS CloudFormation

一般的に

AWS CloudFormation では、作成したテンプレートを使用して、安全で反復可能な方法で AWS リソースをプロビジョニングおよび管理できます。AWS CloudFormation テンプレートおよび StackSets を使用して、バックアップ計画、バックアップリソースの選択、バックアップボールトを管理できます。AWS CloudFormation 使用の詳細については、AWS CloudFormation ユーザーガイドの「AWS CloudFormation の仕組み」を参照してください。

AWS CloudFormation テンプレートまたは StackSet を作成する前に、以下の点を考慮してください。

- バックアップ計画とバックアップボールト用に個別のテンプレートを作成します。削除できるのは、空のバックアップボールトのみです。バックアップボールトを含むスタックに、復旧ポイントが含まれている場合は削除できません。
- スタックを作成する前に、利用可能なサービスロールがあることを確認してください。AWS Backup デフォルトのサービスロールは、リソースをバックアップ計画に初めて割り当てるときに作成されます。バックアッププランにリソースを割り当てていない場合は、スタックを作成する前にリソースを割り当ててください。作成するカスタムロールを指定することもできます。ロールの詳細については、「IAM サービスロール」をご参照ください。

AWS CloudFormation を使用して、バックアップボールト、バックアッププラン、およびリソース割り当てをデプロイする

バックアップボールト、バックアッププラン、およびリソース割り当てを展開するサンプル AWS CloudFormation テンプレートについては、「を使用したリソースの割り当て AWS CloudFormation」を参照してください。

AWS CloudFormation を使用したバックアッププランのデプロイ

バックアッププランをデプロイするサンプル AWS CloudFormation テンプレートについては、「AWS CloudFormation テンプレートのバックアッププラン」を参照してください。

AWS Backup を使用して、AWS CloudFormation Audit Manager フレームワークおよびレポートプランをデプロイする

AWS CloudFormation Audit Manager フレームワーク、およびレポートプランをデプロイするサンプル AWS Backup テンプレートについては、「AWS CloudFormation テンプレートのバックアッププラン」を参照してください。

AWS CloudFormation を使用してアカウント間でのバックアッププランをデプロイする

AWS CloudFormation 組織の複数のアカウントで AWS StackSets を使用することができます。「AWS CloudFormation ユーザーガイド」でサンプルテンプレートを利用できます。

最適な開始ポイントおよびリファレンスは、AWS を使用した AWS Backup サービス全体での、大規模で一元管理されたバックアップをオートメーション化するという出版物です。Ibukun Oyewumi および Sabith Venkitachalapathy (2021 年 7 月) と。

AWS CloudFormation の詳細について説明します。

AWS CloudFormation で AWS Backup の使用方法の詳細については、AWS Backup ユーザーガイドの「AWS CloudFormation リソースタイプのリファレンス」を参照してください。

AWS を使用して AWS CloudFormation サービスリソースへのアクセスを制御する方法については、AWS Identity and Access Management ユーザーガイドの「AWS CloudFormation によるアクセス制御」を参照してください。

のセキュリティ AWS Backup

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

セキュリティは、 AWS とユーザーの間で共有される責任です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティとして説明しています。

- クラウドのセキュリティ — AWS は、 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 クラウド。また、 は、お客様が安全に使用できるサービス AWS も提供します。AWS コンプライアンスプログラムの一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。に適用されるコンプライアンスプログラムの詳細については AWS Backup、「コンプライアンスAWS プログラムによる対象範囲内のサービス」を参照してください。
- クラウド内のセキュリティ – AWS Backup のお客様の責任には以下が含まれますが、これらに限定されるものではありません。また、お客様は、お客様のデータの機密性、組織の要件、および適用可能な法律および規制などの他の要因についても責任を担います。
  - から受信した通信に応答します AWS。
  - 自分とチームが使用する認証情報の管理。詳細については、「 での Identity and Access Management AWS Backup」を参照してください。
  - 組織のデータ保護ポリシーを反映するようにバックアッププランとリソース割り当てを設定します。詳細については、「バックアッププランの管理」を参照してください。
  - 特定のリカバリポイントを見つけてリストアする機能を定期的にテストします。詳細については、「バックアップの使用」を参照してください。
  - 組織のディザスタリカバリおよびビジネス継続性の文書 AWS Backup 手順に手順を組み込む。開始点については、「AWS Backupの開始方法」を参照してください。
  - 緊急時の組織の手順 AWS Backup とともに、 の使用について従業員が理解し、実践していることを確認します。詳細については、「AWS Well-Architected フレームワーク」を参照してください。

このドキュメントは、 の使用時に責任共有モデルを適用する方法を理解するのに役立ちます AWS Backup。以下のトピックでは、セキュリティおよびコンプライアンスの目的 AWS Backup を達成するために を設定する方法を示します。また、 AWS Backup リソースのモニタリングや保護に役立つ他の AWS のサービスの使用方法についても説明します。

トピック

のコンプライアンス検証 AWS Backup

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、コンプライアンスプログラムAWS のサービス による対象範囲内のコンプライアンスプログラムを参照し、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS 「コンプライアンスプログラム」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「 でのレポートのダウンロード AWS Artifact」の」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 では、コンプライアンスに役立つ以下のリソース AWS を提供しています。

- 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 AWS を にデプロイする手順について説明します。
- での HIPAA セキュリティとコンプライアンスのアーキテクチャ — Amazon Web Services このホワイトペーパーでは、企業が AWS を使用して HIPAA 対象アプリケーションを作成する方法について説明します。

> **Note**
>
> すべて AWS のサービス HIPAA の対象となるわけではありません。詳細については、「HIPAA 対応サービスのリファレンス」を参照してください。

- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- AWS カスタマーコンプライアンスガイド — コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、ガイダンスを保護し AWS のサービス 、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) を含む) のセキュリティコントロールにマッピングするためのベストプラクティスをまとめています。
- 「 デベロッパーガイド」の「 ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub – これにより AWS のサービス 、 内のセキュリティ状態を包括的に把握できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールのリストについては、「Security Hub のコントロールリファレンス」を参照してください。
- Amazon GuardDuty – これにより AWS アカウント、疑わしいアクティビティや悪意のあるアクティビティがないか環境を監視することで、、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービス を検出します。 GuardDuty は、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件への対応に役立ちます。
- AWS Audit Manager – これにより AWS のサービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

でのデータ保護 AWS Backup

AWS Backup は、 AWS 責任共有モデル に準拠しています。 には、データ保護に関する規制とガイドラインが含まれています。 AWS は、すべての AWS サービスを実行するグローバルインフラストラクチャを保護する責任を負います。 AWS は、このインフラストラクチャでホストされるデータの制御を維持します。 これには、顧客コンテンツと個人データを処理するためのセキュリティ設定コントロール、 AWS 顧客および AWS パートナーネットワーク (APN) パートナーが含まれます。データコントローラーまたはデータ処理者として動作し、 は、 に入力した個人データに対して責任を負います AWS クラウド。

データ保護の目的で、 AWS Identity and Access Management (IAM) を使用して AWS アカウント 認証情報を保護し、個々のユーザーアカウントを設定することをお勧めします。このようにすること

で、それぞれの職務を遂行するために必要なアクセス権限のみを各ユーザーに付与することができます。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。
- Secure Sockets Layer (SSL)/Transport Layer Security (TLS) を使用して AWS リソースと通信します。
- AWS 暗号化ソリューションと、 サービス内のすべての AWS デフォルトのセキュリティコントロールを使用します。

顧客のアカウント番号などの機密の識別情報は、[名前] フィールドなどの自由形式のフィールドに配置しないことを強くお勧めします。これは、コンソール、API、 AWS Backup または AWS SDK を使用して AWS CLIまたは他の のサービスを使用する場合も同様です。 AWS SDKs AWS Backup または他のサービスに入力したデータはすべて、診断ログの内容として取得される可能性があります。外部サーバーへの URL を指定するときは、そのサーバーへのリクエストを検証するための認証情報を URL に含めないでください。

データ保護の詳細については、AWS セキュリティブログ のブログ投稿「AWS の責任共有モデルと GDPR」を参照してください。

でのバックアップの暗号化 AWS Backup

> **Note**
>
> AWS Backup Audit Manager は、暗号化されていないバックアップを自動的に検出するのに役立ちます。

を使用して、 でのフル AWS Backup 管理をサポートするリソースタイプの暗号化を設定できます AWS Backup。リソースタイプがフル AWS Backup 管理をサポートしていない場合は、Amazon Elastic Compute Cloud ユーザーガイドの「Amazon EBS 暗号化」など、そのサービスの指示に従ってバックアップ暗号化を設定する必要があります。フル AWS Backup 管理をサポートするリソースタイプのリストを確認するには、リソース別の機能の可用性表の「フル AWS Backup 管理」セクションを参照してください。

以下の表では、サポートされている各リソースタイプ、バックアップ用の暗号化の設定方法を示しています。また、バックアップ用の独立した暗号化がサポートされているかどうかを示しています。AWS Backup がバックアップを個別に暗号化する場合、業界標準の AES-256 暗号化アルゴリズムを使用します。

リソースタイプ	暗号化を設定する方法	独立した AWS Backup 暗号化
Amazon Simple Storage Service (Amazon S3)	Amazon S3 バックアップは、バックアップボールトに関連付けられた AWS KMS （ AWS Key Management Service) キーを使用して暗号化されます。 AWS KMS キーは、カスタマー管理の CMK でも、AWS Backup サービスに関連付けられた AWS管理の CMK でもかまいません。 は、ソース Amazon S3 バケットが AWS Backup 暗号化されていない場合でも、すべてのバックアップを暗号化します。	サポート
VMware 仮想マシン	VM バックアップは常に暗号化されます。仮想マシンバックアップの AWS KMS 暗号化キーは、仮想マシンバックアップが保存されている AWS Backup ボールトで設定されます。	サポート
アドバンスト DynamoDB バックアップを有効にした後の Amazon DynamoDB	DynamoDB バックアップは常に暗号化されます。DynamoDB バックアップの AWS KMS 暗号化キーは、DynamoDB バックアップが保存されている AWS Backup ボールトで設定されます。	サポート
アドバンスト DynamoDB バックアップ を有効にしない Amazon DynamoDB	DynamoDB スナップショットは、ソース DynamoDB テーブルの暗号化に使用されたものと同じ暗号化キーで自動的に	非サポート

リソースタイプ	暗号化を設定する方法	独立した AWS Backup 暗号化
	暗号化されます。暗号化されていない DynamoDB テーブルのスナップショットは引き続き暗号化されません。 **Note** AWS Backup が暗号化された DynamoDB テーブルのバックアップを作成するには、バックアップに使用される IAM ロール`kms:GenerateDataKey` に アクセス許可 `kms:Decrypt` と を追加する必要があります。または、 AWS Backup デフォルトのサービスロールを使用することもできます。	
Amazon Elastic File System (Amazon EFS)	Amazon EFS バックアップは常に暗号化されます。Amazon EFS バックアップの AWS KMS 暗号化キーは、Amazon EFS バックアップが保存されている AWS Backup ボールトで設定されます。	サポート

リソースタイプ	暗号化を設定する方法	独立した AWS Backup 暗号化
Amazon Elastic Block Store (Amazon EBS)	デフォルトでは、Amazon EBS バックアップは、ソースボリュームの暗号化に使用されたキーを使用して暗号化されるか、暗号化されないかのいずれかです。復元時には、KMS キーを指定してデフォルトの暗号化方法を無効にする選択ができます。	サポートされていません
Amazon Elastic Compute Cloud (Amazon EC2) AMI	AMIs暗号化されません。EBS スナップショットは、EBS バックアップのデフォルトの暗号化ルールによって暗号化されます (EBS のエントリを参照) 。データおよびルートボリュームの EBS スナップショットは暗号化して AMI にアタッチできます。	サポートされていません

リソースタイプ	暗号化を設定する方法	独立した AWS Backup 暗号化
Amazon Relational Database Service (Amazon RDS)	Amazon RDS スナップショットは、ソース Amazon RDS データベースの暗号化に使用されたものと同じ暗号化キーで自動的に暗号化されます。暗号化されていない Amazon RDS データベースのスナップショットは引き続き暗号化されません。 **Note** AWS Backup は現在、Amazon Aurora を含むすべての Amazon RDS データベースエンジンをサポートしています。	サポートされていません
Amazon Aurora	Aurora クラスタースナップショットは、ソース Amazon Auroraーの暗号化に使用されたものと同じ暗号化キーで自動的に暗号化されます。暗号化されていない Aurora クラスターのスナップショットは引き続き暗号化されません。	サポートされていません

リソースタイプ	暗号化を設定する方法	独立した AWS Backup 暗号化
AWS Storage Gateway	Storage Gateway スナップショットは、ソース Storage Gateway ボリュームの暗号化に使用されたものと同じ暗号化キーで自動的に暗号化されます。暗号化されていない Storage Gatewayボリュームのスナップショットは引き続き暗号化されません。 **Note** Storage Gateway を有効化するために、すべてのサービスでカスタマー管理キーを使用する必要はありません。Storage Gateway のバックアップを、KMS キーを設定した保管庫にコピーするだけです。これは、Storage Gateway にサービス固有の AWS KMS マネージドキーがないためです。	サポートされていません

リソースタイプ	暗号化を設定する方法	独立した AWS Backup 暗号化
Amazon FSx	Amazon FSx ファイルシステムの暗号化機能は、基盤となるファイルシステムによって異なります。特定の Amazon FSx ファイルシステムの詳細については、FSx ユーザーガイドの該当するサイトを参照してください。	サポートされていません
Amazon DocumentDB	Amazon DocumentDB クラスタースナップショットは、ソース Amazon DocumentDB クラスターの暗号化に使用されたものと同じ暗号化キーで自動的に暗号化されます。暗号化されていない Amazon DocumentDB クラスターのスナップショットは引き続き暗号化されません。	サポートされていません
Amazon Neptune	Neptune クラスタースナップショットは、ソース Neptune クラスターの暗号化に使用されたものと同じ暗号化キーで自動的に暗号化されます。暗号化されていない Neptune クラスターのスナップショットは引き続き暗号化されません。	サポートされていません

リソースタイプ	暗号化を設定する方法	独立した AWS Backup 暗号化
Amazon Timestream	Timestream テーブルスナップショットのバックアップは常に暗号化されます。Timestream バックアップ用の AWS KMS 暗号化キーは、Timestream バックアップが保存されるバックアップボールトに設定されます。	サポート
Amazon Redshift	Amazon Redshift クラスタースナップショットは、ソースの Amazon Redshift クラスターの暗号化に使用されたものと同じ暗号化キーで自動的に暗号化されます。暗号化されていない Amazon Redshift クラスターのスナップショットは引き続き暗号化されません。	サポートされていません
AWS CloudFormation	CloudFormation バックアップは常に暗号化されます。CloudFormation バックアップの CloudFormation 暗号化キーは、 CloudFormation バックアップが保存されている CloudFormation ボールトで設定されます。	サポート

リソースタイプ	暗号化を設定する方法	独立した AWS Backup 暗号化
Amazon EC2 インスタンスでの SAP HANA データベース	SAP HANA データベースのバックアップは常に暗号化されます。SAP HANA データベースバックアップの AWS KMS 暗号化キーは、データベースバックアップが保存されている AWS Backup ボールトで設定されます。	サポート

バックアップコピーの暗号化

AWS Backup を使用してアカウントまたはリージョン間でバックアップをコピーすると、 AWS Backup 元のバックアップが暗号化されていない場合でも、 はほとんどのリソースタイプでそれらのコピーを自動的に暗号化します。 はターゲットボールトの KMS キーを使用してコピーを AWS Backup 暗号化します。ただし、暗号化されていない Aurora、Amazon DocumentDB、Neptune クラスターのスナップショットも暗号化されません。

暗号化コピーとバックアップコピー

AWS マネージド KMS キーを使用したクロスアカウントコピーは、 によって完全に管理されていないリソースではサポートされていません AWS Backup。フルマネージドされているリソースフル AWS Backup 管理を確認するには、「」を参照してください。

によって完全に管理されているリソースの場合 AWS Backup、バックアップはバックアップボールトの暗号化キーで暗号化されます。によって完全に管理されていないリソースの場合 AWS Backup、クロスアカウントコピーはソースリソースと同じ KMS キーを使用します。詳細については、「暗号化キーとクロスアカウントコピー」を参照してください。

仮想マシンのハイパーバイザー認証情報の暗号化

ハイパーバイザーによって管理される仮想マシンは、AWS Backup Gateway を使用してオンプレミスシステムを AWS Backupに接続します。ハイパーバイザーも同じように堅牢で信頼性の高いセキュリティを備えていることが重要です。このセキュリティは、 AWS 所有キーまたはカスタマーマネージドキーのいずれかでハイパーバイザーを暗号化することで実現できます。

AWS 所有キーとカスタマーマネージドキー

AWS Backup は、ハイパーバイザーの認証情報を暗号化して、 AWS が所有する暗号化キーを使用して顧客のログイン情報を保護します。代わりにカスタマーマネージドキーを使用することもできます。

デフォルトでは、ハイパーバイザーの認証情報の暗号化に使用されるキーは、 AWS が所有するキーです。 AWS Backup は、これらのキーを使用してハイパーバイザーの認証情報を自動的に暗号化します。 AWS 所有キーを表示、管理、使用することも、その使用を監査することもできません。ただし、データを暗号化するキーを保護するためのアクションの実施やプログラムの変更を行う必要はありません。詳細については、「 AWS KMS デベロッパーガイド」の「 AWS 所有キー」を参照してください。

または、カスタマーマネージドキーを使用して認証情報を暗号化することもできます。 AWS Backup は、暗号化を実行するための、ユーザーが作成、所有、管理する、対称型のカスタマーマネージドキーの使用をサポートします。この暗号化を完全に制御できるため、次のようなタスクを実行できます。

- キーポリシーの策定と維持
- IAM ポリシーとグラントの策定と維持
- キーポリシーの有効化と無効化
- 暗号化素材のローテーション
- タグの追加
- キーエイリアスの作成
- 削除のためのキースケジューリング

カスタマーマネージドキーを使用する場合、 は、ロールにこのキーを使用して復号するアクセス許可 AWS Backup があるかどうかを検証します (バックアップジョブまたは復元ジョブが実行される前に) 。バックアップまたは復元ジョブの開始に使用するロールに `kms:Decrypt` アクションを追加する必要があります。

`kms:Decrypt` アクションはデフォルトのバックアップロールには追加できないため、カスタマーマネージドキーを使用するにはデフォルトのバックアップロール以外のロールを使用する必要があります。

詳細については、「AWS Key Management Service デベロッパーガイド」の「カスタマーマネージドキー」を参照してください。

カスタマーマネージドキーを使用する場合に必要な許可

AWS KMS には、カスタマーマネージドキーを使用するための許可が必要です。カスタマーマネージドキーで暗号化されたハイパーバイザー設定をインポートすると、 は にCreateGrantリクエストを送信してユーザーに代わって許可 AWS Backup を作成します AWS KMS。 は、お客様のアカウントの KMS キーにアクセスするための許可 AWS Backup を使用します。

権限へのアクセスを取り消すことも、カスタマーマネージドキーへの AWS Backupのアクセスを削除することもできます。その場合、ハイパーバイザーに関連付けられているすべてのゲートウェイは、カスタマーマネージドキーで暗号化されたハイパーバイザーのユーザー名とパスワードにアクセスできなくなり、バックアップジョブと復元ジョブに影響します。具体的には、このハイパーバイザー内の仮想マシンで実行するバックアップジョブと復元ジョブは失敗します。

ハイパーバイザーを削除するときに、バックアップゲートウェイは `RetireGrant` 操作を使用して許可を削除します。

暗号化キーのモニタリング

AWS Backup リソースで AWS KMS カスタマーマネージドキーを使用する場合、 AWS CloudTrailまたは Amazon CloudWatch Logs を使用して、 AWS Backup が に送信するリクエストを追跡できます AWS KMS。

カスタマーマネージドキーによって暗号化されたデータにアクセスするために によって AWS KMS 呼び出されるオペレーションをモニタリング AWS Backup するには、 に次の`"eventName"`フィールドを持つ AWS CloudTrail イベントを探します。

- `"eventName": "CreateGrant"`
- `"eventName": "Decrypt"`
- `"eventName": "Encrypt"`
- `"eventName": "DescribeKey"`

での Identity and Access Management AWS Backup

へのアクセスには認証情報 AWS Backup が必要です。これらの認証情報には、Amazon DynamoDB インスタンスや Amazon EFS ファイルシステムなどの AWS リソースに対するアクセス許可が含まれている必要があります。さらに、 がサポートする一部のサービス AWS Backup に対して AWS Backupによって作成された復旧ポイントは、ソースサービス (Amazon EFS など) を使用して削除できません。これらの復旧ポイントは、 を使用して削除できます AWS Backup。

以下のセクションでは、 AWS Identity and Access Management (IAM) と を使用して AWS Backup リソースへの安全なアクセスを確保する方法について詳しく説明します。

> **Warning**
>
> AWS Backup は、リカバリポイントのライフサイクルを管理するためにリソースを割り当てるときに選択したのと同じ IAM ロールを使用します。そのロールを削除または変更した場合、 AWS Backup は復旧ポイントのライフサイクルを管理できません。この場合、サービスにリンクされたロールを使用して、ライフサイクルを管理しようとします。ごく一部のケースでは、これがうまくいかず、ストレージ上に EXPIRED リカバリポイントを残し、不要なコストが発生する可能性があります。EXPIRED リカバリポイントを削除するには、バックアップの削除の手順を使用して手動で削除してください。

トピック

- 認証
- アクセスコントロール
- IAM サービスロール
- の管理ポリシー AWS Backup
- AWS Backupのサービスにリンクされたロールの使用
- サービス間の混乱した代理の防止

認証

バックアップする AWS Backup または AWS サービスにアクセスするには、 がリクエストの認証 AWS に使用できる認証情報が必要です。には、次のいずれかのタイプの ID AWS としてアクセスできます。

- AWS アカウント ルートユーザー – にサインアップするときは AWS、アカウント AWS に関連付けられた E メールアドレスとパスワードを指定します。これは AWS アカウント のルートユーザーです。その認証情報により、すべての AWS リソースへの完全なアクセスが提供されます。

> **Important**
>
> セキュリティ上の理由から、管理者を作成する場合にのみルートユーザーを使用することをお勧めします。管理者は、 AWS アカウントに対する完全なアクセス許可を持つ IAM

ユーザーです。この管理者ユーザーを使用して、制限された許可を持つ他の IAM ユーザーとロールを作成できます。詳細については、IAM ユーザーガイドの「IAM のベストプラクティス」および「最初の IAM 管理者のユーザーおよびグループの作成」を参照してください。

- IAM ユーザー – IAM ユーザーは、 AWS アカウント 内で特定のカスタムアクセス許可 (バックアップ保存用のバックアップ保管庫を作成するためのアクセス許可など) を持つアイデンティティです。IAM ユーザー名とパスワードを使用して、、 AWS ディスカッションフォーラムAWS Management Console、 AWS Support センターなどの安全な AWS ウェブページにサインインできます。

  ユーザー名とパスワードに加えて、各ユーザーのアクセスキーを作成することもできます。これらのキーは、複数の SDKs のいずれかまたは AWS Command Line Interface （ AWS CLI) を使用してプログラムで AWS サービスにアクセスするときに使用できます。SDK と AWS CLI ツールでは、アクセスキーを使用してリクエストが暗号で署名されます。 AWS ツールを使用しない場合は、リクエストを自分で署名する必要があります。リクエストの認証の詳細については、『』の「署名バージョン 4 の署名プロセスAWS 全般のリファレンス」を参照してください。

- IAM ロール - IAM ロールは、アカウントで作成して特定のアクセス許可を付与できるもうひとつの IAM 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、特定のユーザーに関連付けられていません。IAM ロールを使用すると、 AWS のサービスやリソースへのアクセスに使用できる一時的なアクセスキーを取得できます。IAM ロールと一時的な認証情報は、次の状況で役立ちます:

  - フェデレーティッドユーザーアクセス — IAM ユーザーを作成する代わりに、、エンタープライズユーザーディレクトリ AWS Directory Service、またはウェブ ID プロバイダーの既存のユーザー ID を使用できます。このようなユーザーはフェデレーションユーザーと呼ばれます。AWS では、ID プロバイダーを通じてアクセスがリクエストされたとき、フェデレーションユーザーにロールを割り当てます。フェデレーティッドユーザーの詳細については、「IAM ユーザーガイド」の「フェデレーティッドユーザーとロール」を参照してください。
  - クロスアカウント管理 – アカウントの IAM ロールを使用して、アカウントのリソースを管理するための別の AWS アカウント アクセス許可を付与できます。例については、「IAM ユーザーガイド」の「チュートリアル: IAM ロール AWS アカウント を使用した 間のアクセスの委任」を参照してください。
  - AWS サービスアクセス – アカウントの IAM ロールを使用して、アカウントのリソースにアクセスするための AWS サービスアクセス許可を付与できます。詳細については、「IAM ユーザーガイド」の「 AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。

- Amazon Elastic Compute Cloud (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、Amazon EC2 インスタンスで実行され、 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。 AWS ロールを EC2 インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時認証情報を取得することができます。詳細については、IAM ユーザーガイドの「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して権限を付与する」を参照してください。

アクセスコントロール

リクエストを認証するために有効な認証情報を持つことができますが、適切なアクセス許可がない限り、バックアップボールトなどの AWS Backup リソースにアクセスすることはできません。Amazon Elastic Block Store (Amazon EBS) ボリュームなどの AWS リソースをバックアップすることもできません。

すべての AWS リソースは によって所有され AWS アカウント、リソースを作成またはアクセスするためのアクセス許可はアクセス許可ポリシーによって管理されます。アカウント管理者は、 AWS Identity and Access Management (IAM) ID (ユーザー、グループ、ロール) にアクセス許可ポリシーをアタッチできます。また、一部のサービスでは、アクセス権限ポリシーをリソースにアタッチすることができます。

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

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

以下のセクションでは、アクセスポリシーのしくみと、それらのポリシーを使用してバックアップを保護する方法について説明します。

トピック

- リソースおよびオペレーション
- リソース所有権
- ポリシー要素 (アクション、効果、プリンシパル) の指定
- ポリシーでの条件の指定
- API のアクセス許可: アクション、リソース、条件リファレンス
- タグ権限のコピー
- アクセスポリシー

リソースおよびオペレーション

リソースは、service. AWS Backup resources 内に存在するオブジェクトです。これには、バックアッププラン、バックアップボールト、バックアップが含まれます。Backup は、 に存在するさまざまなタイプのバックアップリソースを指す一般的な用語です AWS。たとえば、Amazon EBS スナップショット、Amazon Relational Database Service (Amazon RDS) スナップショット、および Amazon DynamoDB バックアップはすべて、バックアップリソースのタイプです。

では AWS Backup、バックアップはリカバリポイント とも呼ばれます。を使用する場合 AWS Backup、Amazon EBS ボリュームや DynamoDB テーブルなど、保護しようとしている他の AWS サービスのリソースも操作します。これらのリソースには、一意の Amazon リソースネーム (ARN) が関連付けられています。ARNs AWS リソースを一意に識別します。IAM ポリシーや API コールなど、すべての AWSでリソースを明確に指定する必要がある場合は、ARN が必要です。

以下の表では、リソース、サブリソース、ARN 形式、および一意の ID の例を示しています。

AWS Backup リソース ARNs

リソースタイプ	ARN 形式	一意の ID の例
バックアッププラン	`arn:aws:backup:`*region*`:`*account-id*`:backup-plan:*`	
バックアップボールト	`arn:aws:backup:`*region*`:`*account-id*`:backup-vault:*`	

リソースタイプ	ARN 形式	一意の ID の例
Amazon EBS の復旧ポイント	arn:aws:ec2: *region*::snapshot/*	snapshot/snap-05f426fd8kdjb4224
Amazon EC2 の復旧ポイントのイメージ	arn:aws:ec2: *region*::image/ami-*	image/ami-1a2b3e4f5e6f7g890
Amazon RDS の復旧ポイント	arn:aws:rds: *region*:*account-id* :snapshot:awsbackup:*	awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453
Aurora の復旧ポイント	arn:aws:rds: *region*:*account-id* :cluster-snapshot:awsbackup:*	awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453
Storage Gateway の復旧ポイント	arn:aws:ec2: *region*::snapshot/*	snapshot/snap-0d40e49137e31d9e0
アドバンスト DynamoDB バックアップ なしの DynamoDB の復旧ポイント	arn:aws:dynamodb: *region*:*account-id* :table/*/backup/*	table/MyDynamoDBTable/backup/01547087347000-c8b6kdk3
アドバンスト DynamoDB バックアップ が有効な DynamoDB の復旧ポイント	arn:aws:backup: *region*:*account-id* :recovery-point:*	12a34a56-7bb8-901c-cd23-4567d8e9ef01
Amazon EFS の復旧ポイント	arn:aws:backup: *region*:*account-id* :recovery-point:*	d99699e7-e183-477e-bfcd-ccb1c6e5455e

リソースタイプ	ARN 形式	一意の ID の例
Amazon FSx の復旧ポイント	arn:aws:fsx: *region*:*account-id* :backup/backup-*	backup/backup-1a20e49137e31d9e0
仮想マシンの復旧ポイント	arn:aws:backup: *region*:*account-id* :recovery-point:*	1801234a-5b6b-7dc8-8032-836f7ffc623b
Amazon S3 継続的バックアップの復旧ポイント	arn:aws:backup: *region*:*account-id* :recovery-point:*	*my-bucket* -5ec207d0
S3 定期バックアップのリカバリポイント	arn:aws:backup: *region*:*account-id* :recovery-point:*	*my-bucket* -20211231900000-5ec207d0
Amazon DocumentDB の復旧ポイント	arn:aws:rds: *region*:*account-id* :cluster-snapshot:awsbackup:*	awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012
Neptune の復旧ポイント	arn:aws:rds: *region*:*account-id* :cluster-snapshot:awsbackup:*	awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012
Amazon Redshift の復旧ポイント	arn:aws:redshift: *region*:*account-id* :snapshot: *resource*/awsbackup:*	awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012
Amazon Timestream の復旧ポイント	arn:aws:backup: *region*:*account-id* :recovery-point:*	recovery-point:1a2b3cde-f405-6789-012g-3456hi789012_beta

リソースタイプ	ARN 形式	一意の ID の例
AWS CloudFormation テンプレートの復旧ポイント	arn:aws:backup: *region*:*account-id* :recovery-point:*	recovery-point:1a2b3cde-f405-6789-012g-3456hi789012
Amazon EC2 インスタンス上の SAP HANA データベースの復旧ポイント	arn:aws:backup: *region*:*account-id* :recovery-point:*	recovery-point:1a2b3cde-f405-6789-012g-3456hi789012

フル AWS Backup 管理をサポートするリソースはすべて、 形式のリカバリポイントを持ちますarn:aws:backup:*region*:*account-id:*:recovery-point:*。 を使用すると、これらのリカバリポイントを保護するためのアクセス許可ポリシーを簡単に適用できます。どのリソースがフル AWS Backup 管理をサポートしているかを確認するには、リソース別の機能の可用性表の セクションを参照してください。

AWS Backup は、 AWS Backup リソースを操作するための一連のオペレーションを提供します。使用可能なオペレーションのリストについては、「 AWS Backup アクション」を参照してください。

リソース所有権

は、リソースを作成したユーザーに関係なく、アカウントで作成されたリソース AWS アカウントを所有します。具体的には、リソース所有者は、リソース作成リクエスト AWS アカウント を認証するプリンシパルエンティティ (AWS アカウント ルートユーザー、IAM ユーザー、または IAM ロール) の です。次の例は、この仕組みを示しています。

- の AWS アカウント ルートユーザー認証情報を使用してバックアップボールト AWS アカウントを作成する場合、 AWS アカウント はボールトの所有者です。
- で IAM ユーザーを作成し AWS アカウント 、そのユーザーにバックアップボールトを作成するアクセス許可を付与すると、そのユーザーはバックアップボールトを作成できます。ただし、バックアップ保管庫リソースを所有しているのは、このユーザーが属する AWS です。
- バックアップボールトを作成するアクセス許可 AWS アカウント を持つ に IAM ロールを作成すると、ロールを引き受けることのできるすべてのユーザーがボールトを作成できます。ロールが属 AWS アカウントする がバックアップボールトリソースを所有します。

ポリシー要素 (アクション、効果、プリンシパル) の指定

サービスは AWS Backup 、リソースごとに API オペレーションのセットを定義します (「」を参照リソースおよびオペレーション) アクション。これらの API オペレーションのアクセス許可を付与するために、 はポリシーで指定できる一連のアクション AWS Backup を定義します。1 つの API オペレーションの実行で、複数のアクションのアクセス権限が必要になる場合があります。

最も基本的なポリシーの要素を次に示します。

- リソース– ポリシーで Amazon リソースネーム (ARN) を使用して、ポリシーを適用するリソースを識別します。詳細については、「リソースおよびオペレーション」を参照してください。
- アクション – アクションキーワードを使用して、許可または拒否するリソース操作を特定します。
- 効果 – ユーザーが特定のアクションを要求する際の効果を指定します。許可または拒否のいずれかになります。リソースへのアクセスを明示的に付与 (許可) していない場合、アクセスは暗黙的に拒否されます。また、明示的にリソースへのアクセスを拒否すると、別のポリシーによってアクセスが許可されている場合でも、ユーザーはそのリソースにアクセスできなくなります。
- プリンシパル - ID ベースのポリシー (IAM ポリシー) で、ポリシーがアタッチされているユーザーが黙示的なプリンシパルとなります。リソースベースのポリシーでは、権限 (リソースベースのポリシーにのみ適用) を受け取りたいユーザー、アカウント、サービス、またはその他のエンティティを指定します。

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

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

ポリシーでの条件の指定

許可を付与するとき、IAM ポリシー言語を使用して、ポリシーが有効になる必要がある条件を指定できます。例えば、特定の日付の後にのみ適用されるポリシーが必要になる場合があります。ポリシー言語での条件の指定の詳細については、「IAM ユーザーガイド」の「条件」を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートします。すべての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 Backup は、独自の条件キーのセットを定義します。 AWS Backup 条件キーのリストを確認するには、「サービス認証リファレンス」の「 の条件キー AWS Backup」を参照してください。

API のアクセス許可: アクション、リソース、条件リファレンス

アクセスコントロール をセットアップし、IAM アイデンティティにアタッチできるアクセス権限ポリシー (アイデンティティベースのポリシー) を作成するときは、以下のリストをリファレンスとして使用できます。には、各 AWS Backup API オペレーション、アクションを実行するためのアクセス許可を付与できる対応するアクション、およびアクセス許可を付与できる AWS リソースが含まれます。ポリシーの `Action` フィールドでアクションを指定し、ポリシーの `Resource` フィールドでリソースの値を指定します。`Resource` フィールドが空白の場合は、ワイルドカード (*) を使用してすべてのリソースを含めることができます。

AWS Backup ポリシーで AWS全体の条件キーを使用して条件を表現できます。 AWS全体のキーの完全なリストについては、「IAM ユーザーガイド」の「使用可能なキー」を参照してください。

[1] 既存のボールトアクセスポリシーを使用します。

[2] リソース固有の復旧ポイント ARN AWS Backup リソース ARNsについては、「」を参照してください。 ARNs

[3] では、リソースのメタデータにキーと値のペアStartRestoreJobが必要です。リソースのメタデータを取得するには、`GetRecoveryPointRestoreMetadata` API を呼び出します。

[4] 特定のリソースタイプでは、バックアップに元のリソースタグを含めるか、バックアップにタグを追加するbackup:TagResource場合、バックアップを実行するロールに特定のタグ付けアクセス許可が必要です。で始まる ARN を持つバックアップarn:aws:backup:*region*:*account-id*:recovery-point:、または継続的なバックアップには、このアクセス許可が必要です。backup:TagResource アクセス許可は、 に適用する必要があります。 "*resourcetype*": "arn:aws:backup:*region*:*account-id:*recovery-point:*"

詳細については、「サービス承認リファレンス」の「AWS Backup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。

タグ権限のコピー

がバックアップジョブまたはコピージョブ AWS Backup を実行すると、ソースリソース (コピーの場合は復旧ポイント) から復旧ポイントにタグをコピーしようとします。

> **Note**
>
> AWS Backup は復元ジョブ中にタグをネイティブにコピーしません。復元ジョブ中にタグをコピーするイベント駆動型アーキテクチャについては、「復元ジョブでリソースタグを保持する方法 AWS Backup」を参照してください。

バックアップジョブまたはコピージョブ中に、 はバックアッププラン (またはコピープラン、またはオンデマンドバックアップ) で指定したタグをソースリソースのタグで AWS Backup 集約します。ただし、 では、リソースごとに 50 個のタグの制限 AWS が適用されます。これは を超える AWS Backup ことはできません。バックアップまたはコピージョブがプランとソースリソースからタグを集約すると、合計 50 を超えるタグが検出され、ジョブを完了できず、ジョブが失敗する可能性があります。これは、 AWS全体のタグ付けのベストプラクティスと一致しています。詳細については、AWS 全般のリファレンスガイドの「タグの制限」を参照してください。

- バックアップジョブタグをソースリソースタグに集約した後、リソースには 50 個を超えるタグがあります。 は、リソースごとに最大 50 個のタグ AWS をサポートします。詳細については、「タグの制限」を参照してください。
- に提供する IAM ロールには、ソースタグの読み取りまたは送信先タグの設定を行うアクセス許可 AWS Backup がありません。IAM ロールポリシーの詳細とサンプルについては、「管理ポリシー」を参照してください。

バックアッププランを使用して、ソースリソースタグと矛盾するタグを作成できます。2 つの競合が発生すると、バックアッププランのタグが優先されます。ソースリソースからタグ値をコピーしたくない場合は、この方法を使用します。同じタグキーを指定しますが、バックアッププランを使用して、異なる値または空の値を指定します。

バックアップにタグを割り当てるために必要な権限

リソースタイプ	必要なアクセス権限
Amazon EFS ファイルシステム	`elasticfilesystem:DescribeTags`
Amazon FSx ファイルシステム	`fsx:ListTagsForResource`

Amazon RDS データベースおよび Amazon Aurora クラスター	`rds:AddTagsToResource`
	
	`rds:ListTagsForResource`

リソースタイプ	必要なアクセス権限
Storage Gateway ボリューム	`storagegateway:ListTagsForResource`
Amazon EC2 インスタンスと Amazon EBS ボリューム	`EC2:CreateTags` `EC2:DescribeTags`

DynamoDB は、最初に アドバンスト DynamoDB バックアップ を有効にしない限り、バックアップへのタグの割り当てをサポートしません。

Amazon EC2 バックアップが Image Recovery Point とスナップショットのセットを作成すると、AWS Backup はタグを結果の AMI にコピーします。 AWS Backup また、 は Amazon EC2 インスタンスに関連付けられたボリュームから結果のスナップショットにタグをコピーします。

アクセスポリシー

アクセスポリシーは、誰が何に対するアクセス権を持っているのかを説明します。IAM アイデンティティにアタッチされているポリシーは、[アイデンティティベース] のポリシー (IAM ポリシー) と呼ばれます。リソースにアタッチされたポリシーは、リソースベースのポリシーと呼ばれます。は、アイデンティティベースのポリシーとリソースベースのポリシーの両方 AWS Backup をサポートします。

> **Note**
>
> このセクションでは、 のコンテキストでの IAM の使用について説明します AWS Backup。これは、IAM サービスに関する詳細情報を取得できません。完全な IAM ドキュメンテーションについては、[IAM ユーザーガイド] の [IAM とは] を参照してください。IAM ポリシー構文の詳細と説明については、IAM ユーザーガイドの「IAM JSON ポリシーのリファレンス」を参照してください。

ID ベースのポリシー (IAM ポリシー)

アイデンティティベースのポリシーは、IAM アイデンティティ (ユーザーやロールなど) にアタッチできるポリシーです。例えば、ユーザーが AWS リソースを表示およびバックアップすることを許可するポリシーを定義できますが、バックアップを復元できないようにすることができます。

ユーザー、グループ、ロール、許可の詳細については、「IAM ユーザーガイド」の「アイデンティティ (ユーザー、グループ、ロール)」を参照してください。

IAM ポリシーを使用してバックアップへのアクセスを制御する方法については、「の管理ポリシー AWS Backup」を参照してください。

リソースベースのポリシー

AWS Backup は、バックアップボールトのリソースベースのアクセスポリシーをサポートします。これにより、バックアップ保管庫内の整理された任意のバックアップにどのユーザーがどのようなアクセス許可を持つかを制御できるアクセスポリシーを定義できます。バックアップ保管庫のリソースベースのアクセスポリシーを使用すると、バックアップへのアクセスを簡単に制御できます。

バックアップボールトアクセスポリシーは、 AWS Backup APIsを使用するときのユーザーアクセスを制御します。Amazon Elastic Block Store (Amazon EBS) および Amazon Relational Database Service (Amazon RDS) スナップショットなどの一部のバックアップタイプには、それらのサービスの API を使用してもアクセスできます。バックアップへのアクセスを完全に制御するために、これらの API へのアクセスを制御する個別のアクセスポリシーを IAM で作成できます。

バックアップ保管庫のアクセスポリシーを作成する方法については、「バックアップボールトでのアクセスポリシーの設定」を参照してください。

IAM サービスロール

AWS Identity and Access Management (IAM) ロールは、 AWS アイデンティティが でできることとできないことを決定するアクセス許可ポリシーを持つアイデンティティであるという点で、ユーザーと似ています AWS。ただし、ユーザーは 1 人の特定の人に一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。サービスロールは、 AWS 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ロールです。お客様に代わってバックアップオペレーションを実行するサービスとして、 AWS Backup には、お客様に代わってバックアップオペレーションを実行するときに、ロールを渡す必要があります。IAM ロールの詳細については、「IAM ユーザーガイド」の「IAM ロール」を参照してください。

に渡すロールには、バックアップの作成、復元、期限切れなどのバックアップオペレーションに関連するアクションを実行 AWS Backup するためのアクセス許可を持つ IAM ポリシー AWS Backup が必要です。が AWS Backup サポートするサービスごとに AWS 異なるアクセス許可が必要です。ロールは、 がロールを AWS Backup 引き受けることができる信頼されたエンティティとして AWS Backup リストされている必要もあります。

バックアッププランにリソースを割り当てる場合、またはオンデマンドバックアップ、コピー、または復元を実行する場合は、指定されたリソースで基盤となるオペレーションを実行するためのアクセス権を持つサービスロールを渡す必要があります。 は、このロール AWS Backup を使用して、アカウントでリソースを作成、タグ付け、削除します。

AWS ロールを使用してバックアップへのアクセスを制御する

ロールを使用してバックアップへのアクセスを制御するには、適用範囲を絞り込んだロールを定義し、そのロールを AWS Backupに渡すことのできるユーザーを指定します。例えば、Amazon Relational Database Service (Amazon RDS) データベースをバックアップするアクセス許可のみを付与し、そのロールを に渡すアクセス許可のみを Amazon RDS データベース所有者に付与するロールを作成できます AWS Backup。サポートされているサービスごとに、いくつかの事前定義された管理ポリシー AWS Backup を提供します。これらの管理ポリシーは、作成したロールにアタッチできます。これにより、 が AWS Backup 必要とする適切なアクセス許可を持つサービス固有のロールを簡単に作成できます。

の AWS マネージドポリシーの詳細については AWS Backup、「」を参照してくださいの管理ポリシー AWS Backup。

のデフォルトのサービスロール AWS Backup

AWS Backup コンソールを初めて使用する場合は、 にデフォルトのサービスロール AWS Backup を作成するように選択できます。このロールには、ユーザーに代わってバックアップを作成および復元 AWS Backup するために必要なアクセス許可があります。

> **Note**
>
> デフォルトロールは、 AWS Management Consoleを使用すると自動的に作成されます。AWS Command Line Interface （ AWS CLI) を使用してデフォルトのロールを作成できますが、手動で実行する必要があります。

リソースタイプごとに異なるロールなど、カスタムロールを使用したい場合は、それを実行し、AWS Backupにカスタムロールを渡すこともできます。個々のリソースタイプのバックアップと復元を有効にするロールの例を表示するには、カスタマー管理ポリシー 表を参照してください。

デフォルトのサービスロールの名前は ですAWSBackupDefaultServiceRole。このサービスロールには、 AWSBackupServiceRolePolicyForBackupと の 2 つの管理ポリシーが含まれていますAWSBackupServiceRolePolicyForRestores。

AWSBackupServiceRolePolicyForBackup には、バックアップされるリソースを記述する AWS Backup アクセス許可、暗号化されている AWS KMS キーに関係なくバックアップを作成、削除、記述、または追加する機能を付与する IAM ポリシーが含まれています。

AWSBackupServiceRolePolicyForRestores には、暗号化されている AWS KMS キーに関係なく、バックアップから作成される新しいリソースを作成、削除、または記述する AWS Backup アクセス許可を付与する IAM ポリシーが含まれています。また、新しく作成されたリソースにタグを付けるためのアクセス許可も含まれています。

Amazon EC2 インスタンスをリストアするには、新しいインスタンスを開始する必要があります。

コンソール内でデフォールトのサービスロールを作成する

AWS Backup コンソールで実行する特定のアクションは、 AWS Backup デフォルトのサービスロールを作成します。

AWS アカウントに AWS Backup デフォルトのサービスロールを作成するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. アカウントのロールを作成するには、バックアッププランにリソースを割り当てるか、オンデマンドバックアップを作成します。

   a. バックアッププランを作成し、バックアップにリソースを割り当てます。「スケジュールされたバックアップを作成する」を参照してください。

   b. または、オンデマンドバックアップを作成します。「オンデマンドバックアップを作成する」を参照してください。
3. 次の手順に従って、アカウントに AWSBackupDefaultServiceRole を作成したことを確認します。

   a. 数分待ちます。詳細については、「AWS Identity and Access Management ユーザーガイド」の「行った変更がすぐに表示されないことがある」を参照してください。

   b. にサインイン AWS Management Console し、https://console.aws.amazon.com/iam/ で IAM コンソールを開きます。

   c. 左のナビゲーションメニューから [ロール] を選択します。

   d. 検索バーに「AWSBackupDefaultServiceRole」と入力します この選択が存在する場合は、 AWS Backup デフォルトのロールを作成し、この手順を完了します。

   e. それでも AWSBackupDefaultServiceRole が表示されない場合は、コンソールへのアクセスに使用する IAM ユーザーまたは IAM ロールに次のアクセス許可を追加します。

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:PassRole"
      ],
      "Resource":"arn:aws:iam::*:role/service-role/AWSBackupDefaultServiceRole"
    },
    {
      "Effect":"Allow",
      "Action":[
        "iam:ListRoles"
      ],
      "Resource":"*"
    }
  ]
}
```

中国リージョンの場合は、*aws* を *aws-cn* に置き換えてください。 AWS GovCloud (US) リージョンの場合は、*aws* を に置き換えます*aws-us-gov*。

f. IAM ユーザーまたは IAM ロールにアクセス許可を追加できない場合は、管理者に依頼して、AWSBackupDefaultServiceRole 以外の名前のロールを手動で作成し、そのロールを以下の管理ポリシーにアタッチするよう依頼します。

- AWSBackupServiceRolePolicyForBackup
- AWSBackupServiceRolePolicyForRestores

の管理ポリシー AWS Backup

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のアイデンティティベースのポリシーです AWS アカウント。ポリシーをプリンシパルエンティティにアタッチすると、ポリシーで定義されたアクセス権限がエンティティに付与されます。

AWS 管理ポリシーは、 によって作成および管理されます AWS。 AWS 管理ポリシーで定義されているアクセス許可は変更できません。が AWS 管理ポリシーで定義されたアクセス許可 AWS を更新

すると、その更新はポリシーがアタッチされているすべてのプリンシパル ID (ユーザー、グループ、ロール) に影響します。

カスタマー管理ポリシーでは、 でバックアップへのアクセスを設定するためのきめ細かな制御が可能です AWS Backup。たとえば、それらを使用して、データベースバックアップ管理者に Amazon RDS バックアップへのアクセス権を付与できますが、Amazon EFS バックアップにはアクセスできません。

詳細については、「IAM ユーザーガイド」の「 管理ポリシー」を参照してください。

AWS マネージドポリシー

AWS Backup は、一般的なユースケース向けに以下の AWS マネージドポリシーを提供します。これらのポリシーではより簡単に、適切なアクセス許可を定義し、バックアップへのアクセスを制御できます。管理ポリシーには 2 種類あります。1 つのタイプは、 AWS Backupへのアクセスを制御するためにユーザーに割り当てられるように設計されています。もう 1 つのタイプは、 AWS Backupに渡すロールにアタッチされるように設計されています。以下の表では、 AWS Backup が提供するすべての管理ポリシーを示し、それらのポリシーがどのように定義されているかを説明しています。これらの管理ポリシーは、IAM コンソールのポリシーセクションでも確認できます。

ポリシー

- AWSBackupAuditAccess
- AWSBackupDataTransferAccess
- AWSBackupFullAccess
- AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync
- AWSBackupOperatorAccess
- AWSBackupOrganizationAdminAccess
- AWSBackupRestoreAccessForSAPHANA
- AWSBackupServiceLinkedRolePolicyForBackup
- AWSBackupServiceLinkedRolePolicyForBackupTest
- AWSBackupServiceRolePolicyForBackup
- AWSBackupServiceRolePolicyForRestores
- AWSBackupServiceRolePolicyForS3Backup
- AWSBackupServiceRolePolicyForS3Restore
- AWSServiceRolePolicyForBackupReports
- AWSServiceRolePolicyForBackupRestoreTesting

AWSBackupAuditAccess

このポリシーは、 AWS Backup リソースとアクティビティに対する期待を定義するコントロールとフレームワークを作成し、定義されたコントロールとフレームワークに対して AWS Backup リソースとアクティビティを監査するアクセス許可をユーザーに付与します。このポリシーは、監査を実行するユーザーの期待を説明するアクセス許可を AWS Config および同様のサービスに付与します。

このポリシーは、Amazon S3 および同様のサービスに監査レポートを配信するアクセス権限も付与し、ユーザーは監査レポートを見つけて開くことができます。

このポリシーのアクセス許可を確認するには、「 管理ポリシーリファレンスAWSBackupAuditAccess」の「」を参照してください。 AWS

AWSBackupDataTransferAccess

このポリシーは、 AWS Backup ストレージプレーンのデータ転送 APIsに対するアクセス許可を提供し、 AWS Backint エージェントが AWS Backup ストレージプレーンとのバックアップデータ転送を完了できるようにします。このポリシーは、 Backint エージェントを使用して SAP HANA を実行する Amazon EC2 インスタンスが引き受けるロールにアタッチできます。

このポリシーのアクセス許可を確認するには、「 マネージドポリシーリファレンスAWSBackupDataTransferAccess」の「」を参照してください。 AWS

AWSBackupFullAccess

バックアップ管理者は、バックアッププランの作成または編集、バックアッププランへの AWS リソースの割り当て、バックアップの復元などの AWS Backup オペレーションにフルアクセスできます。バックアップ管理者は、バックアップのコンプライアンスの決定と実施を担当し、組織のビジネスおよび規制関連の要件を満たすバックアッププランを定義します。また、バックアップ管理者は、組織の AWS リソースが適切な計画に割り当てられていることを確認します。

このポリシーのアクセス許可を確認するには、「 マネージドポリシーリファレンスAWSBackupFullAccess」の「」を参照してください。 AWS

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

このポリシーのアクセス許可を確認するには、「 AWS マネージドポリシーリファレンス」の「」を参照してください。

AWSBackupOperatorAccess

バックアップオペレーターは、担当するリソースが適切にバックアップされていることを確認する責任のあるユーザーです。バックアップオペレーターには、バックアップ管理者が作成するバックアッ

ププランに AWS リソースを割り当てるアクセス許可があります。また、 AWS リソースのオンデマンドバックアップを作成し、オンデマンドバックアップの保持期間を設定するアクセス許可も持っています。バックアップオペレーターは、バックアッププランを作成または編集したり、スケジュールされたバックアップを作成後に削除したりするためのアクセス許可は持っていません。バックアップオペレーターはバックアップをリストアできます。バックアップオペレーター がバックアッププランに割り当てることができるリソースタイプや、バックアップからリストアできるリソースタイプを制限できます。これを行うには、特定のリソースタイプのアクセス許可 AWS Backup を持つ特定のサービスロールのみを に渡します。

このポリシーのアクセス許可を確認するには、「 管理ポリシーリファレンスAWSBackupOperatorAccess」の「」を参照してください。 AWS

AWSBackupOrganizationAdminAccess

組織管理者は、バックアップポリシーの作成、編集、削除、アカウントと組織単位へのバックアップポリシーの割り当て、組織内のバックアップアクティビティのモニタリングなど、 AWS Organizations オペレーションへのフルアクセスが可能です。組織管理者は、組織のビジネス要件および規制要件を満たすバックアップポリシーを定義して割り当てることによって、組織内のアカウントを保護する責任があります。

このポリシーのアクセス許可を確認するには、「 マネージドポリシーリファレンスAWSBackupOrganizationAdminAccess」の「」を参照してください。 AWS

AWSBackupRestoreAccessForSAPHANA

このポリシーは、Amazon EC2 で SAP HANA のバックアップを復元する AWS Backup アクセス許可を提供します。

このポリシーのアクセス許可を確認するには、「 マネージドポリシーリファレンスAWSBackupRestoreAccessForSAPHANA」の「」を参照してください。 AWS

AWSBackupServiceLinkedRolePolicyForBackup

このポリシーは、 という名前のサービスにリンクされたロールにアタッチされ AWSServiceRoleforBackup、 AWS Backup がユーザーに代わって AWS サービスを呼び出してバックアップを管理できるようにします。詳細については、「the section called “バックアップとコピー”」を参照してください。

このポリシーのアクセス許可を確認するには、「 マネージドポリシーリファレンス AWSBackupServiceLinkedRolePolicyforBackup」の「」を参照してください。 AWS

AWSBackupServiceLinkedRolePolicyForBackupTest

このポリシーのアクセス許可を確認するには、「 マネージドポリシーリファレンスAWSBackupServiceLinkedRolePolicyForBackupTest」の「」を参照してください。 AWS

AWSBackupServiceRolePolicyForBackup

ユーザーに代わって、サポートされているすべてのリソースタイプのバックアップを作成する AWS Backup アクセス許可を提供します。

このポリシーのアクセス許可を確認するには、「 マネージドポリシーリファレンスAWSBackupServiceRolePolicyForBackup」の「」を参照してください。 AWS

AWSBackupServiceRolePolicyForRestores

ユーザーに代わって、サポートされているすべてのリソースタイプのバックアップを復元する AWS Backup アクセス許可を提供します。

このポリシーのアクセス許可を確認するには、「 マネージドポリシーリファレンスAWSBackupServiceRolePolicyForRestores」の「」を参照してください。 AWS

EC2 インスタンスのリストアでは、EC2 インスタンスを起動するために次の権限も含める必要があります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account-id:role/role-name",
            "Effect": "Allow"
        }
    ]
}
```

AWSBackupServiceRolePolicyForS3Backup

このポリシーには、 が S3 バケット AWS Backup をバックアップするために必要なアクセス許可が含まれています。これには、バケット内のすべてのオブジェクトおよび関連する AWS KMS キーへのアクセスが含まれます。

このポリシーのアクセス許可を確認するには、「 マネージドポリシーリファレンスAWSBackupServiceRolePolicyForS3Backup」の「」を参照してください。 AWS

AWSBackupServiceRolePolicyForS3Restore

このポリシーには、 が S3 バックアップ AWS Backup をバケットに復元するために必要なアクセス許可が含まれています。これには、バケットへの読み取りおよび書き込みのアクセス許可と、S3 オペレーションに関する任意の AWS KMS キーの使用が含まれます。

このポリシーのアクセス許可を確認するには、「 マネージドポリシーリファレンスAWSBackupServiceRolePolicyForS3Restore」の「」を参照してください。 AWS

AWSServiceRolePolicyForBackupReports

AWS Backup はAWSServiceRoleForBackupReports、サービスにリンクされたロールにこのポリシーを使用します。このサービスにリンクされたロールは、バックアップ設定、ジョブ、およびリソースのフレームワークへの準拠をモニタリングおよびレポートする AWS Backup アクセス許可を付与します。

このポリシーのアクセス許可を確認するには、「 管理ポリシーリファレンスAWSServiceRolePolicyForBackupReports」の「」を参照してください。 AWS

AWSServiceRolePolicyForBackupRestoreTesting

このポリシーのアクセス許可を確認するには、「 管理ポリシーリファレンスAWSServiceRolePolicyForBackupRestoreTesting」の「」を参照してください。 AWS

カスタマー管理ポリシー

以下のセクションでは、 でサポートされている およびサードパーティーアプリケーションに推奨されるバックアップ AWS のサービス および復元のアクセス許可について説明します AWS Backup。既存の AWS 管理ポリシーをモデルとして使用して独自のポリシードキュメントを作成し、カスタマイズして AWS リソースへのアクセスをさらに制限できます。

Amazon Aurora

バックアップ

から次のステートメントから始めますAWSBackupServiceRolePolicyForBackup。

- `DynamoDBBackupPermissions`
- `RDSClusterModifyPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`

- KMSPermissions

復元

から RDSPermissionsステートメントから開始しますAWSBackupServiceRolePolicyForRestores。

Amazon DynamoDB

バックアップ

から次のステートメントから始めますAWSBackupServiceRolePolicyForBackup。

- DynamoDBPermissions
- DynamoDBBackupResourcePermissions
- DynamodbBackupPermissions
- KMSDynamoDBPermissions

復元

から次のステートメントから始めますAWSBackupServiceRolePolicyForRestores。

- DynamoDBPermissions
- DynamoDBBackupResourcePermissions
- DynamoDBRestorePermissions
- KMSPermissions

Amazon EBS

バックアップ

から次のステートメントから始めますAWSBackupServiceRolePolicyForBackup。

- EBSResourcePermissions
- EBSTagAndDeletePermissions
- EBSCopyPermissions
- EBSSnapshotTierPermissions
- GetResourcesPermissions

- BackupVaultPermissions

復元

から EBSPermissionsステートメントから開始しますAWSBackupServiceRolePolicyForRestores。

次のステートメントを追加します。

```
{
      "Effect":"Allow",
      "Action": [
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes"
      ],
      "Resource":"*"
},
```

Amazon EC2

バックアップ

からの次のステートメントから始めますAWSBackupServiceRolePolicyForBackup。

- EBSCopyPermissions
- EC2CopyPermissions
- EC2Permissions
- EC2TagPermissions
- EC2ModifyPermissions
- EBSResourcePermissions
- GetResourcesPermissions
- BackupVaultPermissions

復元

からの次のステートメントから始めますAWSBackupServiceRolePolicyForRestores。

- EBSPermissions
- EC2DescribePermissions

- EC2RunInstancesPermissions
- EC2TerminateInstancesPermissions
- EC2CreateTagsPermissions

次のステートメントを追加します。

```
{
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/role-name"
},
```

Amazon EFS

バックアップ

からの次のステートメントから始めますAWSBackupServiceRolePolicyForBackup。

- EFSPermissions
- GetResourcesPermissions
- BackupVaultPermissions

復元

から EFSPermissionsステートメントから開始しますAWSBackupServiceRolePolicyForRestores。

Amazon FSx

バックアップ

からの次のステートメントから始めますAWSBackupServiceRolePolicyForBackup。

- FsxBackupPermissions
- FsxCreateBackupPermissions
- FsxPermissions
- FsxVolumePermissions
- FsxListTagsPermissions
- FsxDeletePermissions

- FsxResourcePermissions
- KMSPermissions

復元

からの次のステートメントから始めますAWSBackupServiceRolePolicyForRestores。

- FsxPermissions
- FsxTagPermissions
- FsxBackupPermissions
- FsxDeletePermissions
- FsxDescribePermissions
- FsxVolumeTagPermissions
- FsxBackupTagPermissions
- FsxVolumePermissions
- DSPermissions
- KMSDescribePermissions

Amazon RDS

バックアップ

から次のステートメントから始めますAWSBackupServiceRolePolicyForBackup。

- DynamoDBBackupPermissions
- RDSBackupPermissions
- RDSClusterModifyPermissions
- GetResourcesPermissions
- BackupVaultPermissions
- KMSPermissions

復元

から RDSPermissionsステートメントから開始しますAWSBackupServiceRolePolicyForRestores。

Amazon S3

バックアップ

「AWSBackupServiceRolePolicyForS3Backup」から開始してください。

バックアップを別のアカウントにコピーする必要がある場合は、 BackupVaultPermissionsおよび BackupVaultCopyPermissionsステートメントを追加します。

復元

「AWSBackupServiceRolePolicyForS3Restore」から開始してください。

AWS Storage Gateway

バックアップ

からの次のステートメントから始めますAWSBackupServiceRolePolicyForBackup。

- StorageGatewayPermissions
- EBSTagAndDeletePermissions
- GetResourcesPermissions
- BackupVaultPermissions

次のステートメントを追加します。

```
{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSnapshots"
      ],
      "Resource":"*"
},
```

復元

からの次のステートメントから始めますAWSBackupServiceRolePolicyForRestores。

- StorageGatewayVolumePermissions
- StorageGatewayGatewayPermissions
- StorageGatewayListPermissions

仮想マシン

バックアップ

からの BackupGatewayBackupPermissionsステートメントから開始しますAWSBackupServiceRolePolicyForBackup。

復元

からの GatewayRestorePermissionsステートメントから開始しますAWSBackupServiceRolePolicyForRestores。

暗号化バックアップ

暗号化されたバックアップを復元するには、次のいずれかの操作を行います。

- AWS KMS キーポリシーの許可リストにロールを追加する
- 復元のために、 から IAM ロールAWSBackupServiceRolePolicyForRestoresに次のステートメントを追加します。
  - KMSDescribePermissions
  - KMSPermissions
  - KMSCreateGrantPermissions

のポリシーの更新 AWS Backup

このサービスがこれらの変更の追跡を開始した AWS Backup 以降の の AWS マネージドポリシーの更新に関する詳細を表示します。

変更	説明	日付
AWSBackupServiceRolePolicyForBackup - 既存ポリシーへの更新	AWS Backup このポリシーbackup:TagResource に 許可を追加しました。 アクセス許可は、リカバリポイントの作成中にタグ付けアクセス許可を取得するために必要です。	2024 年 5 月 17 日

変更	説明	日付
AWSBackupServiceRolePolicyForS3Backup – 既存ポリシーへの更新	AWS Backup このポリシーbackup:TagResource に 許可を追加しました。 アクセス許可は、リカバリポイントの作成中にタグ付けアクセス許可を取得するために必要です。	2024 年 5 月 17 日
AWSBackupServiceLinkedRolePolicyForBackup – 既存ポリシーへの更新	AWS Backup このポリシーbackup:TagResource に 許可を追加しました。 アクセス許可は、リカバリポイントの作成中にタグ付けアクセス許可を取得するために必要です。	2024 年 5 月 17 日
AWSBackupServiceRolePolicyForBackup – 既存ポリシーへの更新	アクセス許可 を追加しましたrds:DeleteDBInstanceAutomatedBackups 。 このアクセス許可は、 が Amazon RDS インスタンス point-in-time-restore の継続的なバックアップと をサポートする AWS Backup のに必要です。	2024 年 5 月 1 日

変更	説明	日付
AWSBackupFullAccess – 既存ポリシーへの更新	AWS Backup Storage Gateway API モデルの変更に対応するため、 は 許可 の Amazon リソースネーム (ARN) を `storagegateway:ListVolumes` から `arn:aws:storagegateway:*:*:gateway/*` *に更新しました。	2024 年 5 月 1 日
AWSBackupOperatorAccess – 既存ポリシーへの更新	AWS Backup Storage Gateway API モデルの変更に対応するため、 は 許可 の Amazon リソースネーム (ARN) を `storagegateway:ListVolumes` から `arn:aws:storagegateway:*:*:gateway/*` *に更新しました。	2024 年 5 月 1 日

変更	説明	日付
AWSServiceRolePolicyForBackupRestoreTesting – 既存ポリシーへの更新	復元テストプランを実行するために、復旧ポイントと保護されたリソースを記述および一覧表示するためのアクセス許可 backup:DescribeRecoveryPoint 、backup:DescribeProtectedResource 、backup:ListProtectedResources 、 を追加しましたbackup:ListRecoveryPointsByResource 。 Amazon EBS アーカイブ階層ストレージec2:DescribeSnapshotTierStatus をサポートするアクセス許可を追加しました。 Amazon Aurora の継続的バックアップrds:DescribeDBClusterAutomatedBackups をサポートするアクセス許可を追加しました。 Amazon Redshift バックアップの復元テストをサポートするために、 redshift:DescribeClusters およびredshift:DeleteCluster のアクセス許可を追加しました 。 Amazon Timestream バックアップの復元テス	2024 年 2 月 14 日

変更	説明	日付
	トtimestream:DeleteTable をサポートするアクセス許可を追加しました。	
AWSBackupServiceRolePolicyForRestores – 既存ポリシーへの更新	アクセス許可 ec2:DescribeSnapshotTierStatus と を追加しましたec2:RestoreSnapshotTier 。 これらのアクセス許可は、 に保存された Amazon EBS リソースをアーカイブストレージ AWS Backup から復元するオプションをユーザーが持つために必要です。 EC2 インスタンスの復元では、EC2 インスタンスを起動するために次のポリシーステートメントに示されているアクセス許可も含める必要があります。	2023 年 11 月 27 日

変更	説明	日付
AWSBackupServiceRolePolicyForBackup – 既存ポリシーへの更新	アーカイブストレージ階層に移行`ec2:ModifySnapshotTier` するためにバックアップされた Amazon EBS リソースの追加ストレージオプションをサポートするアクセス許可 `ec2:DescribeSnapshotTierStatus` と を追加しました。 これらのアクセス許可は、 に保存された Amazon EBS リソースをアーカイブストレージに移行するオプション AWS Backup をユーザーが持つために必要です。	2023 年 11 月 27 日

変更	説明	日付
AWSBackupServiceLinkedRolePolicyForBackup – 既存ポリシーへの更新	アーカイブストレージ階層に移行`ec2:ModifySnapshotTier` するためにバックアップされた Amazon EBS リソースの追加ストレージオプションをサポートするアクセス許可 `ec2:DescribeSnapshotTierStatus` と を追加しました。 これらのアクセス許可は、 に保存された Amazon EBS リソースをアーカイブストレージに移行するオプション AWS Backup をユーザーが持つために必要です。 Aurora クラスターの PITR (point-in-time 復元) `rds:RestoreDBClusterToPointInTime` に必要なアクセス許可 `rds:DescribeDBClusterSnapshots` と を追加しました。	

変更	説明	日付
AWSServiceRolePolicyForBackupRestoreTesting - 新しいポリシー	復元テストを実行するために必要なアクセス許可を提供します。アクセス許可には、Aurora、DocumentDB、DynamoDB、Amazon EBS、Amazon EC2、Amazon EFS、FSx for Lustre、FSx for Windows File Server、FSx for ONTAP、FSx for OpenZFS、Amazon Neptune、Amazon RDS、Amazon S3 といったサービスを復元テストに含めるための、`list`, `read`, and `write` アクションが含まれます。	2023 年 11 月 27 日
AWSBackupFullAccess – 既存ポリシーへの更新	`restore-testing.backup.amazonaws.com` が`IamPassRolePermissions` と`IamCreateServiceLinkedRolePermissions` に追加されました。この追加は、 がお客様に代わって復元テストを実行する AWS Backup ために必要です。	2023 年 11 月 27 日
AWSBackupServiceRolePolicyForRestores – 既存ポリシーへの更新	Aurora クラスターの PITR (point-in-time 復元) `rds:RestoreDBClusterToPointInTime` に必要なアクセス許可 `rds:DescribeDBClusterSnapshots` と を追加しました。	2023 年 9 月 6 日

変更	説明	日付
AWSBackupFullAccess – 既存ポリシーへの更新	Aurora クラスターの継続的なバックアップと point-in-time 復元`rds:DescribeDBClusterAutomatedBackups` に必要なアクセス許可 を追加しました。	2023 年 9 月 6 日
AWSBackupOperatorAccess – 既存ポリシーへの更新	Aurora クラスターの継続的なバックアップと point-in-time 復元`rds:DescribeDBClusterAutomatedBackups` に必要なアクセス許可 を追加しました。	2023 年 9 月 6 日

変更	説明	日付
AWSBackupServiceRolePolicyForBackup – 既存ポリシーへの更新	アクセス許可 を追加しましたrds:DescribeDBClusterAutomatedBackups 。このアクセス許可は、Aurora クラスターの継続的なバックアップと point-in-time 復元 AWS Backup をサポートするために必要です。 保持期間が終了したときに AWS Backup 、ライフサイクルrds:DeleteDBClusterAutomatedBackups が Amazon Aurora 継続的リカバリポイントを削除および関連付け解除できるようにするアクセス許可を追加しました。このアクセス許可は、Aurora 復旧ポイントが EXIPIRED の状態への移行を回避するために必要です。 rds:ModifyDBCluster が Aurora クラスターとやり取り AWS Backup できるようにするアクセス許可を追加しました。この追加により、ユーザーは必要な設定に基づいて継続的バックアップを有効または無効にすることができます。	2023 年 9 月 6 日

変更	説明	日付
AWSBackupFullAccess – 既存ポリシーへの更新	新しいボールトタイプのリソース共有の関連付けを取得するアクセス許可をユーザーに付与ram:GetResourceShareAssociations するアクションを追加しました。	2023 年 8 月 8 日
AWSBackupOperatorAccess – 既存ポリシーへの更新	新しいボールトタイプのリソース共有の関連付けを取得するアクセス許可をユーザーに付与ram:GetResourceShareAssociations するアクションを追加しました。	2023 年 8 月 8 日
AWSBackupServiceRolePolicyForS3Backup – 既存ポリシーへの更新	バケットインベントリを使用してバックアップのパフォーマンス速度s3:PutInventoryConfiguration を向上させるアクセス許可を追加しました。	2023 年 8 月 1 日

変更	説明	日付
AWSBackupServiceRolePolicyForRestores – 既存ポリシーへの更新	リソースを復元するためのタグを追加するアクセス許可をユーザーに付与するアクションとしてstoragegateway:AddTagsToResource 、、elasticfilesystem:TagResource 、 RunInstances のいずれかを含む ec2:CreateTags のみ、fsx:TagResource 、および CreateVolume が追加されec2:CreateAction ましたcloudformation:TagResource 。	2023 年 5 月 22 日
AWSBackupAuditAccess – 既存ポリシーへの更新	API 内のリソース選択をワイルドカードリソースconfig:DescribeComplianceByConfigRule に置き換え、ユーザーがリソースを簡単に選択できるようにしました。	2023 年 4 月 11 日
AWSBackupServiceRolePolicyForRestores – 既存ポリシーへの更新	カスタマーマネージドキーを使用して Amazon EFS を復元するアクセス許可 を追加しましたkms:GenerateDataKeyWithoutPlaintext 。これにより、ユーザーに Amazon EFS リソースを復元するために必要なアクセス許可が付与されます。	2023 年 3 月 27 日

変更	説明	日付
AWSServiceRolePolicyForBackupReports – 既存ポリシーへの更新	Audit Manager が Audit Manager マネージド AWS Config ルールにアクセスできるように AWS Backup 、AWS Backup `config:DescribeConfigRules` および `config:DescribeConfigRuleEvaluationStatus` アクションを更新しました。	2023 年 3 月 9 日
AWSBackupServiceRolePolicyForS3Restore – 既存ポリシーへの更新	ポリシー `s3:GetBucketOwnershipControls` に `kms:Decrypt` 、`s3:PutBucketOwnershipControls` 、 のアクセス許可を追加しましたAWSBackupServiceRolePolicyForS3Restore 。これらのアクセス許可は、元のバックアップで KMS 暗号化が使用されている場合はオブジェクトの復元をサポートし、オブジェクトの所有権が ACL ではなく元のバケットに設定されている場合にオブジェクトを復元するために必要です。	2023 年 2 月 13 日

変更	説明	日付
AWSBackupFullAccess – 既存ポリシーへの更新	仮想マシンの VMware タグを使用してバックアップをスケジュールしbackup-gateway:GetHypervisorPropertyMappings 、スケジュールベースの帯域幅スロットリングをサポートするためにbackup-gateway:GetVirtualMachine 、、、、backup-gateway:PutHypervisorPropertyMappings 、backup-gateway:GetHypervisor 、backup-gateway:StartVirtualMachinesMetadataSync backup-gateway:GetBandwidthRateLimitSchedule 、および のアクセス許可を追加しましたbackup-gateway:PutBandwidthRateLimitSchedule 。	2022 年 12 月 15 日

変更	説明	日付
AWSBackupOperatorAccess – 既存ポリシーへの更新	仮想マシンの VMware タグを使用してバックアップをスケジュールし、スケジュールベースの帯域幅スロットリングをサポートするためにbackup-gateway:GetHypervisorPropertyMappings 、、backup-gateway:GetVirtualMachine 、、backup-gateway:GetHypervisor および のアクセス許可を追加しましたbackup-gateway:GetBandwidthRateLimitSchedule 。	2022 年 12 月 15 日
AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync - 新しいポリシー	オンプレミスネットワーク内の仮想マシンのメタデータを Backup AWS Backup Gateway と同期するためのアクセス許可を Gateway に提供します。	2022 年 12 月 15 日

変更	説明	日付
AWSBackupServiceRolePolicyForBackup – 既存ポリシーへの更新	Timestream バックアッププジョブをサポートするために、、timestream:StartAwsBackupJob 、timestream:GetAwsBackupStatus 、、timestream:ListTables 、timestream:ListDatabases timestream:ListTagsForResource 、timestream:DescribeTable 、および のアクセス許可を追加timestream:DescribeDatabase しましたtimestream:DescribeEndpoints 。	2022 年 12 月 13 日

変更	説明	日付
AWSBackupServiceRolePolicyForRestores – 既存ポリシーへの更新	Timestream 復元ジョブをサポートするために、、timestream:StartAwsRestoreJob 、、timestream:GetAwsRestoreStatus 、timestream:ListTables 、timestream:ListTagsForResource 、timestream:ListDatabases 、timestream:DescribeTable 、および のアクセス許可を追加timestream:DescribeDatabase s3:GetBucketAcl しましたtimestream:DescribeEndpoints 。	2022 年 12 月 13 日
AWSBackupFullAccess – 既存ポリシーへの更新	Timestream リソースをサポートするために、timestream:ListTables 、、timestream:ListDatabases s3:ListAllMyBuckets および のアクセス許可を追加しましたtimestream:DescribeEndpoints 。	2022 年 12 月 13 日

変更	説明	日付
AWSBackupOperatorAccess – 既存ポリシーへの更新	Timestream リソースをサポートするために、timestream:ListDatabases 、、timestream:ListTables 、およびのアクセス許可を追加s3:ListAllMyBuckets しましたtimestream:DescribeEndpoints 。	2022 年 12 月 13 日
AWSBackupServiceLinkedRolePolicyForBackup – 既存ポリシーへの更新	Timestream リソースをサポートするために、、timestream:ListDatabases 、、timestream:ListTables 、timestream:ListTagsForResource 、timestream:DescribeDatabase 、timestream:GetAwsBackupStatus 、timestream:DescribeTable およびのアクセス許可を追加timestream:GetAwsRestoreStatus しましたtimestream:DescribeEndpoints 。	2022 年 12 月 13 日

変更	説明	日付
AWSBackupFullAccess – 既存ポリシーへの更新	Amazon Redshift リソースをサポートするために、、redshift:DescribeClusters 、、redshift:DescribeClusterSubnetGroups 、redshift:DescribeNodeConfigurationOptions 、redshift:DescribeOrderableClusterOptions redshift:DescribeClusterParameterGroups 、redshift:DescribeClusterTracks 、および のアクセス許可を追加redshift:DescribeSnapshotSchedules しましたec2:DescribeAddresses 。	2022 年 11 月 27 日

変更	説明	日付
AWSBackupOperatorAccess – 既存ポリシーへの更新	Amazon Redshift リソースをサポートするために、、redshift:DescribeClusters 、、redshift:DescribeClusterSubnetGroups 、redshift:DescribeNodeConfigurationOptions redshift:DescribeOrderableClusterOptions 、redshift:DescribeClusterParameterGroups, redshift:DescribeClusterTracks 、および のアクセス許可を追加redshift:DescribeSnapshotSchedules しましたec2:DescribeAddresses 。	2022 年 11 月 27 日

変更	説明	日付
AWSBackupServiceRolePolicyForRestores – 既存ポリシーへの更新	Amazon Redshift 復元ジョブをサポートするために、`redshift:RestoreFromClusterSnapshot`、、`redshift:RestoreTableFromClusterSnapshot` 、および のアクセス許可を追加`redshift:DescribeClusters` しました`redshift:DescribeTableRestoreStatus` 。	2022 年 11 月 27 日
AWSBackupServiceRolePolicyForBackup – 既存ポリシーへの更新	Amazon Redshift バックアップジョブをサポートするために、、`redshift:CreateClusterSnapshot` 、`redshift:DescribeClusterSnapshots` 、、`redshift:DeleteClusterSnapshot` 、および `redshift:DescribeTags` のアクセス許可を追加`redshift:DescribeClusters` しました`redshift:CreateTags` 。	2022 年 11 月 27 日
AWSBackupFullAccess – 既存ポリシーへの更新	CloudFormation リソースをサポートする次のアクセス許可を追加しました: `cloudformation:ListStacks` 。	2022 年 11 月 27 日

変更	説明	日付
AWSBackupOperatorAccess – 既存ポリシーへの更新	CloudFormation リソースをサポートする次のアクセス許可を追加しました: `cloudformation:ListStacks` 。	2022 年 11 月 27 日
AWSBackupServiceLinkedRolePolicyForBackup – 既存ポリシーへの更新	CloudFormation リソースをサポートするために、`redshift:DescribeClusterSnapshots` 、、`redshift:DescribeTags` 、および のアクセス許可を追加`redshift:DeleteClusterSnapshot` しましたredshift:DescribeClusters 。	2022 年 11 月 27 日
AWSBackupServiceRolePolicyForBackup – 既存ポリシーへの更新	AWS CloudFormation アプリケーションスタックのバックアップジョブをサポートするためにcloudformation:GetTemplate 、、cloudformation:DescribeStacks 、および のアクセス許可を追加しましたcloudformation:ListStackResources 。	2022 年 11 月 16 日

変更	説明	日付
AWSBackupServiceRolePolicyForRestores – 既存ポリシーへの更新	AWS CloudFormation アプリケーションスタックのバックアップジョブをサポートするために、次のアクセス許可を追加`cloudformation:CreateChangeSet` しました。`cloudformation:DescribeChangeSet`	2022 年 11 月 16 日
AWSBackupOrganizationAdminAccess – 既存ポリシーへの更新	組織管理者が委任管理者機能を使用できるように、このポリシーに次のアクセス許可を追加しました: `organizations:ListDelegatedAdministrator` 、`organizations:RegisterDelegatedAdministrator` 、および `organizations:DeregisterDelegatedAdministrator`	2022 年 11 月 27 日
AWSBackupServiceRolePolicyForBackup – 既存ポリシーへの更新	Amazon EC2 インスタンスで SAP HANA をサポートするために、`ssm-sap:GetOperation` 、、`ssm-sap:ListDatabases` 、`ssm-sap:BackupDatabase` 、`ssm-sap:UpdateHanaBackupSettings` `ssm-sap:GetDatabase` およびのアクセス許可を追加しました`ssm-sap:ListTagsForResource` 。	2022 年 11 月 20 日

変更	説明	日付
AWSBackupFullAccess – 既存ポリシーへの更新	Amazon EC2 インスタンスで SAP HANA をサポートするためにssm-sap:ListDatabases 、ssm-sap:GetOperation 、、ssm-sap:GetDatabase 、および のアクセス許可を追加しましたssm-sap:ListTagsForResource 。	2022 年 11 月 20 日
AWSBackupOperatorAccess – 既存ポリシーへの更新	Amazon EC2 インスタンスで SAP HANA をサポートするためにssm-sap:ListDatabases 、ssm-sap:GetOperation 、、ssm-sap:GetDatabase 、および のアクセス許可を追加しましたssm-sap:ListTagsForResource 。	2022 年 11 月 20 日
AWSBackupServiceLinkedRolePolicyForBackup – 既存ポリシーへの更新	Amazon EC2 インスタンスで SAP HANA をサポートする次のアクセス許可を追加しました: ssm-sap:GetOperation 。	2022 年 11 月 20 日
AWSBackupServiceRolePolicyForRestores – 既存ポリシーへの更新	EC2 インスタンスへの Backup ゲートウェイの復元ジョブをサポートするアクセス許可 を追加しましたec2:CreateTags 。	2022 年 11 月 20 日

変更	説明	日付
AWSBackupDataTransferAccess – 既存ポリシーへの更新	SAP HANA On Amazon EC2 リソースの安全なストレージデータ転送をサポートするために、backup-storage:StartObject 、、backup-storage:PutChunk 、backup-storage:GetChunk 、backup-storage:ListChunks 、backup-storage:ListObjects backup-storage:GetObjectMetadata および のアクセス許可を追加しましたbackup-storage:NotifyObjectComplete 。	2022 年 11 月 20 日

変更	説明	日付
AWSBackupRestoreAccessForSAPHANA – 既存ポリシーへの更新	リソース所有者が SAP HANA On Amazon EC2 リソースの復元を実行するためのアクセス許可としてbackup:Get* 、、backup:List* 、backup:Describe* 、backup:StartBackupJob 、backup:StartRestoreJob 、ssm-sap:GetOperation ssm-sap:ListDatabases 、、ssm-sap:BackupDatabase 、ssm-sap:GetDatabase 、、ssm-sap:RestoreDatabase ssm-sap:UpdateHanaBackupSettings を追加しましたssm-sap:ListTagsForResource 。	2022 年 11 月 20 日
AWSBackupServiceRolePolicyForS3Backup – 既存ポリシーへの更新	for Amazon S3 のバックアップオペレーションs3:GetBucketAcl をサポートするアクセス許可を追加 AWS Backup しました。	2022 年 8 月 24 日
AWSBackupServiceRolePolicyForRestores – 既存ポリシーへの更新	マルチアベイラビリティーゾーン (マルチ AZ) 機能をサポートするデータベースインスタンスを作成するためのアクセス権を付与するアクションを追加しましたrds:CreateDBInstance 。	2022 年 7 月 20 日

変更	説明	日付
AWSBackupServiceLinkedRolePolicyForBackup – 既存ポリシーへの更新	リソースワイルドカードでバックアップするバケットを選択するアクセス許可をユーザーにs3:GetBucketTagging 付与するアクセス許可を追加しました。このアクセス許可がないと、リソースワイルドカードでバックアップするバケットを選択するユーザーは失敗します。	2022 年 5 月 6 日
AWSBackupServiceRolePolicyForBackup – 既存ポリシーへの更新	既存の fsx:CreateBackup および fsx:ListTagsForResource アクションの範囲にボリュームリソースを追加し、FSx for ONTAP ボリュームレベルのバックアップfsx:DescribeVolumes をサポートする新しいアクションを追加しました。	2022 年 4 月 27 日
AWSBackupServiceRolePolicyForRestores – 既存ポリシーへの更新	次のアクションを追加して、FSx for ONTAP ボリューム fsx:DescribeVolumes 、、fsx:CreateVolumeFromBackup 、fsx:DeleteVolume および を復元するアクセス許可をユーザーに付与しましたfsx:UntagResource 。	2022 年 4 月 27 日

変更	説明	日付
AWSBackupServiceRolePolicyForS3Backup – 既存ポリシーへの更新	バックアップオペレーション中に Amazon S3 バケットへの変更の通知を受け取るアクセス許可をユーザーに付与するアクションとして、 `s3:GetBucketNotification` および を追加しました`s3:PutBucketNotification` 。	2022 年 2 月 25 日

変更	説明	日付
AWSBackupServiceRolePolicyForS3Backup - 新しいポリシー	Amazon S3 バケットをバックアップするアクセス許可をユーザーに付与するアクションとしてs3:GetInventoryConfiguration 、、s3:PutInventoryConfiguration 、s3:ListBucketVersions 、s3:ListBucket 、、s3:GetBucketVersioning 、s3:GetBucketTagging s3:GetBucketNotification s3:GetBucketLocation が追加されました。 s3:ListAllMyBuckets Amazon S3 オブジェクトをバックアップするアクセス許可をユーザーに付与するアクションとしてs3:GetObject 、、s3GetObjectAcl 、s3:GetObjectVersionTagging 、s3:GetObjectVersionAcl 、s3:GetObjectTagging が追加されましたs3:GetObjectVersion 。 暗号化された Amazon S3 データをバックアップするアクセス許可をユーザーに付与するアクションとして	2022 年 2 月 17 日

変更	説明	日付
	、 kms:Decrypt および を追加しましたkms:DescribeKey 。 Amazon EventBridge ルールを使用して Amazon S3 データの増分バックアップを作成するアクセス許可をユーザーに付与するアクションとしてevents:DescribeRule 、、events:EnableRule 、events:PutRule 、events:DeleteRule 、events:PutTargets 、events:RemoveTargets 、events:ListTargetsByRule 、events:DisableRule 、 が追加されましたcloudwatch:GetMetricData events:ListRules 。	

変更	説明	日付
AWSBackupServiceRolePolicyForS3Restore - 新しいポリシー	Amazon S3 バケットを復元するアクセス許可をユーザーに付与するアクションとしてs3:CreateBucket 、、s3:ListBucketVersions 、、s3:ListBucket s3:GetBucketVersioning 、s3:GetBucketLocation 、 が追加されましたs3:PutBucketVersioning 。 Amazon S3 バケットを復元するアクセス許可をユーザーに付与するアクションとしてs3:GetObject 、、s3:GetObjectVersion 、s3:DeleteObject 、s3:PutObjectVersionAcl 、s3:GetObjectVersionAcl 、s3:GetObjectTagging 、s3:PutObjectTagging 、s3:GetObjectAcl 、s3:PutObjectAcl s3:PutObject 、 が追加されましたs3:ListMultipartUploadParts 。 復元された Amazon S3 データを暗号化するアクセス許可をユーザーに付与するア	2022 年 2 月 17 日

変更	説明	日付
	クションとしてkms:Decrypt 、、kms:DescribeKey 、および が追加されましたkms:GenerateDataKey 。	
AWSBackupServiceLinkedRolePolicyForBackup – 既存ポリシーへの更新	s3:ListAllMyBuckets バケットのリストを表示し、バックアッププランに割り当てるバケットを選択するアクセス許可をユーザーに付与するために を追加しました。	2022 年 2 月 14 日
AWSBackupServiceLinkedRolePolicyForBackup – 既存ポリシーへの更新	仮想マシンのリストを表示し、バックアッププランに割り当てる仮想マシンを選択するアクセス許可をユーザーにbackup-gateway:ListVirtualMachines 付与するために を追加しました。 仮想マシンのタグを一覧表示するアクセス許可をユーザーに付与backup-gateway:ListTagsForResource するために を追加しました。	2021 年 11 月 30 日

変更	説明	日付
AWSBackupServiceRolePolicyForBackup – 既存ポリシーへの更新	仮想マシンのバックアップを復元するアクセス許可backup-gateway:Backup をユーザーに付与backup-gateway:ListTagsForResource するために を追加しました。AWS Backup また、仮想マシンのバックアップに割り当てられたタグを一覧表示するアクセス許可をユーザーに付与するために を追加しました。	2021 年 11 月 30 日
AWSBackupServiceRolePolicyForRestores – 既存ポリシーへの更新	仮想マシンのバックアップを復元するアクセス許可をユーザーに付与backup-gateway:Restore するために を追加しました。	2021 年 11 月 30 日

変更	説明	日付
AWSBackupFullAccess – 既存ポリシーへの更新	Gateway を使用して仮想マシンをバックアップ、復元、管理 AWS Backup するためのアクセス許可をユーザーに付与するアクションとして、backup-gateway:AssociateGatewayToServer 、backup-gateway:CreateGateway backup-gateway:DeleteGateway 、backup-gateway:DeleteHypervisor 、backup-gateway:DisassociateGatewayFromServer 、、backup-gateway:ImportHypervisorConfiguration 、backup-gateway:ListGateways backup-gateway:ListHypervisors 、、backup-gateway:ListTagsForResource backup-gateway:ListVirtualMachines 、backup-gateway:PutMaintenanceStartTime 、、backup-gateway:TagResource backup-gateway:TestHypervisorConfigu	2021 年 11 月 30 日

変更	説明	日付
	ration backup-gateway:UntagResource backup-gateway:UpdateGatewayInformation 、、 が追加されましたbackup-gateway:UpdateHypervisor 。	
AWSBackupOperatorAccess – 既存ポリシーへの更新	仮想マシンをバックアップするアクセス許可をユーザーに付与するアクションとしてbackup-gateway:ListGateways 、、backup-gateway:ListHypervisors 、backup-gateway:ListTagsForResource 、 が追加されましたbackup-gateway:ListVirtualMachines 。	2021 年 11 月 30 日
AWSBackupServiceLinkedRolePolicyForBackup – 既存ポリシーへの更新	dynamodb:ListTagsOfResource の高度な DynamoDB バックアップ機能を使用してバックアップする DynamoDB テーブル AWS Backupのタグを一覧表示するアクセス許可をユーザーに付与するために を追加しました。	2021 年 11 月 23 日

変更	説明	日付
AWSBackupServiceRolePolicyForBackup – 既存ポリシーへの更新	高度なバックアップ機能を使用して DynamoDB テーブルをバックアップするアクセス許可をユーザーに付与dynamodb:StartAwsBackupJob するために を追加しました。 ソース DynamoDB テーブルからバックアップにタグをコピーするアクセス許可をユーザーにdynamodb:ListTagsOfResource 付与するために を追加しました。	2021 年 11 月 23 日
AWSBackupServiceRolePolicyForRestores – 既存ポリシーへの更新	の高度な DynamoDB バックアップ機能を使用してバックアップされた DynamoDB テーブル AWS Backupを復元するアクセス許可をユーザーに付与dynamodb:RestoreTableFromAwsBackup するために を追加しました。	2021 年 11 月 23 日
AWSBackupServiceRolePolicyForRestores – 既存ポリシーへの更新	の高度な DynamoDB バックアップ機能を使用してバックアップされた DynamoDB テーブル AWS Backupを復元するアクセス許可をユーザーに付与dynamodb:RestoreTableFromAwsBackup するために を追加しました。	2021 年 11 月 23 日

変更	説明	日付
AWSBackupOperatorAccess – 既存ポリシーへの更新	アクション backup:GetRecoveryPointRestoreMetadata とは冗長rds:DescribeDBSnapshots であるため、を削除しました。 AWS Backup は、backup:Get* の一部として backup:GetRecoveryPointRestoreMetadata との両方を必要としませんでしたAWSBackupOperatorAccess 。また、rds:describeDBSnapshots の一部として rds:DescribeDBSnapshots との両方は必要ありません AWS Backup でしたAWSBackupOperatorAccess 。	2021 年 11 月 23 日

変更	説明	日付
AWSBackupServiceLinkedRolePolicyForBackup – 既存ポリシーへの更新	バックアッププランに割り当てるリソースを選択する際に`elasticfilesystem:DescribeFileSystems` 、 がサポートするリソースのリストを表示および選択`fsx:DescribeFileSystems` できるように、新しいアクション AWS Backup`rds:DescribeDBClusters` 、`dynamodb:ListTables` `storagegateway:ListVolumes` `ec2:DescribeVolumes` `ec2:DescribeInstances` `rds:DescribeDBInstances` 、、、、、 を追加しました。	2021 年 11 月 10 日
AWSBackupAuditAccess - 新しいポリシー	AWS Backup Audit Manager を使用するためのアクセス許可をユーザーに`AWSBackupAuditAccess` 付与するために を追加しました。権限には、コンプライアンスフレームワークを設定し、レポートを生成する機能が含まれます。	2021 年 8 月 24 日

変更	説明	日付
AWSServiceRolePolicyForBackupReports - 新しいポリシー	ユーザーが設定したフレームワークに準拠するためのバックアップ設定、ジョブ、およびリソースのモニタリングを自動化する、サービスにリンクされたロールのアクセス許可を付与`AWSServiceRolePolicyForBackupReports` する を追加しました。	2021 年 8 月 24 日
AWSBackupFullAccess – 既存ポリシーへの更新	サービスにリンクされたロールを (ベストエフォートベースで) 作成し、期限切れの復旧ポイントの削除を自動化`iam:CreateServiceLinkedRole` するように を追加しました。このサービスにリンクされたロールがない場合、お客様がリカバリポイントの作成に使用した元の IAM ロールを削除した後は、期限切れのリカバリポイントを削除 AWS Backup することはできません。	2021 年 7 月 5 日
AWSBackupServiceLinkedRolePolicyForBackup – 既存ポリシーへの更新	バックアッププランのライフサイクル設定に基づいて、期限切れの DynamoDB リカバリポイントの削除を自動化する`DeleteRecoveryPoint` アクセス許可を付与 `dynamodb:DeleteBackup` する新しいアクションを追加しました。	2021 年 7 月 5 日

変更	説明	日付
AWSBackupOperatorAccess – 既存ポリシーへの更新	アクション backup:GetRecoveryPointRestoreMetadata とは冗長rds:DescribeDBSnapshots であるため、を削除しました。 AWS Backup はbackup:Get* 、の一部として backup:GetRecoveryPointRestoreMetadata と AWSBackupOperatorAccess の両方を必要としませんでした。また、rds:describeDBSnapshots の一部として rds:DescribeDBSnapshots と AWS Backup の両方を必要としませんでした。 AWSBackupOperatorAccess	2021 年 5 月 25 日

変更	説明	日付
AWSBackupOperatorAccess – 既存ポリシーへの更新	アクション backup:GetRecoveryPointRestoreMetadata とは冗長rds:DescribeDBSnapshots であるため、を削除しました。 AWS Backup は、backup:Get* の一部として backup:GetRecoveryPointRestoreMetadata との両方を必要としませんでしたAWSBackupOperatorAccess 。また、rds:describeDBSnapshots の一部として rds:DescribeDBSnapshots との両方は必要ありません AWS Backup でしたAWSBackupOperatorAccess 。	2021 年 5 月 25 日
AWSBackupServiceRolePolicyForRestores – 既存ポリシーへの更新	復元プロセス中に Amazon FSx ファイルシステムにタグを適用するためのStartRestoreJob アクセス許可fsx:TagResource を付与する新しいアクションを追加しました。	2021 年 5 月 24 日

変更	説明	日付
AWSBackupServiceRolePolicyForRestores – 既存ポリシーへの更新	リカバリポイントから Amazon EC2 インスタンス`ec2:DescribeInstances` を復元するための`StartRestoreJob` アクセス許可を付与する新しいアクション `ec2:DescribeImages` および を追加しました。	2021 年 5 月 24 日
AWSBackupServiceRolePolicyForBackup – 既存ポリシーへの更新	リージョンとアカウント間で Amazon FSx リカバリポイントをコピーするための`StartCopyJob` アクセス許可`fsx:CopyBackup` を付与する新しいアクションを追加しました。	2021 年 4 月 12 日
AWSBackupServiceLinkedRolePolicyForBackup – 既存ポリシーへの更新	リージョンとアカウント間で Amazon FSx リカバリポイントをコピーするための`StartCopyJob` アクセス許可`fsx:CopyBackup` を付与する新しいアクションを追加しました。	2021 年 4 月 12 日

変更	説明	日付
AWSBackupServiceRolePolicyForBackup – 既存ポリシーへの更新	次の要件に準拠するように更新されました。 AWS Backup で暗号化された DynamoDB テーブルのバックアップを作成するには、バックアップに使用される IAM ロール`kms:GenerateDataKey` に アクセス許可 `kms:Decrypt` と を追加する必要があります。	2021 年 3 月 10 日

変更	説明	日付
AWSBackupFullAccess – 既存ポリシーへの更新	次の要件に準拠するように更新されました。 AWS Backup を使用して Amazon RDS データベースの継続的バックアップを設定するには、バックアッププラン設定で定義された IAM ロールに API アクセス許可`rds:ModifyDBInstance` が存在することを確認します。 Amazon RDS 連続バックアップをリストアするには、リストアジョブ用に送信した IAM ロールに `rds:RestoreDBInstanceToPointInTime` 権限を追加する必要があります。 AWS Backup コンソールで、point-in-time リカバリに使用できる時間の範囲を記述するには、IAM 管理ポリシーに `rds:DescribeDBInstanceAutomatedBackups` API アクセス許可を含める必要があります。	2021 年 3 月 10 日
AWS Backup が変更の追跡を開始しました	AWS Backup が AWSマネージドポリシーの変更の追跡を開始しました。	2021 年 3 月 10 日

AWS Backupのサービスにリンクされたロールの使用

AWS Backup は AWS Identity and Access Management 、 (IAM) サービスにリンクされたロール を使用します。サービスにリンクされたロールは、 に直接リンクされた一意のタイプの IAM ロールです AWS Backup。サービスにリンクされたロールは によって事前定義 AWS Backup されており、ユーザーに代わってサービスから他の AWS のサービスを呼び出すために必要なすべてのアクセス許可が含まれています。

トピック

- ロールを使用したバックアップとコピー
- AWS Backup Audit Manager でのロールの使用
- 復元テストでロールを使用する

ロールを使用したバックアップとコピー

AWS Backup は AWS Identity and Access Management 、 (IAM) サービスにリンクされたロール を使用します。サービスにリンクされたロールは、 に直接リンクされた一意のタイプの IAM ロールです AWS Backup。サービスにリンクされたロールは によって事前定義 AWS Backup されており、ユーザーに代わってサービスから他の AWS のサービスを呼び出すために必要なすべてのアクセス許可が含まれています。

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

サービスリンクロールを削除するには、まずその関連リソースを削除します。これにより、 AWS Backup リソースにアクセスするためのアクセス許可を誤って削除することがないため、リソースが保護されます。

サービスリンクロールをサポートする他のサービスについては、「IAM と連携するAWS のサービス」を参照して、[サービスリンクロール] 列が [はい] のサービスを探してください。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[はい] リンクを選択します。

のサービスにリンクされたロールのアクセス許可 AWS Backup

AWS Backup は、 という名前のサービスにリンクされたロールを使用しますAWSServiceRoleForBackup。バックアップできるリソースを一覧表示し、バックアップをコピーするための AWS Backup アクセス許可を提供します。

AWS Backup は、 ロールを使用して、Amazon EC2 を除くすべてのリソースタイプのすべてのバックアップを削除します。

AWSServiceRoleForBackup サービスにリンクされたロールは、次のサービスを信頼してロールを引き受けます。

- `backup.amazonaws.com`

このポリシーのアクセス許可を確認するには、「 マネージドポリシーリファレンス AWSBackupServiceLinkedRolePolicyforBackup」の「」を参照してください。 AWS

サービスリンクロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、アクセス許可を設定する必要があります。詳細については、IAM ユーザーガイドの「サービスリンクロールの権限」を参照してください。

AWS Backupのサービスリンクロールの作成

サービスリンクロールを手動で作成する必要はありません。、、または AWS API でバックアップ、クロスアカウントバックアップの設定 AWS CLI、またはバックアップを実行するリソースを一覧表示すると、 AWS Management Console AWS Backup によってサービスにリンクされたロールが作成されます。

> **Important**
>
> このサービスリンクロールは、このロールでサポートされている機能を使用する別のサービスでアクションが完了した場合にアカウントに表示されます。詳細については、「IAM アカウントに新しいロールが表示される」を参照してください。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は、同じ手順でアカウントにロールを再作成できます。バックアップ、クロスアカウントバックアップの設定、またはバックアップを実行するリソースを一覧表示すると、サービスにリンクされたロールが再度 AWS Backup 作成されます。

AWS Backupのサービスにリンクされたロールの編集

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

AWS Backupのサービスリンクロールの削除

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、モニタリングや保守が積極的に行われていない未使用のエンティティを排除できます。ただし、手動で削除する前に、サービスリンクロールをクリーンアップする必要があります。

サービスリンクロールのクリーンアップ

IAM を使用してサービスリンクロールを削除するには、最初に、そのロールで使用されているリソースをすべて削除する必要があります。まず、すべてのリカバリポイントを削除する必要があります。次に、すべてのバックアップ保管庫を削除する必要があります。

> **Note**
>
> リソースを削除しようとしたときに AWS Backup サービスがロールを使用している場合、削除が失敗する可能性があります。失敗した場合は、数分待ってから再度オペレーションを実行してください。

によって使用されている AWS Backup リソースを削除するには AWSServiceRoleForBackup （ コンソール ）

1. すべてのリカバリポイントとバックアップ保管庫 (デフォルト保管庫を除く) を削除するには、「バックアップ保管庫を削除する」の手順に従います。
2. デフォルトの保管庫を削除するには、 AWS CLIの次のコマンドを使用します。

```
aws backup delete-backup-vault --backup-vault-name Default --region us-east-1
```

AWSServiceRoleForBackup（ AWS CLI) が使用する AWS Backup リソースを削除するには

1. すべての復旧ポイントを削除するには、 を使用しますdelete-recovery-point。
2. バックアップ保管庫をすべて削除するには、`delete-backup-vault` を使用します。

AWSServiceRoleForBackup (API) が使用する AWS Backup リソースを削除するには

1. すべてのリカバリポイントを削除するには、`DeleteRecoveryPoint` を使用します。
2. バックアップ保管庫をすべて削除するには、`DeleteBackupVault` を使用します。

サービスリンクロールの手動による削除

IAM コンソール、、または AWS API を使用して AWS CLI、サービスにリンクされたロールを削除します AWSServiceRoleForBackup。詳細については、IAM ユーザーガイド の「サービスリンクロールの削除」を参照してください。

AWS Backup のサービスにリンクされたロールをサポートするリージョン

AWS Backup は、サービスが利用可能なすべてのリージョンでサービスにリンクされたロールの使用をサポートします。詳細については、サポートされているAWS Backup 機能とリージョンを参照してください。

AWS Backup Audit Manager でのロールの使用

AWS Backup は AWS Identity and Access Management (IAM) サービスにリンクされたロール を使用します。サービスにリンクされたロールは、 に直接リンクされた一意のタイプの IAM ロールです AWS Backup。サービスにリンクされたロールは によって事前定義 AWS Backup されており、ユーザーに代わってサービスから他の AWS のサービスを呼び出すために必要なすべてのアクセス許可が含まれています。

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

サービスリンクロールを削除するには、まずその関連リソースを削除します。これにより、 AWS Backup リソースにアクセスするためのアクセス許可を誤って削除することがないため、リソースが保護されます。

サービスリンクロールをサポートする他のサービスについては、「IAM と連携するAWS のサービス」を参照して、[サービスリンクロール] 列が [はい] のサービスを探してください。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[はい] リンクを選択します。

のサービスにリンクされたロールのアクセス許可 AWS Backup

AWS Backup は、 という名前のサービスにリンクされたロールを使用します AWSServiceRoleForBackupReports – コントロール、フレームワーク、レポートを作成するアクセス許可を AWS Backup に提供します。

AWSServiceRoleForBackupReports サービスにリンクされたロールは、次のサービスを信頼してロールを引き受けます。

- `backup.amazonaws.com`

このポリシーのアクセス許可を確認するには、「 マネージドポリシーリファレンスAWSServiceRolePolicyForBackupReports」の「」を参照してください。 AWS

サービスリンクロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、アクセス許可を設定する必要があります。詳細については、IAM ユーザーガイドの「サービスリンクロールの権限」を参照してください。

AWS Backupのサービスリンクロールの作成

サービスリンクロールを手動で作成する必要はありません。、、または AWS API AWS Backup でフレームワークまたはレポートプランを作成する AWS Management Consoleと AWS CLI、 によってサービスにリンクされたロールが作成されます。

> **Important**
>
> このサービスリンクロールは、このロールでサポートされている機能を使用する別のサービスでアクションが完了した場合にアカウントに表示されます。詳細については、「IAM アカウントに新しいロールが表示される」を参照してください。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は、同じ手順でアカウントにロールを再作成できます。フレームワークまたはレポートプランを作成すると、 によってサービスにリンクされたロールが再度 AWS Backup 作成されます。

AWS Backupのサービスにリンクされたロールの編集

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

AWS Backupのサービスリンクロールの削除

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、モニタリングや保守が積極的に行われていない未使用のエンティティを排除できます。ただし、手動で削除する前に、サービスリンクロールをクリーンアップする必要があります。

サービスリンクロールのクリーンアップ

IAM を使用してサービスリンクロールを削除するには、最初に、そのロールで使用されているリソースをすべて削除する必要があります。すべてのフレームワークとレポートプランを削除する必要があります。

> **Note**
>
> リソースを削除しようとしたときに AWS Backup サービスがロールを使用している場合、削除が失敗する可能性があります。失敗した場合は、数分待ってから再度オペレーションを実行してください。

によって使用されている AWS Backup リソースを削除するには AWSServiceRoleForBackupReports（コンソール）

1. すべてのフレームワークを削除するには、「フレームワークの削除」を参照してください。
2. すべてのレポートプランを削除するには、「レポートプランの削除」を参照してください。

AWSServiceRoleForBackupReports（ AWS CLI) が使用する AWS Backup リソースを削除するには

1. すべてのフレームワークを削除するには、delete-framework を使用してください。
2. すべてのレポートプランを削除するには、 を使用しますdelete-report-plan。

AWSServiceRoleForBackupReports (API) が使用する AWS Backup リソースを削除するには

1. すべてのフレームワークを削除するには、DeleteFramework を使用します。
2. すべてのレポートプランを削除するには、 を使用しますDeleteReportPlan。

サービスリンクロールの手動による削除

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

AWS Backup のサービスにリンクされたロールをサポートするリージョン

AWS Backup は、サービスが利用可能なすべてのリージョンでサービスにリンクされたロールの使用をサポートします。詳細については、サポートされているAWS Backup 機能とリージョンを参照してください。

復元テストでロールを使用する

AWS Backup は AWS Identity and Access Management 、 (IAM) サービスにリンクされたロール を使用します。サービスにリンクされたロールは、 に直接リンクされた一意のタイプの IAM ロールです AWS Backup。サービスにリンクされたロールは によって事前定義 AWS Backup されており、ユーザーに代わってサービスから他の AWS のサービスを呼び出すために必要なすべてのアクセス許可が含まれています。

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

サービスリンクロールを削除するには、まずその関連リソースを削除します。これにより、 AWS Backup リソースにアクセスするためのアクセス許可を誤って削除することがないため、リソースが保護されます。

サービスリンクロールをサポートする他のサービスについては、「IAM と連携するAWS のサービス」を参照して、[サービスリンクロール] 列が [はい] のサービスを探してください。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[はい] リンクを選択します。

のサービスにリンクされたロールのアクセス許可 AWS Backup

AWS Backup は、 という名前のサービスにリンクされたロールを使用しますAWSServiceRolePolicyForBackupRestoreTesting。復元テストを実行するためのバックアップ許可を提供します。

AWSServiceRolePolicyForBackupRestoreTesting サービスにリンクされたロールは、次のサービスを信頼してロールを引き受けます。

- `backup.amazonaws.com`

このポリシーのアクセス許可を確認するには、「 マネージドポリシーリファレンスAWSServiceRolePolicyForBackupRestoreTesting」の「」を参照してください。 AWS

サービスリンクロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、アクセス許可を設定する必要があります。詳細については、IAM ユーザーガイドの「サービスリンクロールの権限」を参照してください。

AWS Backupのサービスリンクロールの作成

サービスリンクロールを手動で作成する必要はありません。、 AWS Management Console、または AWS API AWS Backup で復元テストを実行すると AWS CLI、 によってサービスにリンクされたロールが作成されます。

> **Important**
>
> このサービスリンクロールは、このロールでサポートされている機能を使用する別のサービスでアクションが完了した場合にアカウントに表示されます。詳細については、「IAM アカウントに新しいロールが表示される」を参照してください。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は、同じ手順でアカウントにロールを再作成できます。復元テストを実行すると、 によってサービスにリンクされたロールが再度 AWS Backup 作成されます。

AWS Backupのサービスにリンクされたロールの編集

AWS Backup では、 AWSServiceRolePolicyForBackupRestoreTesting サービスにリンクされたロールを編集することはできません。サービスリンクロールを作成した後は、多くのエンティティによっ

てロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロールの説明の編集はできます。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールの編集」を参照してください。

AWS Backupのサービスリンクロールの削除

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、モニタリングや保守が積極的に行われていない未使用のエンティティを排除できます。ただし、手動で削除する前に、サービスリンクロールをクリーンアップする必要があります。

サービスリンクロールのクリーンアップ

IAM を使用してサービスリンクロールを削除するには、最初に、そのロールで使用されているリソースをすべて削除する必要があります。すべての復元テストプランを削除する必要があります。

> **Note**
>
> リソースを削除しようとしたときに AWS Backup サービスがロールを使用している場合、削除が失敗する可能性があります。失敗した場合は、数分待ってから再度オペレーションを実行してください。

によって使用されている AWS Backup リソースを削除するには AWSServiceRolePolicyForBackupRestoreTesting（コンソール）

- すべての復元テストプランを削除するには、「復元テスト」を参照してください。

AWSServiceRolePolicyForBackupRestoreTesting（AWS CLI) が使用する AWS Backup リソースを削除するには

- 復元テストプランを削除するには、`delete-restore-testing-plan` を使用します。

AWSServiceRolePolicyForBackupRestoreTesting (API) が使用する AWS Backup リソースを削除するには

- 復元テストプランを削除するには、`DeleteRestoreTestingPlan` を使用します。

サービスリンクロールの手動による削除

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

AWS Backup のサービスにリンクされたロールをサポートするリージョン

AWS Backup は、サービスが利用可能なすべてのリージョンでサービスにリンクされたロールの使用をサポートします。詳細については、サポートされているAWS Backup 機能とリージョンを参照してください。

サービス間の混乱した代理の防止

混乱した代理問題とは、アクションを実行する許可を持たないエンティティが、より高い特権を持つエンティティにそのアクションの実行を強制できるというセキュリティ問題です。AWS では、サービス間でのなりすましによって、混乱した代理問題が発生する場合があります。サービス間でのなりすましは、1 つのサービス (呼び出し元サービス) が、別のサービス (呼び出し対象サービス) を呼び出すときに発生する可能性があります。呼び出し元サービスは、本来ならアクセスすることが許可されるべきではない方法でその許可を使用して、別のお客様のリソースに対する処理を実行するように操作される場合があります。これを防ぐため、AWS では、アカウント内のリソースへのアクセスが付与されたサービスプリンシパルですべてのサービスのデータを保護するために役立つツールを提供しています。

リソースポリシーで `aws:SourceArn` および `aws:SourceAccount` のグローバル条件コンテキストキーを使用して、AWS Backup が別のサービスに付与する許可をそのリソースに制限することをお勧めします。両方のグローバル条件コンテキストキーを使用しており、それらが同じポリシーステートメントで使用されるときは、`aws:SourceAccount` 値と、`aws:SourceArn` 値のアカウントが同じアカウント ID を使用する必要があります。

AWS Backup を使って、代わりに Amazon SNS トピックを公開する場合、`aws:SourceArn` の値は AWS Backup 保管庫である必要があります。

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

のインフラストラクチャセキュリティ AWS Backup

マネージドサービスである AWS Backup は、 AWS グローバルネットワークセキュリティで保護されています。 AWS セキュリティサービスと がインフラストラクチャ AWS を保護する方法の詳細については、AWS 「 クラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには、「 Security Pillar AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

が AWS 公開している API コールを使用して、ネットワーク AWS Backup 経由で にアクセスします。クライアントは、Transport Layer Security (TLS) 1.2 以降をサポートする必要があります。また、Ephemeral Diffie-Hellman (DHE) や Elliptic Curve Ephemeral Diffie-Hellman (ECDHE) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートもサポートしている必要があります。これらのモードは、Java 7 以降など、ほとんどの最新システムでサポートされています。

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。

におけるデータの整合性 AWS Backup

AWS Backup データ整合性の目標

AWS Backup は、データの送信、保存、処理中に整合性を維持しようとします。 は、保存されたリソースデータをコンテンツに依存しない重要な情報として AWS Backup 扱います。保存されるデータの種類に関係なく、お客様に同じ高レベルのセキュリティを提供します。当社はお客様のセキュリティに注意を払い、不正アクセスに対して高度な技術的および物理的対策を講じています。データの分類方法、データを保存するリージョン、データを管理する方法、アーカイブする方法、開示から保護する方法については、お客様が完全に管理できます。

AWS Backup データ整合性の実装

AWS Backup は、他の AWS および Amazon のサービスと連携して、保存およびやり取りするデータの整合性を維持します。使用するツールはさまざまで、次のようなものがあります (ただしこれらに限定されません)。

- オブジェクトの破損を防ぐため、チェックサムと照合してオブジェクトを継続的に検証するもの

- 転送中および保管時のデータの整合性を確認するための内部チェックサム
- プライマリストアから作成されたバックアップ内のデータに基づいて計算されるチェックサム
- ディスクが破損したり、デバイス障害が検出されたりした場合に、オブジェクトストレージの冗長性を通常のレベルに自動的に復元しようとする試行
- 物理的に複数の場所にわたるデータの冗長ストレージ
- 初回書き込み時の複数のアベイラビリティーゾーンにわたるオブジェクトの耐久性の向上と、デバイスが利用不能になった場合やビットロートが検出された場合のさらなるレプリケーションとの組み合わせ
- すべてのネットワークトラフィックをチェックサムしたえうでの、データを保存または取得する際のデータパケットの破損の検出

AWS Backup Backup ゲートウェイを介して接続された VMware で実行されている Amazon DynamoDB、Amazon EFS、Amazon S3、Amazon Timestream、仮想マシンのデータをネイティブに保存します。 AWS Backup は、Amazon Aurora、Amazon DocumentDB、Amazon DynamoDB、Amazon EBS、Amazon EC2、Amazon FSx for Windows File Server、Amazon FSx for Lustre、Amazon FSx for OpenZFS、Amazon RDS、Amazon Redshift など、他の のサービスに保存されているデータのバックアップを容易にします。 FSx NetApp Amazon Neptune

AWS Backup データ整合性の客観的確認と監査

によって直接保存されるデータと AWS Backup 、 が AWS Backup やり取りする他の AWS のサービスと連携して保存されるデータは、このデータの整合性を支える Amazon Simple Storage Service (Amazon S3) の厳格なプロセスの対象となります。この整合性は、「AWS Management Console」の「AWS Artifact」から入手できる年次 SOC 監査報告書を通じて、独立した第三者監査人によって確認されています。

リーガルホールドおよび AWS Backup

リーガルホールドは、ホールド中にバックアップが削除されないようにする管理ツールです。ホールドが実施されている間、ホールド状態にあるバックアップは削除できず、バックアップステータスを変更することになるライフサイクルポリシー (`Deleted` 状態への移行など) は、リーガルホールドが削除されるまで延期されます。1 つのバックアップについて、リーガルホールドが複数ある場合があります。

リーガルホールドは、ライフサイクルで許可されている AWS Backup 場合に、 によって作成された 1 つ以上のバックアップ (復旧ポイントとも呼ばれます) に適用できます。継続的バックアップと呼

ばれるタイプのバックアップの最大ライフサイクルは 35 日です。リーガルホールドでは、継続的なバックアップライフサイクルは延長されません。

リーガルホールドを作成すると、リソースタイプやリソース ID などの特定のフィルター条件を考慮に入れることができます。さらに、リーガルホールドに含めるバックアップの作成日の範囲を定義できます。リーガルホールドとバックアップには多対多の関係があります。つまり、1 つのバックアップには複数のリーガルホールドを設定でき、1 つのリーガルホールドには複数のバックアップを含めることができます。各アカウントで一度に最大 50 個のリーガルホールドを有効化できます。

リーガルホールドは、そのリーガルホールドがある元のバックアップにのみ適用されます。バックアップがリージョン間またはアカウント間でコピーされた場合 (リソースがそれをサポートしている場合)、そのバックアップは保持されず、そのリーガルホールドも移行されません。他のリソースと同様に、リーガルホールドは、一意の Amazon リソースネーム (ARN) が関連付けられています。リーガルホールドの一部に AWS Backup できるのは、 によって作成された復旧ポイントのみです。

AWS Backup ボールトロックが、ボールトに対する追加の保護とイミュータビリティを提供するのに対して、リーガルホールドは個々のバックアップ (復旧ポイント) の削除に対する保護を強化することに注意してください。リーガルホールドは失効せず、バックアップ内のデータは無期限に保持されます。ホールドは、十分なアクセス許可を持つユーザーによってリリースされるまでアクティブのままです。

リーガルホールドの作成

リーガルホールドが作成されると、そのリーガルホールドには作成済みの復旧ポイントのみが含まれます。ステータスが EXPIRED または DELETING のバックアップ (復旧ポイント) はリーガルホールドに含まれません。ステータスが CREATING の復旧ポイント (バックアップ) は、完了時期によってはリーガルホールドに含まれない場合があります。

リーガルホールドは、必要な IAM アクセス許可を持つユーザーが追加できます。

コンソールを使用してリーガルホールドを作成する

リーガルホールドを作成するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. コンソールの左側にあるダッシュボードで、[マイアカウント] を探します。リーガルホールドを選択します。
3. リーガルホールドの追加 を選択します。

4. リーガルホールドの詳細 、リーガルホールドスコープ 、リーガルホールドタグ の 3 つのパネルが表示されます。

   a. [リーガルホールドの詳細] で、表示されるテキストボックスにリーガルホールドのタイトルとリーガルホールドの説明を入力します。

   b. [リーガルホールドの範囲] パネルで、ホールドに含めるリソースの選択方法を選択します。ホールドを作成するときは、リーガルホールド内のリソースを選択するために使用される方法を選択します。次のいずれかを含める選択ができます。

      - 特定のリソースタイプと IDs
      - バックアップボールトの選択
      - アカウント内のすべてのリソースタイプまたはすべてのバックアップボールト

   c. リーガルホールドの日付範囲を指定します。日付を YYYY:MM:DD の形式で入力します (日付も含まれます)。

   d. オプションで、リーガルホールドタグ の下にホールドのタグを追加できます。タグは、将来的な参照や整理のためにホールドを分類するのに役立ちます。最大 50 個のタグを追加できます。

5. 新しいリーガルホールドの設定を確認したら、[新規ホールドを追加] ボタンをクリックします。

を使用してリーガルホールドを作成する AWS CLI

create-legal-hold コマンドを使用してリーガルホールドを作成できます。

```
aws backup create-legal-hold --title "my title" \
    --description "my description" \
    --recovery-point-selection
 "VaultNames=string,DateRange={FromDate=timestamp,ToDate=timestamp}"
```

リーガルホールドを表示する

リーガルホールドの詳細は、 AWS Backup コンソールまたはプログラムで確認できます。

コンソールを使用してリーガルホールドを表示する

バックアップコンソールを使用してアカウント内のすべてのリーガルホールドを表示するには、

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ダッシュボードの左側にある [マイアカウント] で [リーガルホールド] をクリックします。

3. [リーガルホールド] テーブルには、既存のホールドのタイトル、ステータス、説明、ID、作成日が表示されます。テーブルヘッダーの横にあるカラット (下矢印)をクリックすると、テーブルが、選択した列別でフィルターされます。

リーガルホールドをプログラムで表示する

すべてのリーガルホールドをプログラムで表示するには、 ListLegalHoldsおよび の API コールを使用できますGetLegalHold。

次の JSON テンプレートを に使用できますGetLegalHold。

```
GET /legal-holds/{legalHoldId} HTTP/1.1

Request

empty body

Response

{
    Title: string,
    Status: LegalHoldStatus,
    Description: string, // 280 chars max
    CancelDescription: string, // this is provided during cancel // 280 chars max
    LegalHoldId: string,
    LegalHoldArn: string,
    CreatedTime: number,
    CanceledTime: number,

   ResourceSelection: {
        VaultArns: [ string ]
        Resources: [ string ]
   },
   ResourceFilters: {
        DateRange: {
          FromDate: number,
          ToDate: number
        }
   }
}
```

次の JSON テンプレートを に使用できますListLegalHolds。

```
GET /legal-holds/
  &maxResults=MaxResults
  &nextToken=NextToken


Request

empty body
url params:
  MaxResults: number  // optional,
  NextToken: string  // optional

status: Valid values: CREATING | ACTIVE | CANCELED | CANCELING
maxResults: 1-1000



Response

{
  NextToken: token,
  LegalHolds: [
    Title: string,
    Status: string,
    Description: string, // 280 chars max
    CancelDescription: string, // this is provided during cancel // 280 chars max
    LegalHoldId: string,
    LegalHoldArn: string,
    CreatedTime: number,
    CanceledTime: number,
  ]

}
```

以下は、可能なステータス値です。

ステータス	説明
CREATING	リクエストされた復旧ポイントはリーガルホールドのプロセスに入っていますが、リーガルホールドの作成がまだ完了していないため、そ

ステータス	説明
	れらの復旧ポイントの削除リクエストが成功する可能性があります。
ACTIVE	リーガルホールドが作成されました。このリーガルホールドに含まれるすべての復旧ポイントが保持されます。
CANCELLING	リーガルホールドは削除中のため、ホールドの対象になっている復旧ポイントの削除リクエストが成功する可能性があります。
CANCELED	リーガルホールドは完全に解除され、無効になっています。復旧ポイントは削除できます。

リーガルホールドを解除する

リーガルホールドは、十分なアクセス許可を持つユーザーによって削除されるまで有効です。リーガルホールドの削除は、リーガルホールドのキャンセル、解除とも呼ばれます。リーガルホールドを削除すると、そのリーガルホールドがアタッチされていたすべてのバックアップからリーガルホールドが削除されます。リーガルホールド中に期限切れになったバックアップは、リーガルホールドが削除されてから 24 時間以内に削除されます。

コンソールを使用してリーガルホールドを解除する

コンソールを使用してホールドを解除するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. 解除に関連付ける説明を入力します。
3. 詳細を確認し、[ホールドを解除] をクリックします。
4. [ホールドを解除] ダイアログボックスが表示されたら、テキストボックスに [confirm] と入力してホールドを解除することを確認します。

    - ホールドを解除することを確認するボックスにチェックを入れます。

[リーガルホールド] ページでは、すべてのホールドを確認できます。解除が成功すると、そのホールドのステータスが Released と表示されます。

プログラムによるリーガルホールドの解除

プログラムで保留を削除するには、 API コール を使用しますCancelLegalHold。

次の JSON テンプレートを使用します。

```
DELETE /legal-holds/{legalHoldId}


Request

{
   CancelDescription: String
   DeleteAfterDays: number // optional
}


DeleteAfterDays: optional.
  Defaults to 180 days. how long to keep legal hold record after canceled.
  This applies to the actual legal hold record only.
  Recovery points are unlocked as soon as cancelation processes and are not subject to
 this date.

Response

Empty body

200 if successful
other standard codes
```

AWS PrivateLink

AWS PrivateLink では、インターフェイス VPC AWS Backup エンドポイントを作成して、仮想プライベートクラウド (VPC) とエンドポイント間のプライベート接続を確立できます。インターフェイスエンドポイントはAWS PrivateLink、VPC と Amazon ネットワーク間のすべてのネットワークトラフィックを制限することで AWS Backup APIs AWS Backup にプライベートにアクセスできるテクノロジーである を利用しています。

AWS PrivateLink を使用すると、インターネットゲートウェイ、NAT デバイス、VPN 接続、または AWS Direct Connect 接続なしで、 AWS Backup オペレーションにプライベートにアクセスできます。VPC 内のインスタンスは、 AWS Backup API エンドポイントとの通信にパブリック IP アドレ

スを必要としません。また、インスタンスは、使用可能な AWS Backup API および Backup ゲートウェイ API オペレーションを使用するためにパブリック IP アドレスを必要としません。VPC と 間のトラフィック AWS Backup は Amazon ネットワークを離れません。

VPC エンドポイントの詳細については、「Amazon VPC ユーザーガイド」の「インターフェイス VPC エンドポイント (AWS PrivateLink)」を参照してください。

Amazon VPC エンドポイントに関する考慮事項

AWS Backup エンドポイントのインターフェイス VPC エンドポイントを設定する前に、「Amazon VPC ユーザーガイド」の「インターフェイスエンドポイントのプロパティと制限」を参照してください。

Amazon Backup リソースの管理に関連するすべての AWS Backup オペレーションは、 を使用して VPC から利用できます AWS PrivateLink。

VPC エンドポイントポリシーは、バックアップエンドポイントでサポートされます。デフォルトでは、エンドポイント経由でバックアップオペレーションへのフルアクセスが許可されます。詳細については、「Amazon VPC ユーザーガイド」の「VPC エンドポイントによるサービスのアクセスコントロール」を参照してください。

AWS Backup VPC エンドポイントの作成

Amazon VPC コンソールまたは (AWS CLI) AWS Backup を使用して、 用の VPC AWS Command Line Interface エンドポイントを作成できます。詳細については、Amazon VPC ユーザーガイドのインターフェイスエンドポイントの作成を参照してください。

サービス名 AWS Backup を使用して 用の VPC エンドポイントを作成しますcom.amazonaws.*region*.backup。

中国 (北京) リージョンョンおよび中国 (寧夏) リージョンでは、サービス名は cn.com.amazonaws.*region*.backup でなければなりません。

バックアップゲートウェイエンドポイントの場合は、com.amazonaws.*region*.backup-gateway を使用してください。

バックアップゲートウェイ用の VPC エンドポイントを作成する場合、セキュリティグループで次の TCP ポートを許可する必要があります。

- TCP 443

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

[プロトコル]	[ポート]	[Direction] (方向)	ソース	デスティネーション	使用方法
TCP	443 (HTTPS)	アウトバウンド	Backup ゲートウェイ	AWS	Backup Gateway から AWS サービスエンドポイントへの通信用

VPC エンドポイントの使用

エンドポイントのプライベート DNS を有効にすると、 などの AWS リージョンのデフォルト DNS 名を使用して、VPC エンドポイント AWS Backup で に API リクエストを実行できますbackup.us-east-1.amazonaws.com。

ただし、中国 (北京) リージョンおよび中国 (寧夏) リージョン では AWS リージョン、backup.cn-northwest-1.amazonaws.com.cnそれぞれ backup.cn-north-1.amazonaws.com.cnと を使用して VPC エンドポイントで API リクエストを行う必要があります。

詳細については、「Amazon VPC ユーザーガイド」の「インターフェイスエンドポイントを介したサービスへのアクセス」を参照してください。

VPCエンドポイントポリシーの作成

VPC エンドポイントに Amazon バックアップ API へのアクセスを制御するエンドポイントポリシーをアタッチできます。このポリシーでは以下の内容を指定します。

- アクションを実行できるプリンシパル。
- 実行可能なアクション。

- このアクションを実行できるリソース。

> **Important**
>
> のインターフェイス VPC エンドポイントにデフォルト以外のポリシーが適用されると AWS Backup、 からの失敗など、失敗した特定の API リクエストが `RequestLimitExceeded` AWS CloudTrail または Amazon に口グ記録されない場合があります CloudWatch。

詳細については、「Amazon VPC ユーザーガイド」の「VPC エンドポイントによるサービスのアクセスコントロール」を参照してください。

例: AWS Backup アクションの VPC エンドポイントポリシー

のエンドポイントポリシーの例を次に示します AWS Backup。このポリシーは、エンドポイントにアタッチされると、すべてのリソースのすべての原則について、リストされた AWS Backup アクションへのアクセスを許可します。

```
{
  "Statement":[
    {
      "Action":"backup:*",
      "Effect":"Allow",
      "Principal":"*",
      "Resource":"*"
    }
  ]
}
```

例: 指定した AWS アカウントからのすべてのアクセスを拒否する VPC エンドポイントポリシー

次の VPC エンドポイントポリシーは、エンドポイントを使用したリソースへの123456789012すべてのアクセスを AWS アカウントで拒否します。このポリシーは、他のアカウントからのすべてのアクションを許可します。

```
{
  "Id":"Policy1645236617225",
  "Version":"2012-10-17",
  "Statement":[
    {
```

```
      "Sid":"Stmt1645236612384",
      "Action":"backup:*",
      "Effect":"Deny",
      "Resource":"*",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      }
    }
  ]
}
```

使用可能な API レスポンスの詳細については、「API ガイド」を参照してください。

可用性 AWS Backup は現在、次の AWS リージョンで VPC エンドポイントをサポートしています。

- 米国東部 (オハイオ) リージョン
- 米国東部(バージニア州北部) リージョン
- 米国西部 (オレゴン) リージョン
- US West (N. California) リージョン
- アフリカ (ケープタウン) リージョン
- アジアパシフィック (香港) リージョン
- アジアパシフィック (ムンバイ) リージョン
- アジアパシフィック (大阪) リージョン
- Asia Pacific (Seoul) Region
- アジアパシフィック (シンガポール) リージョン
- アジアパシフィック (シドニー) リージョン
- アジアパシフィック (東京) リージョン
- カナダ (中部) リージョン
- Europe (Frankfurt) Region
- 欧州 (アイルランド) リージョン
- 欧州 (ロンドン) リージョン
- 欧州 (パリ) リージョン

- 欧州 (ストックホルム) リージョン
- 欧州 (ミラノ) リージョン
- 中東 (バーレーン) リージョン
- 南米 (サンパウロ) リージョン
- アジアパシフィック (ジャカルタ) リージョン
- アジアパシフィック (大阪) リージョン
- 中国 (北京) リージョン
- 中国 (寧夏) リージョン
- AWS GovCloud （ 米国東部 ）
- AWS GovCloud （ 米国西部 ）

> **Note**
>
> AWS Backup for VMware は、中国リージョン (中国 (北京) リージョンおよび中国 (寧夏) リージョン) またはアジアパシフィック (ジャカルタ) リージョンでは使用できません。

の耐障害性 AWS Backup

AWS Backup は、その耐障害性とデータセキュリティを非常に重視しています。

AWS Backup は、リソースの元の AWS サービスがバックアップした場合と同等以上の回復力と耐久性でバックアップを保存します。

AWS Backup は、 AWS グローバルインフラストラクチャを使用して複数のアベイラビリティーゾーンにバックアップをレプリケートするように設計されており、現在の AWS Backup ドキュメントに従っている限り、任意の年に 99.999999999% (11 9) の耐久性を実現します。

AWS Backup は、保管中のバックアッププランを暗号化し、継続的にバックアップします。 AWS Identity and Access Management (IAM) 認証情報とポリシーを使用して、バックアッププランへのアクセスを制限することもできます。詳細については、「認証」「アクセスコントロール」、および「IAM のセキュリティベストプラクティス」を参照してください。

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。 は、低レイテンシー、高スループット、および高度に冗長なネットワークで接続された、物理的に分離された複数のアベイラビリティーゾーン AWS リージョン を提供しま

す。 は、アベイラビリティーゾーン間でバックアップ AWS Backup を保存します。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、耐障害性、およびスケーラビリティが優れています。詳細については、「AWS Backup サービスレベルアグリーメント (SLA)」を参照してください。

さらに、 AWS Backup を使用すると、リージョン間でバックアップをコピーして、耐障害性をさらに高めることができます。 AWS Backup クロスリージョンコピー機能の詳細については、「バックアップコピーの作成」を参照してください。

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。

AWS Backup クォータ

を使用する場合、次のクォータが適用されます AWS Backup。リソースタイプサービスで許可されている場合は、多くの AWS Backup クォータを調整できます。クォータ調整をリクエストするには、ユースケースを「AWS Support」に説明します。

AWS Backup クォータ

リソース	クォータ	メモ
アカウントあたり、リージョンあたりのバックアップボールトの数	300	調整をリクエストできます。
バックアップボールトあたりの復旧ポイント数	1,000,000	調整をリクエストできます。
アカウントあたり、リージョンあたりのバックアッププランの数	300	調整をリクエストできます。
バックアッププランあたりのバージョン数	2,000	調整をリクエストできます。
バックアッププランあたりのリソース割り当て数	100	調節できません。
アカウントあたりのアクティブなバックアップジョブ数	無制限	
送信先リージョンへの、アカウントあたりの同時バックアップコピー数	100	特定のリソース (Amazon EC2 インスタンス上の仮想マシン、Advanced DynamoDB、Timestream、Amazon EFS、SAP HANA データベース) の調整をリクエストできます。

リソース	クォータ	メモ
上限 (上記エントリ) に達した後の、アカウント内の送信先バックアップボールトごとの同時コピー数	5	調節できません。
同じリソースを同じ送信先リージョンに同時に作成できるクロスアカウントコピーの数	30	調節できません。
リソースあたりの同時バックアップおよびコピーのジョブ数	1	調節できません。このクォータは、ワークロードのパフォーマンスを維持するのに役立ちます。
バックアップあたりのメタデータタグ数	50	調整をリクエストすることはできません。 は、すべてのリソースにこのクォータ AWS を適用します。「AWS ジェネラルリファレンス」の「タグ名の制限と要件」を参照してください。
クロスアカウントバックアップポリシーでのリソース選択あたりのタグ数	30	調節できません。複数のリソース割り当てまたはバックアッププランを利用することで、追加のタグを含めることができます。
ハイパーバイザー数	10	調節できません。
リーガルホールドの数	アカウントあたり 50	調節できません。
アプリケーションスタックのネストされたバックアップレイヤーの最大数	10	調節できません。

AWS Backup Amazon Timestream リソースクォータの

リソース	クォータ	メモ
アカウントあたりの同時 Timestream バックアップジョブ数	4	調整をリクエストできます。
アカウントあたりの同時 Timestream 復元ジョブ数	1	調整をリクエストできます。

1 つのバックアップルールでは、単一リソース割り当てに対するクォータが設定されます。複数のバックアップルールでバックアッププランを作成できます。

AWS Backup Audit Manager のクォータ

リソース	クォータ	メモ
リージョンあたり、アカウントあたりのフレームワーク数	15	調整をリクエストできます。
リージョンあたり、アカウントあたりのコントロール数	50	調整をリクエストできます。
アカウントあたりのレポートプラン数	20	調整をリクエストできます。
レポートプランあたりのフレームワーク数	1,000	調節できません。
最大アカウント数に、レポートプランのリージョンを掛けた値	300	調節できません。

復元テストプランのクォータ

リソース	クォータ	メモ
復元テストプラン	100	調節できません。

リソース	クォータ	メモ
プランあたりのタグの数	50	調節できません。
プランあたりの選択の数	30	調節できません。
復元テスト選択あたりの ARN	30	調節できません。
選択あたりの条件の数	30	`StringEquals` と `StringNotEquals` に含まれるもの両方。
復元テスト選択あたりのボールト選択項目	30	調節できません。
選択期間の最大値 (日)	365 日間	
開始期間の時間範囲	最小: 1 時間、最大: 168 時間	
復元テストプラン名の最大文字長	50 文字	英数字とアンダースコア、スペースなし
復元テスト選択名の最大文字長	50 文字	英数字とアンダースコア、スペースなし

AWS Backup gateway クォータ

リソース	クォータ	メモ
ゲートウェイごとのバックアップジョブまたは復元ジョブ	4	調整をリクエストできません。代わりに、ゲートウェイをさらに作成してハイパーバイザーに接続してください。

を使用して複数のアカウント間でバックアップを管理すると AWS Organizations、 が AWS Organizations 課すクォータが発生する可能性があります。これらのクォータについては、AWS Organizations ユーザーガイドの「AWS Organizationsのクォータ」を参照してください。

また、 AWS Backupがサポートするサービスによって次のようなクォータが発生することもあります。

- Amazon Elastic File System
- Amazon Elastic Block Store
- Amazon RDS
- Amazon Aurora
- Amazon EC2
- AWS Storage Gateway
- Amazon DynamoDB
- Amazon FSx for Lustre
- Amazon FSx for Windows File Server
- Amazon DocumentDB
- Amazon Neptune
- Amazon Simple Storage Service
- Amazon Timestream

モニタリング

AWS Backup は他の AWS ツールと連携して、ワークロードをモニタリングできるようにします。これらのツールには次のものが含まれます。

- AWS Backup コンソールダッシュボード
  - ジョブダッシュボードにはジョブの状態をモニタリングする機能があり、ジョブの成功と失敗を示すメトリクスを、理由、アカウント、リージョン、リソースタイプでフィルタリングして表示できます。
  - ジョブダッシュボードは、 AWS Backup Audit Manager がサポートされているリージョンで使用できます。該当するリージョンについては「による機能の可用性 AWS リージョン」を参照してください。他のすべてのリージョンは、CloudWatch ダッシュボードにアクセスできます。
- AWS Backup プロセスをモニタリングする Amazon CloudWatch と Amazon EventBridge。
  - を使用して CloudWatch 、メトリクスの追跡、アラームの作成、ダッシュボードの表示を行うことができます。
  - を使用して EventBridge 、 AWS Backup イベントを表示およびモニタリングできます。

  詳細については、「Amazon を使用した AWS Backup イベントのモニタリング EventBridge」を参照してください。
- AWS CloudTrail AWS Backup API コールをモニタリングする 。これらのコールを行う時間、送信元 IP、ユーザー、およびアカウントを特定できます。詳細については、「を使用した AWS Backup API コールのログ記録 CloudTrail」を参照してください。
- Amazon Simple Notification Service (Amazon SNS) は、バックアップ、復元、コピーイベントなどの AWS Backup関連のトピックをサブスクライブします。詳細については、「の通知オプション AWS Backup」を参照してください。

AWS Backup コンソールダッシュボード

> **Note**
>
> ジョブダッシュボードは、 AWS Backup Audit Manager がサポートされているすべてのリージョンで使用できます。該当するリージョンについては「による機能の可用性 AWS リージョン」を参照してください。他のすべてのリージョンは、CloudWatch ダッシュボードにアクセスできます。

トピック

Backup ダッシュボードの概要

AWS Backup は、バックアップ、コピー、復元ジョブの状態をモニタリングするのに役立つジョブダッシュボードを コンソールに提供します。コンソールに視覚的に表示されるのと同じデータは、を介してコマンドラインで取得できます AWS CLI。

ジョブダッシュボードを使用すると、組織レベルまたはメンバーアカウントによるモニタリングを通じて、バックアップ、コピー、復元の各ジョブに関する問題を特定できます。この情報により、イベントや起こり得る問題を特定して診断できるため、アクティビティの信頼性を確保できます。

ジョブダッシュボードには 2 つの時間枠を表示できます。デフォルトでは過去 14 日間のデータが表示されますが、表示を変更して過去 7 日間のデータを表示することもできます。時間枠を変更すると、データが更新されて新しい時間間隔が反映されます。

ダッシュボードには直近の 0:00 UTC までのデータが表示されることに注意してください。つまり、当日のデータは含まれません。ダッシュボードは毎日、UTC の 1:30 ~ 2:30 頃に更新されます。

ダッシュボードの表示

ジョブダッシュボードを表示するには、AWS Backup コンソールにログインし、左側のナビゲーションバーでジョブダッシュボードを選択します。

ジョブダッシュボードページで、バックアップ、コピー、または復元ジョブのタブから選択できます。

ジョブダッシュボードの概要には、完了したジョブ、完了したが問題があるジョブ、期限切れのジョブ、失敗したジョブなど、指定された期間におけるジョブアクティビティの集計ビューが表示されます。デフォルトでは過去 14 日間のデータが表示されますが、7 日間のデータを表示するように変更することもできます。

> **Note**
>
> [Completed with issues] はコンソールに表示されるジョブのステータスの 1 つで、ステータスメッセージ付きで完了したジョブを表します。

ジョブの状態

折れ線グラフに、ジョブの成功率と失敗率の線が時系列で表示されます。成功率の線には、完了したジョブと完了したが問題があるジョブの合計が表示されます。失敗率の線には、指定した時間範囲における失敗したジョブと期限切れのジョブの合計が表示されます。

未完了または失敗していない状態のジョブ ([作成済み]、[保留中]、[実行中]、[中止しました]、[中止しています]、または [部分的] のステータスのジョブ) は含まれず、パーセンテージの合計は 100% にならない場合があります。

時間の経過に伴うジョブステータス

棒グラフを使用して、各カテゴリ ([完了済み]、[完了しましたが、問題が発生しました]、[失敗]、[期限切れ]) のジョブ数を日別に示すカスタム棒グラフを生成できます。

ドロップダウンメニューで、グラフに表示するステータス (複数可) 、リソースタイプ、 AWS リージョンを選択します。選択内容をさらに詳しく調べる場合は、[ジョブを表示] を選択すると、ジョブ/クロスアカウントモニタリングページのフィルタリング済みの部分が表示されます。

バーの上にマウスを移動すると、選択した日付の詳細なジョブデータを示すポップオーバーが表示されます。

問題のあるジョブ

問題のあるジョブとは、ステータスが、[失敗]、[期限切れ]、または [完了しましたが、問題が発生しました] のジョブです。各グラフには、問題のあるジョブの数が最も多いアカウント、リソースタイプ、または上位の理由のいずれかを含む、対応するメトリクスが表示されます。

デフォルト表示では、ダッシュボードウィジェットが指定されたメトリクスで降順にソートされ、問題のあるジョブが最も多く属するメトリクスから順に表示されます。

問題のある上位アカウントの表示は、管理者アカウントや委任された管理者アカウントなど、Organizations を通じてアクセスできるアカウントでのみ表示されます。表示されている場合

は、アカウントにカーソルを合わせると、選択したアカウントに属する問題のあるジョブの数が表示されます。

グラフ内のバーを選択すると、ポップアップウィンドウが開きます。このウィンドウでは、ジョブステータスを選択し、選択したステータスでフィルタリングされたジョブ/クロスアカウントモニタリングテーブルを開くことができます。

問題のあるジョブの理由

問題の上位の理由を示すウィジェットには、エラーメッセージが属するメッセージコードカテゴリが表示されます。ただし、カテゴリだけではジョブで発生する問題が把握できない場合があります。以下のメッセージコードカテゴリを展開すると、ジョブで発生する可能性のある特定のメッセージやエラーに関する詳細が表示されます。

「VSS_ERROR」

- 「インスタンスまたは SSM エージェントの状態が無効であるか、アクセス許可が不十分であるため、Windows VSS バックアップの試行に失敗しました」
- 「この操作を実行するためのアクセス許可が不十分であるため、Windows VSS バックアップの試行に失敗しました」
- 「ec2-vss-agent.exe がインスタンスにインストールされていないため、Windows VSS バックアップの試行に失敗しました」
- 「Windows VSS バックアップジョブエラーが発生しました。通常のバックアップを試みています」
- 「VSS 対応スナップショットの作成のタイムアウトにより、Windows VSS バックアップの試行に失敗しました」
- 「Windows Server のバージョンがサポートされていないため、Windows VSS バックアップの試行に失敗しました。サポートされているバージョンは Windows Server 2012 以降です」
- 「VSS 対応スナップショットの作成のタイムアウトにより、Windows VSS バックアップの試行に失敗しました」

「LIMIT_EXCEEDED」

- 「サブスクライバーの制限を超えました。同時バックアップの最大数である 300 に達しました。別のジョブが終了してからもう一度試してください。また、 AWS Support に連絡してクォータの引き上げをリクエストすることもできます。」
- 「1 つのボリュームで許可される進行中のスナップショットの最大数を超えました」

- 「アクティブスナップショットの最大許容上限を超えました」
- 「20 を超えるユーザースナップショットは作成できません」
- 「作成されるタグセットのユーザータグは 50 以下でなければなりません」
- 「アカウント/データベースでサポートされるバックアップの最大数に達しました。詳細については、『Timestream デベロッパーガイド』の『クォータ』を参照してください」
- 「パブリックイメージとプライベートイメージの数がこのリージョンで許可されているクォータである 50,000 に達しました。未使用のイメージの登録を解除するか、AMI クォータの引き上げをリクエストできます」
- 「バックアップは成功しましたが、サイズが内部制限を超えたため NetworkInterfaces 、メタデータを保持できませんでした」
- 「REGEX#サブスクライバーの制限を超過しました」
- 「REGEX#50 を超えるタグが指定されました」
- 「REGEX#許容される最大数」

「ACCESS_DENIED」

- 「この操作を実行する権限がありません」
- AWS Backup 「サービスの呼び出しを拒否されました」
- 「 からのイメージを別の AWS アカウントにコピー AWS Marketplace することはできません」
- 「送信先のバックアップボールトがデフォルトのバックアップサービス管理キーで暗号化されているため、コピージョブに失敗しました。このボールトの内容はコピーできません。 AWS KMS キーで暗号化された Backup ボールトの内容のみをコピーできます。
- で暗号化されたスナップショットは共有 AWS マネージドキー できません。別のスナップショットを指定してください。
- 「Amazon EBS デフォルトキーで暗号化されたスナップショットは共有できません」
- 「コピージョブに失敗しました。送信元と送信先のアカウントは同じ組織のメンバーでなければなりません」
- 「REGEX#アクセスが拒否されました」
- 「REGEX#権限がありません」
- 「REGEX# は で引き受けることができません AWS Backup
- 「REGEX#アクセス許可がありません」
- 「REGEX#アクセス許可が見つかりません」

「CONCURRENT_JOB」

- 「同じリソースで実行中のジョブがあったため、バックアップジョブに失敗しました」

「FEATURE_NOT_ENABLED」

- 「コピージョブに失敗しました。現在の組織ではクロスアカウントコピー機能が有効になっていません」

「JOB_EXPIRED」

- 「バックアップジョブは完了前に期限切れになりました」

「INVALID_LIFECYCLE」

- 「コピージョブに失敗しました。ジョブで指定された保持期間は、ターゲットのバックアップボールトに指定された範囲内にありません」
- 「REGEX#設定されている週ごとのメンテナンス期間と重なっているか、またはそれに近すぎるため、開始できませんでした」
- 「REGEX#設定されている自動バックアップ期間と重なっているか、またはそれに近すぎるため、開始できませんでした」

「INVALID_STATE」

- 「REGEX#インスタンスの状態が異なります」
- 「REGEX#使用可能な状態ではありません」
- 「REGEX#使用可能な状態ではありません」
- 「REGEX#ボリュームのスナップショットを作成できません」

「KMS_KEY_ERROR」

- 「KMS キーが無効になっているか、削除が保留されているか、KMS キーへのアクセスが拒否されています」
- 「指定されたキー ID にはアクセスできません」

- 「AMI スナップショットのコピーがエラーにより失敗しました。指定されたキー ID にアクセスできません。デフォルトの CMK に対する DescribeKey アクセス許可が必要です」
- 「REGEX#kms キー」

「ACCESS_KEY_ERROR」

- 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」

「HYPERVISOR_OFFLINE」

- 「指定されたハイパーバイザーはオンラインではないため、この操作は無効です」

「RESOURCE_NOT_FOUND」

- 「指定されたボリュームは、見つかりませんでした」
- 「仮想マシンが見つかりません」
- 「指定された ID は存在しません」
- 「REGEX#存在しません」
- 「REGEX#リソースが見つかりませんでした」
- 「REGEX#クライオポッドが見つかりませんでした」
- 「REGEX#復旧ポイントが見つかりませんでした」
- 「REGEX#リソースが見つかりません」
- 「REGEX#現在利用できません」
- 「REGEX#無効です」

「RESOURCE_NOT_SUPPORTED」

- 「REGEX#サポートされていないリソースタイプ」
- 「REGEX#サポートされていないリソースタイプです」

「TAG_COPY_ERROR」

- 「内部障害が発生したため、リソースタグをバックアップにコピーできません」

- 「送信元または送信先の復旧ポイントが使用できないため、リソースタグをバックアップにコピーできません」

「TOKEN_EXPIRED」

- 「トークンの期限が切れています。もう一度試してください」

「UNSUPPORTED_OPERATION」

- 「スナップショット作成中のハイパーバイザーではCreateSnapshot メソッドはサポートされていません。バックアップジョブを中止しました」
- UnsupportedOperation 「: Storage Gateway のバックアップコピーには、ユーザーが作成したバックアップボールトと CMK がコピー先で必要です」
- 「REGEX#この機能は指定されたリソースタイプではサポートされていません」

「FATAL_ERROR」

- 「内部エラーが発生しました」
- 「コピージョブに致命的なエラーが発生しました。詳細については AWS 、 サポートにお問い合わせください。」
- 「コピージョブに致命的なエラーが発生しました」
- 「REGEX#バックアップジョブに致命的なエラーが発生しました」

によるダッシュボードデータの取得 AWS CLI

コマンドラインを使用して、コンソールに表示されるものと同じデータを取得できます。以下のいずれかの CLI コマンドを使用します。

- list-backup-job-summaries
- list-copy-job-summaries
- list-restore-job-summaries

各コマンドには、以下の有効なパラメータを含めることができます。

```
BackupJobSummaries (list)
```

```
    Region (string),
    Account (string),
    State (string),
    ResourceType (string),
    MessageCategory (string),
AggregationPeriod: (string),
NextToken (string),
MaxResults (number)

CopyJobSummaries (list)
    Region (string),
    Account (string),
    State (string),
    ResourceType (string),
    MessageCategory (string),
AggregationPeriod: (string),
NextToken (string),
MaxResults (number)

RestoreJobSummaries (list)
    Region (string),
    Account (string),
    State (string),
    ResourceType (string),
AggregationPeriod: (string),
NextToken (string)
```

次の例は、ユーザーが list-backup-job-summaries を入力したリクエストのサンプルです。過去 14 日間に渡り FAILED の状態の使用可能なアカウントをすべて返すように求めています。

```
GET /audit/backup-job-summaries/
    ?accountId=ANY
    &state=FAILED
    &aggregationPeriod=FOURTEEN_DAYS
```

ステータスが completed with issues のジョブの数を取得するには、COMPLETED の合計数から MessageCategory が SUCCESS の COMPLETED ジョブの数を引きます。

Amazon を使用した AWS Backup イベントのモニタリング EventBridge

AWS Backup は、バックアップジョブまたはコピージョブの状態が変更された EventBridge ときにイベントを Amazon に送信します。を使用して AWS Backup イベント EventBridge をモニタリングできます。例えば、バックアップジョブが失敗したときにアラームを受け取ることができます。は、5 分ごとにベストエフォート方式 EventBridge で にイベント AWS Backup を発行します。

を使用してイベントを追跡するには EventBridge、以下を参照してください。

- イベントに反応するルールの作成 (Amazon EventBridge ユーザーガイド)
- の Amazon CloudWatch イベントとメトリクス AWS Backup (ブログ -「Amazon に送信する AWS Backup イベントの設定 EventBridge」を参照)

一部のイベントが `status: COMPLETED` と報告しているのに対し、他のイベントは `state: COMPLETED` と報告しています。これは AWS Backup API と一致しています。一部のステータスは AWS Backup コンソールに固有です。ステータス`Completed with issues`ステータスは、ステータスメッセージを含む`Completed`ジョブを表します。`Completed with issues` イベントをモニタリングするには、ステータスメッセージを含む `COMPLETED` ジョブをモニタリングします。

別の方法として、 AWS Backup 通知 API を使用して Amazon Simple Notification Service (Amazon SNS) で AWS Backup イベントを追跡することもできます。ただし、 は、バックアップボールト、コピージョブの状態、リージョン設定、コールドリカバリポイントまたはウォームリカバリポイント数の変更など、通知 API よりも多くの変更 EventBridge を追跡します。

イベント

- バックアップジョブイベント
- Backup プランイベント
- Backup Vault イベント
- ジョブイベントのコピー
- 復旧ポイントイベント
- リージョン設定イベント
- 復元ジョブイベント

バックアップジョブイベント

イベントの例を次に示します。

状態

- 状態: FAILED
- 状態: 完了
- 状態: 実行中
- 状態: 中止
- 状態: 期限切れ
- 状態: 保留中
- 状態: 作成済み

状態: FAILED


```
{
  "version": "0",
  "id": "710b0398-d48e-f3c3-afca-cfeb2fdaa656",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T20:15:26Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "34176239-e96d-4e1d-9fad-529dbb3c3556",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:9ab3e749-82c6-4342-9320-5edbf4918b86",
    "backupVaultName": "9ab3e749-82c6-4342-9320-5edbf4918b86",
    "bytesTransferred": "0",
    "creationDate": "2020-07-29T20:13:07.392Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
    "state": "FAILED",
    "statusMessage": "\"Backup job failed because backup vault arn:aws:backup:us-
west-2:1112233445566:backup-vault:9ab3e749-82c6-4342-9320-5edbf4918b86 does not exist.
\"",
    "startBy": "2020-07-30T04:13:07.392Z",
```

```
    "percentDone": 0,
    "retryCount": 3
  }
}
```

状態: 完了

```
{
  "version": "0",
  "id": "dafac799-9b88-0134-26b7-fef4d54a134f",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T21:41:17Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:f1d966fe-a3bd-410b-
b292-99f442d13b56"
  ],
  "detail": {
    "backupJobId": "a827233a-d405-4a86-a440-759fa94f34dd",
    "backupSizeInBytes": "36048",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:9732c1b4-1091-472a-9d9f-52e0565ee39a",
    "backupVaultName": "9732c1b4-1091-472a-9d9f-52e0565ee39a",
    "bytesTransferred": "36048",
    "creationDate": "2020-07-15T21:40:31.207Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
    "state": "COMPLETED",
    "completionDate": "2020-07-15T21:41:05.921Z",
    "startBy": "2020-07-16T05:40:31.207Z",
    "percentDone": 100,
    "retryCount": 3
  }
}
```

状態: 実行中

```
{
  "version": "0",
```

```
  "id": "44946c39-b519-3505-44e6-ba74afeb2e30",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T21:39:13Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "B6EC38D2-CB3C-EF0A-F5A4-3CF324EF4945",
    "backupSizeInBytes": "3221225472",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:e6625738-0655-4aa9-bd37-6ec1dd183b15",
    "backupVaultName": "e6625738-0655-4aa9-bd37-6ec1dd183b15",
    "bytesTransferred": "0",
    "creationDate": "2020-07-15T21:38:31.152Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/FullBackupTestRole",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/vol-0b5ae24f2ee72d926",
    "resourceType": "EBS",
    "state": "RUNNING",
    "startBy": "2020-07-16T05:00:00Z",
    "expectedCompletionDate": "Jul 15, 2020 9:39:07 PM",
    "percentDone": 99,
    "createdBy": {
      "backupPlanId": "bde0f455-4e24-4668-aeaa-4932a97f5cc5",
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:bde0f455-4e24-4668-aeaa-4932a97f5cc5",
      "backupPlanVersion": "YTkzNmM0MmUtMWRhNS00Y2RkLThmZGUtNjA5NTc4NGM1YTc5",
      "backupPlanRuleId": "1f97bafa-14d6-4f39-94fd-94b51bd6d0d5"
    }
  }
}
```

状態: 中止

```
{
  "version": "0",
  "id": "4c91ceb0-b798-da82-6818-c29b3dce7543",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T21:33:16Z",
  "region": "us-west-2",
  "resources": [],
```

```
  "detail": {
    "backupJobId": "58cdef95-7680-4c74-80d5-1b64093999c8",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:f59bffcd-2538-4bbe-8343-1c60dae27c27",
    "backupVaultName": "f59bffcd-2538-4bbe-8343-1c60dae27c27",
    "bytesTransferred": "0",
    "creationDate": "2020-07-15T21:33:00.803Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
    "state": "ABORTED",
    "statusMessage": "\"Backup job was stopped by user.\"",
    "completionDate": "2020-07-15T21:33:01.621Z",
    "startBy": "2020-07-16T05:33:00.803Z",
    "percentDone": 0
  }
}
```

状態: 期限切れ

```
{
  "version": "0",
  "id": "1d7bbc04-6120-1145-13b9-49b0af465328",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T13:04:57Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "01EE26DC-7107-4D8E-0C54-EAC27C662BA4",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:aws/backup/
AutomatedBackupVaultDel2",
    "backupVaultName": "aws/backup/AutomatedBackupVaultDel2",
    "bytesTransferred": "0",
    "creationDate": "2020-07-29T05:10:20.077Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
    "state": "EXPIRED",
    "statusMessage": "\"Backup job failed because there was a running job for the same
 resource.\"",
    "completionDate": "2020-07-29T13:02:15.234Z",
```

```
    "startBy": "2020-07-29T13:00:00Z",
    "percentDone": 0,
    "createdBy": {
      "backupPlanId": "aws/efs/414a5bd4-f880-47ad-95f3-f085108a4c3b",
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-plan:aws/
efs/414a5bd4-f880-47ad-95f3-f085108a4c3b",
      "backupPlanVersion": "NjBjOTUzZjYtYzZiNi00NjhlLWIzMTEtNWRjOWY0YTNjN2Vj",
      "backupPlanRuleId": "3eb0017c-f262-4211-a802-302cebb11dc2"
    }
  }
}
```

状態: 保留中

```
{
  "version": "0",
  "id": "64dd1897-f863-31a3-9ee5-b05e306d81ff",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T20:03:30Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "2cffdb68-d6ed-485f-9f9b-8b530749f1c2",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:ed1f2661-5587-48bf-8a98-fadb977bf975",
    "backupVaultName": "ed1f2661-5587-48bf-8a98-fadb977bf975",
    "bytesTransferred": "0",
    "creationDate": "2020-07-29T20:01:06.224Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
    "state": "PENDING",
    "statusMessage": "",
    "startBy": "2020-07-30T04:01:06.224Z",
    "percentDone": 0
  }
}
```

状態: 作成済み

```
{
```

```
  "version": "0",
  "id": "29af2bf2-eace-58ab-da3a-8c0bf738d692",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-22T20:32:53Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "7e8845b5-ca30-415f-a842-e0152bf4d0ca",
    "state": "CREATED",
    "creationDate": "2020-06-22T20:32:47.466Z"
  }
}
```

Backup プランイベント

イベントの例を次に示します。

状態

- 状態: 変更済み
- 状態: 削除済み
- 状態: 作成済み

状態: 変更済み

```
{
  "version": "0",
  "id": "2895aefb-dd4a-0a23-6071-2652abd92c3f",
  "detail-type": "Backup Plan State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:25Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-plan:83fcb8ee-2d93-42ac-
b06f-591563f3f8de"
  ],
  "detail": {
    "backupPlanId": "83fcb8ee-2d93-42ac-b06f-591563f3f8de",
    "versionId": "NjIwNDFjMDEtNmZlNC00M2JmLTkzZDgtNzNkZjQyNzkxNDk0",
```

```
    "modifiedAt": "2020-06-24T23:18:19.168Z",
    "state": "MODIFIED"
  }
}
```

状態: 削除済み

```
{
  "version": "0",
  "id": "33fc5c1d-6db2-b3d9-1e70-1c9a2c23645c",
  "detail-type": "Backup Plan State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:25Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-plan:83fcb8ee-2d93-42ac-
b06f-591563f3f8de"
  ],
  "detail": {
    "backupPlanId": "83fcb8ee-2d93-42ac-b06f-591563f3f8de",
    "versionId": "NjIwNDFjMDEtNmZlNC00M2JmLTkzZDgtNzNkZjQyNzkxNDk0",
    "deletionDate": "2020-06-24T23:18:19.411Z",
    "state": "DELETED"
  }
}
```

状態: 作成済み

```
{
  "version": "0",
  "id": "b64fb2d0-ae16-ff9a-faf6-0bdd0d4bfdef",
  "detail-type": "Backup Plan State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:19Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-plan:2c103c5f-6d6e-4cac-9147-
d3afa4c84f59"
  ],
  "detail": {
    "backupPlanId": "2c103c5f-6d6e-4cac-9147-d3afa4c84f59",
```

```
    "versionId": "N2Q4OTczMzEtZmY1My00N2UwLWE3ODUtMjViYWYyOTUzZWY4",
    "creationDate": "2020-06-24T23:18:15.318Z",
    "state": "CREATED"
  }
}
```

Backup Vault イベント

イベントの例を次に示します。

状態

- 状態: 作成済み
- 状態: 変更済み
- 状態: 削除済み

状態: 作成済み

```
{
  "version": "0",
  "id": "d415609e-5f35-d9a2-76d1-613683e4e024",
  "detail-type": "Backup Vault State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:19Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:d8864642-155c-4283-a168-
a04f40e12c97"
  ],
  "detail": {
    "backupVaultName": "d8864642-155c-4283-a168-a04f40e12c97",
    "state": "CREATED"
  }
}
```

状態: 変更済み

```
{
  "version": "0",
  "id": "1a2b3cd4-5e6f-7g8h-9i0j-123456k7l890",
```

```
  "detail-type": "Backup Vault State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:19Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:nameOfTestBackup"
  ],
  "detail": {
    "backupVaultName": "vaultName",
    "state": "MODIFIED",
    "isLocked": "true"
  }
}
```

状態: 削除済み

```
{
  "version": "0",
  "id": "344bccc1-6d2e-da93-3adf-b3f82460294d",
  "detail-type": "Backup Vault State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-22T02:42:37Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:e8189629-1f8e-4ed2-af7d-
b32415d04db1"
  ],
  "detail": {
    "backupVaultName": "e8189629-1f8e-4ed2-af7d-b32415d04db1",
    "state": "DELETED"
  }
}
```

ジョブイベントのコピー

イベントの例を次に示します。

状態

- 状態: FAILED
- 状態: 実行中

- 状態: 完了
- 状態: 作成済み

状態: FAILED


```
{
  "version": "0",
  "id": "4660bc92-a44d-c939-4542-cda503f14855",
  "detail-type": "Copy Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T20:37:34Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::image/ami-00179b33a7a88cac5"
  ],
  "detail": {
    "copyJobId": "47C8EF56-74D8-059D-1301-C5BE1D5C926E",
    "backupSizeInBytes": 22548578304,
    "creationDate": "2020-07-15T20:36:13.239Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/
RoleForEc2BackupWithNoDescribeTagsPermissions",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:instance/i-0515aee7de03f58e1",
    "resourceType": "EC2",
    "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:55aa945e-c46a-421b-aa27-f94b074e31b7",
    "state": "FAILED",
    "statusMessage": "Access denied exception while trying to list tags",
    "completionDate": "2020-07-15T20:37:28.704Z",
    "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:55aa945e-c46a-421b-aa27-f94b074e31b7",
    "destinationRecoveryPointArn": {}
  }
}
```


状態: 実行中


```
{
  "version": "0",
  "id": "d17480ae-7042-edb2-0ff5-8b94822c58e4",
  "detail-type": "Copy Job State Change",
```

```
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T22:07:48Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::snapshot/snap-03886bc8d6ef3a1f9"
  ],
  "detail": {
    "copyJobId": "0175DE71-5784-589F-D8AC-541ACCB4CAC8",
    "backupSizeInBytes": 3221225472,
    "creationDate": "2020-07-15T22:06:27.234Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/OrganizationCanaryTestRole",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/vol-050eba21ee4d3c001",
    "resourceType": "EBS",
    "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:846869de-4589-45c3-ab60-4fbbabcdd3ec",
    "state": "RUNNING",
    "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:846869de-4589-45c3-ab60-4fbbabcdd3ec",
    "destinationRecoveryPointArn": {},
    "createdBy": {
      "backupPlanId": "b58e3621-1c53-4997-ad8a-afc3347a850e",
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:b58e3621-1c53-4997-ad8a-afc3347a850e",
      "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
      "backupPlanRuleId": "78e356d3-1a11-4f61-8585-af5d6b69bb18"
    }
  }
}
```

状態: 完了

```
{
  "version": "0",
  "id": "47deb974-6473-aef1-56c2-52c3eaedfceb",
  "detail-type": "Copy Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T22:08:04Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::snapshot/snap-03886bc8d6ef3a1f9"
  ],
```

```
  "detail": {
    "copyJobId": "0175DE71-5784-589F-D8AC-541ACCB4CAC8",
    "backupSizeInBytes": 3221225472,
    "creationDate": "2020-07-15T22:06:27.234Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/OrganizationCanaryTestRole",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/vol-050eba21ee4d3c001",
    "resourceType": "EBS",
    "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:846869de-4589-45c3-ab60-4fbbabcdd3ec",
    "state": "COMPLETED",
    "completionDate": "2020-07-15T22:07:58.111Z",
    "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:846869de-4589-45c3-ab60-4fbbabcdd3ec",
    "destinationRecoveryPointArn": "arn:aws:ec2:us-west-2::snapshot/
snap-0726fe70935586180",
    "createdBy": {
      "backupPlanId": "b58e3621-1c53-4997-ad8a-afc3347a850e",
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:b58e3621-1c53-4997-ad8a-afc3347a850e",
      "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
      "backupPlanRuleId": "78e356d3-1a11-4f61-8585-af5d6b69bb18"
    }
  }
}
```

状態: 作成済み

```
{
  "version": "0",
  "id": "8398a4c4-8fe8-2b49-a4b9-fd4fdcd34a4e",
  "detail-type": "Copy Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-22T21:06:32Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::image/ami-0888b126e2170b98e"
  ],
  "detail": {
    "creationDate": "2020-06-22T21:06:25.754Z",
    "state": "CREATED",
    "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:ef09da5a-21a6-461f-a98f-857e9e621a17",
```

```
    "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:ef09da5a-21a6-461f-a98f-857e9e621a17"
  }
}
```

復旧ポイントイベント

イベントの例を次に示します。

状態

- 状態: 完了
- 状態: 削除済み
- 状態: 変更済み

状態: 完了

```
{
    "version": "0",
    "id": "ab32977c-378d-2122-e985-fgh4596f0709",
    "detail-type": "Recovery Point State Change",
    "source": "aws.backup",
    "account": "1112233445566",
    "time": "2020-07-15T21:39:07Z",
    "region": "us-west-2",
    "resources": [
        "arn:aws:rds:us-west-2:1112233445566:cluster-snapshot:awsbackup:job-4ece7121-
d60e-00c2-5c3b-49960142d03b"
    ],
    "detail": {
        "backupVaultName": "e6625738-0655-4aa9-bd37-6ec1dd183b15",
        "backupVaultArn": "arn:aws:backup:us-west-2:496821122410:backup-
vault:e6625738-0655-4aa9-bd37-6ec1dd183b15",
        "creationDate": "2020-07-15T21:38:31.152Z",
        "iamRoleArn": "arn:aws:iam::1112233445566:role/FullBackupTestRole",
        "resourceType": "Aurora",
        "resourceArn": "arn:aws:rds:us-west-2:1112233445566:cluster:id",
        "status": "COMPLETED",
        "isEncrypted": "false",
        "storageClass": "WARM",
        "completionDate": "2020-07-15T21:39:05.689Z",
```

```
        "createdBy": {
            "backupPlanId": "bde0f455-4e24-4668-aeaa-4932a97f5cc5",
            "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:bde0f455-4e24-4668-aeaa-4932a97f5cc5",
            "backupPlanVersion": "YTkzNmM0MmUtMWRhNS00Y2RkLThmZGUtNjA5NTc4NGM1YTc5",
            "backupPlanRuleId": "1f97bafa-14d6-4f39-94fd-94b51bd6d0d5"
        },
        "lifecycle": {
            "deleteAfterDays": 100
        },
        "calculatedLifeCycle": {
            "deleteAt": "2020-10-23T21:38:31.152Z"
        }
    }
}
```

状態: 削除済み

```
{
  "version": "0",
  "id": "6089ee76-d856-0d7c-cee7-0a431cd43343",
  "detail-type": "Recovery Point State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T22:38:49Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:157f892e-
fe46-48da-9dbe-4154f91f8acc",
    "arn:aws:rds:us-west-2:1112233445566:snapshot:awsbackup:job-c1a6d40a-32d1-4d54-
bd70-bced933ef107"
  ],
  "detail": {
    "state": "DELETED",
    "lifecycle": {
      "deleteAfterDays": 300
    },
    "calculatedLifeCycle": {
      "deletedAt": "2021-05-25T22:29:02.452Z"
    }
  }
}
```

状態: 変更済み

```
{
  "version": "0",
  "id": "14365bb1-adef-bc00-1ee3-8fac188d7996",
  "detail-type": "Recovery Point State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-02T23:33:57Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:helo12312",
    "arn:aws:dynamodb:us-west-2:1112233445566:table/test/
backup/01593730512469-033578ce"
  ],
  "detail": {
    "calculatedLifeCycle": {
      "toColdStorageAfterDays": "Fri Dec 04 22:55:11 UTC 2020"
    },
    "state": "MODIFIED"
  }
}
```

リージョン設定イベント

以下に示しているのは、イベントの例です。

```
{
  "version": "0",
  "id": "e7ed82ba-4955-4de5-10d6-dbafcfb68b4f",
  "detail-type": "Region Setting State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T22:55:03Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "modifiedAt": "2020-06-24T22:54:57.161Z",
    "ResourceTypeOptInPreference": {
      "Aurora": true
    },
    "state": "MODIFIED"
  }
```

```
}
```

復元ジョブイベント

イベントの例を次に示します。

状態

- 状態: FAILED
- 状態: 実行中
- 状態: 完了
- 状態: 保留中
- 状態: 作成済み

状態: FAILED

```
{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T20:19:29Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::image/ami-12b3456dfb7f8cf90"
  ],
  "detail": {
    "restoreJobId": "1B234A56-789B-01CD-2A34-4567A08901FD",
    "backupSizeInBytes": "22548578304",
    "creationDate": "2020-07-15T20:19:07.303Z",
    "createdBy": [
      "arn:aws:backup:us-east-1:123456789012:restore-testing-plan:TestPlan1-
a12b3c45-6d78-90e1-f234-56789b012gh3"
    ],
    "iamRoleArn": "arn:aws:iam::1112233445566:role/TestAWSBackupRole",
    "percentDone": 0,
    "resourceType": "EC2",
    "status": "FAILED",
    "statusMessage": "AWS Backup does not permit attaching a new instance profile to an
 EC2 instance. Please restore using the backed up instance profile."
```

```
  }
}
```

状態: 実行中

```
{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T20:26:06Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::snapshot/snap-0fe123ca456cfad7c"
  ],
  "detail": {
    "restoreJobId": "1B234A56-789B-01CD-2A34-4567A08901FD",
    "backupSizeInBytes": "3221225472",
    "creationDate": "2020-07-29T20:26:00.098Z",
    "createdBy": [
      "arn:aws:backup:us-east-1:123456789012:restore-testing-plan:TestPlan1-
a12b3c45-6d78-90e1-f234-56789b012gh3"
    ],
    "iamRoleArn": "arn:aws:iam::1112233445566:role/RestoreTestRole",
    "percentDone": 0,
    "resourceType": "EBS",
    "status": "RUNNING"
  }
}
```

状態: 完了

```
{
  "version":"0",
  "id":"ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type":"Restore Job State Change",
  "source":"aws.backup",
  "account":"1112233445566",
  "time":"2020-07-15T03:14:58Z",
  "region":"us-west-2",
  "resources":[
```

```
    "arn:aws:rds:us-
west-2:1112233445566:snapshot:awsbackup:job-1a2bcd34-567e-8901-23f4-5g6hijkl7890"
  ],
  "detail":{
    "restoreJobId":"AB123456-78C9-0123-456D-789012E34567",
    "backupSizeInBytes":"0",
    "creationDate":"2020-07-15T03:10:01.742Z",
    "createdBy": [
      "arn:aws:backup:us-east-1:123456789012:restore-testing-plan:TestPlan1-
a12b3c45-6d78-90e1-f234-56789b012gh3"
    ],
    "iamRoleArn":"arn:aws:iam::1112233445566:role/RestoreTestRole",
    "percentDone":0,
    "resourceType":"RDS",
    "status":"COMPLETED",
    "createdResourceArn":"arn:aws:rds:us-
west-2:1112233445566:db:testinginstance1a2bcd34-567e-8901-23f4-5g6hijkl7890",
    "completionDate":"2020-07-15T03:14:53.128Z"
  }
}
```

状態: 保留中

```
{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T20:08:26Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:42bb8260-92cd-46a2-ab8d-
b29f4edb47b1"
  ],
  "detail": {
    "restoreJobId": "123EA45F-C678-EFE9-0123-4D56FC0E789A",
    "backupSizeInBytes": "36048",
    "creationDate": "2020-07-29T20:08:21.083Z",
    "createdBy": [
      "arn:aws:backup:us-east-1:123456789012:restore-testing-plan:TestPlan1-
a12b3c45-6d78-90e1-f234-56789b012gh3"
    ],
```

```
    "iamRoleArn": "arn:aws:iam::1112233445566:role/RestoreTestRole",
    "percentDone": 0,
    "resourceType": "EC2",
    "status": "PENDING"
  }
}
```

状態: 作成済み

```
{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-22T18:50:49Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:a6560b33-3660-494c-8d47-
efgh939ij32k"
  ],
  "detail": {
    "restoreJobId": "123EA45F-C678-EFE9-0123-4D56FC0E789A",
    "creationDate": "2020-06-22T18:50:46.407Z",
    "createdBy": [
      "arn:aws:backup:us-east-1:123456789012:restore-testing-plan:TestPlan1-
a12b3c45-6d78-90e1-f234-56789b012gh3"
    ],
    "state": "CREATED"
  }
}
```

AWS Backup Amazon での メトリクス CloudWatch

トピック

- CloudWatch ダッシュボード
- を使用したメトリクス CloudWatch

CloudWatch ダッシュボード

> **Note**
>
> コンソールダッシュボードは、コンソールにアクセスしているリージョンによって異なります。ジョブダッシュボードにアクセスできるリージョンを確認するには、「による機能の可用性 AWS リージョン」を参照してください。リストにないリージョンは、ダッシュボードにアクセスできます CloudWatch。

AWS Backup コンソールには、完了した、または失敗したバックアップ、コピー、復元ジョブのメトリクスを表示するダッシュボードが含まれています。このダッシュボードでは、ジョブのステータスを期間ごとに表示でき、希望する期間に合わせてカスタマイズできます。

ダッシュボードへのアクセス

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. 左側のナビゲーションペインの [ダッシュボード] を選択します。

ダッシュボードの表示および理解

CloudWatch ダッシュボードには複数のウィジェットが表示されます。各ウィジェットには、ジョブメトリクスがカウントごとに表示されます。各ウィジェットには複数の折れ線グラフが表示されます。各行は保護されているリソースに対応しています (期待するリソースが表示されない場合は、[設定] でそのリソースがオンになっていることを確認してください)。ディスプレイには進行中のジョブは表示されません。

Y 軸 (垂直値) にはカウント数が表示されます。X 軸 (水平値) にはポイントインタイムが表示されます。選択したジョブのステータスに視覚化するデータポイントがない場合は、X 軸に水平線が表示され、値は 0 に設定されます。リソースを示す凡例は引き続き表示されます。

メトリクスには、現在のログインに関連するアカウント固有およびリージョン固有の情報が表示されます。他のアカウントまたはリージョンを表示するには、選択したアカウントでログインする必要があります。

ダッシュボードのカスタマイズ

デフォルトでは、表示される期間は 1 週間です。上部のメニューには、表示される期間を再定義するためのオプションがあります。1 時間、3 時間、12 時間、1 日、3 日、1 週間から選択できま

す。また、[カスタム] を選択して別の値を指定することもできます。カスタマイズを行うと、現在のビューが仕様に合わせて一時的に変更されます。

ウィジェットにカーソルを合わせると、ウィジェットの右上に [拡大] ボタンが表示されます。[拡大] をクリックすると、ウィジェットを全画面表示で開きます。全画面表示では、期間 (各データポイント間の時間) を変更するなど、グラフ表示をカスタマイズするオプションが他にもあります。全画面表示を閉じると、変更内容は保持されません。

一度に 1 つのリソースタイプのみを表示するには、グラフの凡例に表示したいリソースタイプのラベルテキストをクリックします。これにより、他のすべてのリソースタイプの選択が解除されます。これを逆に行うには、凡例にあるリソースタイプのカラーボックスをクリックします。すべてのラベルが選択されたすべてのリソースタイプをデフォルト表示に戻すには、選択したリソースタイプのラベルテキストをもう一度クリックします。

ウィジェットの右上隅にある 3 つの縦の点をクリックすると、ドロップダウンメニューが開き、更新、拡大、メトリクスの表示、およびログの表示のオプションが表示されます。「メトリクスで表示」は、 CloudWatch コンソールのウィジェットで使用されるメトリクスを開きます。ウィジェットに変更を加え、そのウィジェットを CloudWatch ダッシュボードのカスタムダッシュボードに追加できます。 CloudWatch ダッシュボードで行った変更は、 AWS Backup コンソールのダッシュボードに反映されません。 CloudWatch コンソールで「ログとして表示」でログビューページが開きます。

独自のカスタム CloudWatch ダッシュボードに表示されるウィジェットを追加するには、ダッシュボードの右上にあるダッシュボードに追加ボタンをクリックします。これにより、 CloudWatch コンソールが開き、6 つのウィジェットすべてを追加するカスタムダッシュボードを選択できます。

詳細については、「Amazon CloudWatch メトリクスの使用」を参照してください。

を使用したメトリクス CloudWatch

を使用して AWS Backup メトリクス CloudWatch をモニタリングできます。AWS/Backup 名前空間では、次のメトリクスを追跡できます。 は、更新されたメトリクスを 5 分 CloudWatch ごとに に AWS Backup 出力します。

このドキュメントページの目的は、 CloudWatch のモニタリングに使用する参考資料を提供することです AWS Backup。を使用してメトリクスをモニタリングする方法については CloudWatch、ブログ「Amazon CloudWatch Events and Metrics for AWS Backup」またはCloudWatch 「 ユーザーガイド」の「Focus on Metrics and Alarms in a Single AWS Service」を参照してください。アラームを設定するには、「 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。

カテゴリ	メトリクス	ディメンションの例	ユースケースの例
ジョブ	CREATED、PENDING、R 、FAILED および EXPIRED を含む各状態でのバックアップ、復元、コピージョブの数。 ジョブタイプによって、使用可能な状態は異なります。	リソースタイプ、ボールト名。 コピージョブのボールト名は、コピー先のボールトの名前です。	1 つ以上の特定のバックアップボールト内の失敗したバックアップジョブの数をモニタリングします。1 時間以内に失敗したジョブが 5 つ以上ある場合は、Amazon SNS を使用して電子メールまたは SMS を送信するか、エンジニアリングチームにチケットを開いて調査します。 レポート条件: ゼロ以外の値がある
復旧ポイント	各状態におけるウォームリカバリポイントとコールドリカバリポイントの数: MODIFIED、COMPLETE 、PARTIAL、EXPIREI	リソースタイプ、ボールト名。	Amazon EBS ボリュームで削除されたリカバリポイントの数を追跡し、各バックアップボールト内のウォームリカバリポイントとコールドリカバリポイントの数を個別に追跡します。 レポート条件: ゼロ以外の値がある

> **Note**
>
> のジョブステータス`Completed with issues`はコンソール AWS Backup にのみ固有であり、 経由で追跡することはできません CloudWatch。

以下の表では、使用できるすべてのメトリクスを示しています。

メトリクス	説明
`NumberOfBackupJobsCreated`	が AWS Backup 作成したバックアップジョブの数。
`NumberOfBackupJobsPending`	AWS Backupで実行しようとしているバックアップジョブの数。
`NumberOfBackupJobsRunning`	で現在実行されているバックアップジョブの数 AWS Backup。
`NumberOfBackupJobsAborted`	ユーザーがキャンセルしたバックアップジョブの数。
`NumberOfBackupJobsCompleted`	AWS Backup 完了したバックアップジョブの数。
`NumberOfBackupJobsFailed`	スタータスが `Failed` になっているバックアップジョブの数。多くの場合、データベースリソースの前または 1 時間、Amazon FSx メンテナンスウィンドウまたは自動バックアップウィンドウの前または 4 時間の間にバックアップジョブをスケジュールし、 AWS Backup を使用して point-in-time 復元の継続的なバックアップを実行しないことが原因です。サポートされている サービスのリストと、 AWS Backup を使用して継続的なバックアップを取る方法、またはバックアップジョブを再スケジュールする方法については、「ポイントインタイムリカバリ」を参照してください。

メトリクス	説明
NumberOfBackupJobsExpired	ステータスが のバックアップジョブの数EXPIRED。 バックアップジョブCREATEDEXPIREDが開始ウィンドウ時間内に開始できない場合、バックアップジョブは ステータスから に変わります。
NumberOfCopyJobsCreated	AWS Backup が作成したクロスアカウントおよびクロスリージョンコピージョブの数。
NumberOfCopyJobsRunning	AWS Backupで現在実行されているクロスアカウントおよびクロスリージョンコピージョブの数。
NumberOfCopyJobsCompleted	AWS Backup が終了させたクロスアカウントおよびクロスリージョンコピージョブの数。
NumberOfCopyJobsFailed	AWS Backup 試行したが完了できなかったクロスアカウントおよびクロスリージョンコピージョブの数。
NumberOfRestoreJobsPending	AWS Backupで実行しようとしている復元ジョブの数。
NumberOfRestoreJobsRunning	で現在実行されている復元ジョブの数 AWS Backup。
NumberOfRestoreJobsCompleted	AWS Backup 完了した復元ジョブの数。
NumberOfRestoreJobsFailed	AWS Backup が試行したが、完了できなかった復元ジョブの数。
NumberOfRecoveryPointsCompleted	が AWS Backup 作成した復旧ポイントの数。

メトリクス	説明
NumberOfRecoveryPointsPartial	が作成 AWS Backup を開始したが、終了できなかった復旧ポイントの数。 は後でプロセスを AWS 再試行しますが、再試行は後で発生するため、部分的な復旧ポイントが保持されます。
NumberOfRecoveryPointsExpired	バックアップ保持ライフサイクルに基づいて削除を試み AWS Backup たが、削除できなかった復旧ポイントの数。期限切れのバックアップが消費するストレージに対して課金されるため、手動で削除する必要があります。
NumberOfRecoveryPointsDeleting	AWS Backup 削除する復旧ポイントの数。
NumberOfRecoveryPointsCold	コールドストレージに AWS Backup 階層化された復旧ポイントの数。

表に示されているディメンション以外にも、より多くのディメンションを使用できます。メトリクスのすべてのディメンションを表示するには、そのメトリクスの名前を CloudWatch コンソールのメトリクスセクションの名前AWS/Backup空間に入力します。

を使用した AWS Backup API コールのログ記録 CloudTrail

AWS Backup はAWS CloudTrail、ユーザー、ロール、または AWS のサービス のサービスによって実行されたアクションを記録するサービスと統合されています。 は、 のすべての API コールをイベント AWS Backup として CloudTrail キャプチャします。キャプチャされた呼び出しには、 AWS Backup コンソールからの呼び出しと AWS Backup API オペレーションへのコード呼び出しが含まれます。によって収集された情報を使用して CloudTrail、 に対するリクエスト AWS Backup、リクエスト元の IP アドレス、リクエスト日時などの詳細を確認できます。

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます:

- ルートユーザーまたはユーザー認証情報のどちらを使用してリクエストが送信されたか
- リクエストが IAM Identity Center ユーザーに代わっ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 のサービスによって送信されたかどうか。

CloudTrail アカウント AWS アカウント を作成すると、 は でアクティブになり、 CloudTrail イベント履歴 に自動的にアクセスできます。 CloudTrail イベント履歴は、 に記録された過去 90 日間の管理イベントの表示可能、検索可能、ダウンロード可能、およびイミュータブルなレコードを提供します AWS リージョン。詳細については、「 ユーザーガイド」の CloudTrail 「イベント履歴の使用AWS CloudTrail 」を参照してください。イベント履歴を表示するための料金はかかりません CloudTrail。

AWS アカウント 過去 90 日間のイベントの継続的な記録については、証跡または CloudTrail Lake イベントデータストアを作成します。

CloudTrail 証跡

証跡により CloudTrail 、 はログファイルを Amazon S3 バケットに配信できます。を使用して作成された証跡はすべてマルチリージョン AWS Management Console です。 AWS CLIを使用する際は、単一リージョンまたは複数リージョンの証跡を作成できます。 AWS リージョン アカウントのすべての でアクティビティをキャプチャするため、マルチリージョン証跡を作成することをお勧めします。単一リージョンの証跡を作成する場合、証跡の AWS リージョンに記録されたイベントのみを表示できます。証跡の詳細については、「AWS CloudTrail ユーザーガイド」の「AWS アカウントの証跡の作成」および「組織の証跡の作成」を参照してください。

証跡を作成 CloudTrail することで、 から Amazon S3 バケットに継続的な管理イベントのコピーを 1 つ無料で配信できますが、Amazon S3 ストレージ料金が発生します。 CloudTrail 料金の詳細については、「 の料金AWS CloudTrail」を参照してください。Amazon S3 の料金に関する詳細については、「Amazon S3 の料金」を参照してください。

CloudTrail Lake イベントデータストア

CloudTrail Lake では、イベントに対して SQL ベースのクエリを実行できます。 CloudTrail Lake は、既存のイベントを行ベースの JSON 形式で Apache ORC 形式に変換します。ORC は、データを高速に取得するために最適化された単票ストレージ形式です。イベントはイベントデータストアに集約されます。イベントデータストアは、高度なイベントセレクタを適用することによって選択する条件に基いた、イベントのイミュータブルなコレクションです。どのイベントが存続し、クエリに使用できるかは、イベントデータストアに適用するセレクタが制御します。CloudTrail Lake の詳細については、「 ユーザーガイド」の AWS CloudTrail 「Lake の使用AWS CloudTrail 」を参照してください。

CloudTrail Lake イベントデータストアとクエリにはコストがかかります。イベントデータストアを作成する際に、イベントデータストアに使用する料金オプションを選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、そのイベントデータストアのデフォルトと最長の保持期間が決まります。 CloudTrail 料金の詳細については、「 の料金AWS CloudTrail」を参照してください。

AWS Backup の イベント CloudTrail

AWS Backup は、バックアップ、復元、コピー、または通知を実行すると、これらの CloudTrail イベントを生成します。これらのイベントは、 AWS Backup 必ずしもパブリック APIsを使用して生成されるわけではありません。詳細については、「 ユーザーガイド」の「 AWS のサービス イベントAWS CloudTrail 」を参照してください。

- `BackupDeleted`
- `BackupJobCompleted`
- `BackupJobStarted`
- `BackupSelectionDeletedDueToSLRDeletion`
- `BackupTransitionedToCold`
- `CopyJobCompleted`
- `CopyJobStarted`
- `ReportJobCompleted`
- `ReportJobStarted`
- `RestoreCompleted`
- `RestoreStarted`
- `PutBackupVaultNotifications`

AWS Backup ログファイルエントリについて

証跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信できるようにする設定です。 CloudTrail ログファイルには 1 つ以上のログエントリが含まれます。イベントは任意のソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどに関する情報が含まれます。 CloudTrail ログファイルはパブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

次の例は、StartBackupJob、、および DeleteRecoveryPointアクションと StartRestoreJobBackupJobCompletedイベントを示す CloudTrail ログエントリを示しています。


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-01-10T12:24:50Z"
            }
        }
    },
    "eventTime": "2019-01-10T13:45:24Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "StartBackupJob",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "12.34.567.89",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.465
 Linux/4.9.124-0.1.ac.198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
 java/1.8.0_192",
    "requestParameters": {
        "backupVaultName": "Default",
        "resourceArn": "arn:aws:ec2:us-east-1:123456789012:volume/
vol-00a422a05b9c6asd3",
        "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
        "startWindowMinutes": 60
    },
    "responseElements": {
        "backupJobId": "8a3c2a87-b23e-4d56-b045-fa9e88ede4e6",
        "creationDate": "Jan 10, 2019 1:45:24 PM"
    },
    "requestID": "98cf4d59-8c76-49f7-9201-790743931234",
    "eventID": "fe8146a5-7812-4a95-90ad-074498be1234",
    "eventType": "AwsApiCall",
    "recipientAccountId": "account-id"
},
```

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-01-10T12:24:50Z"
            }
        }
    },
    "eventTime": "2019-01-10T13:49:50Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "StartRestoreJob",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "12.34.567.89",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.465
 Linux/4.9.124-0.1.ac.198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
 java/1.8.0_192",
    "requestParameters": {
        "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-00a129455bdbc9d99",
        "metadata": {
            "volumeType": "gp2",
            "availabilityZone": "us-east-1b",
            "volumeSize": "100"
        },
        "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
        "idempotencyToken": "a9c8b4fb-d369-4a58-944b-942e442a8fe3",
        "resourceType": "EBS"
    },
    "responseElements": {
        "restoreJobId": "9808E090-8C76-CCB8-4CEA-407CF6AC4C43"
    },
    "requestID": "783ddddc-6d7e-4539-8fab-376aa9668543",
    "eventID": "ff35ddea-7577-4aec-a132-964b7e9dd423",
    "eventType": "AwsApiCall",
    "recipientAccountId": "account-id"
},
{
    "eventVersion": "1.05",
```

```
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-01-10T12:24:50Z"
            }
        }
    },
    "eventTime": "2019-01-10T14:52:42Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "DeleteRecoveryPoint",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "12.34.567.89",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.465
 Linux/4.9.124-0.1.ac.198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
 java/1.8.0_192",
    "requestParameters": {
        "backupVaultName": "Default",
        "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-05f426fd9daab3433"
    },
    "responseElements": null,
    "requestID": "f1f1b33a-48da-436c-9a8f-7574f1ab5fd7",
    "eventID": "2dd70080-5aba-4a79-9a0f-92647c9f0846",
    "eventType": "AwsApiCall",
    "recipientAccountId": "account-id"
},
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "backup.amazonaws.com"
    },
    "eventTime": "2019-01-10T08:24:39Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "BackupJobCompleted",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "backup.amazonaws.com",
    "userAgent": "backup.amazonaws.com",
    "requestParameters": null,
```

```
    "responseElements": null,
    "eventID": "2e7e4fcf-0c52-467f-9fd0-f61c2fcf7d17",
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "account-id",
    "serviceEventDetails": {
        "completionDate": {
            "seconds": 1547108091,
            "nanos": 906000000
        },
        "state": "COMPLETED",
        "percentDone": 100,
        "backupJobId": "8A8E738B-A8C5-E058-8224-90FA323A3C0E",
        "backupVaultName": "BackupVault",
        "backupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-
vault:BackupVault",
        "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-07ce8c3141d361233",
        "resourceArn": "arn:aws:ec2:us-east-1:123456789012:volume/
vol-06692095a6a421233",
        "creationDate": {
            "seconds": 1547101638,
            "nanos": 272000000
        },
        "backupSizeInBytes": 8589934592,
        "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
        "resourceType": "EBS"
    }
}
```


クロスアカウント管理イベントのログ記録

を使用すると AWS Backup、 AWS Organizations構造 AWS アカウント 内のすべてのバックアップを管理できます。 は、 AWS Organizations バックアップポリシー (メンバーアカウントにバックアッププランを適用する) を作成、更新、または削除するとき、または無効な組織バックアッププランがある場合に、これらの CloudTrail イベント AWS Backup を生成します。

- `CreateOrganizationalBackupPlan`
- `UpdateOrganizationalBackupPlan`
- `DeleteOrganizationalBackupPlan`
- `InvalidOrganizationalBackupPlan`

例: クロスアカウント管理用の AWS Backup ログファイルエントリ

証跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信できるようにする設定です。 CloudTrail ログファイルには 1 つ以上のログエントリが含まれます。イベントは任意のソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどに関する情報が含まれます。 CloudTrail ログファイルはパブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

次の例は、 CreateOrganizationalBackupPlanアクションを示す CloudTrail ログエントリを示しています。


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "backup.amazonaws.com"},
    "eventTime": "2020-06-02T00:34:00Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "CreateOrganizationalBackupPlan",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "backup.amazonaws.com",
    "userAgent": "backup.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "f2642255-af77-4203-8c37-7ca19d898e84",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "account-id",
    "serviceEventDetails": {
        "backupPlanId": "orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
        "backupPlanVersionId": "ZTA1Y2ZjZDYtNmRjMy00ZTA1LWIyNTAtM2M1NzQ4OThmNzRj",
        "backupPlanArn": "arn:aws:backup:ca-central-1:123456789012:backup-
plan:orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
        "backupPlanName": "mybackupplan",
        "backupRules": "[{\"id\":\"745fd0ea-7f57-3f35-8a0e-ed4b8c48a8e2\",
\"name\":\"hourly\",\"description\":null,\"cryopodArn\":\"arn:aws:backup:ca-
central-1:123456789012:backup-vault:CryoControllerCAMTestBackupVault\",
\"scheduleExpression\":\"cron(0 0/1 ? * * *)\",\"startWindow\":\"PT1H\",
\"completionWindow\":\"PT2H\",\"lifecycle\":{\"moveToColdStorageAfterDays\":null,
\"deleteAfterDays\":\"7\"},\"tags\":null,\"copyActions\":[]}]",
        "backupSelections": "[{\"name\":\"selectiondatatype\",\"arn\":
\"arn:aws:backup:ca-central-1:123456789012:selection:8b40c6d9-3641-3d49-926d-
a075ea715686\",\"role\":\"arn:aws:iam::123456789012:role/OrganizationmyRoleTestRole\",
```

```
\"resources\":[],\"notResources\":[],\"conditions\":[{\"type\":\"STRINGEQUALS\",\"key
\":\"dataType\",\"value\":\"PII\"},{\"type\":\"STRINGEQUALS\",\"key\":\"dataType\",
\"value\":\"RED\"}],\"creationDate\":\"2020-06-02T00:34:00.695Z\",\"creatorRequestId
\":null}]",
        "creationDate": {
            "seconds": 1591058040,
            "nanos": 695000000
        },
        "organizationId": "org-id",
        "accountId": "123456789012"
    }
}
```

次の例は、 DeleteOrganizationalBackupPlanアクションを示す CloudTrail ログエントリを示しています。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "backup.amazonaws.com"
    },
    "eventTime": "2020-06-02T00:34:25Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "DeleteOrganizationalBackupPlan",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "backup.amazonaws.com",
    "userAgent": "backup.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "5ce66cd0-b90c-4957-8e00-96ea1077b4fa",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "account-id",
    "serviceEventDetails": {
        "backupPlanId": "orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
        "backupPlanVersionId": "ZTA1Y2ZjZDYtNmRjMy00ZTA1LWIyNTAtM2M1NzQ4OThmNzRj",
        "backupPlanArn": "arn:aws:backup:ca-central-1:123456789012:backup-
plan:orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
        "backupPlanName": "mybackupplan",
        "deletionDate": {
            "seconds": 1591058065,
            "nanos": 519000000
```

```
        },
        "organizationId": "org-id",
        "accountId": "123456789012"
    }
}
```

次の例は、 が Organizations から無効なバックアッププラン AWS Backup を受信したときにInvalidOrganizationBackupPlan送信されるイベント を示す CloudTrail ログエントリを示しています。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "backup.amazonaws.com"
    },
    "eventTime": "2022-06-11T13:29:23Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "InvalidOrganizationBackupPlan",
    "awsRegion": "Region",
    "sourceIPAddress": "backup.amazonaws.com",
    "userAgent": "backup.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "ab1de234-fg56-7890-h123-45ij678k9l01",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "987654321098",
    "serviceEventDetails": {
        "effectivePolicyVersion": 7,
        "effectivePolicyId": "12345678-a9b0-123c-45d6-78e901f23456",
        "lastUpdatedTimestamp": "Jun 11, 2022 1:29:22 PM",
        "policyType": "BACKUP_POLICY",
        "effectiveBackupPlan": {
            "logicalName": "logical-name",
            "regions": [
                "Region"
            ],
            "rules": [
                {
                    "name": "test-orgs",
                    "targetBackupVaultName": "vault-name",
```

```
                    "ruleLifecycle": {
                        "deleteAfterDays": 100
                    },
                    "copyActions": [],
                    "enableContinuousBackup": true
                }
            ],
            "selections": {
                "tagSelections": [
                    {
                        "selectionName": "selection-name",
                        "iamRoleArn": "arn:aws:iam::$account:role/role",
                        "targetedTags": [
                            {
                                "tagKey": "key",
                                "tagValue": "value"
                            }
                        ]
                    }
                ]
            },
            "backupPlanTags": {
                "key": "value"
            }
        },
        "organizationId": "org-id",
        "accountId": "123456789012"
    },
    "eventCategory": "Management"
}
```

の通知オプション AWS Backup

に関する通知を受信するには、次の 2 つの方法があります AWS Backup。

- AWS ユーザー通知は、Amazon CloudWatch アラームなどの通知 AWS Support、およびその他のサービスの通知を送信できます。
- Amazon Simple Notification Service は AWS Backup 、イベントを通知できます。

AWS ユーザー通知と AWS Backup

AWS Backup は、AWS ユーザー通知コンソール からのバックアップ通知の管理をサポートします。AWS ユーザー通知を使用すると、バックアップ、コピー、復元ジョブの進行状況や、バックアップポリシー、ボールト、復旧ポイント、設定の変更をユーザー通知センターから確認できます。

Amazon CloudWatch、Amazon EventBridge アラーム、 AWS Support ケースの更新は、コンソールから管理できる他のタイプの通知です。さらに、E メール、 AWS Chatbot 通知、 AWS Console Mobile Application プッシュ通知など、いくつかの配信オプションを設定できます。

Amazon SNS と AWS Backup イベント

AWS Backup は、Amazon Simple Notification Service (Amazon SNS) によって配信される堅牢な通知を利用します。Amazon SNS コンソールから AWS Backup イベントを通知するように Amazon SNS を設定できます。

制限事項

- Amazon SNS サービスはクロスアカウント通知を許可します AWS Backup が、現在この機能をサポートしていません。独自の AWS アカウント ID とトピックのリソース ARN を指定する必要があります。
- AWS Backup は、SNS ベストエフォート重複除外の標準トピックをサポートしていますが、現在、厳格な重複除外の SNS FIFO トピック AWS Backup はサポートされていません。

一般的なユースケース

- 「失敗したジョブの通知を AWS プレミアムサポートから受け取るにはどうすればよいですか？」の手順に従って、失敗したバックアップ AWS Backup ジョブの通知を設定します。
- 以下の「イベントの例」一覧表で、完了、失敗、期限切れのバックアップジョブのサンプル Amazon SNS 通知 JSON を確認します。

Amazon SNS の詳細については、Amazon Simple Notification Service 開発者ガイドの「Amazon SNS の開始方法」を参照してください。

AWS Backup 通知 APIs

Amazon SNS コンソールまたは () を使用してトピックを作成したら、次の AWS Backup API オペレーションを使用してバックアップ通知を管理できます。 AWS Command Line Interface AWS CLI

- DeleteBackupVaultNotifications — 指定されたバックアップボールトのイベント通知を削除します。
- GetBackupVaultNotifications — 指定されたバックアップボールトのすべてのイベント通知を一覧表示します。
- PutBackupVaultNotifications — 指定されたトピックとイベントの通知をオンにします。

AWS Backup は、次のイベントをサポートします。

ジョブタイプ	イベント
バックアップジョブ	`BACKUP_JOB_STARTED` | `BACKUP_JOB_COMPLETED` | `CONTINUOUS_BACKUP_INTERRUPTED`
コピージョブ	`COPY_JOB_STARTED` | `COPY_JOB_SUCCESSFUL` | `COPY_JOB_FAILED`
復元ジョブ	`RESTORE_JOB_STARTED` | `RESTORE_JOB_COMPLETED`
復旧ポイント	`RECOVERY_POINT_MODIFIED`

AWS Backup for S3 は、次の 2 つの追加イベントをサポートします。

- `S3_BACKUP_OBJECT_FAILED` がバックアップジョブ中に AWS Backup がバックアップに失敗した S3 オブジェクトを通知します。
- `S3_RESTORE_OBJECT_FAILED` が復元ジョブ中に AWS Backup が復元に失敗した S3 オブジェクトを通知します。

イベントの例

Example 例: バックアップジョブが完了しました

```
{
    "Records": [{
        "EventSource": "aws:sns",
```

```
        "EventVersion": "1.0",
        "EventSubscriptionArn": "arn:aws:sns:...-a3802aa1ed45",
        "Sns": {
            "Type": "Notification",
            "MessageId": "12345678-abcd-123a-def0-abcd1a234567",
            "TopicArn": "arn:aws:sns:us-west-1:123456789012:backup-2sqs-sns-topic",
            "Subject": "Notification from AWS Backup",
            "Message": "An AWS Backup job was completed successfully. Recovery point
 ARN: arn:aws:ec2:us-west-1:123456789012:volume/vol-012f345df6789012d. Resource ARN :
 arn:aws:ec2:us-west-1:123456789012:volume/vol-012f345df6789012e. BackupJob ID :
 1b2345b2-f22c-4dab-5eb6-bbc7890ed123",
            "Timestamp": "2019-08-02T18:46:02.788Z",
            ...
            "MessageAttributes": {
                "EventType": {"Type":"String","Value":"BACKUP_JOB"},
                "State": {"Type":"String","Value":"COMPLETED"},
                "AccountId": {"Type":"String","Value":"123456789012"},
                "Id": {"Type":"String","Value":"1b2345b2-f22c-4dab-5eb6-bbc7890ed123"},
                "StartTime": {"Type":"String","Value":"2019-09-02T13:48:52.226Z"}
            }
        }
    }]
}
```

Example 例: バックアップジョブが失敗しました

```
{
    "Records": [{
        "EventSource": "aws:sns",
        "EventVersion": "1.0",
        "EventSubscriptionArn": "arn:aws:sns:...-a3802aa1ed45",
        "Sns": {
            "Type": "Notification",
            "MessageId": "12345678-abcd-123a-def0-abcd1a234567",
            "TopicArn": "arn:aws:sns:us-west-1:123456789012:backup-2sqs-sns-topic",
            "Subject": "Notification from AWS Backup",
            "Message": "An AWS Backup job failed. Resource ARN : arn:aws:ec2:us-
west-1:123456789012:volume/vol-012f345df6789012e. BackupJob ID : 1b2345b2-
f22c-4dab-5eb6-bbc7890ed123",
            "Timestamp": "2019-08-02T18:46:02.788Z",
            ...
            "MessageAttributes": {
                "EventType": {"Type":"String","Value":"BACKUP_JOB"},
```

```
                "State": {"Type":"String","Value":"FAILED"},
                "AccountId": {"Type":"String","Value":"123456789012"},
                "Id": {"Type":"String","Value":"1b2345b2-f22c-4dab-5eb6-bbc7890ed123"},
                "StartTime": {"Type":"String","Value":"2019-09-02T13:48:52.226Z"}
            }
        }
    }]
}
```

Example 例: バックアップウィンドウ中にバックアップジョブを完了できませんでした

```
{
    "Records": [{
        "EventSource": "aws:sns",
        "EventVersion": "1.0",
        "EventSubscriptionArn": "arn:aws:sns:...-a3802aa1ed45",
        "Sns": {
            "Type": "Notification",
            "MessageId": "12345678-abcd-123a-def0-abcd1a234567",
            "TopicArn": "arn:aws:sns:us-west-1:123456789012:backup-2sqs-sns-topic",
            "Subject": "Notification from AWS Backup",
            "Message": "An AWS Backup job failed to complete in time. Resource ARN :
 arn:aws:ec2:us-west-1:123456789012:volume/vol-012f345df6789012e. BackupJob ID :
 1b2345b2-f22c-4dab-5eb6-bbc7890ed123",
            "Timestamp": "2019-08-02T18:46:02.788Z",
            ...
            "MessageAttributes" : {
              "EventType" : {"Type":"String","Value":"BACKUP_JOB"},
              "State" : {"Type":"String","Value":"EXPIRED"},
              "AccountId" : {"Type":"String","Value":"123456789012"},
              "Id" : {"Type":"String","Value":"1b2345b2-f22c-4dab-5eb6-bbc7890ed123"},
              "StartTime" : {"Type":"String","Value":"2019-09-02T13:48:52.226Z"}
            }
        }
    }]
}
```

AWS Backup 通知コマンドの例

AWS CLI コマンドを使用して、 AWS Backup イベントの Amazon SNS 通知をサブスクライブ、一覧表示、削除できます。

バックアップボールトのプット通知の例

次のコマンドは、復元ジョブが開始または完了したとき、または復旧ポイントが変更されたときに通知する、指定されたバックアップボールトの Amazon SNS トピックをサブスクライブします。

```
aws backup put-backup-vault-notifications
    --backup-vault-name myBackupVault
    --sns-topic-arn arn:aws:sns:region:account-id:myBackupTopic
    --backup-vault-events RESTORE_JOB_STARTED RESTORE_JOB_COMPLETED
 RECOVERY_POINT_MODIFIED
```

バックアップボールト取得通知の例

次のコマンドは、指定したバックアップボールトの Amazon SNS トピックに現在サブスクライブされているすべてのイベントを一覧表示します。

```
aws backup get-backup-vault-notifications
    --backup-vault-name myVault
```

次に出力例を示します。

```
{
    "SNSTopicArn": "arn:aws:sns:region:account-id:myBackupTopic",
    "BackupVaultEvents": [
        "RESTORE_JOB_STARTED",
        "RESTORE_JOB_COMPLETED",
        "RECOVERY_POINT_MODIFIED"
    ],
    "BackupVaultName": "myVault",
    "BackupVaultArn": "arn:aws:backup:region:account-id:backup-vault:myVault"
}
```

バックアップボールトの削除通知の例

次のコマンドは、指定されたバックアップボールトの Amazon SNS トピックからサブスクライブを解除します。

```
aws backup delete-backup-vault-notifications
    --backup-vault-name myVault
```

サービスプリンシパル AWS Backup としての の指定

> **Note**
>
> AWS Backup がユーザーに代わって SNS トピックを発行できるようにするには、 をサービスプリンシパル AWS Backup として指定する必要があります。

AWS Backup イベントの追跡に使用する Amazon SNS トピックのアクセスポリシーに、次の JSON を含めます。トピックのリソースの Amazon リソースネーム (ARN) を指定する必要があります。

```
{
      "Sid": "My-statement-id",
      "Effect": "Allow",
      "Principal": {
        "Service": "backup.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:myTopic"
}
```

Amazon SNS アクセスポリシーでサービスプリンシパルを指定する方法の詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「任意の AWS リソースにトピックへの発行を許可する」を参照してください。

> **Note**
>
> トピックが暗号化されている場合は、 がトピックに発行できるように、ポリシー AWS Backup に追加のアクセス許可を含める必要があります。サービスが暗号化されたトピックに発行できるようにする方法の詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「 AWS サービスからのイベントソースと暗号化されたトピック間の互換性を有効にする」を参照してください。

トラブルシューティング AWS Backup

を使用すると AWS Backup、問題が発生する可能性があります。以降のセクションは、発生する可能性のある一般的な問題のトラブルシューティングに役立ちます。

に関する一般的な質問については AWS Backup、よくある質問を参照してくださいAWS Backup。また、AWS Backup フォーラムで回答を検索したり、質問を投稿することもできます。

トピック

- 一般的な問題のトラブルシューティング
- リソース作成のトラブルシューティング
- リソースの削除のトラブルシューティング
- リソース復元のトラブルシューティング
- フォーマットエラーのトラブルシューティング

一般的な問題のトラブルシューティング

リソースをバックアップおよび復元するときは、 を使用するアクセス許可 AWS Backup と、保護するリソースにアクセスするためのアクセス許可が必要です。適切な権限を取得する最も簡単な方法は、バックアッププランにリソースを割り当てるときにデフォルトロールすることです。での AWS Identity and Access Management (IAM) を使用したアクセスコントロールの詳細については AWS Backup、「」を参照してくださいアクセスコントロール。

バックアップボールトなどのリソースにアクセス AWS Backup しようとしたときにAccessDenied`AccessDenied`エラーが発生した場合は、リソースが存在しないか、リソースへのアクセス許可がありません。

特定のリソースタイプのバックアップと復元で問題が発生した場合は、そのリソースのバックアップと復元のトラブルシューティングのトピックを確認すると便利です。詳細については、「 がサポートされている AWS サービスと AWS Backup 連携する方法」のリンクを参照してください。

がリソースの作成または削除に AWS Backup 失敗した場合、 AWS CloudTrail を使用してエラーメッセージまたはログを表示することで、問題の詳細を確認できます。で を使用する CloudTrail方法の詳細については、 AWS Backup「」を参照してくださいを使用した AWS Backup API コールのログ記録 CloudTrail。

リソース作成のトラブルシューティング

次の情報は、バックアップの作成の問題をトラブルシューティングするのに役立ちます。

- 一般に、AWS データベースサービスは、メンテナンスウィンドウまたは自動バックアップウィンドウの 1 時間前またはウィンドウ中に、バックアップを開始できません。Amazon FSx は、メンテナンスウィンドウまたは自動バックアップウィンドウの 4 時間前またはウィンドウの間に、バックアップを開始することはできません (Amazon Aurora は、このメンテナンスウィンドウ制限の対象外です)。その間にスケジュールされたスナップショットバックアップは失敗します。1 つの例外: サポートされているサービスのスナップショットバックアップと継続的バックアップの両方 AWS Backup に を使用することをオプトインすると、 AWS Backup がスケジュールするため、これらのウィンドウについて心配する必要がなくなります。サポートされている サービスのリストと、 AWS Backup を使用して継続的なバックアップを作成する方法については、「ポイントインタイムリカバリ」を参照してください。
- DynamoDB テーブルのバックアップの作成は、テーブルの作成中に失敗します。通常、DynamoDB テーブルの作成には数分かかります。
- ファイルシステムが非常に大きい場合、Amazon EFS ファイルシステムのバックアップには最大 7 日かかることがあります。Amazon EFS ファイルシステムのキューに入れることができる同時バックアップは、一度に 1 つのみです。前のバックアップがまだ進行中の間に後続のバックアップがキューに入れられると、バックアップウィンドウが期限切れになることがあり、バックアップは作成されません。
- Amazon EBS のソフトクォータは、アカウント AWS リージョン ごとに 100,000 バックアップであり、このクォータに達すると追加のバックアップは失敗します。このクォータに達した場合は、余分なバックアップを削除するか、クォータの引き上げをリクエストできます。クォータ増加の要求の詳細については、AWS のService Quotasを参照してください。
- Amazon Relational Database Service (RDS) のバックアップを作成するときは、次の点を考慮してください。
  - AWS Backup を使用して、Amazon RDS スナップショットと継続的バックアップの両方を point-in-time リカバリで管理しない場合、ユーザーが設定可能な毎日の 30 分のバックアップ期間中にスケジュールまたはオンデマンドで開始すると、バックアップは失敗します。Amazon RDS の自動バックアップの詳細については、Amazon RDS ユーザーガイドの「バックアップの使用」を参照してください。を使用して Amazon RDS スナップショットと継続的バックアップの両方 AWS Backup を point-in-time リカバリで管理することで、この制限を回避できます。
  - Amazon RDS コンソールからバックアップジョブを開始すると、Aurora クラスターのバックアップジョブと競合し、`Backup job expired before completion.` エラーが発生する可

能性があります。この問題が発生した場合は、 AWS Backupで長いバックアップウィンドウを設定します。

- AWS Backup コピージョブの作成時に、 は現在 TDE オプショングループを渡しません。コピージョブの作成にこのオプショングループを使用する場合は、 AWS Backup ツールの代わりに Amazon RDS コンソールまたは Amazon RDS API を使用する必要があります。詳細については、「Amazon Relational Database Service ユーザーガイド」の「オプショングループのコピー」を参照してください。
- エラー: オンデマンドバックアップは完了しましたが、「ソーススナップショットの KMS キーが存在しないか、有効になっていないか、アクセス権限がありません」というエラーが表示され、スケジュールされたバックアップが失敗します。オンデマンドジョブは、KMS アクセスを必要としない API 呼び出し `CopyDBSnapshot` を使用するため完了しました。

  対処法: KMS キーに IAM ロールを追加します。これは KMS キーポリシーでロールを許可することで実現できます。

  ポリシーを編集するには、

  1. KMS コンソールを開きます。
  2. 左のナビゲーションバーで、[カスタマーマネージドキー] を選択します。
  3. 編集する [カスタマーマネージドキー] をクリックします。
  4. [キーポリシー] 行で、[ポリシービューへの切り替え] を選択します。
  5. [Edit (編集)] をクリックします。
  6. ロールを追加します。

リソースの削除のトラブルシューティング

によって作成された復旧ポイントは AWS Backup 、保護されたリソースのコンソールウィンドウで削除できません。 AWS Backup コンソールでそれらを削除するには、保存されているボールトでそれらを選択し、 の削除を選択します。

復旧ポイントまたはバックアップボールトを削除するには、適切な権限が必要です。で IAM を使用するアクセスコントロールの詳細については AWS Backup、「」を参照してくださいアクセスコントロール。

リソース復元のトラブルシューティング

API を使った復元

バックアップをプログラムで復元するには、StartRestoreJob API オペレーションを使用します。

バックアップの作成に使用した設定メタデータを取得するには、GetRecoveryPointRestoreMetadata を呼び出します。

詳細については、「バックアップの復元」を参照してください。

コンソールを使用した復元

- Amazon S3 データの復元
- 仮想マシンの復元
- Amazon FSx ファイルシステムの復元
- Amazon EBS ボリュームの復元
- Amazon EFS ファイルシステムの復元
- Amazon DynamoDB テーブルの復元
- Amazon RDS データベースの復元
- Aurora クラスターの復元
- Amazon EC2 インスタンスの復元
- Storage Gateway ボリュームの復元
- Amazon DocumentDB クラスターの復元
- Neptune クラスターの復元

フォーマットエラーのトラブルシューティング

パラメータの値にワイルドカード (*) が含まれている場合、ワイルドカードは空白以外の値を含むように処理されます。空白を含むキーと値のペアの値は、ワイルドカードの一部として含まれません。

AWS Backup API

コンソールの使用に加えて、AWS Backup API アクションおよびデータタイプを使用して、プログラミングにより AWS Backup およびそのリソースを設定し、管理できます。このセクションでは、AWS Backup アクションおよびデータタイプについて記述します。これには、AWS Backup の API リファレンスが含まれています。

AWS Backup API

- AWS Backup アクション
- AWS Backup データタイプ

アクション

以下のアクションが AWS Backup によってサポートされています。

- CancelLegalHold
- CreateBackupPlan
- CreateBackupSelection
- CreateBackupVault
- CreateFramework
- CreateLegalHold
- CreateLogicallyAirGappedBackupVault
- CreateReportPlan
- CreateRestoreTestingPlan
- CreateRestoreTestingSelection
- DeleteBackupPlan
- DeleteBackupSelection
- DeleteBackupVault
- DeleteBackupVaultAccessPolicy
- DeleteBackupVaultLockConfiguration
- DeleteBackupVaultNotifications
- DeleteFramework

- DeleteRecoveryPoint
- DeleteReportPlan
- DeleteRestoreTestingPlan
- DeleteRestoreTestingSelection
- DescribeBackupJob
- DescribeBackupVault
- DescribeCopyJob
- DescribeFramework
- DescribeGlobalSettings
- DescribeProtectedResource
- DescribeRecoveryPoint
- DescribeRegionSettings
- DescribeReportJob
- DescribeReportPlan
- DescribeRestoreJob
- DisassociateRecoveryPoint
- DisassociateRecoveryPointFromParent
- ExportBackupPlanTemplate
- GetBackupPlan
- GetBackupPlanFromJSON
- GetBackupPlanFromTemplate
- GetBackupSelection
- GetBackupVaultAccessPolicy
- GetBackupVaultNotifications
- GetLegalHold
- GetRecoveryPointRestoreMetadata
- GetRestoreJobMetadata
- GetRestoreTestingInferredMetadata
- GetRestoreTestingPlan
- GetRestoreTestingSelection

- GetSupportedResourceTypes
- ListBackupJobs
- ListBackupJobSummaries
- ListBackupPlans
- ListBackupPlanTemplates
- ListBackupPlanVersions
- ListBackupSelections
- ListBackupVaults
- ListCopyJobs
- ListCopyJobSummaries
- ListFrameworks
- ListLegalHolds
- ListProtectedResources
- ListProtectedResourcesByBackupVault
- ListRecoveryPointsByBackupVault
- ListRecoveryPointsByLegalHold
- ListRecoveryPointsByResource
- ListReportJobs
- ListReportPlans
- ListRestoreJobs
- ListRestoreJobsByProtectedResource
- ListRestoreJobSummaries
- ListRestoreTestingPlans
- ListRestoreTestingSelections
- ListTags
- PutBackupVaultAccessPolicy
- PutBackupVaultLockConfiguration
- PutBackupVaultNotifications
- PutRestoreValidationResult
- StartBackupJob

- StartCopyJob
- StartReportJob
- StartRestoreJob
- StopBackupJob
- TagResource
- UntagResource
- UpdateBackupPlan
- UpdateFramework
- UpdateGlobalSettings
- UpdateRecoveryPointLifecycle
- UpdateRegionSettings
- UpdateReportPlan
- UpdateRestoreTestingPlan
- UpdateRestoreTestingSelection

以下のアクションが AWS Backup gateway によってサポートされています。

- AssociateGatewayToServer
- CreateGateway
- DeleteGateway
- DeleteHypervisor
- DisassociateGatewayFromServer
- GetBandwidthRateLimitSchedule
- GetGateway
- GetHypervisor
- GetHypervisorPropertyMappings
- GetVirtualMachine
- ImportHypervisorConfiguration
- ListGateways
- ListHypervisors
- ListTagsForResource

- ListVirtualMachines
- PutBandwidthRateLimitSchedule
- PutHypervisorPropertyMappings
- PutMaintenanceStartTime
- StartVirtualMachinesMetadataSync
- TagResource
- TestHypervisorConfiguration
- UntagResource
- UpdateGatewayInformation
- UpdateGatewaySoftwareNow
- UpdateHypervisor

AWS Backup

以下のアクションが AWS Backup によってサポートされています。

- CancelLegalHold
- CreateBackupPlan
- CreateBackupSelection
- CreateBackupVault
- CreateFramework
- CreateLegalHold
- CreateLogicallyAirGappedBackupVault
- CreateReportPlan
- CreateRestoreTestingPlan
- CreateRestoreTestingSelection
- DeleteBackupPlan
- DeleteBackupSelection
- DeleteBackupVault
- DeleteBackupVaultAccessPolicy
- DeleteBackupVaultLockConfiguration
- DeleteBackupVaultNotifications

- DeleteFramework
- DeleteRecoveryPoint
- DeleteReportPlan
- DeleteRestoreTestingPlan
- DeleteRestoreTestingSelection
- DescribeBackupJob
- DescribeBackupVault
- DescribeCopyJob
- DescribeFramework
- DescribeGlobalSettings
- DescribeProtectedResource
- DescribeRecoveryPoint
- DescribeRegionSettings
- DescribeReportJob
- DescribeReportPlan
- DescribeRestoreJob
- DisassociateRecoveryPoint
- DisassociateRecoveryPointFromParent
- ExportBackupPlanTemplate
- GetBackupPlan
- GetBackupPlanFromJSON
- GetBackupPlanFromTemplate
- GetBackupSelection
- GetBackupVaultAccessPolicy
- GetBackupVaultNotifications
- GetLegalHold
- GetRecoveryPointRestoreMetadata
- GetRestoreJobMetadata
- GetRestoreTestingInferredMetadata
- GetRestoreTestingPlan

- GetRestoreTestingSelection
- GetSupportedResourceTypes
- ListBackupJobs
- ListBackupJobSummaries
- ListBackupPlans
- ListBackupPlanTemplates
- ListBackupPlanVersions
- ListBackupSelections
- ListBackupVaults
- ListCopyJobs
- ListCopyJobSummaries
- ListFrameworks
- ListLegalHolds
- ListProtectedResources
- ListProtectedResourcesByBackupVault
- ListRecoveryPointsByBackupVault
- ListRecoveryPointsByLegalHold
- ListRecoveryPointsByResource
- ListReportJobs
- ListReportPlans
- ListRestoreJobs
- ListRestoreJobsByProtectedResource
- ListRestoreJobSummaries
- ListRestoreTestingPlans
- ListRestoreTestingSelections
- ListTags
- PutBackupVaultAccessPolicy
- PutBackupVaultLockConfiguration
- PutBackupVaultNotifications
- PutRestoreValidationResult

- StartBackupJob
- StartCopyJob
- StartReportJob
- StartRestoreJob
- StopBackupJob
- TagResource
- UntagResource
- UpdateBackupPlan
- UpdateFramework
- UpdateGlobalSettings
- UpdateRecoveryPointLifecycle
- UpdateRegionSettings
- UpdateReportPlan
- UpdateRestoreTestingPlan
- UpdateRestoreTestingSelection

CancelLegalHold

サービス: AWS Backup

復旧ポイントで指定されたリーガルホールドを削除します。このアクションを実行できるのは、十分な権限を持つユーザーのみです。

リクエストの構文

```
DELETE /legal-holds/legalHoldId?
cancelDescription=CancelDescription&retainRecordInDays=RetainRecordInDays HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

CancelDescription

リーガルホールドを削除する理由を説明する文字列。

必須: はい

legalHoldId

リーガルホールドの ID。

必須: はい

RetainRecordInDays

リーガルホールドを削除する日数の整数量。

リクエスト本文

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 201
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 201 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

InvalidResourceStateException

AWS Backup は、この復旧ポイントで既にアクションを実行しています。最初のアクションが終了するまで、リクエストしたアクションを実行できません。後ほどもう一度試してください。」

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2

- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateBackupPlan

サービス: AWS Backup

バックアッププラン名およびバックアップルールを使用してバックアッププランを作成します。バックアッププランは、 AWS Backup がリソースのリカバリポイントを作成するタスクをスケジュールするために使用する情報を含むドキュメントです。

CreateBackupPlan すでに存在するプランで電話する場合は、AlreadyExistsException の例外を受信します。

リクエストの構文

```
PUT /backup/plans/ HTTP/1.1
Content-type: application/json

{
   "BackupPlan": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
```

```
                "OptInToArchiveForSupportedResources": boolean
            },
            "RecoveryPointTags": {
                "string" : "string"
            },
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
        }
    ]
  },
  "BackupPlanTags": {
    "string" : "string"
  },
  "CreatorRequestId": "string"
}
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

BackupPlan

バックアッププランの本文。1 つの BackupPlanName と1 つ以上の Rules のセットを含む。

型: BackupPlanInput オブジェクト

必須: はい

BackupPlanTags

バックアッププランに割り当てるタグ。

型: 文字列間のマッピング

必須: いいえ

CreatorRequestId

オペレーションを 2 回実行するリスクなしに、リクエストを識別し、失敗したリクエストを再試行できます。リクエストに既存のバックアッププランと一致する CreatorRequestId が含まれる場合、そのプランが返されます。このパラメータはオプションです。

使用する場合、このパラメータには 1 ~ 50 文字の英数字または「-_」を含める必要があります 。

タイプ: 文字列

必須: いいえ

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "AdvancedBackupSettings": [
      {
         "BackupOptions": {
            "string" : "string"
         },
         "ResourceType": "string"
      }
   ],
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "CreationDate": number,
   "VersionId": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

AdvancedBackupSettings

リソースタイプの設定。このオプションは、Windows ボリュームシャドウコピーサービス (VSS) バックアップジョブでのみ使用できます。

型: AdvancedBackupSetting オブジェクトの配列

BackupPlanArn

たとえば、arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50などのバックアップ計画を一意に識別する Amazon リソースネーム (ARN) です。

型: 文字列

BackupPlanId

バックアッププランの ID。

型: 文字列

CreationDate

バックアッププランが作成された日時 (Unix 時刻形式および協定世界時 (UTC))。CreationDateの値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

VersionId

一意のランダムに生成された UTF-8 エンコード Unicode 文字列 (最大 1,024 バイト長)。編集することはできません。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AlreadyExistsException

必要なリソースは既に存在します。

HTTP ステータスコード：400

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

LimitExceededException

たとえば、リクエストで許可されるアイテムの最大数などのリクエストの制限を超えました。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateBackupSelection

サービス: AWS Backup

バックアップ計画に割り当てる一連のリソースを指定する JSON ドキュメントを作成します。例については、「プログラムによるリソースの割り当て」を参照してください。

リクエストの構文

```
PUT /backup/plans/backupPlanId/selections/ HTTP/1.1
Content-type: application/json

{
   "BackupSelection": {
      "Conditions": {
         "StringEquals": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringLike": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringNotEquals": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringNotLike": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ]
      },
      "IamRoleArn": "string",
      "ListOfTags": [
         {
            "ConditionKey": "string",
```

```
            "ConditionType": "string",
            "ConditionValue": "string"
         }
      ],
      "NotResources": [ "string" ],
      "Resources": [ "string" ],
      "SelectionName": "string"
   },
   "CreatorRequestId": "string"
}
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

backupPlanId

バックアッププランの ID。

必須: はい

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

BackupSelection

バックアッププランに一連のリソースを割り当てるリクエストの本文。

型: BackupSelection オブジェクト

必須: はい

CreatorRequestId

オペレーションを 2 回実行するリスクなしに、失敗したリクエストを再試行できるリクエストを識別する一意の文字列。このパラメータはオプションです。

使用する場合、このパラメータには 1 ~ 50 文字の英数字または「-_」を含める必要があります 。

タイプ: 文字列

必須: いいえ

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanId": "string",
   "CreationDate": number,
   "SelectionId": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

BackupPlanId

バックアッププランの ID。

型: 文字列

CreationDate

Unix 形式および協定世界時 (UTC)でバックアップ選択が作成された日時。CreationDateの値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前 12:11:30.087 を表します。

型: タイムスタンプ

SelectionId

バックアップ計画に一連のリソースを割り当てるためのリクエストを一意に識別します。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AlreadyExistsException

必要なリソースは既に存在します。

HTTP ステータスコード：400

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

LimitExceededException

たとえば、リクエストで許可されるアイテムの最大数などのリクエストの制限を超えました。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateBackupVault

サービス: AWS Backup

バックアップを保存する論理コンテナを作成します。CreateBackupVault リクエストは、名前、1 つ以上のリソースタグ (省略可能)、暗号化キー、およびリクエスト ID を含みます。

> **Note**
>
> パスポート番号などの機密データは、バックアップボールトの名前に含めないでください。

リクエストの構文

```
PUT /backup-vaults/backupVaultName HTTP/1.1
Content-type: application/json

{
   "BackupVaultTags": {
      "string" : "string"
   },
   "CreatorRequestId": "string",
   "EncryptionKeyArn": "string"
}
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

backupVaultName

バックアップを保存する論理コンテナの名前。バックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先の AWS リージョンに一意の名前で識別されます。それらは文字、数字、およびハイフン (-) で構成されます。

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

必須: はい

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

BackupVaultTags

バックアップボールトに割り当てるタグ。

型: 文字列間のマッピング

必須: いいえ

CreatorRequestId

リクエストを識別するための一意の文字列で、失敗したリクエストを再試行する際に、オペレーションを2回実行するリスクを回避することができます。このパラメータはオプションです。

使用する場合、このパラメータには 1～50 文字の英数字または「-_」を含める必要があります 。

タイプ: 文字列

必須: いいえ

EncryptionKeyArn

たとえば、arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab などのバックアップを保護するために使用されるサーバー側の暗号化キーです。

型: 文字列

必須: いいえ

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CreationDate": number
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

BackupVaultArn

`arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`などのバックアップボールトを一意に識別する Amazon リソースネーム (ARN)。

型: 文字列

BackupVaultName

バックアップを保存する論理コンテナの名前。バックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先の リージョンに一意の名前で識別されます。それらは、小文字の英文字、数字、およびハイフン (-) で構成されます。

型: 文字列

パターン：`^[a-zA-Z0-9\-\_]{2,50}$`

CreationDate

Unix 時刻形式および協定世界時 (UTC) でバックアップボールトが作成された日付と時刻。`CreationDate`の値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AlreadyExistsException

必要なリソースは既に存在します。

HTTP ステータスコード：400

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

LimitExceededException

たとえば、リクエストで許可されるアイテムの最大数などのリクエストの制限を超えました。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateFramework

サービス: AWS Backup

1 つ以上のコントロールを持つフレームワークを作成します。フレームワークは、バックアッププラクティスを評価するために使用できるコントロールの集まりです。事前に構築されたカスタマイズ可能なコントロールを使用してポリシーを定義することで、バックアッププラクティスがポリシーに準拠しているかどうか、およびまだ準拠していないリソースを評価できます。

リクエストの構文

```
POST /audit/frameworks HTTP/1.1
Content-type: application/json

{
   "FrameworkControls": [
      {
         "ControlInputParameters": [
            {
               "ParameterName": "string",
               "ParameterValue": "string"
            }
         ],
         "ControlName": "string",
         "ControlScope": {
            "ComplianceResourceIds": [ "string" ],
            "ComplianceResourceTypes": [ "string" ],
            "Tags": {
               "string" : "string"
            }
         }
      }
   ],
   "FrameworkDescription": "string",
   "FrameworkName": "string",
   "FrameworkTags": {
      "string" : "string"
   },
   "IdempotencyToken": "string"
}
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

FrameworkControls

フレームワークを構成するコントロール。リスト内の各コントロールには、名前、入力パラメータ、およびスコープがあります。

型: FrameworkControl オブジェクトの配列

必須: はい

FrameworkDescription

最大 1,024 文字のフレームワークの任意の記述。

型: 文字列

長さの制限: 最小長は 0 です。最大長は 1,024 です。

パターン: `.*\S.*`

必須: いいえ

FrameworkName

フレームワークの一意の名前。名前は文字から始まる1～256文字で、文字 (a~z、A～Z)、数字 (0~9)、およびアンダースコア (_)により構成されます。

型: 文字列

長さの制限：最小長は 1 です。最大長は 256 です。

パターン：`[a-zA-Z][_a-zA-Z0-9]*`

必須：はい

FrameworkTags

フレームワークに割り当てるタグ。

型: 文字列間のマッピング

必須: いいえ

IdempotencyToken

別の CreateFrameworkInput への同じコール間を区別するために使用できる顧客が選択した文字列。同じ冪等性トークンで成功したリクエストを再試行すると、アクションは実行されず、成功メッセージが表示されます。

タイプ: 文字列

必須: いいえ

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "FrameworkArn": "string",
   "FrameworkName": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

FrameworkArn

リソースを一意に識別する Amazon リソースネーム (ARN)。ARN の形式は、リソースタイプによって異なります。

型: 文字列

FrameworkName

フレームワークの一意の名前。名前は文字から始まる1～256文字で、文字 (a~z、A～Z)、数字 (0~9)、およびアンダースコア (_)により構成されます。

型: 文字列

長さの制限：最小長は 1 です。最大長は 256 です。

パターン：[a-zA-Z][_a-zA-Z0-9]*

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AlreadyExistsException

必要なリソースは既に存在します。

HTTP ステータスコード：400

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

LimitExceededException

たとえば、リクエストで許可されるアイテムの最大数などのリクエストの制限を超えました。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2

- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateLegalHold

サービス: AWS Backup

復旧ポイント (バックアップ) にリーガルホールドを作成します。リーガルホールドとは、権限のあるユーザーがリーガルホールドをキャンセルするまでの間の、バックアップの変更または削除の制限です。復旧ポイントに 1 つ以上の有効なリーガルホールドがある場合、復旧ポイントを削除するまたは関連付けを解除する操作はすべてエラーで失敗します。

リクエストの構文

```
POST /legal-holds/ HTTP/1.1
Content-type: application/json

{
   "Description": "string",
   "IdempotencyToken": "string",
   "RecoveryPointSelection": {
      "DateRange": {
         "FromDate": number,
         "ToDate": number
      },
      "ResourceIdentifiers": [ "string" ],
      "VaultNames": [ "string" ]
   },
   "Tags": {
      "string" : "string"
   },
   "Title": "string"
}
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

Description

リーガルホールドの説明。

型: 文字列

必須: はい

IdempotencyToken

別の、同じコール間を区別するために使用される、ユーザーが選択した文字列。同じ冪等性トークンで成功したリクエストを再試行すると、アクションは実行されず、成功メッセージが表示されます。

タイプ: 文字列

必須: いいえ

RecoveryPointSelection

リソースタイプやバックアップボールトなど、一連のリソースを割り当てる基準。

タイプ：RecoveryPointSelection オブジェクト

必須: いいえ

Tags

追加するタグは任意です。タグは、リソースの管理、フィルタリング、検索に使用できるキーと値のペアです。使用可能な文字は、UTF-8の文字、数字、スペース、および以下の文字です。+ - = . _ : /。

型: 文字列間のマッピング

必須: いいえ

Title

リーガルホールドのタイトル。

型: 文字列

必須: はい

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
```

```
   "CreationDate": number,
   "Description": "string",
   "LegalHoldArn": "string",
   "LegalHoldId": "string",
   "RecoveryPointSelection": {
      "DateRange": {
         "FromDate": number,
         "ToDate": number
      },
      "ResourceIdentifiers": [ "string" ],
      "VaultNames": [ "string" ]
   },
   "Status": "string",
   "Title": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

CreationDate

リーガルホールドが作成された時刻。

型: タイムスタンプ

Description

リーガルホールドの説明。

型: 文字列

LegalHoldArn

リーガルホールドの Amazon リソースネーム (ARN)。

型: 文字列

LegalHoldId

リーガルホールドの ID。

型: 文字列

RecoveryPointSelection

リソースタイプやバックアップボールトなど、一連のリソースに割り当てる基準。

タイプ：RecoveryPointSelection オブジェクト

Status

リーガルホールドのステータス。

型: 文字列

有効な値：CREATING | ACTIVE | CANCELING | CANCELED

Title

リーガルホールドのタイトル。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

LimitExceededException

たとえば、リクエストで許可されるアイテムの最大数などのリクエストの制限を超えました。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateLogicallyAirGappedBackupVault

サービス: AWS Backup

バックアップをコピーできる論理コンテナを作成します。

このリクエストには、名前、リージョン、最大保持日数、最小保持日数が含まれます。また、オプションでタグと作成者リクエスト ID を含めることができます。

> **Note**
>
> パスポート番号などの機密データは、バックアップボールトの名前に含めないでください。

リクエストの構文

```
PUT /logically-air-gapped-backup-vaults/backupVaultName HTTP/1.1
Content-type: application/json

{
   "BackupVaultTags": {
      "string" : "string"
   },
   "CreatorRequestId": "string",
   "MaxRetentionDays": number,
   "MinRetentionDays": number
}
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

backupVaultName

バックアップを保存する論理コンテナの名前。論理的にエアギャップのあるバックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先のリージョンに一意の名前で識別されます。

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

必須: はい

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

BackupVaultTags

ボールトに割り当てるタグ。

型: 文字列間のマッピング

必須: いいえ

CreatorRequestId

作成リクエストの ID。

このパラメータはオプションです。使用する場合、このパラメータには 1～50 文字の英数字または「-_」を含める必要があります 。

タイプ: 文字列

必須: いいえ

MaxRetentionDays

ボールトが復旧ポイントを保持する最大保持期間。このパラメータを指定しない場合、 AWS Backup はボールト内の復旧ポイントに最大保持期間を強制しません (無期限ストレージを許可)。

指定した場合、ボールトへのバックアップジョブもしくはコピージョブには、保存期間が最大保存期間と同等もしくは以下のライフサイクル· ポリシーを持つ必要があります。ジョブの保持期間がその最大保持期間よりも長い場合、ボールトはバックアップジョブもしくはコピージョブに失敗するため、ライフサイクル設定を変更するか、別のボールトを使用する必要があります。

タイプ: Long

必須: はい

MinRetentionDays

この設定は、ボールトが復旧ポイントを保持する最小保持期間を指定します。このパラメータを指定しない場合、最小保持期間が強制されません。

指定した場合、ボールトへのバックアップジョブまたはコピージョブには、最小保存期間以上の保存期間を持つライフサイクルポリシーが必要です。ジョブの保持期間がその最小保持期間より

短い場合、ボールトはバックアップジョブまたはコピージョブに失敗するため、ライフサイクル設定を変更するか、別のボールトを使用する必要があります。

タイプ: Long

必須: はい

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CreationDate": number,
   "VaultState": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

BackupVaultArn

ボールトの ARN (Amazon リソースネーム) 。

型: 文字列

BackupVaultName

バックアップを保存する論理コンテナの名前。論理的に工アギャップのあるバックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先のリージョンに一意の名前で識別されます。

型: 文字列

パターン：`^[a-zA-Z0-9\-\_]{2,50}$`

CreationDate

ボールドが作成された日時。

この値は、Unix 形式、協定世界時 (UTC) 、ミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

VaultState

ボールトの現在の状態。

型: 文字列

有効な値：CREATING | AVAILABLE | FAILED

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AlreadyExistsException

必要なリソースは既に存在します。

HTTP ステータスコード：400

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

InvalidRequestException

リクエストへの入力に何らかの問題が発生していることを示します。たとえば、パラメータのタイプが間違っています。

HTTP ステータスコード：400

LimitExceededException

たとえば、リクエストで許可されるアイテムの最大数などのリクエストの制限を超えました。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateReportPlan

サービス: AWS Backup

レポート計画を作成します。レポートプランは、レポートの内容と がレポートを提供する場所に関する情報を含むドキュメント AWS Backup です。

CreateReportPlan すでに存在するプランで電話する場合は、AlreadyExistsException の例外を受信します。

リクエストの構文

```
POST /audit/report-plans HTTP/1.1
Content-type: application/json

{
   "IdempotencyToken": "string",
   "ReportDeliveryChannel": {
      "Formats": [ "string" ],
      "S3BucketName": "string",
      "S3KeyPrefix": "string"
   },
   "ReportPlanDescription": "string",
   "ReportPlanName": "string",
   "ReportPlanTags": {
      "string" : "string"
   },
   "ReportSetting": {
      "Accounts": [ "string" ],
      "FrameworkArns": [ "string" ],
      "NumberOfFrameworks": number,
      "OrganizationUnits": [ "string" ],
      "Regions": [ "string" ],
      "ReportTemplate": "string"
   }
}
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

IdempotencyToken

別の CreateReportPlanInput への同じコール間を区別するために使用できる顧客が選択した文字列。同じ冪等性トークンで成功したリクエストを再試行すると、アクションは実行されず、成功メッセージが表示されます。

タイプ: 文字列

必須: いいえ

ReportDeliveryChannel

レポートを配信する場所および方法について。特に Amazon S3 バケット名、S3 key prefix、レポートの形式に関する情報を含む構造。

型: ReportDeliveryChannel オブジェクト

必須: はい

ReportPlanDescription

最大 1,024 文字までのレポートプランの任意の記述。

型: 文字列

長さの制限: 最小長は 0 です。最大長は 1,024 です。

パターン: .*\S.*

必須: いいえ

ReportPlanName

レポートプランの一意の名前。名前は文字から始まる1～256文字で、文字 (a~z、A～Z)、数字 (0~9)、およびアンダースコア (_)により構成されます。

型: 文字列

長さの制限：最小長は 1 です。最大長は 256 です。

パターン：[a-zA-Z][_a-zA-Z0-9]*

必須：はい

ReportPlanTags

レポートプランに割り当てるタグ。

型: 文字列間のマッピング

必須: いいえ

ReportSetting

レポートのレポートテンプレートを識別します。レポートは、レポートテンプレートを使用して構築されます。レポートテンプレートは次のとおりです。

RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT

レポートテンプレートが RESOURCE_COMPLIANCE_REPORTまたは の場合CONTROL_COMPLIANCE_REPORT、この API リソースは AWS リージョン および フレームワークによるレポートカバレッジも記述します。

型: ReportSetting オブジェクト

必須: はい

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "ReportPlanArn": "string",
   "ReportPlanName": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

CreationTime

Unix 時刻形式および協定世界時 (UTC)でのバックアップボールトが作成された日時。CreationTimeの値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

ReportPlanArn

リソースを一意に識別する Amazon リソースネーム (ARN)。ARN の形式は、リソースタイプによって異なります。

型: 文字列

ReportPlanName

レポートプランの一意の名前。

型: 文字列

長さの制限：最小長は 1 です。最大長は 256 です。

パターン：`[a-zA-Z][_a-zA-Z0-9]*`

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AlreadyExistsException

必要なリソースは既に存在します。

HTTP ステータスコード：400

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

LimitExceededException

たとえば、リクエストで許可されるアイテムの最大数などのリクエストの制限を超えました。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateRestoreTestingPlan

サービス: AWS Backup

復元テストプランを作成します。

復元テストプランを作成するための 2 つのステップのうち最初のステップ。このリクエストが成功したら、 を使用して手順を完了します CreateRestoreTestingSelection。

リクエストの構文

```
PUT /restore-testing/plans HTTP/1.1
Content-type: application/json

{
   "CreatorRequestId": "string",
   "RestoreTestingPlan": {
      "RecoveryPointSelection": {
         "Algorithm": "string",
         "ExcludeVaults": [ "string" ],
         "IncludeVaults": [ "string" ],
         "RecoveryPointTypes": [ "string" ],
         "SelectionWindowDays": number
      },
      "RestoreTestingPlanName": "string",
      "ScheduleExpression": "string",
      "ScheduleExpressionTimezone": "string",
      "StartWindowHours": number
   },
   "Tags": {
      "string" : "string"
   }
}
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

CreatorRequestId

リクエストを識別するための一意の文字列で、失敗したリクエストを再試行する際に、オペレーションを 2 回実行するリスクを回避することができます。このパラメータはオプションです。使用する場合、このパラメータには 1～50 文字の英数字または「-_」を含める必要があります 。

タイプ: 文字列

必須: いいえ

RestoreTestingPlan

復元テストプランには、作成した一意の RestoreTestingPlanName 文字列と ScheduleExpression cron を含める必要があります。オプションで StartWindowHours 整数と CreatorRequestId 文字列を含めることができます。

RestoreTestingPlanName は復元テストプランの名前を表す一意の文字列です。これは作成後に変更できず、英数字とアンダースコアのみで構成されている必要があります。

型: RestoreTestingPlanForCreate オブジェクト

必須: はい

Tags

復元テストプランに割り当てるタグ。

型: 文字列間のマッピング

必須: いいえ

レスポンスの構文

```
HTTP/1.1 201
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string"
}
```

レスポンス要素

アクションが成功すると、HTTP 201 レスポンスが返されます。

サービスから以下のデータが JSON 形式で返されます。

CreationTime

復元テストプランが作成された日時を Unix 形式、および協定世界時 (UTC) で表しています。CreationTime の値は、ミリ秒単位の精度です。例えば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前 12:11:30.087 を表します。

型: タイムスタンプ

RestoreTestingPlanArn

作成された復元テストプランを一意に識別する Amazon リソースネーム (ARN) です。

型: 文字列

RestoreTestingPlanName

この一意の文字列は復元テストプランの名前です。

作成後にこの名前を変更することはできません。名前には英数字とアンダースコアのみを使用できます。最大長は 50 文字です。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AlreadyExistsException

必要なリソースは既に存在します。

HTTP ステータスコード：400

ConflictException

AWS Backup は、前のアクションの実行が完了するまで、リクエストしたアクションを実行できません。後ほどもう一度試してください。」

HTTP ステータスコード：400

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

LimitExceededException

たとえば、リクエストで許可されるアイテムの最大数などのリクエストの制限を超えました。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateRestoreTestingSelection

サービス: AWS Backup

このリクエストは、 CreateRestoreTestingPlan リクエストが正常に返された後に送信できます。これはリソーステスト計画の作成の 2 番目のステップで、順番に完了する必要があります。

これは、RestoreTestingSelectionName、ProtectedResourceType と、以下のいずれかで構成されます。

- ProtectedResourceArns
- ProtectedResourceConditions

保護対象リソースのタイプごとに値を 1 つ設定できます。

復元テスト選択には、ProtectedResourceArns のワイルドカード値 (「*」) を ProtectedResourceConditions と併せて含めることができます。または、ProtectedResourceArns に保護対象リソースの ARN を最大 30 個まで含めることもできます。

保護対象リソースのタイプと特定の ARN の両方で選択することはできません。両方が含まれている場合、リクエストは失敗します。

リクエストの構文

```
PUT /restore-testing/plans/RestoreTestingPlanName/selections HTTP/1.1
Content-type: application/json

{
   "CreatorRequestId": "string",
   "RestoreTestingSelection": {
      "IamRoleArn": "string",
      "ProtectedResourceArns": [ "string" ],
      "ProtectedResourceConditions": {
         "StringEquals": [
            {
               "Key": "string",
               "Value": "string"
            }
         ],
         "StringNotEquals": [
            {
```

```
                "Key": "string",
                "Value": "string"
            }
         ]
      },
      "ProtectedResourceType": "string",
      "RestoreMetadataOverrides": {
         "string" : "string"
      },
      "RestoreTestingSelectionName": "string",
      "ValidationWindowHours": number
   }
}
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

RestoreTestingPlanName

関連する CreateRestoreTestingPlan リクエストから返された復元テストプラン名を入力します。

必須: はい

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

CreatorRequestId

リクエストを識別するための一意の文字列 (オプション) で、失敗したリクエストを再試行する際に、オペレーションを 2 回実行するリスクを回避することができます。使用する場合、このパラメータには 1～50 文字の英数字または「-_」を含める必要があります 。

タイプ: 文字列

必須: いいえ

RestoreTestingSelection

これは、RestoreTestingSelectionName、ProtectedResourceType と、以下のいずれかで構成されます。

- ProtectedResourceArns

- ProtectedResourceConditions

保護対象リソースのタイプごとに値を 1 つ設定できます。

復元テスト選択には、ProtectedResourceArns のワイルドカード値 (「*」) を ProtectedResourceConditions と併せて含めることができます。または、ProtectedResourceArns に保護対象リソースの ARN を最大 30 個まで含めることもできます。

型: RestoreTestingSelectionForCreate オブジェクト

必須: はい

レスポンスの構文

```
HTTP/1.1 201
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
   "RestoreTestingSelectionName": "string"
}
```

レスポンス要素

アクションが成功すると、HTTP 201 レスポンスが返されます。

サービスから以下のデータが JSON 形式で返されます。

CreationTime

リソーステスト選択が作成された時刻。

型: タイムスタンプ

RestoreTestingPlanArn

復元テスト選択が関連付けられている復元テストプランの ARN。

型: 文字列

RestoreTestingPlanName

復元テストプランの名前。

作成後にこの名前を変更することはできません。名前には英数字とアンダースコアのみを使用できます。最大長は 50 文字です。

型: 文字列

RestoreTestingSelectionName

関連する復元テストプランの復元テスト選択の名前。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AlreadyExistsException

必要なリソースは既に存在します。

HTTP ステータスコード：400

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

LimitExceededException

たとえば、リクエストで許可されるアイテムの最大数などのリクエストの制限を超えました。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteBackupPlan

サービス: AWS Backup

バックアッププランを削除します。バックアッププランは、関連付けられた選択リソースがすべて削除された後に削除できます。バックアッププランを削除すると、バックアッププランの現在のバージョンが削除されます。以前のバージョン (存在する場合) は引き続き存在します。

リクエストの構文

```
DELETE /backup/plans/backupPlanId HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

backupPlanId

バックアップ計画を一意に識別します。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "DeletionDate": number,
   "VersionId": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

BackupPlanArn

たとえば、arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50などのバックアップ計画を一意に識別する Amazon リソースネーム (ARN) です。

型: 文字列

BackupPlanId

バックアップ計画を一意に識別します。

型: 文字列

DeletionDate

Unix 形式および協定世界時 (UTC)でバックアップ計画が削除される日時。DeletionDateの値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前 12:11:30.087 を表します。

型: タイムスタンプ

VersionId

一意のランダムに生成された UTF-8 エンコード Unicode 文字列 (最大 1,024 バイト長)。バージョン ID を編集することはできません。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

InvalidRequestException

リクエストへの入力に何らかの問題が発生していることを示します。たとえば、パラメータのタイプが間違っています。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteBackupSelection

サービス: AWS Backup

SelectionId で指定されたバックアッププランに関連付けられているリソース選択を削除します。

リクエストの構文

```
DELETE /backup/plans/backupPlanId/selections/selectionId HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

backupPlanId

バックアップ計画を一意に識別します。

必須: はい

selectionId

バックアップ計画に一連のリソースを割り当てるためのリクエストの本文を一意に識別します。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteBackupVault

サービス: AWS Backup

名前で識別されるバックアップボールトを削除します。ボールトは、空である場合に限り、削除できます。

リクエストの構文

```
DELETE /backup-vaults/backupVaultName HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

backupVaultName

バックアップを保存する論理コンテナの名前。バックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先の AWS リージョンに一意の名前で識別されます。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

InvalidRequestException

リクエストへの入力に何らかの問題が発生していることを示します。たとえば、パラメータのタイプが間違っています。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteBackupVaultAccessPolicy

サービス: AWS Backup

バックアップボールトの権限を管理するポリシードキュメントを削除します。

リクエストの構文

```
DELETE /backup-vaults/backupVaultName/access-policy HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

backupVaultName

バックアップを保存する論理コンテナの名前。バックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先の AWS リージョンに一意の名前で識別されます。それらは、小文字の英文字、数字、およびハイフン (-) で構成されます。

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteBackupVaultLockConfiguration

サービス: AWS Backup

バックアップボールト名で指定されたバックアップボールトからボールト AWS Backup ロックを削除します。

ボールトロックの設定が不変の場合、API オペレーションを使用してボールトロックを削除することはできず、それを試みると `InvalidRequestException` を受信します。詳細については、「AWS Backup デベロッパーガイド」の「ボールトロック」を参照してください。

リクエストの構文

```
DELETE /backup-vaults/backupVaultName/vault-lock HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

backupVaultName

ボールトロックを削除するバックアップ AWS Backup ボールトの名前。

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

InvalidRequestException

リクエストへの入力に何らかの問題が発生していることを示します。たとえば、パラメータのタイプが間違っています。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3

- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteBackupVaultNotifications

サービス: AWS Backup

指定されたバックアップボールトのイベント通知を削除します。

リクエストの構文

```
DELETE /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

backupVaultName

バックアップを保存する論理コンテナの名前。バックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先の リージョンに一意の名前で識別されます。

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteFramework

サービス: AWS Backup

フレームワーク名で指定されたフレームワークを削除します。

リクエストの構文

```
DELETE /audit/frameworks/frameworkName HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

frameworkName

フレームワークの一意の名前。

長さの制限：最小長は 1 です。最大長は 256 です。

パターン：[a-zA-Z][_a-zA-Z0-9]*

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

ConflictException

AWS Backup は、前のアクションの実行が完了するまで、リクエストしたアクションを実行できません。後ほどもう一度試してください。」

HTTP ステータスコード：400

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteRecoveryPoint

サービス: AWS Backup

リカバリポイント ID で指定されたリカバリポイントを削除します。

リカバリポイント ID が連続バックアップに属している場合、このエンドポイントを呼び出すと、既存の連続バックアップが削除され、今後の継続バックアップが停止します。

IAM ロールのアクセス許可がこの API を呼び出すのに不十分な場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを送り返しますが、復旧ポイントは削除されません。代わりに、EXPIRED 状態に入ります。

IAM ロールに `iam:CreateServiceLinkedRole` アクションが適用されたら、この API を使用して EXPIRED 復旧ポイントを削除できます。このロールの追加について詳しくは、「手動削除のトラブルシューティング」を参照してください。

ユーザーまたはロールが削除されるか、ロール内のアクセス許可が削除されると、削除は成功せず、EXPIRED 状態になります。

リクエストの構文

```
DELETE /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

backupVaultName

バックアップを保存する論理コンテナの名前。バックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先の AWS リージョンに一意の名前で識別されます。

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

必須：はい

recoveryPointArn

`arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`などのリカバリポイントを一意に識別する Amazon リソースネーム (ARN) です。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

InvalidRequestException

リクエストへの入力に何らかの問題が発生していることを示します。たとえば、パラメータのタイプが間違っています。

HTTP ステータスコード：400

InvalidResourceStateException

AWS Backup は、この復旧ポイントで既にアクションを実行しています。最初のアクションが終了するまで、リクエストしたアクションを実行できません。後ほどもう一度試してください。」

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteReportPlan

サービス: AWS Backup

レポートプラン名で指定されたレポートプランを削除します。

リクエストの構文

```
DELETE /audit/report-plans/reportPlanName HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

reportPlanName

レポートプランの一意の名前。

長さの制限：最小長は 1 です。最大長は 256 です。

パターン：`[a-zA-Z][_a-zA-Z0-9]*`

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

ConflictException

AWS Backup は、前のアクションの実行が完了するまで、リクエストしたアクションを実行できません。後ほどもう一度試してください。」

HTTP ステータスコード：400

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteRestoreTestingPlan

サービス: AWS Backup

このリクエストは、指定された復元テストプランを削除します。

削除は、関連するすべての復元テスト選択を最初に削除した場合にのみ正常に行われます。

リクエストの構文

```
DELETE /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

RestoreTestingPlanName

削除する復元テストプランの一意の名前 (必須) です。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 204
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 204 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidRequestException

リクエストへの入力に何らかの問題が発生していることを示します。たとえば、パラメータのタイプが間違っています。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteRestoreTestingSelection

サービス: AWS Backup

復元テストプラン名と復元テスト選択名を入力します。

復元テストプランを削除する前に、復元テストプランに関連するすべてのテスト選択を削除する必要があります。

リクエストの構文

```
DELETE /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

RestoreTestingPlanName

削除する復元テスト選択を含む復元テストプランの一意の名前 (必須) です。

必須: はい

RestoreTestingSelectionName

削除する復元テスト選択の一意の名前 (必須) です。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 204
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 204 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeBackupJob

サービス: AWS Backup

指定された BackupJobId のバックアップジョブの詳細を返します。

リクエストの構文

```
GET /backup-jobs/backupJobId HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

backupJobId

リソースをバックアップ AWS Backup する へのリクエストを一意に識別します。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "AccountId": "string",
   "BackupJobId": "string",
   "BackupOptions": {
      "string" : "string"
   },
   "BackupSizeInBytes": number,
   "BackupType": "string",
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "BytesTransferred": number,
   "ChildJobsInState": {
      "string" : number
   },
```

```
   "CompletionDate": number,
   "CreatedBy": {
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
      "BackupPlanVersion": "string",
      "BackupRuleId": "string"
   },
   "CreationDate": number,
   "ExpectedCompletionDate": number,
   "IamRoleArn": "string",
   "InitiationDate": number,
   "IsParent": boolean,
   "MessageCategory": "string",
   "NumberOfChildJobs": number,
   "ParentJobId": "string",
   "PercentDone": "string",
   "RecoveryPointArn": "string",
   "ResourceArn": "string",
   "ResourceName": "string",
   "ResourceType": "string",
   "StartBy": number,
   "State": "string",
   "StatusMessage": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

AccountId

バックアップジョブを所有するアカウント ID を返します。

型: 文字列

パターン：^[0-9]{12}$

BackupJobId

リソースをバックアップ AWS Backup する へのリクエストを一意に識別します。

型: 文字列

BackupOptions

バックアッププランまたはオンデマンドバックアップジョブの一部として指定されたオプションを表します。

型: 文字列から文字列へのマッピング

キーパターン: ^[a-zA-Z0-9\-_\.]{1,50}$

値パターン:^[a-zA-Z0-9\-_\.]{1,50}$

BackupSizeInBytes

バックアップのサイズ (バイト単位)。

型: 長整数

BackupType

バックアップジョブに対して選択された実際のバックアップタイプを表します。たとえば、Windows ボリュームシャドウコピーサービス (VSS) バックアップが正常に実行された場合、BackupType は "WindowsVSS" を返します。BackupTypeが空の場合、バックアップタイプは通常のバックアップでした。

型: 文字列

BackupVaultArn

arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVaultなどのバックアップボールトを一意に識別する Amazon リソースネーム (ARN)。

型: 文字列

BackupVaultName

バックアップを保存する論理コンテナの名前。バックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先の AWS リージョンに一意の名前で識別されます。

型: 文字列

パターン：^[a-zA-Z0-9\-_]{2,50}$

BytesTransferred

ジョブステータスの照会時にバックアップボールトに転送されたバイト単位のサイズ。

型: 長整数

ChildJobsInState

これにより、含まれている子 (ネストされた) バックアップジョブの統計が返されます。

タイプ: 文字列を long にマッピング

有効なキー: CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL

CompletionDate

Unix 形式および協定世界時 (UTC)で、バックアップジョブを作成するジョブが完了した日時。CompletionDateの値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

CreatedBy

バックアップジョブの作成のために使用されるバックアッププランのBackupPlanArn、BackupPlanId、BackupPlanVersion、およびBackupRuleIdを含むバックアップジョブの作成に関する識別情報が含まれます。

タイプ：RecoveryPointCreator オブジェクト

CreationDate

Unix 時刻形式および協定世界時 (UTC)で、バックアップジョブが作成された日時。CreationDateの値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

ExpectedCompletionDate

Unix 形式および協定世界時 (UTC)で、リソースをバックアップするジョブが完了すると予想される日時 。ExpectedCompletionDateの値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

IamRoleArn

たとえば、arn:aws:iam::123456789012:role/S3Accessなどのターゲットリカバリポイントの作成に使用する IAM ロール ARN を指定します。

型: 文字列

InitiationDate

バックアップジョブが開始された日付。

型: タイムスタンプ

IsParent

これにより、バックアップジョブが親 (複合) ジョブであることを示すブール値が返されます。

型: ブール値

MessageCategory

指定されたメッセージカテゴリのジョブ数。

文字列の例としては AccessDenied、SUCCESS、AGGREGATE_ALL、および INVALIDPARAMETERS があります。受け入れられた MessageCategory 文字列のリストのモニタリングを表示します。

型: 文字列

NumberOfChildJobs

これにより、子 (ネストされた) バックアップジョブの数が返されます。

型: 長整数

ParentJobId

これにより、親 (複合) リソースのバックアップジョブ ID が返されます。

型: 文字列

PercentDone

ジョブのステータスが照会された時点でジョブが完了した推定パーセンテージが含まれます。

型: 文字列

RecoveryPointArn

たとえば、arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45などのリカバリポイントを一意に識別する ARN。

型: 文字列

ResourceArn

保存済みのリソースを一意に識別する ARN。ARN の形式は、リソースタイプによって異なります。

型: 文字列

ResourceName

指定されたバックアップに属するリソースの一意でない名前。

型: 文字列

ResourceType

バックアップする AWS リソースのタイプ。Amazon Elastic Block Store (Amazon EBS) ボリュームや Amazon Relational Database Service (Amazon RDS) データベースなど。

型: 文字列

パターン：`^[a-zA-Z0-9\-\_\.]{1,50}$`

StartBy

バックアップジョブがキャンセルされる前に開始する必要がある時刻を Unix 形式および協定世界時 (UTC) で指定します。この値は、スケジュールされた時刻に開始ウィンドウを追加して計算されます。そのため、予定時刻が午後6時でスタートウィンドウが2時間であれば、`StartBy`時刻は指定された日付の午後 8:00 になります。`StartBy`の値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

State

バックアップジョブの現在の状態です。

型: 文字列

有効な値：`CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

StatusMessage

リソースをバックアップするジョブのステータスを説明する詳細なメッセージ。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

DependencyFailureException

依存 AWS するサービスまたはリソースが AWS Backup サービスにエラーを返し、アクションを完了できません。

HTTP ステータスコード：500

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeBackupVault

サービス: AWS Backup

名前で指定されたバックアップボールトに関するメタデータを返します。

リクエストの構文

```
GET /backup-vaults/backupVaultName?backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

BackupVaultAccountId

指定されたバックアップボールトのアカウント ID。

backupVaultName

バックアップを保存する論理コンテナの名前。バックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先の AWS リージョンに一意の名前で識別されます。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CreationDate": number,
   "CreatorRequestId": "string",
   "EncryptionKeyArn": "string",
   "LockDate": number,
   "Locked": boolean,
   "MaxRetentionDays": number,
   "MinRetentionDays": number,
```

```
    "NumberOfRecoveryPoints": number,
    "VaultType": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

BackupVaultArn

arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVaultなどのバックアップボールトを一意に識別する Amazon リソースネーム (ARN)。

型: 文字列

BackupVaultName

バックアップを保存する論理コンテナの名前。バックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先の リージョンに一意の名前で識別されます。

型: 文字列

CreationDate

Unix 時刻形式および協定世界時 (UTC)で、バックアップボールトが作成された日時。CreationDateの値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

CreatorRequestId

リクエストを識別するための一意の文字列で、失敗したリクエストを再試行する際に、オペレーションを2回実行するリスクを回避することができます。このパラメータはオプションです。使用する場合、このパラメータには 1～50 文字の英数字または「-_」を含める必要があります 。

型: 文字列

EncryptionKeyArn

たとえば、arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab などのバックアップを保護するために使用されるサーバー側の暗号化キーです。

型: 文字列

LockDate

AWS Backup ボールトロック設定を変更または削除できない日時。

ロック日を指定せずにボールトロックをボールトに適用した場合は、いつでもボールトロックの設定を変更したり、ボールトからボールトロックを完全に削除したりできます。

この値は、Unix 形式および協定世界時 (UTC)で、ミリ秒まで正確です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

Locked

AWS Backup ボールトロックが現在バックアップボールトを保護しているかどうかを示すブール値。 は、ボールトロックがボールトに保存されている復旧ポイントの削除または更新オペレーションを失敗させるTrueことを意味します。

型: ブール値

MaxRetentionDays

AWS Backup ボールトが復旧ポイントを保持する最大保持期間を指定するボールトロック設定。このパラメータを指定しない場合、Vault Lock はボールト内のリカバリポイントに最大保持期間を強制しません (無期限ストレージを許可)。

指定した場合、ボールトへのバックアップジョブもしくはコピージョブには、保存期間が最大保存期間と同等もしくは以下のライフサイクル・ポリシーを持つ必要があります。ジョブの保持期間がその最大保存期間よりも長い場合、ボールトはバックアップジョブもしくはコピージョブに失敗するため、ライフサイクル設定を変更するか、別のボールトを使用する必要があります。ボールトロックの前にボールトにすでに格納されているリカバリポイントは影響を受けません。

型: 長整数

MinRetentionDays

AWS Backup ボールトが復旧ポイントを保持する最小保持期間を指定するボールトロック設定。このパラメータを指定しない場合、ボールトロックは最小保持期間を強制しません。

指定した場合、ボールトへのバックアップジョブまたはコピージョブには、最小保存期間以上の保存期間を持つライフサイクルポリシーが必要です。ジョブの保持期間がその最小保存期間より短い場合、ボールトはバックアップジョブまたはコピージョブに失敗するため、ライフサイクル

設定を変更するか、別のボールトを使用する必要があります。ボールトロックの前にボールトにすでに格納されているリカバリポイントは影響を受けません。

型: 長整数

NumberOfRecoveryPoints

バックアップボールトに保存されている復旧ポイントの数。

型: 長整数

VaultType

説明されているボールトのタイプ。

型: 文字列

有効な値：BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeCopyJob

サービス: AWS Backup

リソースのコピーの作成に関連するメタデータを返します。

リクエストの構文

```
GET /copy-jobs/copyJobId HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

copyJobId

コピージョブを一意に識別する。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "CopyJob": {
      "AccountId": "string",
      "BackupSizeInBytes": number,
      "ChildJobsInState": {
         "string" : number
      },
      "CompletionDate": number,
      "CompositeMemberIdentifier": "string",
      "CopyJobId": "string",
      "CreatedBy": {
         "BackupPlanArn": "string",
         "BackupPlanId": "string",
         "BackupPlanVersion": "string",
         "BackupRuleId": "string"
```

```
      },
      "CreationDate": number,
      "DestinationBackupVaultArn": "string",
      "DestinationRecoveryPointArn": "string",
      "IamRoleArn": "string",
      "IsParent": boolean,
      "MessageCategory": "string",
      "NumberOfChildJobs": number,
      "ParentJobId": "string",
      "ResourceArn": "string",
      "ResourceName": "string",
      "ResourceType": "string",
      "SourceBackupVaultArn": "string",
      "SourceRecoveryPointArn": "string",
      "State": "string",
      "StatusMessage": "string"
   }
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

CopyJob

コピージョブに関する詳細情報が含まれています。

型: CopyJob オブジェクト

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeFramework

サービス: AWS Backup

指定された FrameworkName のフレームワークの詳細を返します。

リクエストの構文

```
GET /audit/frameworks/frameworkName HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

frameworkName

フレームワークの一意の名前。

長さの制限：最小長は 1 です。最大長は 256 です。

パターン：[a-zA-Z][_a-zA-Z0-9]*

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "DeploymentStatus": "string",
   "FrameworkArn": "string",
   "FrameworkControls": [
      {
         "ControlInputParameters": [
            {
               "ParameterName": "string",
               "ParameterValue": "string"
            }
```

```
         ],
         "ControlName": "string",
         "ControlScope": {
            "ComplianceResourceIds": [ "string" ],
            "ComplianceResourceTypes": [ "string" ],
            "Tags": {
               "string" : "string"
            }
         }
      }
   ],
   "FrameworkDescription": "string",
   "FrameworkName": "string",
   "FrameworkStatus": "string",
   "IdempotencyToken": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

CreationTime

フレームワークが作成された日付と時刻を ISO 8601 で表したものです。CreationTime の値は、ミリ秒単位の精度です。例えば、2020-07-10T15:00:00.000-08:00 は 2020 年 7 月 10 日午後 3 時 (UTC から 8 時間遅れ) を表します。

型: タイムスタンプ

DeploymentStatus

フレームワークのデプロイステータス。ステータスは次のとおりです。

CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED | FAILED

型: 文字列

FrameworkArn

リソースを一意に識別する Amazon リソースネーム (ARN)。ARN の形式は、リソースタイプによって異なります。

型: 文字列

FrameworkControls

フレームワークを構成するコントロール。リスト内の各コントロールには、名前、入力パラメータ、およびスコープがあります。

型: FrameworkControl オブジェクトの配列

FrameworkDescription

フレームワークの説明 (省略可能)。

型: 文字列

長さの制限: 最小長は 0 です。最大長は 1,024 です。

パターン: `.*\S.*`

FrameworkName

フレームワークの一意の名前。

型: 文字列

長さの制限：最小長は 1 です。最大長は 256 です。

パターン：`[a-zA-Z][_a-zA-Z0-9]*`

FrameworkStatus

フレームワークは、1 つ以上のコントロールで構成されます。各コントロールは、バックアッププラン、バックアップ選択、バックアップボールト、復旧ポイントなどのリソースを管理します。また、各リソースの AWS Config 録音をオンまたはオフに切り替えることもできます。ステータスは次のとおりです。

- `ACTIVE`フレームワークによって管理されるすべてのリソースで記録が有効になっている場合。
- `PARTIALLY_ACTIVE`フレームワークによって管理されている少なくとも 1 つのリソースについて記録がオフになっている場合。
- `INACTIVE`フレームワークによって管理されるすべてのリソースで記録がオフになっている場合。
- `UNAVAILABLE` 現時点で AWS Backup が記録ステータスを検証できない場合。

型: 文字列

IdempotencyToken

別の DescribeFrameworkOutput への同じコール間を区別するために使用できる顧客が選択した文字列。同じ冪等性トークンで成功したリクエストを再試行すると、アクションは実行されず、成功メッセージが表示されます。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeGlobalSettings

サービス: AWS Backup

AWS アカウントがクロスアカウントバックアップにオプトインされているかどうかを記述します。アカウントが組織のメンバーでない場合、エラーを返します。例: `describe-global-settings --region us-west-2`

リクエストの構文

```
GET /global-settings HTTP/1.1
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "GlobalSettings": {
      "string" : "string"
   },
   "LastUpdateTime": number
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

GlobalSettings

フラグ `isCrossAccountBackupEnabled` のステータス。

型: 文字列間のマッピング

LastUpdateTime

フラグ `isCrossAccountBackupEnabled` が最後に更新された日時。この更新プログラムは Unix 形式および協定世界時 (UTC) です。`LastUpdateTime`の値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidRequestException

リクエストへの入力に何らかの問題が発生していることを示します。たとえば、パラメータのタイプが間違っています。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeProtectedResource

サービス: AWS Backup

最後にバックアップされた日時、Amazon リソースネーム (ARN)、保存されたリソース AWS のサービスタイプなど、保存されたリソースに関する情報を返します。

リクエストの構文

```
GET /resources/resourceArn HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

resourceArn

リソースを一意に識別する Amazon リソースネーム (ARN)。ARN の形式は、リソースタイプによって異なります。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "LastBackupTime": number,
   "LastBackupVaultArn": "string",
   "LastRecoveryPointArn": "string",
   "LatestRestoreExecutionTimeMinutes": number,
   "LatestRestoreJobCreationDate": number,
   "LatestRestoreRecoveryPointCreationDate": number,
   "ResourceArn": "string",
   "ResourceName": "string",
   "ResourceType": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

LastBackupTime

Unix 形式および協定世界時 (UTC)でリソースが最後にバックアップされた日時)。LastBackupTimeの値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

LastBackupVaultArn

最新のバックアップ復旧ポイントを含むバックアップボールトの ARN (Amazon リソースネーム) 。

型: 文字列

LastRecoveryPointArn

最新の復旧ポイントの ARN (Amazon リソースネーム) 。

型: 文字列

LatestRestoreExecutionTimeMinutes

最新の復元ジョブが完了するまでにかかった分単位の時間。

型: 長整数

LatestRestoreJobCreationDate

最新の復元ジョブの作成日。

型: タイムスタンプ

LatestRestoreRecoveryPointCreationDate

最新の復旧ポイントが作成された日付。

型: タイムスタンプ

ResourceArn

リソースを一意に識別する ARN。ARN の形式は、リソースタイプによって異なります。

型: 文字列

ResourceName

指定されたバックアップに属するリソースの名前。

型: 文字列

ResourceType

リカバリポイントとして保存された AWS リソースのタイプ。Amazon EBS ボリュームや Amazon RDS データベースなど。

型: 文字列

パターン：`^[a-zA-Z0-9\-\_\.]{1,50}$`

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeRecoveryPoint

サービス: AWS Backup

ID、ステータス、暗号化およびライフサイクルなど、リカバリポイントに関連付けられたメタデータを返します。

リクエストの構文

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn?
backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

BackupVaultAccountId

指定されたバックアップボールトのアカウント ID。

Pattern: ^[0-9]{12}$

backupVaultName

バックアップを保存する論理コンテナの名前。バックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先の AWS リージョンに一意の名前で識別されます。

Pattern: ^[a-zA-Z0-9\-_]{2,50}$

必須：はい

recoveryPointArn

arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45などのリカバリポイントを一意に識別する Amazon リソースネーム (ARN) です。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupSizeInBytes": number,
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CalculatedLifecycle": {
      "DeleteAt": number,
      "MoveToColdStorageAt": number
   },
   "CompletionDate": number,
   "CompositeMemberIdentifier": "string",
   "CreatedBy": {
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
      "BackupPlanVersion": "string",
      "BackupRuleId": "string"
   },
   "CreationDate": number,
   "EncryptionKeyArn": "string",
   "IamRoleArn": "string",
   "IsEncrypted": boolean,
   "IsParent": boolean,
   "LastRestoreTime": number,
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   },
   "ParentRecoveryPointArn": "string",
   "RecoveryPointArn": "string",
   "ResourceArn": "string",
   "ResourceName": "string",
   "ResourceType": "string",
   "SourceBackupVaultArn": "string",
   "Status": "string",
   "StatusMessage": "string",
   "StorageClass": "string",
   "VaultType": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

BackupSizeInBytes

バックアップのサイズ (バイト単位)。

型: 長整数

BackupVaultArn

バックアップボールトを一意に識別する ARN、例えば、`arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault` です。

型: 文字列

BackupVaultName

バックアップを保存する論理コンテナの名前。バックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先の リージョンに一意の名前で識別されます。

型: 文字列

パターン：`^[a-zA-Z0-9\-\_]{2,50}$`

CalculatedLifecycle

`DeleteAt` および `MoveToColdStorageAt` タイムスタンプを含む `CalculatedLifecycle` オブジェクト。

タイプ：CalculatedLifecycle オブジェクト

CompletionDate

Unix 形式および協定世界時 (UTC)で、リカバリポイントを作成するジョブが完了した日時。`CompletionDate`の値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

CompositeMemberIdentifier

複合 (親) スタックに属するネストされた (子) 復旧ポイントなど、複合グループ内のリソースの識別子。ID はスタック内の論理 ID から転送されます。

型: 文字列

CreatedBy

作成に使用したバックアッププランの BackupPlanArn、BackupPlanId、BackupPlanVersion、および BackupRuleId を含むリカバリポイントの作成に関する識別情報を含んでいます。

タイプ：RecoveryPointCreator オブジェクト

CreationDate

Unix 時刻形式および協定世界時 (UTC)で、リカバリポイントが作成された日時。CreationDateの値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

EncryptionKeyArn

arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab などの、バックアップを保護するために使用されるサーバー側の暗号化キー。

型: 文字列

IamRoleArn

たとえば、arn:aws:iam::123456789012:role/S3Accessなどのターゲットリカバリポイントの作成に使用する IAM ロール ARN を指定します。

型: 文字列

IsEncrypted

TRUE 指定したリカバリポイントが暗号化されている場合、または FALSE リカバリポイントが暗号化されていない場合かどうか返すブール値。

型: ブール値

IsParent

これにより、復旧ポイントが親 (複合) ジョブであることを示すブール値が返されます。

型: ブール値

LastRestoreTime

Unix 形式および協定世界時 (UTC)で、リカバリポイントが最後に復元された日時。LastRestoreTimeの値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

Lifecycle

ライフサイクルは、保護されたリソースがコールドストレージに移行するタイミングと、期限切れになるタイミングを定義します。 は、定義したライフサイクルに従ってバックアップを自動的に AWS Backup 移行および期限切れにします。

コールドストレージに移行されたバックアップは、そこに最低 90 日保存される必要があります。したがって、「保持期間」の設定は、「コールドへの移行 (日数)」設定から 90 日以上あける必要があります。バックアップがコールドに移行された後で、「コールドへの移行 (日数)」設定を変更することはできません。

コールドストレージに移行できるリソースタイプは、「リソース別の機能の可用性」表に記載されています。他のリソースタイプでは、この式は AWS Backup 無視されます。

タイプ : Lifecycle オブジェクト

ParentRecoveryPointArn

これは、親 (複合) リカバリーポイントを一意に識別する ARN、例えば、arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45です。

型: 文字列

RecoveryPointArn

たとえば、arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45などのリカバリポイントを一意に識別する ARN。

型: 文字列

ResourceArn

保存済みのリソースを一意に識別する ARN。ARN の形式は、リソースタイプによって異なります。

型: 文字列

ResourceName

指定されたバックアップに属するリソースの名前。

型: 文字列

ResourceType

復旧ポイントとして保存する AWS リソースのタイプ。Amazon Elastic Block Store (Amazon EBS) ボリュームや Amazon Relational Database Service (Amazon RDS) データベースなど。

型: 文字列

パターン：`^[a-zA-Z0-9\-\_\.]{1,50}$`

SourceBackupVaultArn

たとえば、`arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault` などのリソースが最初にバックアップされたソースボールトを一意に識別する Amazon リソースネーム (ARN)。リカバリが同じ AWS アカウントまたはリージョンに復元された場合、この値はになりますnull。

型: 文字列

Status

リカバリポイントの状態を指定するステータスコード。

PARTIAL ステータスは、バックアップウィンドウが閉じられる前にリカバリポイントを作成 AWS Backup できなかったことを示します。API を使用してバックアッププランウィンドウを増やすには、「」を参照してくださいUpdateBackupPlan。コンソールを使用して、バックアッププランを選択、編集して、バックアッププランのウィンドウを増やすこともできます。

EXPIRED ステータスは、復旧ポイントが保持期間を超過したが、アクセス許可 AWS Backup がないか、削除できないことを示します。これらの復旧ポイントを手動で削除するには、「開始方法」の「リソースのクリーンアップ」セクションの「ステップ 3: 復旧ポイントの削除」を参照してください。

STOPPED ステータスは、継続的バックアップが無効になるような操作をユーザーが行った場合の継続的バックアップ時に発生します。これは、アクセス許可の削除、バージョニングの無効化、に送信されるイベントの無効化 EventBridge、または によって設定された EventBridge ルールの無効化が原因である可能性があります AWS Backup。

STOPPED ステータスを解決するには、要求されたアクセス許可がすべて揃っていて、S3 バケットでバージョニングが有効になっていることを確認してください。これらの条件が満たされると、実行されるバックアップルールの次のインスタンスでは、新しい継続的復旧ポイントが作成されます。停止ステータスの復旧ポイントは削除する必要はありません。

Amazon EC2 上の SAP HANA では、ユーザーアクション、アプリケーションの設定ミス、またはバックアップ障害が原因で STOPPED ステータスが発生します。将来の継続的バックアップを確実に成功させるには、復旧ポイントのステータスを参照し、SAP HANA で詳細を確認してください。

型: 文字列

有効な値：COMPLETED | PARTIAL | DELETING | EXPIRED

StatusMessage

復旧ポイントのステータスを説明する詳細なメッセージです。

型: 文字列

StorageClass

リカバリポイントのストレージクラスを指定します。有効な値は WARM または COLD です。

型: 文字列

有効な値：WARM | COLD | DELETED

VaultType

記述された復旧ポイントが保存されるボールトのタイプ。

型: 文字列

有効な値：BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeRegionSettings

サービス: AWS Backup

リージョンの現在のサービスオプトイン設定を返します。サービスでサービスオプトインが有効になっている場合、 は、リソースがオンデマンドバックアップまたはスケジュールされたバックアッププランに含まれているときに、このリージョン内のサービスのリソースを保護し AWS Backup ようとします。それ以外の場合は、 AWS Backup は、このリージョンのそのサービスのリソースを保護しようとしません。

リクエストの構文

```
GET /account-settings HTTP/1.1
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "ResourceTypeManagementPreference": {
      "string" : boolean
   },
   "ResourceTypeOptInPreference": {
      "string" : boolean
   }
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

ResourceTypeManagementPreference

がリソースタイプのバックアップ AWS Backup を完全に管理するかどうかを返します。

フル AWS Backup 管理の利点については、「フル AWS Backup 管理」を参照してください。

リソースタイプのリストと、各 がフル AWS Backup 管理をサポートしているかどうかについては、「リソース別の機能の可用性」表を参照してください。

の場合`"DynamoDB":false`、 の高度な DynamoDB バックアップ機能 を有効にすることで、DynamoDB バックアップの完全な AWS Backup 管理を有効にできます。 AWS Backup DynamoDB

タイプ:ブールマップへの文字列。

キーパターン: `^[a-zA-Z0-9\-\_\.]{1,50}$`

ResourceTypeOptInPreference

リージョンのオプトイン設定とともにサービス。

タイプ:ブールマップへの文字列。

キーパターン: `^[a-zA-Z0-9\-\_\.]{1,50}$`

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeReportJob

サービス: AWS Backup

ReportJobId により指定されたレポートの作成に関連する詳細を返します。

リクエストの構文

```
GET /audit/report-jobs/reportJobId HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

reportJobId

レポートジョブの識別子。一意のランダムに生成された UTF-8 エンコード Unicode 文字列 (最大 1,024 バイト長)。レポートジョブ ID を編集することはできません。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "ReportJob": {
      "CompletionTime": number,
      "CreationTime": number,
      "ReportDestination": {
         "S3BucketName": "string",
         "S3Keys": [ "string" ]
      },
      "ReportJobId": "string",
      "ReportPlanArn": "string",
      "ReportTemplate": "string",
      "Status": "string",
      "StatusMessage": "string"
```

```
    }
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

ReportJob

完了時刻と作成時刻、レポート送信先、一意のレポートジョブ ID、Amazon リソースネーム (ARN)、レポートテンプレート、ステータス、ステータスメッセージなど、レポートジョブに関する情報。

型: ReportJob オブジェクト

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeReportPlan

サービス: AWS Backup

AWS アカウント および のすべてのレポートプランのリストを返します AWS リージョン。

リクエストの構文

```
GET /audit/report-plans/reportPlanName HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

reportPlanName

レポートプランの一意の名前。

長さの制限：最小長は 1 です。最大長は 256 です。

パターン：`[a-zA-Z][_a-zA-Z0-9]*`

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "ReportPlan": {
      "CreationTime": number,
      "DeploymentStatus": "string",
      "LastAttemptedExecutionTime": number,
      "LastSuccessfulExecutionTime": number,
      "ReportDeliveryChannel": {
         "Formats": [ "string" ],
         "S3BucketName": "string",
```

```
            "S3KeyPrefix": "string"
         },
         "ReportPlanArn": "string",
         "ReportPlanDescription": "string",
         "ReportPlanName": "string",
         "ReportSetting": {
            "Accounts": [ "string" ],
            "FrameworkArns": [ "string" ],
            "NumberOfFrameworks": number,
            "OrganizationUnits": [ "string" ],
            "Regions": [ "string" ],
            "ReportTemplate": "string"
         }
      }
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

ReportPlan

名前で指定されたレポートプランの詳細を返します。これらの詳細には、レポートプランの Amazon リソースネーム (ARN)、説明、設定、配信チャネル、デプロイステータス、作成時間、最後に試行された実行時間と成功した実行時間が含まれます。

型: ReportPlan オブジェクト

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeRestoreJob

サービス: AWS Backup

ジョブ ID で指定された復元ジョブに関連付けられたメタデータを返します。

リクエストの構文

```
GET /restore-jobs/restoreJobId HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

restoreJobId

リカバリポイントを復元するジョブを一意に識別します。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "AccountId": "string",
   "BackupSizeInBytes": number,
   "CompletionDate": number,
   "CreatedBy": {
      "RestoreTestingPlanArn": "string"
   },
   "CreatedResourceArn": "string",
   "CreationDate": number,
   "DeletionStatus": "string",
   "DeletionStatusMessage": "string",
   "ExpectedCompletionTimeMinutes": number,
   "IamRoleArn": "string",
```

```
    "PercentDone": "string",
    "RecoveryPointArn": "string",
    "RecoveryPointCreationDate": number,
    "ResourceType": "string",
    "RestoreJobId": "string",
    "Status": "string",
    "StatusMessage": "string",
    "ValidationStatus": "string",
    "ValidationStatusMessage": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

AccountId

復元ジョブを所有するアカウント ID を返します。

型: 文字列

パターン：^[0-9]{12}$

BackupSizeInBytes

復元されたリソースのサイズ (バイト単位)。

型: 長整数

CompletionDate

リカバリポイントの復元ジョブが完了した日時 (Unix 形式および協定世界時 (UTC))。CompletionDateの値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

CreatedBy

復元ジョブの作成に関する識別情報が含まれます。

タイプ：RestoreJobCreator オブジェクト

CreatedResourceArn

復元ジョブによって作成されたリソースの Amazon リソースネーム (ARN)。

ARN の形式は、バックアップされたリソースのリソースタイプによって異なります。

型: 文字列

CreationDate

復元ジョブが作成された日時 (Unix 時刻形式および協定世界時 (UTC))。CreationDateの値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前 12:11:30.087 を表します。

型: タイムスタンプ

DeletionStatus

復元テストによって生成されたデータのステータス。

型: 文字列

有効な値：DELETING | FAILED | SUCCESSFUL

DeletionStatusMessage

復元ジョブの削除ステータスを示します。

型: 文字列

ExpectedCompletionTimeMinutes

リカバリーポイントを復元するジョブに要する予想される分単位の時間です。

型: 長整数

IamRoleArn

たとえば、arn:aws:iam::123456789012:role/S3Accessなどのターゲットリカバリポイントの作成に使用する IAM ロール ARN を指定します。

型: 文字列

PercentDone

ジョブのステータスが照会された時点でジョブが完了した推定パーセンテージが含まれます。

型: 文字列

RecoveryPointArn

たとえば、arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45などのリカバリポイントを一意に識別する ARN。

型: 文字列

RecoveryPointCreationDate

指定された復元ジョブによって作成された復旧ポイントの作成日。

型: タイムスタンプ

ResourceType

リソースタイプ別にリストされた復元ジョブに関連付けられたメタデータを返します。

型: 文字列

パターン：^[a-zA-Z0-9\-_\.]{1,50}$

RestoreJobId

リカバリポイントを復元するジョブを一意に識別します。

型: 文字列

Status

リカバリポイントを復元 AWS Backup するために によって開始されるジョブの状態を指定するステータスコード。

型: 文字列

有効な値：PENDING | RUNNING | COMPLETED | ABORTED | FAILED

StatusMessage

リカバリポイントを復元するジョブのステータスを示すメッセージ。

型: 文字列

ValidationStatus

指定された復元ジョブで実行された検証のステータス。

型: 文字列

有効な値：FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING

ValidationStatusMessage

ステータスメッセージ。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

DependencyFailureException

依存 AWS するサービスまたはリソースが AWS Backup サービスにエラーを返し、アクションを完了できません。

HTTP ステータスコード：500

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DisassociateRecoveryPoint

サービス: AWS Backup

から指定された継続的バックアップリカバリポイントを削除 AWS Backup し、Amazon RDS などのソースサービスへの継続的バックアップの制御を解放します。ソースサービスは、元のバックアッププランで指定したライフサイクルを使用して、継続的なバックアップを作成および保持します。

スナップショットバックアップリカバリポイントはサポートされていません。

リクエストの構文

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/disassociate
 HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

backupVaultName

AWS Backup ボールトの一意の名前。

Pattern: ^[a-zA-Z0-9\-_]{2,50}$

必須：はい

recoveryPointArn

AWS Backup リカバリポイントを一意に識別する Amazon リソースネーム (ARN)。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

InvalidRequestException

リクエストへの入力に何らかの問題が発生していることを示します。たとえば、パラメータのタイプが間違っています。

HTTP ステータスコード：400

InvalidResourceStateException

AWS Backup は、この復旧ポイントで既にアクションを実行しています。最初のアクションが終了するまで、リクエストしたアクションを実行できません。後ほどもう一度試してください。」

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DisassociateRecoveryPointFromParent

サービス: AWS Backup

このアクションを特定の子 (ネストされた) 復旧ポイントに対して実行すると、指定した復旧ポイントとその親 (複合) 復旧ポイントとの関係が削除されます。

リクエストの構文

```
DELETE /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/
parentAssociation HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

[backupVaultName](#)

子 (ネストされた) 復旧ポイントが保存されている論理コンテナの名前。バックアップボールトは、作成に使用したアカウントと作成先の AWS リージョンに固有の名前で識別されます。

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

必須：はい

[recoveryPointArn](#)

子 (ネストされた) 復旧ポイントを一意に識別する Amazon リソースネーム (ARN)。例えば、`arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 204
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 204 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

InvalidRequestException

リクエストへの入力に何らかの問題が発生していることを示します。たとえば、パラメータのタイプが間違っています。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2

- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ExportBackupPlanTemplate

サービス: AWS Backup

プラン ID で指定されたバックアッププランをバックアップテンプレートとして返します。

リクエストの構文

```
GET /backup/plans/backupPlanId/toTemplate/ HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

backupPlanId

バックアップ計画を一意に識別します。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanTemplateJson": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

BackupPlanTemplateJson

JSON 形式のバックアッププランテンプレートの本文。

> **Note**
>
> これは署名付き JSON ドキュメントで、GetBackupPlanFromJSON. に渡される前に変更することはできません。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetBackupPlan

サービス: AWS Backup

指定された BackupPlanId の BackupPlan 詳細情報を返します。詳細は、計画メタデータに加えて、JSON 形式のバックアッププランの本文です。

リクエストの構文

```
GET /backup/plans/backupPlanId/?versionId=VersionId HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

backupPlanId

バックアップ計画を一意に識別します。

必須: はい

VersionId

一意のランダムに生成された UTF-8 エンコード Unicode 文字列 (最大 1,024 バイト長)。バージョン ID を編集することはできません。

リクエスト本文

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "AdvancedBackupSettings": [
      {
         "BackupOptions": {
            "string" : "string"
         },
         "ResourceType": "string"
      }
   ],
```

```
   "BackupPlan": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
               "OptInToArchiveForSupportedResources": boolean
            },
            "RecoveryPointTags": {
               "string" : "string"
            },
            "RuleId": "string",
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
         }
      ]
   },
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "CreationDate": number,
```

```
    "CreatorRequestId": "string",
    "DeletionDate": number,
    "LastExecutionDate": number,
    "VersionId": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

AdvancedBackupSettings

各リソースタイプごとに BackupOptions のリストが含まれます。このリストには、バックアッププランに詳細オプションが設定されている場合にのみ入力されます。

型: AdvancedBackupSetting オブジェクトの配列

BackupPlan

バックアッププランの本文を指定します。1 つの BackupPlanName と1 つ以上の Rules のセットを含む。

タイプ : BackupPlan オブジェクト

BackupPlanArn

たとえば、arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50などのバックアップ計画を一意に識別する Amazon リソースネーム (ARN) です。

型: 文字列

BackupPlanId

バックアップ計画を一意に識別します。

型: 文字列

CreationDate

バックアッププランが作成された日時 (Unix 時刻形式および協定世界時 (UTC))。CreationDateの値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

CreatorRequestId

オペレーションを 2 回実行するリスクなしに、失敗したリクエストを再試行でき、リクエストを識別する一意の文字列。

型: 文字列

DeletionDate

バックアップ計画が削除される日時 (Unix 形式および協定世界時 (UTC))。DeletionDateの値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前 12:11:30.087 を表します。

型: タイムスタンプ

LastExecutionDate

このバックアッププランが最後に実行された時刻。日時は、Unix 形式および協定世界時 (UTC) です。LastExecutionDateの値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

VersionId

一意のランダムに生成された UTF-8 エンコード Unicode 文字列 (最大 1,024 バイト長)。バージョン ID を編集することはできません。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetBackupPlanFromJSON

サービス: AWS Backup

バックアッププランまたはエラーを指定する有効な JSON ドキュメントを返します。

リクエストの構文

```
POST /backup/template/json/toPlan HTTP/1.1
Content-type: application/json

{
   "BackupPlanTemplateJson": "string"
}
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

BackupPlanTemplateJson

お客様から提供されたJSON 形式のバックアップ計画ドキュメント。

型: 文字列

必須: はい

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlan": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
```

```
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
               "OptInToArchiveForSupportedResources": boolean
            },
            "RecoveryPointTags": {
               "string" : "string"
            },
            "RuleId": "string",
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
         }
      ]
   }
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

BackupPlan

バックアッププランの本文を指定します。1 つの BackupPlanName と1 つ以上の Rules のセットを含む。

型: BackupPlan オブジェクト

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

InvalidRequestException

リクエストへの入力に何らかの問題が発生していることを示します。たとえば、パラメータのタイプが間違っています。

HTTP ステータスコード：400

LimitExceededException

たとえば、リクエストで許可されるアイテムの最大数などのリクエストの制限を超えました。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetBackupPlanFromTemplate

サービス: AWS Backup

バックアッププランとして templateId で指定したテンプレートを返します。

リクエストの構文

```
GET /backup/template/plans/templateId/toPlan HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

templateId

保存されているバックアッププランテンプレートを一意に識別します。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanDocument": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
```

```
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
               "OptInToArchiveForSupportedResources": boolean
            },
            "RecoveryPointTags": {
               "string" : "string"
            },
            "RuleId": "string",
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
         }
      ]
   }
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

BackupPlanDocument

プランの名前、ルール、バックアップボールトなど、ターゲットテンプレートに基づくバックアッププランの本文を返します。

型: BackupPlan オブジェクト

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python

- AWS SDK for Ruby V3

GetBackupSelection

サービス: AWS Backup

選択メタデータと、バックアッププランに関連付けられているリソースのリストを指定する JSON 形式のドキュメントを返します。

リクエストの構文

```
GET /backup/plans/backupPlanId/selections/selectionId HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

backupPlanId

バックアップ計画を一意に識別します。

必須: はい

selectionId

バックアップ計画に一連のリソースを割り当てるためのリクエストの本文を一意に識別します。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanId": "string",
   "BackupSelection": {
      "Conditions": {
         "StringEquals": [
            {
               "ConditionKey": "string",
```

```
                "ConditionValue": "string"
            }
         ],
         "StringLike": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringNotEquals": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringNotLike": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ]
      },
      "IamRoleArn": "string",
      "ListOfTags": [
         {
            "ConditionKey": "string",
            "ConditionType": "string",
            "ConditionValue": "string"
         }
      ],
      "NotResources": [ "string" ],
      "Resources": [ "string" ],
      "SelectionName": "string"
   },
   "CreationDate": number,
   "CreatorRequestId": "string",
   "SelectionId": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

BackupPlanId

バックアップ計画を一意に識別します。

型: 文字列

BackupSelection

一連のリソースをバックアップ計画に割り当てるリクエストの本文を指定します。

タイプ：BackupSelection オブジェクト

CreationDate

バックアップ選択が作成された日時 (Unix 形式および協定世界時 (UTC))。CreationDateの値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前 12:11:30.087 を表します。

型: タイムスタンプ

CreatorRequestId

オペレーションを 2 回実行するリスクなしに、失敗したリクエストを再試行でき、リクエストを識別する一意の文字列。

型: 文字列

SelectionId

バックアップ計画に一連のリソースを割り当てるためのリクエストの本文を一意に識別します。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetBackupVaultAccessPolicy

サービス: AWS Backup

指定されたバックアップボールトに関連付けられているアクセスポリシードキュメントを返します。

リクエストの構文

```
GET /backup-vaults/backupVaultName/access-policy HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

backupVaultName

バックアップを保存する論理コンテナの名前。バックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先の AWS リージョンに一意の名前で識別されます。

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "Policy": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

BackupVaultArn

arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVaultなどのバックアップボールトを一意に識別する Amazon リソースネーム (ARN)。

型: 文字列

BackupVaultName

バックアップを保存する論理コンテナの名前。バックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先の リージョンに一意の名前で識別されます。

型: 文字列

パターン：^[a-zA-Z0-9\-_]{2,50}$

Policy

JSON 形式のバックアップボールトのアクセスポリシードキュメントです。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetBackupVaultNotifications

サービス: AWS Backup

指定されたバックアップボールトのイベント通知を返します。

リクエストの構文

```
GET /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

backupVaultName

バックアップを保存する論理コンテナの名前。バックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先の AWS リージョンに一意の名前で識別されます。

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultEvents": [ "string" ],
   "BackupVaultName": "string",
   "SNSTopicArn": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

BackupVaultArn

arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVaultなどのバックアップボールトを一意に識別する Amazon リソースネーム (ARN)。

型: 文字列

BackupVaultEvents

リソースをバックアップボールトにバックアップするジョブのステータスを示すイベントの配列。

タイプ：文字列の配列

有効な値: BACKUP_JOB_STARTED | BACKUP_JOB_COMPLETED | BACKUP_JOB_SUCCESSFUL | BACKUP_JOB_FAILED | BACKUP_JOB_EXPIRED | RESTORE_JOB_STARTED | RESTORE_JOB_COMPLETED | RESTORE_JOB_SUCCESSFUL | RESTORE_JOB_FAILED | COPY_JOB_STARTED | COPY_JOB_SUCCESSFUL | COPY_JOB_FAILED | RECOVERY_POINT_MODIFIED | BACKUP_PLAN_CREATED | BACKUP_PLAN_MODIFIED | S3_BACKUP_OBJECT_FAILED | S3_RESTORE_OBJECT_FAILED

BackupVaultName

バックアップを保存する論理コンテナの名前。バックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先の リージョンに一意の名前で識別されます。

型: 文字列

パターン：^[a-zA-Z0-9\-_]{2,50}$

SNSTopicArn

Amazon Simple Notification Service (Amazon SNS) のトピックを一意に識別する ARN (例: arn:aws:sns:us-west-2:111122223333:MyTopic)。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetLegalHold

サービス: AWS Backup

このアクションは、指定されたリーガルホールドの詳細を返します。詳細は、メタデータに加えて、JSON 形式のリーガルホールドの本文です。

リクエストの構文

```
GET /legal-holds/legalHoldId/ HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

legalHoldId

リーガルホールドの ID。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "CancelDescription": "string",
   "CancellationDate": number,
   "CreationDate": number,
   "Description": "string",
   "LegalHoldArn": "string",
   "LegalHoldId": "string",
   "RecoveryPointSelection": {
      "DateRange": {
         "FromDate": number,
         "ToDate": number
      },
      "ResourceIdentifiers": [ "string" ],
```

```
      "VaultNames": [ "string" ]
   },
   "RetainRecordUntil": number,
   "Status": "string",
   "Title": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

CancelDescription

リーガルホールドを削除する理由。

型: 文字列

CancellationDate

リーガルホールドがキャンセルされた時刻。

型: タイムスタンプ

CreationDate

リーガルホールドが作成された時刻。

型: タイムスタンプ

Description

リーガルホールドの説明。

型: 文字列

LegalHoldArn

指定されたリーガルホールドのフレームワーク ARN。ARN の形式は、リソースタイプによって異なります。

型: 文字列

LegalHoldId

リーガルホールドの ID。

型: 文字列

RecoveryPointSelection

リソースタイプやバックアップボールトなど、一連のリソースを割り当てる基準。

タイプ：RecoveryPointSelection オブジェクト

RetainRecordUntil

リーガルホールドレコードが保持される日時。

型: タイムスタンプ

Status

リーガルホールドのステータス。

型: 文字列

有効な値：CREATING | ACTIVE | CANCELING | CANCELED

Title

リーガルホールドのタイトル。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetRecoveryPointRestoreMetadata

サービス: AWS Backup

バックアップの作成に使用されたメタデータのキーと値のペアのセットを返します。

リクエストの構文

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/restore-metadata?
backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

BackupVaultAccountId

指定されたバックアップボールトのアカウント ID。

Pattern: ^[0-9]{12}$

backupVaultName

バックアップを保存する論理コンテナの名前。バックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先の AWS リージョンに一意の名前で識別されます。

Pattern: ^[a-zA-Z0-9\-_]{2,50}$

必須：はい

recoveryPointArn

arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45などのリカバリポイントを一意に識別する Amazon リソースネーム (ARN) です。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "BackupVaultArn": "string",
   "RecoveryPointArn": "string",
   "ResourceType": "string",
   "RestoreMetadata": {
      "string" : "string"
   }
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

BackupVaultArn

arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault などのバックアップボールトを一意に識別する ARN。

型: 文字列

RecoveryPointArn

たとえば、arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45などのリカバリポイントを一意に識別する ARN。

型: 文字列

ResourceType

復旧ポイントのリソースタイプ。

型: 文字列

パターン：^[a-zA-Z0-9\-_\.]{1,50}$

RestoreMetadata

バックアップされたリソースの元の構成を記述するメタデータのキーと値のペアのセット。これらの値は、復元されるサービスによって異なります。

型: 文字列間のマッピング

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3

- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetRestoreJobMetadata

サービス: AWS Backup

このリクエストは、指定された復元ジョブのメタデータを返します。

リクエストの構文

```
GET /restore-jobs/restoreJobId/metadata HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

restoreJobId

これは、 内の復元ジョブの一意の識別子です AWS Backup。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "Metadata": {
      "string" : "string"
   },
   "RestoreJobId": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

Metadata

指定されたバックアップジョブのメタデータが含まれます。

型: 文字列間のマッピング

RestoreJobId

これは、 内の復元ジョブの一意の識別子です AWS Backup。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetRestoreTestingInferredMetadata

サービス: AWS Backup

このリクエストは、安全なデフォルト設定で復元ジョブを開始するために必要な最小限のメタデータセットを返します。BackupVaultName と RecoveryPointArn は必須パラメータで、BackupVaultAccountId はオプションのパラメータです。

リクエストの構文

```
GET /restore-testing/inferred-metadata?
BackupVaultAccountId=BackupVaultAccountId&BackupVaultName=BackupVaultName&RecoveryPointArn=Reco
 HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

BackupVaultAccountId

指定されたバックアップボールトのアカウント ID。

BackupVaultName

バックアップを保存する論理コンテナの名前。バックアップボールトは、作成に使用した アカウントと作成先の AWSリージョンに固有の名前で識別されます。名前は、英文字、数字、およびハイフン (-) で構成されます。

必須: はい

RecoveryPointArn

arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45などのリカバリポイントを一意に識別する Amazon リソースネーム (ARN) です。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "InferredMetadata": {
      "string" : "string"
   }
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

InferredMetadata

リクエストから推定されるメタデータの文字列マッピングです。

型: 文字列間のマッピング

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetRestoreTestingPlan

サービス: AWS Backup

指定された RestoreTestingPlanName の RestoreTestingPlan 詳細情報を返します。この詳細情報には、復元テストプランのメタデータに加え、プランの JSON 形式の本文が含まれます。

リクエストの構文

```
GET /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

RestoreTestingPlanName

復元テストプランの一意の名前 (必須) です。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "RestoreTestingPlan": {
      "CreationTime": number,
      "CreatorRequestId": "string",
      "LastExecutionTime": number,
      "LastUpdateTime": number,
      "RecoveryPointSelection": {
         "Algorithm": "string",
         "ExcludeVaults": [ "string" ],
         "IncludeVaults": [ "string" ],
         "RecoveryPointTypes": [ "string" ],
         "SelectionWindowDays": number
      },
```

```
        "RestoreTestingPlanArn": "string",
        "RestoreTestingPlanName": "string",
        "ScheduleExpression": "string",
        "ScheduleExpressionTimezone": "string",
        "StartWindowHours": number
    }
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

RestoreTestingPlan

復元テストプランの本文を示します。RestoreTestingPlanName が含まれます。

型: RestoreTestingPlanForGet オブジェクト

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetRestoreTestingSelection

サービス: AWS Backup

を返します。 RestoreTestingSelection復元テストプランのリソースと要素が表示されます。

リクエストの構文

```
GET /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

RestoreTestingPlanName

復元テストプランの一意の名前 (必須) です。

必須: はい

RestoreTestingSelectionName

復元テスト選択の一意の名前 (必須) です。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "RestoreTestingSelection": {
      "CreationTime": number,
      "CreatorRequestId": "string",
      "IamRoleArn": "string",
      "ProtectedResourceArns": [ "string" ],
      "ProtectedResourceConditions": {
         "StringEquals": [
```

```
            {
               "Key": "string",
               "Value": "string"
            }
         ],
         "StringNotEquals": [
            {
               "Key": "string",
               "Value": "string"
            }
         ]
      },
      "ProtectedResourceType": "string",
      "RestoreMetadataOverrides": {
         "string" : "string"
      },
      "RestoreTestingPlanName": "string",
      "RestoreTestingSelectionName": "string",
      "ValidationWindowHours": number
   }
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

RestoreTestingSelection

復元テスト選択の一意の名前。

型: RestoreTestingSelectionForGet オブジェクト

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetSupportedResourceTypes

サービス: AWS Backup

でサポートされている AWS リソースタイプを返します AWS Backup。

リクエストの構文

```
GET /supported-resource-types HTTP/1.1
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "ResourceTypes": [ "string" ]
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

ResourceTypes

サポートされている AWS リソースタイプの文字列が含まれます。

- Amazon Aurora の場合は `Aurora`
- `CloudFormation` の AWS CloudFormation
- Amazon DocumentDB (MongoDB 互換性) の場合は `DocumentDB`
- Amazon DynamoDB 用の `DynamoDB`
- Amazon Elastic Block Store 用の `EBS`

- Amazon Elastic Compute Cloud 用の `EC2`
- Amazon Elastic File System 用の `EFS`
- Amazon FSx の場合 用の `FSX`
- Amazon Neptune の場合 用の `Neptune`
- Amazon Relational Database Service 用の `RDS`
- Amazon Redshift 用の `Redshift`
- `SAP HANA on Amazon EC2` Amazon Elastic Compute Cloud インスタンス上の for SAP HANA データベース
- `S3` for Amazon Simple Storage Service (Amazon S3)
- `Storage Gateway` の AWS Storage Gateway
- Amazon Timestream 用の `Timestream`
- `VirtualMachine` for VMware 仮想マシン

タイプ：文字列の配列

パターン：`^[a-zA-Z0-9\-\_\.]{1,50}$`

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2

- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListBackupJobs

サービス: AWS Backup

過去 30 日間の認証済みアカウントの既存のバックアップジョブのリストを返します。より長い期間については、これらの モニタリングツール を使用することを検討してください。

リクエストの構文

```
GET /backup-jobs/?
accountId=ByAccountId&backupVaultName=ByBackupVaultName&completeAfter=ByCompleteAfter&completeB
 HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

ByAccountId

ジョブを一覧表示するアカウント ID。指定されたアカウント ID に関連付けられたバックアップジョブのみを返します。

AWS Organizations 管理アカウントから使用する場合、 を渡すと組織全体のすべてのジョブ*が返されます。

Pattern: ^[0-9]{12}$

ByBackupVaultName

指定したバックアップボールトに保存されるバックアップジョブのみを返します。バックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先の AWS リージョンに一意の名前で識別されます。

Pattern: ^[a-zA-Z0-9\-_]{2,50}$

ByCompleteAfter

Unix 形式および協定世界時 (UTC) で表された日付の後に完了したバックアップジョブのみを返します。

ByCompleteBefore

Unix 形式および協定世界時 (UTC) で表される日付より前に完了したバックアップジョブのみを返します。

ByCreatedAfter

指定した日付より後に作成されたバックアップジョブのみを返します。

ByCreatedBefore

指定した日付より前に作成されたバックアップジョブのみを返します。

ByMessageCategory

これは、入力する値 MessageCategory と一致する でジョブをフィルタリングするために使用できるオプションのパラメータです。

文字列の例としては `AccessDenied`、`SUCCESS`、`AGGREGATE_ALL`、および `InvalidParameters` があります。

「モニタリング」を参照してください。

ワイルドカード () はすべてのメッセージカテゴリの数を返します。

`AGGREGATE_ALL` は、すべてのメッセージカテゴリのジョブ数を集計し、その合計を返します。

ByParentJobId

親ジョブ ID に基づいて子 (ネストされた) ジョブを一覧表示するフィルターです。

ByResourceArn

指定されたリソースの Amazon リソースネーム (ARN) に一致するバックアップジョブのみを返します。

ByResourceType

指定されたリソースのバックアップジョブのみを返します。

- Amazon Aurora の場合は `Aurora`
- `CloudFormation` の AWS CloudFormation
- Amazon DocumentDB (MongoDB 互換性) の場合は `DocumentDB`
- Amazon DynamoDB 用の `DynamoDB`
- Amazon Elastic Block Store 用の `EBS`
- Amazon Elastic Compute Cloud 用の `EC2`
- Amazon Elastic File System 用の `EFS`
- Amazon FSx の場合 用の `FSx`

- Amazon Neptune の場合は `Neptune`
- Amazon Redshift の場合は `Redshift`
- Amazon Relational Database Service の場合は `RDS`
- SAP HANA データベースの場合は `SAP HANA on Amazon EC2`
- `Storage Gateway` の AWS Storage Gateway
- Amazon S3 の場合は `S3`
- Amazon Timestream 用の `Timestream`
- 仮想マシンの場合は `VirtualMachine`

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

ByState

指定された状態にあるバックアップジョブのみを返します。

`Completed with issues` は AWS Backup コンソールでのみ表示されるステータスです。API の場合このステータスは、状態が `COMPLETED` で `MessageCategory` の値が `SUCCESS` 以外のジョブ、つまり完了はしているがステータスメッセージがあるジョブを指します。

`Completed with issues` のジョブ数を取得するには、以下のように GET リクエストを 2 回実行し、2 つ目の小さい方の数字を引きます。

GET /backup-jobs/?state=COMPLETED

GET /backup-jobs/?messageCategory=SUCCESS&state=COMPLETED

有効な値 : `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

MaxResults

返されるアイテムの最大数。

有効な範囲: 最小値 は 1 です。最大値は 1000 です。

NextToken

返された項目の一部リストに続く次の項目。たとえば、`MaxResults` アイテム数のリクエストが行われるようにされた場合、`NextToken` では、次のトークンが指す口ケーションから開始して、リスト内のより多くのアイテムを返すことができます。

リクエスト本文

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupJobs": [
      {
         "AccountId": "string",
         "BackupJobId": "string",
         "BackupOptions": {
            "string" : "string"
         },
         "BackupSizeInBytes": number,
         "BackupType": "string",
         "BackupVaultArn": "string",
         "BackupVaultName": "string",
         "BytesTransferred": number,
         "CompletionDate": number,
         "CreatedBy": {
            "BackupPlanArn": "string",
            "BackupPlanId": "string",
            "BackupPlanVersion": "string",
            "BackupRuleId": "string"
         },
         "CreationDate": number,
         "ExpectedCompletionDate": number,
         "IamRoleArn": "string",
         "InitiationDate": number,
         "IsParent": boolean,
         "MessageCategory": "string",
         "ParentJobId": "string",
         "PercentDone": "string",
         "RecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceName": "string",
         "ResourceType": "string",
         "StartBy": number,
         "State": "string",
         "StatusMessage": "string"
```

```
        }
    ],
    "NextToken": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

BackupJobs

JSON 形式で返されたバックアップジョブに関するメタデータを含む構造体の配列。

型: BackupJob オブジェクトの配列

NextToken

返された項目の一部リストに続く次の項目。たとえば、MaxResults アイテム数のリクエストが行われるようにされた場合、NextToken では、次のトークンが指す口ケーションから開始して、リスト内のより多くのアイテムを返すことができます。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListBackupJobSummaries

サービス: AWS Backup

過去 30 日以内に作成または実行されたバックアップジョブの概要を求めるリクエストです。AccountID 、State、、 ResourceType MessageCategory、または パラメータを含めて AggregationPeriod MaxResults、結果を NextToken フィルタリングできます。

このリクエストは、リージョン、アカウント、状態、 ResourceType MessageCategory、 StartTime EndTime、および含まれるジョブの数を含む概要を返します。

リクエストの構文

```
GET /audit/backup-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&MessageCategory=M
 HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

AccountId

指定されたアカウントのジョブ数を返します。

リクエストがメンバーアカウントまたは AWS Organizations の一部ではないアカウントから送信されると、リクエスタのアカウント内のジョブが返されます。

ルート、管理者、および委任された管理者アカウントでは、ANY の値を使用して、組織内のすべてのアカウントのジョブ数を返すことができます。

AGGREGATE_ALL は、認証された組織内のすべてのアカウントのジョブ数を集計し、その合計を返します。

Pattern: ^[0-9]{12}$

AggregationPeriod

返された結果の期間。

- ONE_DAY - 過去 14 日間の毎日のジョブ数。
- SEVEN_DAYS - 過去 7 日間の集計ジョブ数。
- FOURTEEN_DAYS - 過去 14 日間の集計ジョブ数。

有効な値：ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS

MaxResults

返されるアイテムの最大数。

値は整数です。指定できる値の範囲は 1～500 です。

有効範囲: 最小値は 1 です。最大値は 1000 です。

MessageCategory

このパラメータは、指定されたメッセージカテゴリのジョブ数を返します。

使用できる文字列の例として、AccessDenied、Success、InvalidParameters があります。受け入れられた MessageCategory 文字列のリストについては、「モニタリング」を参照してください。

値 ANY は、すべてのメッセージカテゴリの数を返します。

AGGREGATE_ALL は、すべてのメッセージカテゴリのジョブ数を集計し、その合計を返します。

NextToken

返されるリソースの部分的リストに続く次の項目です。例えば、MaxResults の数のリソースを返すようにリクエストが行われた場合、NextToken を使用すると、このトークンが指す場所から開始してさらにリストの項目を返すことができます。

ResourceType

指定されたリソースタイプのジョブ数を返します。リクエスト GetSupportedResourceTypes を使用して、サポートされているリソースタイプの文字列を取得します。

値 ANY は、すべてのリソースタイプの数を返します。

AGGREGATE_ALL は、すべてのリソースタイプのジョブ数を集計し、その合計を返します。

バックアップする AWS リソースのタイプ。Amazon Elastic Block Store (Amazon EBS) ボリュームや Amazon Relational Database Service (Amazon RDS) データベースなど。

Pattern: ^[a-zA-Z0-9\-_\.]{1,50}$

State

このパラメータは、指定された状態のジョブの数を返します。

値 ANY は、すべての状態の数を返します。

AGGREGATE_ALL は、すべての状態のジョブ数を集計し、その合計を返します。

Completed with issues は AWS Backup コンソールでのみ表示されるステータスです。API の場合このステータスは、状態が COMPLETED で MessageCategory の値が SUCCESS 以外のジョブ、つまり完了はしているがステータスメッセージがあるジョブを指します。Completed with issues のジョブ数を取得するには、以下のように GET リクエストを 2 回実行し、2 つ目の小さい方の数字を引きます。

GET /audit/backup-job-summaries ?
AggregationPeriod=FOURTEEN_DAYS&State=COMPLETED

GET /audit/backup-job-summaries ?
AggregationPeriod=FOURTEEN_DAYS&MessageCategory=SUCCESS&State=COMPLETED

有効な値：CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL | AGGREGATE_ALL | ANY

リクエスト本文

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "AggregationPeriod": "string",
   "BackupJobSummaries": [
      {
         "AccountId": "string",
         "Count": number,
         "EndTime": number,
         "MessageCategory": "string",
         "Region": "string",
         "ResourceType": "string",
         "StartTime": number,
         "State": "string"
      }
   ],
```

```
    "NextToken": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

AggregationPeriod

返された結果の期間。

- ONE_DAY - 過去 14 日間の毎日のジョブ数。
- SEVEN_DAYS - 過去 7 日間の集計ジョブ数。
- FOURTEEN_DAYS - 過去 14 日間の集計ジョブ数。

型: 文字列

BackupJobSummaries

概要情報。

型: BackupJobSummary オブジェクトの配列

NextToken

返されるリソースの部分的リストに続く次の項目です。例えば、MaxResults の数のリソースを返すようにリクエストが行われた場合、NextToken を使用すると、このトークンが指す場所から開始してさらにリストの項目を返すことができます。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListBackupPlans

サービス: AWS Backup

アカウントのアクティブなバックアッププランを一覧表示します。

リクエストの構文

```
GET /backup/plans/?
includeDeleted=IncludeDeleted&maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

IncludeDeleted

TRUE に設定されているときに削除されたバックアッププランを返す FALSE のデフォルト値を持つブール値。

MaxResults

返されるアイテムの最大数。

有効な範囲: 最小値 は 1 です。最大値は 1000 です。

NextToken

返された項目の一部リストに続く次の項目。たとえば、MaxResults アイテム数のリクエストが行われるようにされた場合、NextToken では、次のトークンが指す口ケーションから開始して、リスト内のより多くのアイテムを返すことができます。

リクエスト本文

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlansList": [
      {
```

```
         "AdvancedBackupSettings": [
            {
               "BackupOptions": {
                  "string" : "string"
               },
               "ResourceType": "string"
            }
         ],
         "BackupPlanArn": "string",
         "BackupPlanId": "string",
         "BackupPlanName": "string",
         "CreationDate": number,
         "CreatorRequestId": "string",
         "DeletionDate": number,
         "LastExecutionDate": number,
         "VersionId": "string"
      }
   ],
   "NextToken": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

BackupPlansList

バックアッププランに関する情報。

型: BackupPlansListMember オブジェクトの配列

NextToken

返された項目の一部リストに続く次の項目。たとえば、MaxResults アイテム数のリクエストが行われるようにされた場合、NextToken では、次のトークンが指す口ケーションから開始して、リスト内のより多くのアイテムを返すことができます。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListBackupPlanTemplates

サービス: AWS Backup

バックアッププランテンプレートを一覧表示します。

リクエストの構文

```
GET /backup/template/plans?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

MaxResults

返される項目の最大数。

有効範囲: 最小値は 1 です。最大値は 1000 です。

NextToken

返された項目の一部リストに続く次の項目。たとえば、MaxResults アイテム数のリクエストが行われるようにされた場合、NextToken では、次のトークンが指す口ケーションから開始して、リスト内のより多くのアイテムを返すことができます。

リクエスト本文

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanTemplatesList": [
      {
         "BackupPlanTemplateId": "string",
         "BackupPlanTemplateName": "string"
      }
   ],
   "NextToken": "string"
```

```
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

BackupPlanTemplatesList

保存したテンプレートに関するメタデータを含むテンプレートリスト項目の配列。

型: BackupPlanTemplatesListMember オブジェクトの配列

NextToken

返された項目の一部リストに続く次の項目。たとえば、MaxResults アイテム数のリクエストが行われるようにされた場合、NextToken では、次のトークンが指す口ケーションから開始して、リスト内のより多くのアイテムを返すことができます。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListBackupPlanVersions

サービス: AWS Backup

Amazon リソースネーム (ARN)、バックアッププラン ID、作成と削除日、プラン名、バージョン ID など、バックアッププランのバージョンメタデータを返します。

リクエストの構文

```
GET /backup/plans/backupPlanId/versions/?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

backupPlanId

バックアップ計画を一意に識別します。

必須: はい

MaxResults

返されるアイテムの最大数。

有効な範囲: 最小値 は 1 です。最大値は 1000 です。

NextToken

返された項目の一部リストに続く次の項目。たとえば、MaxResults アイテム数のリクエストが行われるようにされた場合、NextToken では、次のトークンが指す口ケーションから開始して、リスト内のより多くのアイテムを返すことができます。

リクエスト本文

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "BackupPlanVersionsList": [
      {
         "AdvancedBackupSettings": [
            {
               "BackupOptions": {
                  "string" : "string"
               },
               "ResourceType": "string"
            }
         ],
         "BackupPlanArn": "string",
         "BackupPlanId": "string",
         "BackupPlanName": "string",
         "CreationDate": number,
         "CreatorRequestId": "string",
         "DeletionDate": number,
         "LastExecutionDate": number,
         "VersionId": "string"
      }
   ],
   "NextToken": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

BackupPlanVersionsList

バックアッププランに関するメタデータを含むバージョンリスト項目の配列。

型: BackupPlansListMember オブジェクトの配列

NextToken

返された項目の一部リストに続く次の項目。たとえば、MaxResults アイテム数のリクエストが行われるようにされた場合、NextToken では、次のトークンが指す口ケーションから開始して、リスト内のより多くのアイテムを返すことができます。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python

- AWS SDK for Ruby V3

ListBackupSelections

サービス: AWS Backup

ターゲットバックアッププランに関連付けられたリソースのメタデータを含む配列を返します。

リクエストの構文

```
GET /backup/plans/backupPlanId/selections/?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

backupPlanId

バックアップ計画を一意に識別します。

必須: はい

MaxResults

返されるアイテムの最大数。

有効な範囲: 最小値 は 1 です。最大値は 1000 です。

NextToken

返された項目の一部リストに続く次の項目。たとえば、MaxResults アイテム数のリクエストが行われるようにされた場合、NextToken では、次のトークンが指す口ケーションから開始して、リスト内のより多くのアイテムを返すことができます。

リクエスト本文

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupSelectionsList": [
      {
```

```
            "BackupPlanId": "string",
            "CreationDate": number,
            "CreatorRequestId": "string",
            "IamRoleArn": "string",
            "SelectionId": "string",
            "SelectionName": "string"
        }
    ],
    "NextToken": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

BackupSelectionsList

リスト内の各リソースに関するメタデータを含むバックアップ選択リスト項目の配列。

型: BackupSelectionsListMember オブジェクトの配列

NextToken

返された項目の一部リストに続く次の項目。たとえば、MaxResults アイテム数のリクエストが行われるようにされた場合、NextToken では、次のトークンが指す口ケーションから開始して、リスト内のより多くのアイテムを返すことができます。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListBackupVaults

サービス: AWS Backup

リカバリポイントのストレージコンテナとその情報のリストを返します。

リクエストの構文

```
GET /backup-vaults/?
maxResults=MaxResults&nextToken=NextToken&shared=ByShared&vaultType=ByVaultType
 HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

ByShared

このパラメータは、ボールトのリストを共有ボールトでソートします。

ByVaultType

このパラメータは、ボールトのリストをボールトタイプでソートします。

有効な値：BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT

MaxResults

返されるアイテムの最大数。

有効な範囲: 最小値 は 1 です。最大値は 1000 です。

NextToken

返された項目の一部リストに続く次の項目。たとえば、MaxResults アイテム数のリクエストが行われるようにされた場合、NextToken では、次のトークンが指す口ケーションから開始して、リスト内のより多くのアイテムを返すことができます。

リクエスト本文

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "BackupVaultList": [
      {
         "BackupVaultArn": "string",
         "BackupVaultName": "string",
         "CreationDate": number,
         "CreatorRequestId": "string",
         "EncryptionKeyArn": "string",
         "LockDate": number,
         "Locked": boolean,
         "MaxRetentionDays": number,
         "MinRetentionDays": number,
         "NumberOfRecoveryPoints": number
      }
   ],
   "NextToken": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

BackupVaultList

Amazon リソースネーム (ARN)、表示名、作成日、保存されたリカバリポイントの数、バックアップボールトに保存されているリソースが暗号化されている場合の暗号化情報など、ボールトメタデータを含むバックアップボールトリストメンバーの配列。

型: BackupVaultListMember オブジェクトの配列

NextToken

返された項目の一部リストに続く次の項目。たとえば、MaxResults アイテム数のリクエストが行われるようにされた場合、NextToken では、次のトークンが指す口ケーションから開始して、リスト内のより多くのアイテムを返すことができます。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListCopyJobs

サービス: AWS Backup

コピージョブに関するメタデータを返します。

リクエストの構文

```
GET /copy-jobs/?
accountId=ByAccountId&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore&createdAfte
 HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

ByAccountId

ジョブを一覧表示するアカウント ID。指定されたアカウント ID に関連付けられたコピージョブのみを返します。

Pattern: `^[0-9]{12}$`

ByCompleteAfter

Unix 形式および協定世界時 (UTC) で表された日付の後に完了したコピージョブのみを返します。

ByCompleteBefore

Unix 形式および協定世界時 (UTC) で表される日付より前に完了したコピージョブのみを返します。

ByCreatedAfter

指定した日付より後に作成されたコピージョブのみを返します。

ByCreatedBefore

指定した日付より前に作成されたコピージョブのみを返します。

ByDestinationVaultArn

たとえば、`arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault` などのバックアップボールトを一意に識別する Amazon リソースネーム (ARN) です。

ByMessageCategory

これは、入力する値 MessageCategory と一致する でジョブをフィルタリングするために使用できるオプションのパラメータです。

文字列の例としては AccessDenied、SUCCESS、AGGREGATE_ALL、および INVALIDPARAMETERS があります。

使用可能な文字列のリストについては、「モニタリング」を参照してください。

値 ANY は、すべてのメッセージカテゴリの数を返します。

AGGREGATE_ALL は、すべてのメッセージカテゴリのジョブ数を集計し、その合計を返します。

ByParentJobId

親ジョブ ID に基づいて子 (ネストされた) ジョブを一覧表示するフィルターです。

ByResourceArn

指定されたリソースの Amazon リソースネーム (ARN) に一致するコピージョブのみを返します。

ByResourceType

指定されたリソースのバックアップジョブのみを返します。

- Amazon Aurora の場合は Aurora
- CloudFormation の AWS CloudFormation
- Amazon DocumentDB (MongoDB 互換性) の場合は DocumentDB
- Amazon DynamoDB 用の DynamoDB
- Amazon Elastic Block Store 用の EBS
- Amazon Elastic Compute Cloud 用の EC2
- Amazon Elastic File System 用の EFS
- Amazon FSx の場合 用の FSx
- Amazon Neptune の場合は Neptune
- Amazon Redshift の場合は Redshift
- Amazon Relational Database Service の場合は RDS
- SAP HANA データベースの場合は SAP HANA on Amazon EC2
- Storage Gateway の AWS Storage Gateway

- Amazon S3 の場合は S3
- Amazon Timestream 用の Timestream
- 仮想マシンの場合は VirtualMachine

Pattern: ^[a-zA-Z0-9\-_\.]{1,50}$

ByState

指定された状態のコピージョブのみを返します。

有効な値：CREATED | RUNNING | COMPLETED | FAILED | PARTIAL

MaxResults

返されるアイテムの最大数。

有効な範囲: 最小値 は 1 です。最大値は 1000 です。

NextToken

返された項目の一部リストに続く次の項目。例えば、項目 MaxResults 数を返すリクエストが行われた場合、 NextToken は次のトークンで指す場所から始まるリスト内のより多くの項目を返すことができます。

リクエスト本文

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "CopyJobs": [
      {
         "AccountId": "string",
         "BackupSizeInBytes": number,
         "ChildJobsInState": {
            "string" : number
         },
         "CompletionDate": number,
         "CompositeMemberIdentifier": "string",
```

```
         "CopyJobId": "string",
         "CreatedBy": {
            "BackupPlanArn": "string",
            "BackupPlanId": "string",
            "BackupPlanVersion": "string",
            "BackupRuleId": "string"
         },
         "CreationDate": number,
         "DestinationBackupVaultArn": "string",
         "DestinationRecoveryPointArn": "string",
         "IamRoleArn": "string",
         "IsParent": boolean,
         "MessageCategory": "string",
         "NumberOfChildJobs": number,
         "ParentJobId": "string",
         "ResourceArn": "string",
         "ResourceName": "string",
         "ResourceType": "string",
         "SourceBackupVaultArn": "string",
         "SourceRecoveryPointArn": "string",
         "State": "string",
         "StatusMessage": "string"
      }
   ],
   "NextToken": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

CopyJobs

JSON 形式で返されたコピージョブに関するメタデータを含む構造体の配列。

型: CopyJob オブジェクトの配列

NextToken

返された項目の一部リストに続く次の項目。例えば、項目 MaxResults 数を返すリクエストが行われた場合、 NextToken は次のトークンで指す場所から始まるリスト内のより多くの項目を返すことができます。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListCopyJobSummaries

サービス: AWS Backup

このリクエストは、過去 30 日以内に作成または実行されたコピージョブのリストを取得します。AccountID 、State、、 ResourceType MessageCategory、または パラメータを含めて AggregationPeriod MaxResults結果を NextToken フィルタリングできます。

このリクエストは、リージョン、アカウント、状態、 RestourceType MessageCategory、StartTime EndTime、および含まれるジョブの数を含む概要を返します。

リクエストの構文

```
GET /audit/copy-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&MessageCategory=M
 HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

AccountId

指定されたアカウントのジョブ数を返します。

リクエストがメンバーアカウントまたは AWS Organizations の一部ではないアカウントから送信されると、リクエスタのアカウント内のジョブが返されます。

ルート、管理者、および委任された管理者アカウントでは、ANY の値を使用して、組織内のすべてのアカウントのジョブ数を返すことができます。

AGGREGATE_ALL は、認証された組織内のすべてのアカウントのジョブ数を集計し、その合計を返します。

Pattern: ^[0-9]{12}$

AggregationPeriod

返された結果の期間。

- ONE_DAY - 過去 14 日間の毎日のジョブ数。
- SEVEN_DAYS - 過去 7 日間の集計ジョブ数。
- FOURTEEN_DAYS - 過去 14 日間の集計ジョブ数。

有効な値：ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS

MaxResults

このパラメータは返されるアイテムの最大数を指定します。

値は整数です。指定できる値の範囲は 1～500 です。

有効範囲: 最小値は 1 です。最大値は 1000 です。

MessageCategory

このパラメータは、指定されたメッセージカテゴリのジョブ数を返します。

使用できる文字列の例として、AccessDenied、Success、InvalidParameters があります。受け入れられた MessageCategory 文字列のリストについては、「モニタリング」を参照してください。

値 ANY は、すべてのメッセージカテゴリの数を返します。

AGGREGATE_ALL は、すべてのメッセージカテゴリのジョブ数を集計し、その合計を返します。

NextToken

返されるリソースの部分的リストに続く次の項目です。例えば、MaxResults の数のリソースを返すようにリクエストが行われた場合、NextToken を使用すると、このトークンが指す場所から開始してさらにリストの項目を返すことができます。

ResourceType

指定されたリソースタイプのジョブ数を返します。リクエスト GetSupportedResourceTypes を使用して、サポートされているリソースタイプの文字列を取得します。

値 ANY は、すべてのリソースタイプの数を返します。

AGGREGATE_ALL は、すべてのリソースタイプのジョブ数を集計し、その合計を返します。

バックアップする AWS リソースのタイプ。Amazon Elastic Block Store (Amazon EBS) ボリュームや Amazon Relational Database Service (Amazon RDS) データベースなど。

Pattern: ^[a-zA-Z0-9\-_\.]{1,50}$

State

このパラメータは、指定された状態のジョブの数を返します。

値 ANY は、すべての状態の数を返します。

AGGREGATE_ALL は、すべての状態のジョブ数を集計し、その合計を返します。

有効な値：CREATED | RUNNING | ABORTING | ABORTED | COMPLETING | COMPLETED | FAILING | FAILED | PARTIAL | AGGREGATE_ALL | ANY

リクエスト本文

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "AggregationPeriod": "string",
   "CopyJobSummaries": [
      {
         "AccountId": "string",
         "Count": number,
         "EndTime": number,
         "MessageCategory": "string",
         "Region": "string",
         "ResourceType": "string",
         "StartTime": number,
         "State": "string"
      }
   ],
   "NextToken": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

AggregationPeriod

返された結果の期間。

- ONE_DAY - 過去 14 日間の毎日のジョブ数。
- SEVEN_DAYS - 過去 7 日間の集計ジョブ数。
- FOURTEEN_DAYS - 過去 14 日間の集計ジョブ数。

型: 文字列

CopyJobSummaries

この戻り値には、含まれているジョブのリージョン、アカウント、状態 ResourceType MessageCategory StartTime、、 EndTime、およびカウントを含む概要が表示されます。

型: CopyJobSummary オブジェクトの配列

NextToken

返されるリソースの部分的リストに続く次の項目です。例えば、MaxResults の数のリソースを返すようにリクエストが行われた場合、NextToken を使用すると、このトークンが指す場所から開始してさらにリストの項目を返すことができます。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListFrameworks

サービス: AWS Backup

AWS アカウント および のすべてのフレームワークのリストを返します AWS リージョン。

リクエストの構文

```
GET /audit/frameworks?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

MaxResults

1 から 1000 の範囲の望ましい結果の数。(オプション)。指定しない場合、クエリは 1 MB のデータを返します。

有効な範囲: 最小値 は 1 です。最大値は 1000 です。

NextToken

リスト内の次の項目のセットを返すために使用できる、この操作に対する前回の呼び出しから返された識別子。

リクエスト本文

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "Frameworks": [
      {
         "CreationTime": number,
         "DeploymentStatus": "string",
         "FrameworkArn": "string",
         "FrameworkDescription": "string",
```

```
            "FrameworkName": "string",
            "NumberOfControls": number
        }
    ],
    "NextToken": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

Frameworks

フレームワーク名、Amazon リソースネーム (ARN)、説明、コントロール数、作成時間、デプロイステータスなど、各フレームワークの詳細を含むフレームワーク。

型: Framework オブジェクトの配列

NextToken

リスト内の次の項目のセットを返すために使用できる、この操作に対する前回の呼び出しから返された識別子。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListLegalHolds

サービス: AWS Backup

このアクションは、アクティブなリーガルホールドと以前のリーガルホールドに関するメタデータを返します。

リクエストの構文

```
GET /legal-holds/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

MaxResults

返されるリソースリストアイテムの最大数。

有効範囲: 最小値は 1 です。最大値は 1000 です。

NextToken

返されるリソースの部分的リストに続く次の項目です。例えば、MaxResults の数のリソースを返すようにリクエストが行われた場合、NextToken を使用すると、このトークンが指す場所から開始してさらにリストの項目を返すことができます。

リクエスト本文

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "LegalHolds": [
      {
         "CancellationDate": number,
         "CreationDate": number,
         "Description": "string",
         "LegalHoldArn": "string",
```

```
            "LegalHoldId": "string",
            "Status": "string",
            "Title": "string"
        }
    ],
    "NextToken": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

LegalHolds

これは、返されたリーガルホールド (アクティブなリーガルホールドと以前のリーガルホールドの両方) の配列です。

型: LegalHold オブジェクトの配列

NextToken

返されるリソースの部分的リストに続く次の項目です。例えば、MaxResults の数のリソースを返すようにリクエストが行われた場合、NextToken を使用すると、このトークンが指す場所から開始してさらにリストの項目を返すことができます。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListProtectedResources

サービス: AWS Backup

リソースの保存時間 AWS Backup、リソースの Amazon リソースネーム (ARN)、リソースタイプなど、 によって正常にバックアップされたリソースの配列を返します。

リクエストの構文

```
GET /resources/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

MaxResults

返されるアイテムの最大数。

有効な範囲: 最小値 は 1 です。最大値は 1000 です。

NextToken

返された項目の一部リストに続く次の項目。たとえば、MaxResults アイテム数のリクエストが行われるようにされた場合、NextToken では、次のトークンが指す口ケーションから開始して、リスト内のより多くのアイテムを返すことができます。

リクエスト本文

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Results": [
      {
         "LastBackupTime": number,
         "LastBackupVaultArn": "string",
         "LastRecoveryPointArn": "string",
```

```
            "ResourceArn": "string",
            "ResourceName": "string",
            "ResourceType": "string"
        }
    ]
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

NextToken

返された項目の一部リストに続く次の項目。たとえば、MaxResults アイテム数のリクエストが行われるようにされた場合、NextToken では、次のトークンが指す口ケーションから開始して、リスト内のより多くのアイテムを返すことができます。

型: 文字列

Results

リソースが保存された時間、リソースの Amazon リソースネーム (ARN)、リソースタイプ AWS Backup を含めて正常にバックアップされたリソースの配列。

型: ProtectedResource オブジェクトの配列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListProtectedResourcesByBackupVault

サービス: AWS Backup

このリクエストには、各バックアップボールトに対応する、保護されたリソースが一覧表示されます。

リクエストの構文

```
GET /backup-vaults/backupVaultName/resources/?
backupVaultAccountId=BackupVaultAccountId&maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

BackupVaultAccountId

アカウント ID で指定したボールト内のバックアップボールトで保護されたリソースのリスト。

Pattern: ^[0-9]{12}$

backupVaultName

名前で指定したボールト内のバックアップボールトによって保護されたリソースのリスト。

Pattern: ^[a-zA-Z0-9\-_]{2,50}$

必須：はい

MaxResults

返されるアイテムの最大数。

有効な範囲: 最小値 は 1 です。最大値は 1000 です。

NextToken

返された項目の一部リストに続く次の項目。たとえば、MaxResults アイテム数のリクエストが行われるようにされた場合、NextToken では、次のトークンが指す口ケーションから開始して、リスト内のより多くのアイテムを返すことができます。

リクエスト本文

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Results": [
      {
         "LastBackupTime": number,
         "LastBackupVaultArn": "string",
         "LastRecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceName": "string",
         "ResourceType": "string"
      }
   ]
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

NextToken

返された項目の一部リストに続く次の項目。たとえば、MaxResults アイテム数のリクエストが行われるようにされた場合、NextToken では、次のトークンが指す口ケーションから開始して、リスト内のより多くのアイテムを返すことができます。

型: 文字列

Results

これらは、リクエスト に対して返される結果です ListProtectedResourcesByBackupVault。

型: ProtectedResource オブジェクトの配列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListRecoveryPointsByBackupVault

サービス: AWS Backup

バックアップボールトに保存されている復旧ポイントの詳細情報を返します。

リクエストの構文

```
GET /backup-vaults/backupVaultName/recovery-points/?
backupPlanId=ByBackupPlanId&backupVaultAccountId=BackupVaultAccountId&createdAfter=ByCreatedAft
 HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

BackupVaultAccountId

このパラメータは、復旧ポイントのリストをアカウント ID でソートします。

Pattern: `^[0-9]{12}$`

backupVaultName

バックアップを保存する論理コンテナの名前。バックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先の AWS リージョンに一意の名前で識別されます。

> **Note**
>
> サポートされているサービスが Backup を作成するときに、バックアップボールト名を使用できないことがあります。

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

必須：はい

ByBackupPlanId

指定したバックアッププラン ID に一致するリカバリポイントのみを返します。

ByCreatedAfter

指定されたタイムスタンプの後に作成されたリカバリポイントのみを返します。

ByCreatedBefore

指定されたタイムスタンプの前に作成されたリカバリポイントのみを返します。

ByParentRecoveryPointArn

これにより、指定された親 (複合) 復旧ポイントの Amazon リソースネーム (ARN) に一致する復旧ポイントのみを返します。

ByResourceArn

指定されたリソースの Amazon リソースネーム (ARN) に一致する復旧ポイントのみを返します。

ByResourceType

指定されたリソースタイプに一致する復旧ポイントのみを返します。

- Amazon Aurora の場合は `Aurora`
- `CloudFormation` の AWS CloudFormation
- Amazon DocumentDB (MongoDB 互換性) の場合は `DocumentDB`
- Amazon DynamoDB 用の `DynamoDB`
- Amazon Elastic Block Store 用の `EBS`
- Amazon Elastic Compute Cloud 用の `EC2`
- Amazon Elastic File System 用の `EFS`
- Amazon FSx の場合 用の `FSx`
- Amazon Neptune の場合は `Neptune`
- Amazon Redshift の場合は `Redshift`
- Amazon Relational Database Service の場合は `RDS`
- SAP HANA データベースの場合は `SAP HANA on Amazon EC2`
- `Storage Gateway` の AWS Storage Gateway
- Amazon S3 の場合は `S3`
- Amazon Timestream 用の `Timestream`
- 仮想マシンの場合は `VirtualMachine`

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

MaxResults

返されるアイテムの最大数。

有効な範囲: 最小値 は 1 です。最大値は 1000 です。

NextToken

返された項目の一部リストに続く次の項目。たとえば、MaxResults アイテム数のリクエストが行われるようにされた場合、NextToken では、次のトークンが指すロケーションから開始して、リスト内のより多くのアイテムを返すことができます。

リクエスト本文

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "RecoveryPoints": [
      {
         "BackupSizeInBytes": number,
         "BackupVaultArn": "string",
         "BackupVaultName": "string",
         "CalculatedLifecycle": {
            "DeleteAt": number,
            "MoveToColdStorageAt": number
         },
         "CompletionDate": number,
         "CompositeMemberIdentifier": "string",
         "CreatedBy": {
            "BackupPlanArn": "string",
            "BackupPlanId": "string",
            "BackupPlanVersion": "string",
            "BackupRuleId": "string"
         },
         "CreationDate": number,
         "EncryptionKeyArn": "string",
         "IamRoleArn": "string",
         "IsEncrypted": boolean,
         "IsParent": boolean,
         "LastRestoreTime": number,
         "Lifecycle": {
```

```
            "DeleteAfterDays": number,
            "MoveToColdStorageAfterDays": number,
            "OptInToArchiveForSupportedResources": boolean
         },
         "ParentRecoveryPointArn": "string",
         "RecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceName": "string",
         "ResourceType": "string",
         "SourceBackupVaultArn": "string",
         "Status": "string",
         "StatusMessage": "string",
         "VaultType": "string"
      }
   ]
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

NextToken

返された項目の一部リストに続く次の項目。たとえば、MaxResults アイテム数のリクエストが行われるようにされた場合、NextToken では、次のトークンが指す口ケーションから開始して、リスト内のより多くのアイテムを返すことができます。

型: 文字列

RecoveryPoints

バックアップボールトに保存された復旧ポイントに関する詳細情報を含むオブジェクトの配列。

型: RecoveryPointByBackupVault オブジェクトの配列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListRecoveryPointsByLegalHold

サービス: AWS Backup

このアクションは、指定されたリーガルホールドの復旧ポイントの ARN (Amazon リソースネーム) を返します。

リクエストの構文

```
GET /legal-holds/legalHoldId/recovery-points?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

legalHoldId

リーガルホールドの ID。

必須: はい

MaxResults

返されるリソースリストアイテムの最大数。

有効範囲: 最小値は 1 です。最大値は 1000 です。

NextToken

返されるリソースの部分的リストに続く次の項目です。例えば、MaxResults の数のリソースを返すようにリクエストが行われた場合、NextToken を使用すると、このトークンが指す場所から開始してさらにリストの項目を返すことができます。

リクエスト本文

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
```

```
   "NextToken": "string",
   "RecoveryPoints": [
      {
         "BackupVaultName": "string",
         "RecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceType": "string"
      }
   ]
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

NextToken

返されるリソースの部分的リストに続く次の項目です。

型: 文字列

RecoveryPoints

復旧ポイント。

型: RecoveryPointMember オブジェクトの配列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListRecoveryPointsByResource

サービス: AWS Backup

リソース Amazon リソースネーム (ARN) で指定されたタイプの復旧ポイントに関する情報。

> **Note**
>
> Amazon EFS および Amazon EC2 の場合、このアクションは AWS Backupによって作成されたリカバリポイントのみを一覧表示します。

リクエストの構文

```
GET /resources/resourceArn/recovery-points/?
managedByAWSBackupOnly=ManagedByAWSBackupOnly&maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

[ManagedByAWSBackupOnly]

この属性は、所有権に基づいて復旧ポイントをフィルタリングします。

これを に設定するとTRUE、 によって管理される選択したリソースに関連付けられた復旧ポイントがレスポンスに含まれます AWS Backup。

これを に設定するとFALSE、レスポンスには、選択したリソースに関連付けられているすべての復旧ポイントが含まれます。

型: ブール値

[MaxResults]

返されるアイテムの最大数。

> **Note**
>
> Amazon RDS では 20 以上の値が必要です。

有効な範囲: 最小値 は 1 です。最大値は 1000 です。

NextToken

返された項目の一部リストに続く次の項目。たとえば、MaxResults アイテム数のリクエストが行われるようにされた場合、NextToken では、次のトークンが指す口ケーションから開始して、リスト内のより多くのアイテムを返すことができます。

resourceArn

リソースを一意に識別する ARN。ARN の形式は、リソースタイプによって異なります。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "RecoveryPoints": [
      {
         "BackupSizeBytes": number,
         "BackupVaultName": "string",
         "CreationDate": number,
         "EncryptionKeyArn": "string",
         "IsParent": boolean,
         "ParentRecoveryPointArn": "string",
         "RecoveryPointArn": "string",
         "ResourceName": "string",
         "Status": "string",
         "StatusMessage": "string",
         "VaultType": "string"
      }
   ]
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

NextToken

返された項目の一部リストに続く次の項目。たとえば、MaxResults アイテム数のリクエストが行われるようにされた場合、NextToken では、次のトークンが指す口ケーションから開始して、リスト内のより多くのアイテムを返すことができます。

型: 文字列

RecoveryPoints

指定されたリソースタイプのリカバリポイントに関する詳細情報を含むオブジェクトの配列。

> **Note**
>
> Amazon EFS と Amazon EC2 リカバリポイントのみが を返します BackupVaultName。

型: RecoveryPointByResource オブジェクトの配列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListReportJobs

サービス: AWS Backup

レポートジョブの詳細を返します。

リクエストの構文

```
GET /audit/report-jobs?
CreationAfter=ByCreationAfter&CreationBefore=ByCreationBefore&MaxResults=MaxResults&NextToken=N
 HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

ByCreationAfter

Unix 形式および協定世界時 (UTC) で指定された日付と時刻の後に作成されたレポートジョブのみを返します。たとえば、1516925490 の値は、2018年 1月 26日 (金) 午前 12:11:30 を表します。

ByCreationBefore

Unix 形式および協定世界時 (UTC) で指定された日付と時刻より前に作成されたレポートジョブのみを返します。たとえば、1516925490 の値は、2018年 1月 26日 (金) 午前 12:11:30 を表します。

ByReportPlanName

指定したレポートプラン名を持つレポートジョブのみを返します。

長さの制限：最小長は 1 です。最大長は 256 です。

パターン：`[a-zA-Z][_a-zA-Z0-9]*`

ByStatus

指定されたステータスのレポートジョブのみを返します。ステータスは次のとおりです。

`CREATED | RUNNING | COMPLETED | FAILED`

MaxResults

1 から 1000 の範囲の望ましい結果の数。（オプション）。指定しない場合、クエリは 1 MB のデータを返します。

有効な範囲: 最小値 は 1 です。最大値は 1000 です。

NextToken

リスト内の次の項目のセットを返すために使用できる、この操作に対する前回の呼び出しから返された識別子。

リクエスト本文

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "ReportJobs": [
      {
         "CompletionTime": number,
         "CreationTime": number,
         "ReportDestination": {
            "S3BucketName": "string",
            "S3Keys": [ "string" ]
         },
         "ReportJobId": "string",
         "ReportPlanArn": "string",
         "ReportTemplate": "string",
         "Status": "string",
         "StatusMessage": "string"
      }
   ]
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

NextToken

リスト内の次の項目のセットを返すために使用できる、この操作に対する前回の呼び出しから返された識別子。

型: 文字列

ReportJobs

JSON 形式のレポートジョブに関する詳細。

型: ReportJob オブジェクトの配列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListReportPlans

サービス: AWS Backup

レポートプランのリストを返します。単一のレポートプランの詳細については、DescribeReportPlan を使用してください。

リクエストの構文

```
GET /audit/report-plans?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

MaxResults

1 から 1000 の範囲の望ましい結果の数。(オプション) 。指定しない場合、クエリは 1 MB のデータを返します。

有効な範囲: 最小値 は 1 です。最大値は 1000 です。

NextToken

リスト内の次の項目のセットを返すために使用できる、この操作に対する前回の呼び出しから返された識別子。

リクエスト本文

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "ReportPlans": [
      {
         "CreationTime": number,
         "DeploymentStatus": "string",
         "LastAttemptedExecutionTime": number,
         "LastSuccessfulExecutionTime": number,
```

```
         "ReportDeliveryChannel": {
            "Formats": [ "string" ],
            "S3BucketName": "string",
            "S3KeyPrefix": "string"
         },
         "ReportPlanArn": "string",
         "ReportPlanDescription": "string",
         "ReportPlanName": "string",
         "ReportSetting": {
            "Accounts": [ "string" ],
            "FrameworkArns": [ "string" ],
            "NumberOfFrameworks": number,
            "OrganizationUnits": [ "string" ],
            "Regions": [ "string" ],
            "ReportTemplate": "string"
         }
      }
   ]
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

NextToken

リスト内の次の項目のセットを返すために使用できる、この操作に対する前回の呼び出しから返された識別子。

型: 文字列

ReportPlans

レポートプランと各プランの詳細情報。この情報には、Amazon リソースネーム（ARN）、レポートプラン名、説明、設定、配信チャネル、デプロイステータス、作成時刻、レポートプランが正常に実行された最後の時間が含まれます。

型: ReportPlan オブジェクトの配列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListRestoreJobs

サービス: AWS Backup

復旧プロセスの詳細を含め、保存されたリソースの復元 AWS Backup を開始したジョブのリストを返します。

リクエストの構文

```
GET /restore-jobs/?
accountId=ByAccountId&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore&createdAfte
 HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

ByAccountId

ジョブを一覧表示するアカウント ID。指定されたアカウント ID に関連付けられた復元ジョブのみを返します。

Pattern: `^[0-9]{12}$`

ByCompleteAfter

Unix 形式および協定世界時 (UTC) で表された日付の後に完了したコピージョブのみを返します。

ByCompleteBefore

Unix 形式および協定世界時 (UTC) で表される日付より前に完了したコピージョブのみを返します。

ByCreatedAfter

指定した日付より後に作成された復元ジョブのみを返します。

ByCreatedBefore

指定した日付より前に作成された復元ジョブのみを返します。

ByResourceType

このパラメータを追加すると、指定されたリソースの復元ジョブのみを返します。

- Amazon Aurora の場合は `Aurora`

- CloudFormation の AWS CloudFormation
- Amazon DocumentDB (MongoDB 互換性) の場合は DocumentDB
- Amazon DynamoDB 用の DynamoDB
- Amazon Elastic Block Store 用の EBS
- Amazon Elastic Compute Cloud 用の EC2
- Amazon Elastic File System 用の EFS
- Amazon FSx の場合 用の FSx
- Amazon Neptune の場合は Neptune
- Amazon Redshift の場合は Redshift
- Amazon Relational Database Service の場合は RDS
- SAP HANA データベースの場合は SAP HANA on Amazon EC2
- Storage Gateway の AWS Storage Gateway
- Amazon S3 の場合は S3
- Amazon Timestream 用の Timestream
- 仮想マシンの場合は VirtualMachine

Pattern: ^[a-zA-Z0-9\-_\.]{1,50}$

ByRestoreTestingPlanArn

指定されたリソースの Amazon リソースネーム (ARN) に一致する復元テストジョブのみを返します。

ByStatus

指定されたジョブステータスに関連付けられた復元ジョブのみを返します。

有効な値：PENDING | RUNNING | COMPLETED | ABORTED | FAILED

MaxResults

返されるアイテムの最大数。

有効な範囲: 最小値 は 1 です。最大値は 1000 です。

NextToken

返された項目の一部リストに続く次の項目。たとえば、MaxResults アイテム数のリクエストが行われるようにされた場合、NextToken では、次のトークンが指す口ケーションから開始して、リスト内のより多くのアイテムを返すことができます。

リクエスト本文

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "RestoreJobs": [
      {
         "AccountId": "string",
         "BackupSizeInBytes": number,
         "CompletionDate": number,
         "CreatedBy": {
            "RestoreTestingPlanArn": "string"
         },
         "CreatedResourceArn": "string",
         "CreationDate": number,
         "DeletionStatus": "string",
         "DeletionStatusMessage": "string",
         "ExpectedCompletionTimeMinutes": number,
         "IamRoleArn": "string",
         "PercentDone": "string",
         "RecoveryPointArn": "string",
         "RecoveryPointCreationDate": number,
         "ResourceType": "string",
         "RestoreJobId": "string",
         "Status": "string",
         "StatusMessage": "string",
         "ValidationStatus": "string",
         "ValidationStatusMessage": "string"
      }
   ]
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

NextToken

返された項目の一部リストに続く次の項目。たとえば、MaxResults アイテム数のリクエストが行われるようにされた場合、NextToken では、次のトークンが指す口ケーションから開始して、リスト内のより多くのアイテムを返すことができます。

型: 文字列

RestoreJobs

保存されたリソースをリストアするためのジョブに関する詳細情報を含むオブジェクトの配列。

型: RestoreJobsListMember オブジェクトの配列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListRestoreJobsByProtectedResource

サービス: AWS Backup

指定された保護対象リソースを含む復元ジョブが返されます。

`ResourceArn` を含める必要があります。オプションで `NextToken`、`ByStatus`、`MaxResults`、`ByRecoveryPointCreationDateAfter`、および `ByRecoveryPointCreationDateBefore` を含めることができます。

リクエストの構文

```
GET /resources/resourceArn/restore-jobs/?
maxResults=MaxResults&nextToken=NextToken&recoveryPointCreationDateAfter=ByRecoveryPointCreatio
 HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

ByRecoveryPointCreationDateAfter

指定した日付より後に作成された復旧ポイントの復元ジョブのみを返します。

ByRecoveryPointCreationDateBefore

指定した日付より前に作成された復旧ポイントの復元ジョブのみを返します。

ByStatus

指定されたジョブステータスに関連付けられた復元ジョブのみを返します。

有効な値：`PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

MaxResults

返されるアイテムの最大数。

有効な範囲: 最小値 は 1 です。最大値は 1000 です。

NextToken

返された項目の一部リストに続く次の項目。例えば、`MaxResults` の数のアイテムを返すようにリクエストが行われた場合、`NextToken` を使用すると、このトークンが指す場所から開始してさらにリストのアイテムを返すことができます。

resourceArn

指定されたリソースの Amazon リソースネーム (ARN) に一致する復元ジョブのみを返します。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "RestoreJobs": [
      {
         "AccountId": "string",
         "BackupSizeInBytes": number,
         "CompletionDate": number,
         "CreatedBy": {
            "RestoreTestingPlanArn": "string"
         },
         "CreatedResourceArn": "string",
         "CreationDate": number,
         "DeletionStatus": "string",
         "DeletionStatusMessage": "string",
         "ExpectedCompletionTimeMinutes": number,
         "IamRoleArn": "string",
         "PercentDone": "string",
         "RecoveryPointArn": "string",
         "RecoveryPointCreationDate": number,
         "ResourceType": "string",
         "RestoreJobId": "string",
         "Status": "string",
         "StatusMessage": "string",
         "ValidationStatus": "string",
         "ValidationStatusMessage": "string"
      }
   ]
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

NextToken

返された項目の一部リストに続く次の項目。例えば、MaxResults の数の項目を返すようにリクエストが行われた場合、NextToken を使用すると、このトークンが指す場所から開始してさらにリストの項目を返すことができます。

型: 文字列

RestoreJobs

保存されたリソースを復元するためのジョブに関する詳細情報を含むオブジェクトの配列。

型: RestoreJobsListMember オブジェクトの配列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListRestoreJobSummaries

サービス: AWS Backup

このリクエストは、過去 30 日以内に作成または実行された復元ジョブの概要を取得します。AccountID、State、 ResourceType、または パラメータを含めて AggregationPeriod MaxResults、結果を NextToken フィルタリングできます。

このリクエストは、リージョン、アカウント、状態、 RestourceType MessageCategory、StartTime EndTime、および含まれるジョブの数を含む概要を返します。

リクエストの構文

```
GET /audit/restore-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&NextToken=NextTok
 HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

AccountId

指定されたアカウントのジョブ数を返します。

リクエストがメンバーアカウントまたは AWS Organizations の一部ではないアカウントから送信されると、リクエスタのアカウント内のジョブが返されます。

ルート、管理者、および委任された管理者アカウントでは、ANY の値を使用して、組織内のすべてのアカウントのジョブ数を返すことができます。

AGGREGATE_ALL は、認証された組織内のすべてのアカウントのジョブ数を集計し、その合計を返します。

Pattern: ^[0-9]{12}$

AggregationPeriod

返された結果の期間。

- ONE_DAY - 過去 14 日間の毎日のジョブ数。
- SEVEN_DAYS - 過去 7 日間の集計ジョブ数。
- FOURTEEN_DAYS - 過去 14 日間の集計ジョブ数。

有効な値：ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS

MaxResults

このパラメータは返されるアイテムの最大数を指定します。

値は整数です。指定できる値の範囲は 1～500 です。

有効範囲: 最小値は 1 です。最大値は 1000 です。

NextToken

返されるリソースの部分的リストに続く次の項目です。例えば、MaxResults の数のリソースを返すようにリクエストが行われた場合、NextToken を使用すると、このトークンが指す場所から開始してさらにリストの項目を返すことができます。

ResourceType

指定されたリソースタイプのジョブ数を返します。リクエスト GetSupportedResourceTypes を使用して、サポートされているリソースタイプの文字列を取得します。

値 ANY は、すべてのリソースタイプの数を返します。

AGGREGATE_ALL は、すべてのリソースタイプのジョブ数を集計し、その合計を返します。

バックアップする AWS リソースのタイプ。Amazon Elastic Block Store (Amazon EBS) ボリュームや Amazon Relational Database Service (Amazon RDS) データベースなど。

Pattern: ^[a-zA-Z0-9\-_\.]{1,50}$

State

このパラメータは、指定された状態のジョブの数を返します。

値 ANY は、すべての状態の数を返します。

AGGREGATE_ALL は、すべての状態のジョブ数を集計し、その合計を返します。

有効な値：CREATED | PENDING | RUNNING | ABORTED | COMPLETED | FAILED | AGGREGATE_ALL | ANY

リクエスト本文

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "AggregationPeriod": "string",
   "NextToken": "string",
   "RestoreJobSummaries": [
      {
         "AccountId": "string",
         "Count": number,
         "EndTime": number,
         "Region": "string",
         "ResourceType": "string",
         "StartTime": number,
         "State": "string"
      }
   ]
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

AggregationPeriod

返された結果の期間。

- ONE_DAY - 過去 14 日間の毎日のジョブ数。
- SEVEN_DAYS - 過去 7 日間の集計ジョブ数。
- FOURTEEN_DAYS - 過去 14 日間の集計ジョブ数。

型: 文字列

NextToken

返されるリソースの部分的リストに続く次の項目です。例えば、MaxResults の数のリソースを返すようにリクエストが行われた場合、NextToken を使用すると、このトークンが指す場所から開始してさらにリストの項目を返すことができます。

型: 文字列

RestoreJobSummaries

この戻り値には、リージョン、アカウント、状態 ResourceType、 MessageCategory、StartTime EndTime、および含まれるジョブの数を含む概要が含まれます。

型: RestoreJobSummary オブジェクトの配列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListRestoreTestingPlans

サービス: AWS Backup

復元テストプランのリストを返します。

リクエストの構文

```
GET /restore-testing/plans?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

MaxResults

返されるアイテムの最大数。

有効な範囲: 最小値 は 1 です。最大値は 1000 です。

NextToken

返された項目の一部リストに続く次の項目。例えば、MaxResults の数の項目を返すようにリクエストが行われた場合、NextToken を使用すると、このトークンが指す場所から開始してさらにリストの項目を返すことができます。

リクエスト本文

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "RestoreTestingPlans": [
      {
         "CreationTime": number,
         "LastExecutionTime": number,
         "LastUpdateTime": number,
         "RestoreTestingPlanArn": "string",
```

```
            "RestoreTestingPlanName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowHours": number
        }
    ]
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

NextToken

返された項目の一部リストに続く次の項目。例えば、MaxResults の数の項目を返すようにリクエストが行われた場合、NextToken を使用すると、このトークンが指す場所から開始してさらにリストの項目を返すことができます。

型: 文字列

RestoreTestingPlans

返される復元テストプランのリストです。

型: RestoreTestingPlanForList オブジェクトの配列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListRestoreTestingSelections

サービス: AWS Backup

復元テスト選択のリストを返します。MaxResults と RestoreTestingPlanName でフィルタリングできます。

リクエストの構文

```
GET /restore-testing/plans/RestoreTestingPlanName/selections?
MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

MaxResults

返されるアイテムの最大数。

有効な範囲: 最小値 は 1 です。最大値は 1000 です。

NextToken

返された項目の一部リストに続く次の項目。例えば、MaxResults の数の項目を返すようにリクエストが行われた場合、NextToken を使用すると、このトークンが指す場所から開始してさらにリストの項目を返すことができます。

RestoreTestingPlanName

指定された復元テストプラン名で復元テスト選択を返します。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "NextToken": "string",
   "RestoreTestingSelections": [
      {
         "CreationTime": number,
         "IamRoleArn": "string",
         "ProtectedResourceType": "string",
         "RestoreTestingPlanName": "string",
         "RestoreTestingSelectionName": "string",
         "ValidationWindowHours": number
      }
   ]
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

NextToken

返された項目の一部リストに続く次の項目。例えば、MaxResults の数の項目を返すようにリクエストが行われた場合、NextToken を使用すると、このトークンが指す場所から開始してさらにリストの項目を返すことができます。

型: 文字列

RestoreTestingSelections

復元テストプランに関連付けられた復元テスト選択を返します。

型: RestoreTestingSelectionForList オブジェクトの配列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListTags

サービス: AWS Backup

ターゲット復旧ポイント、バックアッププラン、バックアップボールトなど、リソースに割り当てられたタグを返します。

完全な AWS Backup バックアップの管理 をサポートする ListTags リソースタイプに対してのみ機能します。これらのリソースタイプは、「リソース別の機能の可用性」表に記載されています。

リクエストの構文

```
GET /tags/resourceArn/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

MaxResults

返されるアイテムの最大数。

有効な範囲: 最小値 は 1 です。最大値は 1000 です。

NextToken

返された項目の一部リストに続く次の項目。たとえば、MaxResults アイテム数のリクエストが行われるようにされた場合、NextToken では、次のトークンが指す口ケーションから開始して、リスト内のより多くのアイテムを返すことができます。

resourceArn

リソースを一意に識別する Amazon リソースネーム (ARN)。ARN の形式はリソースのタイプによって異なります。ListTags の有効なターゲットはリカバリポイント、バックアッププラン、およびバックアップボルトです。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "NextToken": "string",
   "Tags": {
      "string" : "string"
   }
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

NextToken

返された項目の一部リストに続く次の項目。たとえば、MaxResults アイテム数のリクエストが行われるようにされた場合、NextToken では、次のトークンが指す口ケーションから開始して、リスト内のより多くのアイテムを返すことができます。

型: 文字列

Tags

タグに関する情報。

型: 文字列間のマッピング

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutBackupVaultAccessPolicy

サービス: AWS Backup

ターゲットのバックアップボールトのアクセス許可を管理するために使用されるリソースベースのポリシーを設定します。バックアップボールト名と JSON 形式のアクセスポリシードキュメントが必要です。

リクエストの構文

```
PUT /backup-vaults/backupVaultName/access-policy HTTP/1.1
Content-type: application/json

{
   "Policy": "string"
}
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

backupVaultName

バックアップを保存する論理コンテナの名前。バックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先の AWS リージョンに一意の名前で識別されます。

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

必須: はい

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

Policy

JSON 形式のバックアップボールトのアクセスポリシードキュメント。

タイプ: 文字列

必須: いいえ

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutBackupVaultLockConfiguration

サービス: AWS Backup

AWS Backup ボールトロックをバックアップボールトに適用し、バックアップボールトに保存されている、またはバックアップボールトに作成された復旧ポイントの削除を試行しないようにします。また、Vault Lock では、バックアップボールトに現在保存されているリカバリポイントの保持期間を制御するライフサイクルポリシーの更新も防止されます。指定した場合、Vault Lock は、バックアップボールトを対象とする将来のバックアップジョブおよびコピージョブに対して、最小および最大保持期間を適用します。

> **Note**
>
> AWS Backup ボールトロックは、SEC 17a-4、CFTC、および FINRA の規制の対象となる環境での使用について、Cohasset Associates によって評価されています。 AWS Backup ボールトロックがこれらの規制にどのように関連しているかの詳細については、「Cohasset Associates Compliance Assessment」を参照してください。

詳細については、「AWS Backup ボールトロック」を参照してください。

リクエストの構文

```
PUT /backup-vaults/backupVaultName/vault-lock HTTP/1.1
Content-type: application/json

{
   "ChangeableForDays": number,
   "MaxRetentionDays": number,
   "MinRetentionDays": number
}
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

backupVaultName

保護するバックアップ AWS Backup ボールトの名前を指定するボールトロック設定。

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

必須: はい

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

ChangeableForDays

ロック日前の日数を指定する AWS Backup ボールトロック設定。たとえば、2022 年 1 月 1 日午後 8 時 UTC に ChangeableForDays を 30 に設定した場合、2022 年 1 月 31 日午後 8 時 UTC にロック日が設定されます。

AWS Backup は、ボールトロックが有効になりイミュータブルになる前に、72 時間のクーリングオフ期間を適用します。したがって、ChangeableForDays を 3 以上に設定する必要があります。

ロック日より前には、DeleteBackupVaultLockConfiguration を使用して ボールトロックをボールトから削除でき、また、PutBackupVaultLockConfiguration を使用してボールトロックの構成を変更します。ロック日以降では、ボールトロックは不変になり、変更や削除はできません。

このパラメータを指定しない場合は、DeleteBackupVaultLockConfiguration を使用してボールトからボールトロックを削除でき、または、PutBackupVaultLockConfiguration を使用して、いつでもボールトロックの設定を変更できます。

型: Long

必須: いいえ

MaxRetentionDays

AWS Backup ボールトが復旧ポイントを保持する最大保持期間を指定するボールトロック設定。この設定は、たとえば、組織のポリシーで 4 年間 (1460 日) 保持した後に特定のデータを破棄する必要がある場合などに便利です。

このパラメータを指定しない場合、ボールトロックはボールト内のリカバリポイントに最大保持期間を強制しません。このパラメータが値なしで含まれている場合、ボールトロックは最大保持期間を適用しません。

このパラメータを指定した場合、ボールトへのバックアップジョブまたはコピージョブには、保存期間が最大保存期間以下のライフサイクル· ポリシーを持つ必要があります。ジョブの保持期

間がその最大保存期間よりも長い場合、ボールトはバックアップジョブまたはコピージョブに失敗するため、ライフサイクル設定を変更するか、別のボールトを使用する必要があります。指定できる最長の最大保持期間は 36500 日 (約 100 年) です。ボールトロックの前にボールトにすでに保存されている復旧ポイントは影響を受けません。

型: Long

必須: いいえ

MinRetentionDays

AWS Backup ボールトが復旧ポイントを保持する最小保持期間を指定するボールトロック設定。この設定は、たとえば、組織のポリシーで特定のデータを少なくとも 7 年間 (2555 日) 保持する必要がある場合に便利です。

このパラメータは、 を使用してボールトロックを作成する場合に必要です AWS CloudFormation。それ以外の場合、このパラメータはオプションです。このパラメータを指定しない場合、ボールトロックは最小保持期間を強制しません。

このパラメータを指定した場合、ボールトへのバックアップジョブまたはコピージョブには、最小保存期間以上の保存期間を持つライフサイクルポリシーが必要です。ジョブの保持期間がその最小保存期間よりも短い場合、ボールトはそのバックアップジョブまたはコピージョブに失敗するため、ライフサイクル設定を変更するか、別のボールトを使用する必要があります。指定できる最小保持期間は 1 日です。ボールトロックの前にボールトにすでに保存されている復旧ポイントは影響を受けません。

型: Long

必須: いいえ

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

InvalidRequestException

リクエストへの入力に何らかの問題が発生していることを示します。たとえば、パラメータのタイプが間違っています。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3

- AWS SDK for Python
- AWS SDK for Ruby V3

PutBackupVaultNotifications

サービス: AWS Backup

指定されたトピックとイベントのバックアップボールトの通知をオンにします。

リクエストの構文

```
PUT /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
Content-type: application/json

{
   "BackupVaultEvents": [ "string" ],
   "SNSTopicArn": "string"
}
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

backupVaultName

バックアップを保存する論理コンテナの名前。バックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先の AWS リージョンに一意の名前で識別されます。

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

必須: はい

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

BackupVaultEvents

リソースをバックアップボールトにバックアップするジョブのステータスを示すイベントの配列。

一般的なユースケースとコードサンプルについては、Amazon SNSを使用して AWS Backup イベントを追跡する」を参照してください。

次のイベントがサポートされています。

- BACKUP_JOB_STARTED | BACKUP_JOB_COMPLETED

- COPY_JOB_STARTED | COPY_JOB_SUCCESSFUL | COPY_JOB_FAILED
- RESTORE_JOB_STARTED | RESTORE_JOB_COMPLETED | RECOVERY_POINT_MODIFIED
- S3_BACKUP_OBJECT_FAILED | S3_RESTORE_OBJECT_FAILED

> **Note**
>
> 以下のリストには、サポートされるイベントと、使用されなくなった非推奨イベント (参考) の両方が含まれています。非推奨のイベントは、ステータスや通知を返しません。サポートされているイベントについては、上記のリストを参照してください。

タイプ：文字列の配列

有効な値：BACKUP_JOB_STARTED | BACKUP_JOB_COMPLETED | BACKUP_JOB_SUCCESSFUL | BACKUP_JOB_FAILED | BACKUP_JOB_EXPIRED | RESTORE_JOB_STARTED | RESTORE_JOB_COMPLETED | RESTORE_JOB_SUCCESSFUL | RESTORE_JOB_FAILED | COPY_JOB_STARTED | COPY_JOB_SUCCESSFUL | COPY_JOB_FAILED | RECOVERY_POINT_MODIFIED | BACKUP_PLAN_CREATED | BACKUP_PLAN_MODIFIED | S3_BACKUP_OBJECT_FAILED | S3_RESTORE_OBJECT_FAILED

必須: はい

SNSTopicArn

たとえば、arn:aws:sns:us-west-2:111122223333:MyVaultTopic などのバックアップボールトのイベントのトピックを指定する Amazon リソースネーム (ARN)。

型: 文字列

必須: はい

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python

- AWS SDK for Ruby V3

PutRestoreValidationResult

サービス: AWS Backup

このリクエストにより、独立した自己実行による復元テストの検証結果を送信できます。RestoreJobId および ValidationStatus は必須です。オプションで ValidationStatusMessage を入力できます。

リクエストの構文

```
PUT /restore-jobs/restoreJobId/validations HTTP/1.1
Content-type: application/json

{
   "ValidationStatus": "string",
   "ValidationStatusMessage": "string"
}
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

restoreJobId

これは、 内の復元ジョブの一意の識別子です AWS Backup。

必須: はい

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

ValidationStatus

復元検証のステータス。

型: 文字列

有効な値 : FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING

必須: はい

ValidationStatusMessage

オプションのメッセージ文字列で、復元テストの検証のステータスを説明するために入力できます。

タイプ: 文字列

必須: いいえ

レスポンスの構文

```
HTTP/1.1 204
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 204 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

InvalidRequestException

リクエストへの入力に何らかの問題が発生していることを示します。たとえば、パラメータのタイプが間違っています。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

StartBackupJob

サービス: AWS Backup

指定したリソースに対してオンデマンドバックアップジョブを開始します。

リクエストの構文

```
PUT /backup-jobs HTTP/1.1
Content-type: application/json

{
   "BackupOptions": {
      "string" : "string"
   },
   "BackupVaultName": "string",
   "CompleteWindowMinutes": number,
   "IamRoleArn": "string",
   "IdempotencyToken": "string",
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   },
   "RecoveryPointTags": {
      "string" : "string"
   },
   "ResourceArn": "string",
   "StartWindowMinutes": number
}
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

BackupOptions

選択したリソースのバックアップオプション。このオプションは、Windows ボリュームシャドウコピーサービス (VSS) バックアップジョブでのみ使用できます。

有効な値:"WindowsVSS":"enabled" に設定してWindowsVSS バックアップオプションをを有効にし、Windows VSS バックアップを作成します。"WindowsVSS""disabled" に設定して、通常のバックアップを作成します。デフォルトでは、WindowsVSS のオプションは有効になっていません。

型: 文字列から文字列へのマッピング

キーパターン: ^[a-zA-Z0-9\-_\.]{1,50}$

値パターン:^[a-zA-Z0-9\-_\.]{1,50}$

必須: いいえ

BackupVaultName

バックアップを保存する論理コンテナの名前。バックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先の AWS リージョンに一意の名前で識別されます。

型: 文字列

Pattern: ^[a-zA-Z0-9\-_]{2,50}$

必須：はい

CompleteWindowMinutes

正常に開始されたバックアップを完了する必要がある時間（分単位）、または AWS Backup がジョブをキャンセルします。この値はオプションです。この値は、バックアップがスケジュールされた時点からカウントダウンを開始します。StartWindowMinutes またはバックアップがスケジュールより遅れて開始された場合、追加時間は追加されません。

StartWindowMinutes と同様に、このパラメータの最大値は 100 年 (52,560,000 分) です。

型: Long

必須: いいえ

IamRoleArn

ターゲット復旧ポイントの作成に使用する IAM ロール ARN を指定します。例えば、arn:aws:iam::123456789012:role/S3Accessです。

型: 文字列

必須: はい

IdempotencyToken

別の StartBackupJob への同じコール間を区別するために使用できる顧客が選択した文字列。同じ冪等性トークンで成功したリクエストを再試行すると、アクションは実行されず、成功メッセージが表示されます。

タイプ: 文字列

必須: いいえ

Lifecycle

ライフサイクルは、保護されたリソースがコールドストレージに移行するタイミングと有効期限を定義します。 AWS Backup は、定義したライフサイクルに従ってバックアップを自動的に移行して期限切れにします。

コールドストレージに移行されたバックアップは、そこに最低 90 日保存される必要があります。したがって、「保持期間」の設定は、「コールドへの移行 (日数)」設定から 90 日以上あける必要があります。バックアップがコールドに移行された後で、「コールドへの移行 (日数)」設定を変更することはできません。

コールドストレージに移行できるリソースタイプは、「リソース別の機能の可用性」の表に記載されています。他のリソースタイプでは、この式は AWS Backup 無視されます。

このパラメータの最大値は 100 年 (36,500 日) です。

タイプ：Lifecycle オブジェクト

必須: いいえ

RecoveryPointTags

リソースに割り当てるタグ。

型: 文字列間のマッピング

必須: いいえ

ResourceArn

リソースを一意に識別する Amazon リソースネーム (ARN)。ARN の形式は、リソースタイプによって異なります。

型: 文字列

必須: はい

StartWindowMinutes

バックアップがスケジュールされてから、正常に開始されない場合にジョブがキャンセルされるまでの時間の分単位での値。この値はオプションであり、デフォルト値は 8時間です。この値を含める場合、エラーを避けるために少なくとも 60 分必要です。

このパラメータの最大値は 100 年 (52,560,000 分) です。

開始ウィンドウ中、バックアップジョブのステータスは、正常に開始されるか、開始ウィンドウの時間がなくなるまで CREATED ステータスのままになります。開始ウィンドウ時間内にジョブを再試行できるエラー AWS Backup を受け取った場合、 AWS Backup は、バックアップが正常に開始 (ジョブステータスが に変わるRUNNING) するか、ジョブステータスが に変わる EXPIRED (開始ウィンドウ時間が終了すると発生することが予想される) まで、少なくとも 10 分ごとにジョブの開始を自動的に再試行します。

型: Long

必須: いいえ

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupJobId": "string",
   "CreationDate": number,
   "IsParent": boolean,
   "RecoveryPointArn": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

BackupJobId

リソースをバックアップ AWS Backup する へのリクエストを一意に識別します。

型: 文字列

CreationDate

バックアップジョブが作成された日時 (Unix 時刻形式および協定世界時 (UTC))。CreationDateの値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

IsParent

これは親 (複合) バックアップジョブであることを示す、返されたブール値です。

型: ブール値

RecoveryPointArn

注: このフィールドは Amazon EFS リソースと高度な DynamoDB リソースのみで返されます。

リカバリーポイントを一意に識別する ARN、たとえば、arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45 です。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

InvalidRequestException

リクエストへの入力に何らかの問題が発生していることを示します。たとえば、パラメータのタイプが間違っています。

HTTP ステータスコード：400

LimitExceededException

たとえば、リクエストで許可されるアイテムの最大数などのリクエストの制限を超えました。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

StartCopyJob

サービス: AWS Backup

ジョブを開始し、指定したリソースの 1 回限りのコピーを作成します。

連続バックアップをサポートしません。

リクエストの構文

```
PUT /copy-jobs HTTP/1.1
Content-type: application/json

{
   "DestinationBackupVaultArn": "string",
   "IamRoleArn": "string",
   "IdempotencyToken": "string",
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   },
   "RecoveryPointArn": "string",
   "SourceBackupVaultName": "string"
}
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

DestinationBackupVaultArn

たとえば、arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault などのコピーするバックアップボールトを一意に識別する Amazon リソースネーム (ARN) です。

型: 文字列

必須: はい

IamRoleArn

たとえば、arn:aws:iam::123456789012:role/S3Access などのターゲットリカバリポイントのコピーに使用する IAM ロール ARN を指定します。

型: 文字列

必須: はい

IdempotencyToken

別の StartCopyJob への同じコール間を区別するために使用できる顧客が選択した文字列。同じ冪等性トークンで成功したリクエストを再試行すると、アクションは実行されず、成功メッセージが表示されます。

タイプ: 文字列

必須: いいえ

Lifecycle

復旧ポイントがコールドストレージに移行するか、削除されるまでの時間を日数で指定します。

コールドストレージに移行されたバックアップは、そこに最低 90 日保存される必要があります。したがって、コンソールでは、保持設定は、日数設定後のコールドへの移行よりも 90 日長くする必要があります。バックアップがコールドに移行した後、日数設定をコールドに移行することはできません。

コールドストレージに移行できるリソースタイプは、「リソース別の機能の可用性」の表に記載されています。他のリソースタイプでは、この式は AWS Backup 無視されます。

既存のライフサイクルと保持期間を削除し、復旧ポイントを無期限に保持するには、MoveToColdStorageAfterDaysと に -1 を指定しますDeleteAfterDays。

タイプ：Lifecycle オブジェクト

必須: いいえ

RecoveryPointArn

たとえば、arn:aws:backup:us-east-1:123456789012:recovery-point:1eb3456789012:recovery-point:1eb3456789012:recovery-point: 1eb3456789012 などのコピージョブに使用するリカバリポイントを一意に識別する ARN。

型: 文字列

必須: はい

SourceBackupVaultName

バックアップを保存する論理ソースコンテナの名前。バックアップボールトは、作成に使用したアカウントと作成先の AWS リージョンに固有の名前で識別されます。

型: 文字列

Pattern: ^[a-zA-Z0-9\-_]{2,50}$

必須：はい

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "CopyJobId": "string",
   "CreationDate": number,
   "IsParent": boolean
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

CopyJobId

コピージョブを一意に識別する。

型: 文字列

CreationDate

コピージョブが作成された日時 (Unix 時刻形式および協定世界時 (UTC))。CreationDateの値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前 12:11:30.087 を表します。

型: タイムスタンプ

IsParent

これは親 (複合) バックアップジョブであることを示す、返されたブール値です。

型: ブール値

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

InvalidRequestException

リクエストへの入力に何らかの問題が発生していることを示します。たとえば、パラメータのタイプが間違っています。

HTTP ステータスコード：400

LimitExceededException

たとえば、リクエストで許可されるアイテムの最大数などのリクエストの制限を超えました。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

StartReportJob

サービス: AWS Backup

指定したレポートプランのオンデマンドレポートジョブを開始します。

リクエストの構文

```
POST /audit/report-jobs/reportPlanName HTTP/1.1
Content-type: application/json

{
   "IdempotencyToken": "string"
}
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

reportPlanName

レポートプランの一意の名前。

長さの制限：最小長は 1 です。最大長は 256 です。

パターン：`[a-zA-Z][_a-zA-Z0-9]*`

必須: はい

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

IdempotencyToken

別の `StartReportJobInput` への同じコール間を区別するために使用できる顧客が選択した文字列。同じ冪等性トークンで成功したリクエストを再試行すると、アクションは実行されず、成功メッセージが表示されます。

タイプ: 文字列

必須: いいえ

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "ReportJobId": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

ReportJobId

レポートジョブの識別子。一意のランダムに生成された UTF-8 エンコード Unicode 文字列 (最大 1,024 バイト長)。レポートジョブ ID を編集することはできません。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

StartRestoreJob

サービス: AWS Backup

Amazon リソースネーム (ARN) で識別された保存されたリソースを回復します。

リクエストの構文

```
PUT /restore-jobs HTTP/1.1
Content-type: application/json

{
   "CopySourceTagsToRestoredResource": boolean,
   "IamRoleArn": "string",
   "IdempotencyToken": "string",
   "Metadata": {
      "string" : "string"
   },
   "RecoveryPointArn": "string",
   "ResourceType": "string"
}
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

CopySourceTagsToRestoredResource

このパラメータはオプションです。これが `True` に等しい場合、バックアップに含まれるタグは復元されたリソースにコピーされます。

これは、 で作成されたバックアップにのみ適用されます AWS Backup。

型: ブール値

必須: いいえ

IamRoleArn

がターゲットリソースの作成 AWS Backup に使用する IAM ロールの Amazon リソースネーム (ARN)。例: `arn:aws:iam::123456789012:role/S3Access`。

タイプ: 文字列

必須: いいえ

IdempotencyToken

別の StartRestoreJob への同じコール間を区別するために使用できる顧客が選択した文字列。同じ冪等性トークンで成功したリクエストを再試行すると、アクションは実行されず、成功メッセージが表示されます。

タイプ: 文字列

必須: いいえ

Metadata

メタデータのキーと値のペアのセット。

GetRecoveryPointRestoreMetadata を呼び出して、バックアップ時にリソースに関する構成メタデータを取得できます。ただし、GetRecoveryPointRestoreMetadata によって提供される値に加えて値リソースの復元が必要になる場合があります。たとえば、元のリソースがすでに存在する場合は、新しいリソース名を指定する必要があります。

各リソースのメタデータの詳細については、以下を参照してください。

- Amazon Aurora のメタデータ
- Amazon DocumentDB のメタデータ
- のメタデータ AWS CloudFormation
- Amazon DynamoDB のメタデータ
- Amazon EBS のメタデータ
- Amazon EC2 のメタデータ
- Amazon EFS のメタデータ
- Amazon FSx のメタデータ
- Amazon Neptune のメタデータ
- Amazon RDS のメタデータ
- Amazon Redshift のメタデータ
- のメタデータ AWS Storage Gateway
- Amazon S3 のメタデータ
- Amazon Timestream のメタデータ

- 仮想マシンのメタデータ

型: 文字列間のマッピング

必須: はい

RecoveryPointArn

たとえば、arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45などのリカバリポイントを一意に識別する ARN。

型: 文字列

必須: はい

ResourceType

次のいずれかのリソースのリカバリポイントを復元するジョブを開始します。

- Aurora - Amazon Aurora
- DocumentDB - Amazon DocumentDB
- CloudFormation - AWS CloudFormation
- DynamoDB - Amazon DynamoDB
- EBS - Amazon Elastic Block Store
- EC2 - Amazon Elastic Compute Cloud
- EFS - Amazon Elastic File System
- FSx - Amazon FSx
- Neptune - Amazon Neptune
- RDS - Amazon Relational Database Service
- Redshift - Amazon Redshift
- Storage Gateway - AWS Storage Gateway
- S3 - Amazon Simple Storage Service
- Timestream - Amazon Timestream
- VirtualMachine - 仮想マシン

型: 文字列

パターン：^[a-zA-Z0-9\-_\.]{1,50}$

必須: いいえ

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "RestoreJobId": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

RestoreJobId

リカバリポイントをリストアするジョブを一意に識別します。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

InvalidRequestException

リクエストへの入力に何らかの問題が発生していることを示します。たとえば、パラメータのタイプが間違っています。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

StopBackupJob

サービス: AWS Backup

ジョブをキャンセルして、リソースの 1 回限りのバックアップを作成しようとします。

このアクションは、Amazon FSx for Windows File Server、Amazon FSx for Lustre、Amazon FSx for NetApp ONTAP、Amazon FSx for OpenZFS、Amazon DocumentDB (MongoDB 互換) 、Amazon RDS、Amazon Aurora、Amazon Neptune の各サービスではサポートされていません。

リクエストの構文

```
POST /backup-jobs/backupJobId HTTP/1.1
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

backupJobId

リソースをバックアップ AWS Backup する へのリクエストを一意に識別します。

必須: はい

リクエストボディ

リクエストにリクエスト本文がありません。

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

InvalidRequestException

リクエストへの入力に何らかの問題が発生していることを示します。たとえば、パラメータのタイプが間違っています。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

TagResource

サービス: AWS Backup

Amazon リソースネーム (ARN) で識別されるリカバリポイント、バックアッププラン、またはバックアップボールトに、キーと値のペアのセットを割り当てます。

この API は、Aurora、Amazon DocumentDB などのリソースタイプの復旧ポイントでサポートされています。Amazon EBS、Amazon FSxNeptune、Amazon RDS。

リクエストの構文

```
POST /tags/resourceArn HTTP/1.1
Content-type: application/json

{
   "Tags": {
      "string" : "string"
   }
}
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

resourceArn

リソースを一意に識別する ARN。ARN の形式は、タグ付きリソースのタイプによって異なります。

を含まない ARNsbackupは、タグ付けと互換性がありません。 TagResourceおよび UntagResourceの ARNsが無効な場合、エラーが発生します。許容される ARN コンテンツには、 を含めることができますarn:aws:backup:us-east。無効な ARN コンテンツは のようになりますarn:aws:ec2:us-east。

必須: はい

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

Tags

リソースの整理に役立つキーと値のペア。作成したリソースに独自のメタデータを割り当てることができます。わかりやすくするために、[{"Key":"string","Value":"string"}] のタグを割り当てる構造は次のとおりです。

型: 文字列間のマッピング

必須: はい

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

LimitExceededException

たとえば、リクエストで許可されるアイテムの最大数などのリクエストの制限を超えました。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UntagResource

サービス: AWS Backup

Amazon リソースネーム (ARN) で識別されるリカバリポイント、バックアッププラン、またはバックアップボールトから、キーと値のペアのセットを削除します。

この API は、Aurora、Amazon DocumentDB などのリソースタイプの復旧ポイントではサポートされていません。Amazon EBS、Amazon FSxNeptune、Amazon RDS。

リクエストの構文

```
POST /untag/resourceArn HTTP/1.1
Content-type: application/json

{
   "TagKeyList": [ "string" ]
}
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

resourceArn

リソースを一意に識別する ARN。ARN の形式は、タグ付きリソースのタイプによって異なります。

を含まない ARNsbackupは、タグ付けと互換性がありません。 TagResourceおよび UntagResourceの ARNsが無効な場合、エラーが発生します。許容される ARN コンテンツには、 を含めることができますarn:aws:backup:us-east。無効な ARN コンテンツは のようになりますarn:aws:ec2:us-east。

必須: はい

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

TagKeyList

リソースから削除するキーと値のタグを識別するキー。

タイプ：文字列の配列

必須: はい

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateBackupPlan

サービス: AWS Backup

指定されたバックアッププランを更新します。新しいバージョンは ID によって一意に識別されます。

リクエストの構文

```
POST /backup/plans/backupPlanId HTTP/1.1
Content-type: application/json

{
   "BackupPlan": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
               "OptInToArchiveForSupportedResources": boolean
            },
            "RecoveryPointTags": {
               "string" : "string"
```

```
            },
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
         }
      ]
   }
}
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

backupPlanId

バックアッププランの ID。

必須: はい

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

BackupPlan

バックアッププランの本文。1 つの BackupPlanName と1 つ以上の Rules のセットを含む。

型: BackupPlanInput オブジェクト

必須: はい

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "AdvancedBackupSettings": [
      {
         "BackupOptions": {
```

```
            "string" : "string"
         },
         "ResourceType": "string"
      }
   ],
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "CreationDate": number,
   "VersionId": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

AdvancedBackupSettings

リソースタイプごとに BackupOptions のリストが含まれます。

型: AdvancedBackupSetting オブジェクトの配列

BackupPlanArn

たとえば、arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50などのバックアップ計画を一意に識別する Amazon リソースネーム (ARN) です。

型: 文字列

BackupPlanId

バックアップ計画を一意に識別します。

型: 文字列

CreationDate

バックアッププランが作成された日時 (Unix 時刻形式および協定世界時 (UTC))。CreationDateの値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

VersionId

一意のランダムに生成された UTF-8 エンコード Unicode 文字列 (最大 1,024 バイト長)。バージョン ID を編集することはできません。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateFramework

サービス: AWS Backup

指定されたフレームワークを更新します。

リクエストの構文

```
PUT /audit/frameworks/frameworkName HTTP/1.1
Content-type: application/json

{
   "FrameworkControls": [
      {
         "ControlInputParameters": [
            {
               "ParameterName": "string",
               "ParameterValue": "string"
            }
         ],
         "ControlName": "string",
         "ControlScope": {
            "ComplianceResourceIds": [ "string" ],
            "ComplianceResourceTypes": [ "string" ],
            "Tags": {
               "string" : "string"
            }
         }
      }
   ],
   "FrameworkDescription": "string",
   "IdempotencyToken": "string"
}
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

frameworkName

フレームワークの一意の名前。この名前は、文字で始まり、文字 (a~z、A~Z)、数字 (0~9)、およびアンダースコア (_) を含む 1 から 256 文字で構成されます。

長さの制限：最小長は 1 です。最大長は 256 です。

パターン：[a-zA-Z][_a-zA-Z0-9]*

必須: はい

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

FrameworkControls

フレームワークを構成するコントロール。リスト内の各コントロールには、名前、入力パラメータ、およびスコープがあります。

型: FrameworkControl オブジェクトの配列

必須: いいえ

FrameworkDescription

最大 1,024 文字のフレームワークの説明 (オプション)。

型: 文字列

長さの制限: 最小長は 0 です。最大長は 1,024 です。

パターン: .*\S.*

必須: いいえ

IdempotencyToken

別の UpdateFrameworkInput への同じコール間を区別するために使用できる顧客が選択した文字列。同じ冪等性トークンで成功したリクエストを再試行すると、アクションは実行されず、成功メッセージが表示されます。

タイプ: 文字列

必須: いいえ

レスポンスの構文

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "CreationTime": number,
   "FrameworkArn": "string",
   "FrameworkName": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

CreationTime

フレームワークが作成された日付と時刻を ISO 8601 で表したものです。CreationTime の値は、ミリ秒単位の精度です。例えば、2020-07-10T15:00:00.000-08:00 は 2020 年 7 月 10 日午後 3 時 (UTC から 8 時間遅れ) を表します。

型: タイムスタンプ

FrameworkArn

リソースを一意に識別する Amazon リソースネーム (ARN)。ARN の形式は、リソースタイプによって異なります。

型: 文字列

FrameworkName

フレームワークの一意の名前。この名前は、文字で始まり、文字 (a~z、A~Z)、数字 (0~9)、およびアンダースコア (_) を含む 1 から 256 文字で構成されます。

型: 文字列

長さの制限：最小長は 1 です。最大長は 256 です。

パターン：[a-zA-Z][_a-zA-Z0-9]*

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AlreadyExistsException

必要なリソースは既に存在します。

HTTP ステータスコード：400

ConflictException

AWS Backup は、前のアクションの実行が完了するまで、リクエストしたアクションを実行できません。後ほどもう一度試してください。」

HTTP ステータスコード：400

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

LimitExceededException

たとえば、リクエストで許可されるアイテムの最大数などのリクエストの制限を超えました。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateGlobalSettings

サービス: AWS Backup

AWS アカウントがクロスアカウントバックアップにオプトインされているかどうかを更新します。アカウントが Organizations 管理アカウントでない場合は、エラーを返します。DescribeGlobalSettings API を使用して現在の設定を決定します。

リクエストの構文

```
PUT /global-settings HTTP/1.1
Content-type: application/json

{
   "GlobalSettings": {
      "string" : "string"
   }
}
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

GlobalSettings

isCrossAccountBackupEnabled およびリージョンの値。例えば、update-global-settings --global-settings isCrossAccountBackupEnabled=false --region us-west-2 などです。

型: 文字列間のマッピング

必須: いいえ

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

InvalidRequestException

リクエストへの入力に何らかの問題が発生していることを示します。たとえば、パラメータのタイプが間違っています。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2

- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateRecoveryPointLifecycle

サービス: AWS Backup

復旧ポイントの移行ライフサイクルを設定します。

ライフサイクルは、保護されたリソースがコールドストレージに移行するタイミングと、期限切れになるタイミングを定義します。 は、定義したライフサイクルに従ってバックアップを自動的に AWS Backup 移行および期限切れにします。

コールドストレージに移行されたバックアップは、そこに最低 90 日保存される必要があります。したがって、「保持期間」の設定は、「コールドへの移行 (日数)」設定から 90 日以上あける必要があります。バックアップがコールドに移行された後で、「コールドへの移行 (日数)」設定を変更することはできません。

コールドストレージに移行できるリソースタイプは、「リソース別の機能の可用性」の表に記載されています。他のリソースタイプでは、この式は AWS Backup 無視されます。

この操作では、連続バックアップはサポートされません。

リクエストの構文

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
Content-type: application/json

{
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   }
}
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

backupVaultName

バックアップを保存する論理コンテナの名前。バックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先の AWS リージョンに一意の名前で識別されます。

Pattern: ^[a-zA-Z0-9\-_]{2,50}$

必須：はい

recoveryPointArn

arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45などのリカバリポイントを一意に識別する Amazon リソースネーム (ARN) です。

必須: はい

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

Lifecycle

ライフサイクルは、保護されたリソースがコールドストレージに移行するタイミングと、期限切れになるタイミングを定義します。 は、定義したライフサイクルに従ってバックアップを自動的に AWS Backup 移行および期限切れにします。

コールドストレージに移行されたバックアップは、そこに最低 90 日保存される必要があります。したがって、「保持期間」の設定は、「コールドへの移行 (日数)」設定から 90 日以上あける必要があります。バックアップがコールドに移行された後で、「コールドへの移行 (日数)」設定を変更することはできません。

タイプ：Lifecycle オブジェクト

必須: いいえ

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "CalculatedLifecycle": {
      "DeleteAt": number,
      "MoveToColdStorageAt": number
   },
   "Lifecycle": {
```

```
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   },
   "RecoveryPointArn": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

BackupVaultArn

arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault などのバックアップボールトを一意に識別する ARN。

型: 文字列

CalculatedLifecycle

DeleteAt および MoveToColdStorageAt タイムスタンプを含む CalculatedLifecycle オブジェクト

タイプ：CalculatedLifecycle オブジェクト

Lifecycle

ライフサイクルは、保護されたリソースがコールドストレージに移行するタイミングと、期限切れになるタイミングを定義します。 は、定義したライフサイクルに従ってバックアップを自動的に AWS Backup 移行および期限切れにします。

コールドストレージに移行されたバックアップは、そこに最低 90 日保存される必要があります。したがって、「保持期間」の設定は、「コールドへの移行 (日数)」設定から 90 日以上あける必要があります。バックアップがコールドに移行された後で、「コールドへの移行 (日数)」設定を変更することはできません。

コールドストレージに移行できるリソースタイプは、「リソース別の機能の可用性」の表に記載されています。他のリソースタイプでは、この式は AWS Backup 無視されます。

タイプ：Lifecycle オブジェクト

RecoveryPointArn

arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45などのリカバリポイントを一意に識別する Amazon リソースネーム (ARN) です。

型: 文字列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

InvalidRequestException

リクエストへの入力に何らかの問題が発生していることを示します。たとえば、パラメータのタイプが間違っています。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateRegionSettings

サービス: AWS Backup

リージョンの現在のサービスオプトイン設定を更新します。

`DescribeRegionSettings` API を使用してサポートされているリソースタイプを決定します。

リクエストの構文

```
PUT /account-settings HTTP/1.1
Content-type: application/json

{
   "ResourceTypeManagementPreference": {
      "string" : boolean
   },
   "ResourceTypeOptInPreference": {
      "string" : boolean
   }
}
```

URI リクエストパラメータ

リクエストでは URI パラメータを使用しません。

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

ResourceTypeManagementPreference

リソースタイプのバックアップの完全な AWS Backup 管理を有効または無効にします。の高度な DynamoDB バックアップ機能 とともに DynamoDB のフル AWS Backup 管理を有効にするには、手順に従って高度な DynamoDB バックアップをプログラムで有効にします。 AWS Backup DynamoDB

タイプ:ブールマップへの文字列。

キーパターン: `^[a-zA-Z0-9\-\_\.]{1,50}$`

必須: いいえ

ResourceTypeOptInPreference

リージョンのオプトイン設定とともに、サービスのリストを更新します。

リソースの割り当てがタグのみに基づいている場合は、サービスオプトイン設定が適用されます。リソースタイプが、Amazon S3、Amazon EC2、Amazon RDS などのバックアッププランに明示的に割り当てられている場合は、その特定のサービスでオプトインが有効になっていなくてもバックアップに含まれます。リソース割り当てでリソースタイプとタグの両方が指定されている場合、バックアッププランで指定されたリソースタイプがタグ条件よりも優先されます。この場合、サービスオプトイン設定は無視されます。

タイプ:ブールマップへの文字列。

キーパターン: `^[a-zA-Z0-9\-\_\.]{1,50}$`

必須: いいえ

レスポンスの構文

```
HTTP/1.1 200
```

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateReportPlan

サービス: AWS Backup

指定されたレポートプランを更新します。

リクエストの構文

```
PUT /audit/report-plans/reportPlanName HTTP/1.1
Content-type: application/json

{
   "IdempotencyToken": "string",
   "ReportDeliveryChannel": {
      "Formats": [ "string" ],
      "S3BucketName": "string",
      "S3KeyPrefix": "string"
   },
   "ReportPlanDescription": "string",
   "ReportSetting": {
      "Accounts": [ "string" ],
      "FrameworkArns": [ "string" ],
      "NumberOfFrameworks": number,
      "OrganizationUnits": [ "string" ],
      "Regions": [ "string" ],
      "ReportTemplate": "string"
   }
}
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

reportPlanName

レポートプランの一意の名前。この名前は、文字で始まり、文字 (a~z、A~Z)、数字 (0~9)、およびアンダースコア (_) を含む 1 から 256 文字で構成されます。

長さの制限：最小長は 1 です。最大長は 256 です。

パターン：`[a-zA-Z][_a-zA-Z0-9]*`

必須: はい

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

IdempotencyToken

別の UpdateReportPlanInput への同じコール間を区別するために使用できる顧客が選択した文字列。同じ冪等性トークンで成功したリクエストを再試行すると、アクションは実行されず、成功メッセージが表示されます。

タイプ: 文字列

必須: いいえ

ReportDeliveryChannel

レポートの配信先、特に Amazon S3 バケット名、S3 キープレフィックス、レポートの形式に関する情報。

タイプ：ReportDeliveryChannel オブジェクト

必須: いいえ

ReportPlanDescription

最大 1,024 文字のレポートプランの説明（オプション）。

型: 文字列

長さの制限: 最小長は 0 です。最大長は 1,024 です。

パターン: `.*\S.*`

必須: いいえ

ReportSetting

レポートのレポートテンプレート。レポートは、レポートテンプレートを使用して構築されます。レポートテンプレートは次のとおりです。

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

レポートテンプレートが RESOURCE_COMPLIANCE_REPORTまたは の場合CONTROL_COMPLIANCE_REPORT、この API リソースは AWS リージョン および フレームワークによるレポートカバレッジも記述します。

タイプ：ReportSetting オブジェクト

必須: いいえ

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "ReportPlanArn": "string",
   "ReportPlanName": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

CreationTime

レポートプランが作成された日時 (Unix 時刻形式および協定世界時 (UTC))。CreationTimeの値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前 12:11:30.087 を表します。

型: タイムスタンプ

ReportPlanArn

リソースを一意に識別する Amazon リソースネーム (ARN)。ARN の形式は、リソースタイプによって異なります。

型: 文字列

ReportPlanName

レポートプランの一意の名前。

型: 文字列

長さの制限：最小長は 1 です。最大長は 256 です。

パターン：[a-zA-Z][_a-zA-Z0-9]*

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

ConflictException

AWS Backup は、前のアクションの実行が完了するまで、リクエストしたアクションを実行できません。後ほどもう一度試してください。」

HTTP ステータスコード：400

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateRestoreTestingPlan

サービス: AWS Backup

このリクエストは、指定された復元テストプランに対する変更を送信します。RestoreTestingPlanName は、作成後に更新することはできません。

RecoveryPointSelection には以下を含めることができます。

- Algorithm
- ExcludeVaults
- IncludeVaults
- RecoveryPointTypes
- SelectionWindowDays

リクエストの構文

```
PUT /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
Content-type: application/json

{
   "RestoreTestingPlan": {
      "RecoveryPointSelection": {
         "Algorithm": "string",
         "ExcludeVaults": [ "string" ],
         "IncludeVaults": [ "string" ],
         "RecoveryPointTypes": [ "string" ],
         "SelectionWindowDays": number
      },
      "ScheduleExpression": "string",
      "ScheduleExpressionTimezone": "string",
      "StartWindowHours": number
   }
}
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

RestoreTestingPlanName

復元テストプラン名の名前。

必須: はい

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

RestoreTestingPlan

復元テストプランの本文を示します。

型: RestoreTestingPlanForUpdate オブジェクト

必須: はい

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
   "UpdateTime": number
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

CreationTime

リソーステストプランが作成された時刻。

型: タイムスタンプ

RestoreTestingPlanArn

復元テストプランの一意の ARN (Amazon リソースネーム) です。

型: 文字列

RestoreTestingPlanName

作成後にこの名前を変更することはできません。名前には英数字とアンダースコアのみを使用できます。最大長は 50 文字です。

型: 文字列

UpdateTime

復元テストプランの更新が完了した時刻。

型: タイムスタンプ

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

ConflictException

AWS Backup は、前のアクションの実行が完了するまで、リクエストしたアクションを実行できません。後ほどもう一度試してください。」

HTTP ステータスコード：400

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateRestoreTestingSelection

サービス: AWS Backup

指定された復元テストの選択を更新します。

このリクエストで RestoreTestingSelectionName を除くほとんどの要素を更新できます。

保護されたリソース ARNsまたは条件のいずれかを使用できますが、両方を使用することはできません。

リクエストの構文

```
PUT /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
Content-type: application/json

{
   "RestoreTestingSelection": {
      "IamRoleArn": "string",
      "ProtectedResourceArns": [ "string" ],
      "ProtectedResourceConditions": {
         "StringEquals": [
            {
               "Key": "string",
               "Value": "string"
            }
         ],
         "StringNotEquals": [
            {
               "Key": "string",
               "Value": "string"
            }
         ]
      },
      "RestoreMetadataOverrides": {
         "string" : "string"
      },
      "ValidationWindowHours": number
   }
}
```

URI リクエストパラメータ

リクエストでは、次の URI パラメータを使用します。

RestoreTestingPlanName

指定された復元テストプランを更新するには、テストプラン名が必要です。

必須: はい

RestoreTestingSelectionName

更新する復元テスト選択に必要な復元テスト選択名。

必須: はい

リクエストボディ

リクエストは以下の JSON 形式のデータを受け入れます。

RestoreTestingSelection

復元テスト選択を更新するには、保護対象リソースの ARN または条件を使用できますが、両方を使用することはできません。つまり、選択に ProtectedResourceArns が含まれる場合、ProtectedResourceConditions のパラメータを使用して更新をリクエストしても失敗します。

型: RestoreTestingSelectionForUpdate オブジェクト

必須: はい

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
   "RestoreTestingSelectionName": "string",
   "UpdateTime": number
```

```
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

CreationTime

リソーステスト選択が正常に更新された時刻。

型: タイムスタンプ

RestoreTestingPlanArn

復元テストプランの名前を表す一意の文字列です。

型: 文字列

RestoreTestingPlanName

更新された復元テスト選択が関連付けられている復元テストプラン。

型: 文字列

RestoreTestingSelectionName

返された復元テスト選択名。

型: 文字列

UpdateTime

復元テスト選択の更新が完了した時刻。

型: タイムスタンプ

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

ConflictException

AWS Backup は、前のアクションの実行が完了するまで、リクエストしたアクションを実行できません。後ほどもう一度試してください。」

HTTP ステータスコード：400

InvalidParameterValueException

パラメータの値に問題があることを示します。たとえば、値が範囲外であることです。

HTTP ステータスコード：400

MissingParameterValueException

必須パラメータがないことを示します。

HTTP ステータスコード：400

ResourceNotFoundException

アクションに必要なリソースは存在しません。

HTTP ステータスコード：400

ServiceUnavailableException

サーバーの一時的障害のため、リクエストは失敗しました。

HTTP ステータスコード：500

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

AWS Backup gateway

以下のアクションが AWS Backup gateway によってサポートされています。

- AssociateGatewayToServer
- CreateGateway
- DeleteGateway
- DeleteHypervisor
- DisassociateGatewayFromServer
- GetBandwidthRateLimitSchedule
- GetGateway
- GetHypervisor
- GetHypervisorPropertyMappings
- GetVirtualMachine
- ImportHypervisorConfiguration
- ListGateways
- ListHypervisors
- ListTagsForResource
- ListVirtualMachines
- PutBandwidthRateLimitSchedule
- PutHypervisorPropertyMappings
- PutMaintenanceStartTime
- StartVirtualMachinesMetadataSync
- TagResource
- TestHypervisorConfiguration
- UntagResource
- UpdateGatewayInformation
- UpdateGatewaySoftwareNow
- UpdateHypervisor

AssociateGatewayToServer

サービス: AWS Backup gateway

バックアップゲートウェイをサーバに関連付けます。関連付けプロセスの完了後、ゲートウェイ経由で VM をバックアップおよび復元できます。

リクエストの構文

```
{
   "GatewayArn": "string",
   "ServerArn": "string"
}
```

リクエストパラメータ

すべてのアクションに共通のパラメータの詳細については、「共通パラメータ」を参照してください。

リクエストは以下の JSON 形式のデータを受け入れます。

GatewayArn

ゲートウェイの Amazon リソースネーム (ARN) ListGateways オペレーションを使用して、アカウント と のゲートウェイのリストを返します AWS リージョン。

型: 文字列

長さの制限: 最小長は 50 です。最大長は 180 です。

Pattern: ^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$

必須：はい

ServerArn

仮想マシンをホストするサーバーの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。500 の最大長。

Pattern: ^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$

必須：はい

レスポンスの構文

```
{
   "GatewayArn": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

GatewayArn

ゲートウェイの Amazon リソースネーム (ARN)

型: 文字列

長さの制限: 最小長は 50 です。最大長は 180 です。

パターン：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

ConflictException

サポートされていないため、操作を続行できません。

HTTP ステータスコード：400

InternalServerException

内部エラーが発生したために操作は成功しませんでした。後ほどもう一度試してください。」

HTTP ステータスコード：500

ThrottlingException

TPS は、意図的なまたは意図的でない、大量のリクエストを防ぐために制限されています。

HTTP ステータスコード：400

ValidationException

検証エラーが発生したため、操作は成功しませんでした。

HTTP ステータスコード：400

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateGateway

サービス: AWS Backup gateway

バックアップゲートウェイを作成します。ゲートウェイを作成したら、AssociateGatewayToServer オペレーションを使用して、ゲートウェイをサーバに関連付けることができます。

リクエストの構文

```
{
   "ActivationKey": "string",
   "GatewayDisplayName": "string",
   "GatewayType": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

リクエストパラメータ

すべてのアクションに共通のパラメータの詳細については、「共通パラメータ」を参照してください。

リクエストは以下の JSON 形式のデータを受け入れます。

ActivationKey

作成されたゲートウェイのアクティベーションキー。

型: 文字列

長さの制限：最小長は 1 です。最大長は 50 です。

Pattern: ^[0-9a-zA-Z\-]+$

必須：はい

GatewayDisplayName

作成されたゲートウェイの表示名。

型: 文字列

長さの制限: 最小長は 1 です。最大長は 100 です。

パターン: ^[a-zA-Z0-9-]*$

必須：はい

GatewayType

作成されたゲートウェイのタイプ。

型: 文字列

有効な値：BACKUP_VM

必須: はい

Tags

ゲートウェイに割り当てられる最大 50 のタグのリスト。各タグはキーバリューのペアです。

型: Tag オブジェクトの配列

必須: いいえ

レスポンスの構文

```
{
   "GatewayArn": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

GatewayArn

作成するゲートウェイの Amazon リソースネーム (ARN)

型: 文字列

長さの制限: 最小長は 50 です。最大長は 180 です。

パターン：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InternalServerException

内部エラーが発生したために操作は成功しませんでした。後ほどもう一度試してください。」

HTTP ステータスコード：500

ThrottlingException

TPS は、意図的なまたは意図的でない、大量のリクエストを防ぐために制限されています。

HTTP ステータスコード：400

ValidationException

検証エラーが発生したため、操作は成功しませんでした。

HTTP ステータスコード：400

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python

- AWS SDK for Ruby V3

DeleteGateway

サービス: AWS Backup gateway

バックアップゲートウェイを削除します。

リクエストの構文

```
{
   "GatewayArn": "string"
}
```

リクエストパラメータ

すべてのアクションに共通のパラメータの詳細については、「共通パラメータ」を参照してください。

リクエストは以下の JSON 形式のデータを受け入れます。

GatewayArn

削除するゲートウェイの Amazon リソースネーム (ARN)

型: 文字列

長さの制限: 最小長は 50 です。最大長は 180 です。

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必須：はい

レスポンスの構文

```
{
   "GatewayArn": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

GatewayArn

削除されるゲートウェイの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。最大長は 180 です。

パターン：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InternalServerException

内部エラーが発生したために操作は成功しませんでした。後ほどもう一度試してください。」

HTTP ステータスコード：500

ResourceNotFoundException

アクションに必要なリソースが見つかりませんでした。

HTTP ステータスコード：400

ThrottlingException

TPS は、意図的なまたは意図的でない、大量のリクエストを防ぐために制限されています。

HTTP ステータスコード：400

ValidationException

検証エラーが発生したため、操作は成功しませんでした。

HTTP ステータスコード：400

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteHypervisor

サービス: AWS Backup gateway

ハイパーバイザーを削除します。

リクエストの構文

```
{
   "HypervisorArn": "string"
}
```

リクエストパラメータ

すべてのアクションに共通のパラメータの詳細については、「共通パラメータ」を参照してください。

リクエストは以下の JSON 形式のデータを受け入れます。

HypervisorArn

削除するハイパーバイザーの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。500 の最大長。

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必須：はい

レスポンスの構文

```
{
   "HypervisorArn": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

HypervisorArn

削除したハイパーバイザーの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。500 の最大長。

パターン：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

権限が不足しているため、操作を続行できません。

HTTP ステータスコード：400

ConflictException

サポートされていないため、操作を続行できません。

HTTP ステータスコード：400

InternalServerException

内部エラーが発生したために操作は成功しませんでした。後ほどもう一度試してください。」

HTTP ステータスコード：500

ResourceNotFoundException

アクションに必要なリソースが見つかりませんでした。

HTTP ステータスコード：400

ThrottlingException

TPS は、意図的なまたは意図的でない、大量のリクエストを防ぐために制限されています。

HTTP ステータスコード：400

ValidationException

検証エラーが発生したため、操作は成功しませんでした。

HTTP ステータスコード：400

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DisassociateGatewayFromServer

サービス: AWS Backup gateway

指定されたサーバーからバックアップゲートウェイの関連付けを解除します。関連付け解除プロセスが終了すると、ゲートウェイはサーバー上の仮想マシンにアクセスできなくなります。

リクエストの構文

```
{
   "GatewayArn": "string"
}
```

リクエストパラメータ

すべてのアクションに共通のパラメータの詳細については、「共通パラメータ」を参照してください。

リクエストは以下の JSON 形式のデータを受け入れます。

GatewayArn

関連付けを解除するゲートウェイの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。最大長は 180 です。

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必須：はい

レスポンスの構文

```
{
   "GatewayArn": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

GatewayArn

関連付けを解除したゲートウェイの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。最大長は 180 です。

パターン：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

ConflictException

サポートされていないため、操作を続行できません。

HTTP ステータスコード：400

InternalServerException

内部エラーが発生したために操作は成功しませんでした。後ほどもう一度試してください。」

HTTP ステータスコード：500

ResourceNotFoundException

アクションに必要なリソースが見つかりませんでした。

HTTP ステータスコード：400

ThrottlingException

TPS は、意図的なまたは意図的でない、大量のリクエストを防ぐために制限されています。

HTTP ステータスコード：400

ValidationException

検証エラーが発生したため、操作は成功しませんでした。

HTTP ステータスコード：400

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetBandwidthRateLimitSchedule

サービス: AWS Backup gateway

指定されたゲートウェイの帯域幅レート制限スケジュールを取得します。デフォルトでは、ゲートウェイには帯域幅レート制限スケジュールがありません。つまり、帯域幅レート制限は適用されていません。これを使用して、ゲートウェイの帯域幅レート制限スケジュールを取得します。

リクエストの構文

```
{
   "GatewayArn": "string"
}
```

リクエストパラメータ

すべてのアクションに共通のパラメータの詳細については、「共通パラメータ」を参照してください。

リクエストは以下の JSON 形式のデータを受け入れます。

GatewayArn

ゲートウェイの Amazon リソースネーム (ARN) `ListGateways` オペレーションを使用して、アカウント および のゲートウェイのリストを返します AWS リージョン。

型: 文字列

長さの制限: 最小長は 50 です。最大長は 180 です。

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必須：はい

レスポンスの構文

```
{
   "BandwidthRateLimitIntervals": [
      {
         "AverageUploadRateLimitInBitsPerSec": number,
         "DaysOfWeek": [ number ],
```

```
            "EndHourOfDay": number,
            "EndMinuteOfHour": number,
            "StartHourOfDay": number,
            "StartMinuteOfHour": number
        }
    ],
    "GatewayArn": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

BandwidthRateLimitIntervals

ゲートウェイの帯域幅レート制限スケジュールの間隔を含む配列。帯域幅レート制限の間隔がスケジュールされていない場合、配列は空になります。

タイプ：BandwidthRateLimitInterval オブジェクトの配列

配列メンバー：最小数は 0 項目です。最大数は 20 項目です。

GatewayArn

ゲートウェイの Amazon リソースネーム (ARN)。ListGateways オペレーションを使用して、アカウント と のゲートウェイのリストを返します AWS リージョン。

型: 文字列

長さの制限: 最小長は 50 です。最大長は 180 です。

パターン：^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InternalServerException

内部エラーが発生したために操作は成功しませんでした。後ほどもう一度試してください。」

HTTP ステータスコード：500

ResourceNotFoundException

アクションに必要なリソースが見つかりませんでした。

HTTP ステータスコード：400

ThrottlingException

TPS は、意図的なまたは意図的でない、大量のリクエストを防ぐために制限されています。

HTTP ステータスコード：400

ValidationException

検証エラーが発生したため、操作は成功しませんでした。

HTTP ステータスコード：400

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetGateway

サービス: AWS Backup gateway

ARN (Amazon リソースネーム) を指定することで、この API はゲートウェイを返します。

リクエストの構文

```
{
   "GatewayArn": "string"
}
```

リクエストパラメータ

すべてのアクションに共通のパラメータの詳細については、「共通パラメータ」を参照してください。

リクエストは以下の JSON 形式のデータを受け入れます。

GatewayArn

ゲートウェイの Amazon リソースネーム (ARN)

型: 文字列

長さの制限: 最小長は 50 です。最大長は 180 です。

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必須：はい

レスポンスの構文

```
{
   "Gateway": {
      "GatewayArn": "string",
      "GatewayDisplayName": "string",
      "GatewayType": "string",
      "HypervisorId": "string",
      "LastSeenTime": number,
      "MaintenanceStartTime": {
```

```
            "DayOfMonth": number,
            "DayOfWeek": number,
            "HourOfDay": number,
            "MinuteOfHour": number
         },
         "NextUpdateAvailabilityTime": number,
         "VpcEndpoint": "string"
      }
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

Gateway

ARN (Amazon リソースネーム) を指定することで、この API はゲートウェイを返します。

型: GatewayDetails オブジェクト

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InternalServerException

内部エラーが発生したために操作は成功しませんでした。後ほどもう一度試してください。」

HTTP ステータスコード：500

ResourceNotFoundException

アクションに必要なリソースが見つかりませんでした。

HTTP ステータスコード：400

ThrottlingException

TPS は、意図的なまたは意図的でない、大量のリクエストを防ぐために制限されています。

HTTP ステータスコード：400

ValidationException

検証エラーが発生したため、操作は成功しませんでした。

HTTP ステータスコード：400

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetHypervisor

サービス: AWS Backup gateway

このアクションは、ゲートウェイが接続する指定されたハイパーバイザーに関する情報をリクエストします。ハイパーバイザーは、仮想マシンを作成および管理し、それらにリソースを割り当てるハードウェア、ソフトウェア、またはファームウェアです。

リクエストの構文

```
{
   "HypervisorArn": "string"
}
```

リクエストパラメータ

すべてのアクションに共通のパラメータの詳細については、「共通パラメータ」を参照してください。

リクエストは以下の JSON 形式のデータを受け入れます。

HypervisorArn

ハイパーバイザーの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。500 の最大長。

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必須：はい

レスポンスの構文

```
{
   "Hypervisor": {
      "Host": "string",
      "HypervisorArn": "string",
      "KmsKeyArn": "string",
      "LastSuccessfulMetadataSyncTime": number,
```

```
        "LatestMetadataSyncStatus": "string",
        "LatestMetadataSyncStatusMessage": "string",
        "LogGroupArn": "string",
        "Name": "string",
        "State": "string"
    }
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

Hypervisor

リクエストされたハイパーバイザーに関する詳細。

型: HypervisorDetails オブジェクト

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InternalServerException

内部エラーが発生したために操作は成功しませんでした。後ほどもう一度試してください。」

HTTP ステータスコード：500

ResourceNotFoundException

アクションに必要なリソースが見つかりませんでした。

HTTP ステータスコード：400

ThrottlingException

TPS は、意図的なまたは意図的でない、大量のリクエストを防ぐために制限されています。

HTTP ステータスコード：400

ValidationException

検証エラーが発生したため、操作は成功しませんでした。

HTTP ステータスコード：400

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetHypervisorPropertyMappings

サービス: AWS Backup gateway

このアクションは、指定されたハイパーバイザーのプロパティマッピングを取得します。ハイパーバイザープロパティマッピングは、ハイパーバイザーから利用可能なエンティティプロパティと、 で利用可能なプロパティとの関係を表示します AWS。

リクエストの構文

```
{
   "HypervisorArn": "string"
}
```

リクエストパラメータ

すべてのアクションに共通のパラメータの詳細については、「共通パラメータ」を参照してください。

リクエストは以下の JSON 形式のデータを受け入れます。

HypervisorArn

ハイパーバイザーの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。500 の最大長。

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必須：はい

レスポンスの構文

```
{
   "HypervisorArn": "string",
   "IamRoleArn": "string",
   "VmwareToAwsTagMappings": [
      {
         "AwsTagKey": "string",
```

```
            "AwsTagValue": "string",
            "VmwareCategory": "string",
            "VmwareTagName": "string"
        }
    ]
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

HypervisorArn

ハイパーバイザーの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。500 の最大長。

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

IamRoleArn

IAM ロールの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 20 です。最大長は 2,048 です。

Pattern: `^arn:(aws|aws-cn|aws-us-gov):iam::([0-9]+):role/(\S+)$`

VmwareToAwsTagMappings

これは VMware タグと AWS タグとのマッピングの表示です。

型: VmwareToAwsTagMapping オブジェクトの配列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InternalServerException

内部エラーが発生したために操作は成功しませんでした。後ほどもう一度試してください。」

HTTP ステータスコード：500

ResourceNotFoundException

アクションに必要なリソースが見つかりませんでした。

HTTP ステータスコード：400

ThrottlingException

TPS は、意図的なまたは意図的でない、大量のリクエストを防ぐために制限されています。

HTTP ステータスコード：400

ValidationException

検証エラーが発生したため、操作は成功しませんでした。

HTTP ステータスコード：400

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetVirtualMachine

サービス: AWS Backup gateway

ARN (Amazon リソースネーム) を指定することで、この API は仮想マシンを返します。

リクエストの構文

```
{
   "ResourceArn": "string"
}
```

リクエストパラメータ

すべてのアクションに共通のパラメータの詳細については、「共通パラメータ」を参照してください。

リクエストは以下の JSON 形式のデータを受け入れます。

ResourceArn

仮想マシンの Amazon リソースネーム (ARN)です。

型: 文字列

長さの制限: 最小長は 50 です。500 の最大長。

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必須：はい

レスポンスの構文

```
{
   "VirtualMachine": {
      "HostName": "string",
      "HypervisorId": "string",
      "LastBackupDate": number,
      "Name": "string",
      "Path": "string",
      "ResourceArn": "string",
```

```
      "VmwareTags": [
         {
            "VmwareCategory": "string",
            "VmwareTagDescription": "string",
            "VmwareTagName": "string"
         }
      ]
   }
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

VirtualMachine

このオブジェクトには、GetVirtualMachine の出力に含まれる VirtualMachine の基本属性が含まれています。

型: VirtualMachineDetails オブジェクト

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InternalServerException

内部エラーが発生したために操作は成功しませんでした。後ほどもう一度試してください。」

HTTP ステータスコード：500

ResourceNotFoundException

アクションに必要なリソースが見つかりませんでした。

HTTP ステータスコード：400

ThrottlingException

TPS は、意図的なまたは意図的でない、大量のリクエストを防ぐために制限されています。

HTTP ステータスコード：400

ValidationException

検証エラーが発生したため、操作は成功しませんでした。

HTTP ステータスコード：400

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ImportHypervisorConfiguration

サービス: AWS Backup gateway

ハイパーバイザーの設定をインポートして、ハイパーバイザーに接続します。

リクエストの構文

```
{
   "Host": "string",
   "KmsKeyArn": "string",
   "Name": "string",
   "Password": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "Username": "string"
}
```

リクエストパラメータ

すべてのアクションに共通のパラメータの詳細については、「共通パラメータ」を参照してください。

リクエストは以下の JSON 形式のデータを受け入れます。

Host

ハイパーバイザーのサーバーホスト。これは、IP アドレスまたは完全修飾ドメイン名 (FQDN) のいずれかです。

型: 文字列

長さの制限: 最小長は 3 です。最大長は 128 です。

パターン: ^.+$

必須：はい

KmsKeyArn

ハイパーバイザー AWS Key Management Service の 。

型: 文字列

長さの制限: 最小長は 50 です。500 の最大長。

Pattern: `^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

必須: いいえ

Name

ハイパーバイザーの名前。

型: 文字列

長さの制限: 最小長は 1 です。最大長は 100 です。

パターン: `^[a-zA-Z0-9-]*$`

必須：はい

Password

ハイパーバイザーのパスワード。

型: 文字列

長さの制限: 最小長は 1 です。最大長は 100 です。

Pattern: `^[ -~]+$`

必須: いいえ

Tags

インポートするハイパーバイザー設定のタグ。

型: Tag オブジェクトの配列

必須: いいえ

Username

ハイパーバイザーのユーザー名。

型: 文字列

長さの制限: 最小長は 1 です。最大長は 100 です。

Pattern: ^[-\.0-\[\]-~]*[!-\.0-\[\]-~][-\.0-\[\]-~]*$

必須: いいえ

レスポンスの構文

```
{
   "HypervisorArn": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

HypervisorArn

関連付けを解除したハイパーバイザーの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。500 の最大長。

パターン：^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

権限が不足しているため、操作を続行できません。

HTTP ステータスコード：400

ConflictException

サポートされていないため、操作を続行できません。

HTTP ステータスコード：400

InternalServerException

内部エラーが発生したために操作は成功しませんでした。後ほどもう一度試してください。」

HTTP ステータスコード：500

ThrottlingException

TPS は、意図的なまたは意図的でない、大量のリクエストを防ぐために制限されています。

HTTP ステータスコード：400

ValidationException

検証エラーが発生したため、操作は成功しませんでした。

HTTP ステータスコード：400

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListGateways

サービス: AWS Backup gateway

の が所有するバックアップゲートウェイ AWS アカウント を一覧表示します AWS リージョン。返されるリストは、ゲートウェイ Amazon リソース名 (ARN) によって順序付けられます。

リクエストの構文

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

リクエストパラメータ

すべてのアクションに共通のパラメータの詳細については、「共通パラメータ」を参照してください。

リクエストは以下の JSON 形式のデータを受け入れます。

MaxResults

リストするゲートウェイの最大数。

タイプ : 整数

有効な範囲: 最小値 は 1 です。

必須: いいえ

NextToken

返されるリソースの一部リストに続く次のアイテム。例えば、MaxResults の数のリソースを返すようにリクエストが行われた場合、NextToken を使用すると、このトークンが指す場所から開始してさらにリストの項目を返すことができます。

型: 文字列

長さの制限 : 最小長は 1 です。最大長は 1,000 です。

Pattern: ^.+$

必須: いいえ

レスポンスの構文

```
{
   "Gateways": [
      {
         "GatewayArn": "string",
         "GatewayDisplayName": "string",
         "GatewayType": "string",
         "HypervisorId": "string",
         "LastSeenTime": number
      }
   ],
   "NextToken": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

Gateways

ゲートウェイのリスト。

型: Gateway オブジェクトの配列

NextToken

返されるリソースの部分的リストに続く次の項目です。例えば、maxResults の数のリソースを返すようにリクエストが行われた場合、NextToken を使用すると、このトークンが指す場所から開始してさらにリストの項目を返すことができます。

型: 文字列

長さの制限：最小長は 1 です。最大長は 1,000 です。

パターン：^.+$

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InternalServerException

内部エラーが発生したために操作は成功しませんでした。後ほどもう一度試してください。」

HTTP ステータスコード：500

ThrottlingException

TPS は、意図的なまたは意図的でない、大量のリクエストを防ぐために制限されています。

HTTP ステータスコード：400

ValidationException

検証エラーが発生したため、操作は成功しませんでした。

HTTP ステータスコード：400

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListHypervisors

サービス: AWS Backup gateway

ハイパーバイザーを一覧表示します。

リクエストの構文

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

リクエストパラメータ

すべてのアクションに共通のパラメータの詳細については、「共通パラメータ」を参照してください。

リクエストは以下の JSON 形式のデータを受け入れます。

MaxResults

リストするハイパーバイザーの最大数。

タイプ：整数

有効な範囲: 最小値 は 1 です。

必須: いいえ

NextToken

返されるリソースの一部リストに続く次のアイテム。例えば、maxResults の数のリソースを返すようにリクエストが行われた場合、NextToken を使用すると、このトークンが指す場所から開始してさらにリストの項目を返すことができます。

型: 文字列

長さの制限：最小長は 1 です。最大長は 1,000 です。

Pattern: ^.+$

必須: いいえ

レスポンスの構文

```
{
   "Hypervisors": [
      {
         "Host": "string",
         "HypervisorArn": "string",
         "KmsKeyArn": "string",
         "Name": "string",
         "State": "string"
      }
   ],
   "NextToken": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

Hypervisors

リスト Hypervisor Amazon リソースネーム (ARN) の順序が付けられたオブジェクト。

型: Hypervisor オブジェクトの配列

NextToken

返されるリソースの部分的リストに続く次の項目です。例えば、maxResults の数のリソースを返すようにリクエストが行われた場合、NextToken を使用すると、このトークンが指す場所から開始してさらにリストの項目を返すことができます。

型: 文字列

長さの制限：最小長は 1 です。最大長は 1,000 です。

パターン：^.+$

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InternalServerException

内部エラーが発生したために操作は成功しませんでした。後ほどもう一度試してください。」

HTTP ステータスコード：500

ThrottlingException

TPS は、意図的なまたは意図的でない、大量のリクエストを防ぐために制限されています。

HTTP ステータスコード：400

ValidationException

検証エラーが発生したため、操作は成功しませんでした。

HTTP ステータスコード：400

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListTagsForResource

サービス: AWS Backup gateway

リソースの Amazon リソースネーム (ARN) によって識別されるリソースに適用されるタグを一覧表示します。

リクエストの構文

```
{
   "ResourceArn": "string"
}
```

リクエストパラメータ

すべてのアクションに共通のパラメータの詳細については、「共通パラメータ」を参照してください。

リクエストは以下の JSON 形式のデータを受け入れます。

ResourceArn

一覧表示するリソースのタグの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。500 の最大長。

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必須：はい

レスポンスの構文

```
{
   "ResourceArn": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
```

```
    ]
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

ResourceArn

一覧表示したリソースのタグの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。500 の最大長。

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Tags

リソースのタグの一覧表示。

型: Tag オブジェクトの配列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InternalServerException

内部エラーが発生したために操作は成功しませんでした。後ほどもう一度試してください。」

HTTP ステータスコード：500

ResourceNotFoundException

アクションに必要なリソースが見つかりませんでした。

HTTP ステータスコード：400

ThrottlingException

TPS は、意図的なまたは意図的でない、大量のリクエストを防ぐために制限されています。

HTTP ステータスコード：400

ValidationException

検証エラーが発生したため、操作は成功しませんでした。

HTTP ステータスコード：400

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListVirtualMachines

サービス: AWS Backup gateway

仮想マシンを一覧表示します。

リクエストの構文

```
{
   "HypervisorArn": "string",
   "MaxResults": number,
   "NextToken": "string"
}
```

リクエストパラメータ

すべてのアクションに共通のパラメータの詳細については、「共通パラメータ」を参照してください。

リクエストは以下の JSON 形式のデータを受け入れます。

HypervisorArn

仮想マシンに接続されたハイパーバイザーの Amazon リソースネーム (ARN)です。

型: 文字列

長さの制限: 最小長は 50 です。500 の最大長。

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必須: いいえ

MaxResults

一覧表示する仮想マシンの最大数。

タイプ : 整数

有効な範囲: 最小値 は 1 です。

必須: いいえ

NextToken

返されるリソースの一部リストに続く次のアイテム。例えば、maxResults の数のリソースを返すようにリクエストが行われた場合、NextToken を使用すると、このトークンが指す場所から開始してさらにリストの項目を返すことができます。

型: 文字列

長さの制限：最小長は 1 です。最大長は 1,000 です。

Pattern: ^.+$

必須: いいえ

レスポンスの構文

```
{
   "NextToken": "string",
   "VirtualMachines": [
      {
         "HostName": "string",
         "HypervisorId": "string",
         "LastBackupDate": number,
         "Name": "string",
         "Path": "string",
         "ResourceArn": "string"
      }
   ]
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

NextToken

返されるリソースの一部リストに続く次のアイテム。例えば、maxResults の数のリソースを返すようにリクエストが行われた場合、NextToken を使用すると、このトークンが指す場所から開始してさらにリストの項目を返すことができます。

型: 文字列

長さの制限：最小長は 1 です。最大長は 1,000 です。

Pattern: ^.+$

VirtualMachines

あなたのリストVirtualMachine Amazon リソースネーム (ARN) の順序が付けられたオブジェクト。

型: VirtualMachine オブジェクトの配列

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InternalServerException

内部エラーが発生したために操作は成功しませんでした。後ほどもう一度試してください。」

HTTP ステータスコード：500

ThrottlingException

TPS は、意図的なまたは意図的でない、大量のリクエストを防ぐために制限されています。

HTTP ステータスコード：400

ValidationException

検証エラーが発生したため、操作は成功しませんでした。

HTTP ステータスコード：400

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutBandwidthRateLimitSchedule

サービス: AWS Backup gateway

このアクションは、指定されたゲートウェイの帯域幅レート制限スケジュールを設定します。デフォルトでは、ゲートウェイには帯域幅レート制限スケジュールがありません。つまり、帯域幅レート制限は適用されません。これを使用して、ゲートウェイの帯域幅レート制限スケジュールを開始します。

リクエストの構文

```
{
   "BandwidthRateLimitIntervals": [
      {
         "AverageUploadRateLimitInBitsPerSec": number,
         "DaysOfWeek": [ number ],
         "EndHourOfDay": number,
         "EndMinuteOfHour": number,
         "StartHourOfDay": number,
         "StartMinuteOfHour": number
      }
   ],
   "GatewayArn": "string"
}
```

リクエストパラメータ

すべてのアクションに共通のパラメータの詳細については、「共通パラメータ」を参照してください。

リクエストは以下の JSON 形式のデータを受け入れます。

BandwidthRateLimitIntervals

ゲートウェイの帯域幅レート制限スケジュールの間隔を含む配列。帯域幅レート制限の間隔がスケジュールされていない場合、配列は空になります。

タイプ：BandwidthRateLimitInterval オブジェクトの配列

配列メンバー：最小数は 0 項目です。最大数は 20 項目です。

必須: はい

GatewayArn

ゲートウェイの Amazon リソースネーム (ARN)。ListGateways オペレーションを使用して、アカウント と のゲートウェイのリストを返します AWS リージョン。

型: 文字列

長さの制限: 最小長は 50 です。最大長は 180 です。

Pattern: ^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$

必須：はい

レスポンスの構文

```
{
   "GatewayArn": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

GatewayArn

ゲートウェイの Amazon リソースネーム (ARN)。ListGateways オペレーションを使用して、アカウント と のゲートウェイのリストを返します AWS リージョン。

型: 文字列

長さの制限: 最小長は 50 です。最大長は 180 です。

パターン：^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InternalServerException

内部エラーが発生したために操作は成功しませんでした。後ほどもう一度試してください。」

HTTP ステータスコード：500

ResourceNotFoundException

アクションに必要なリソースが見つかりませんでした。

HTTP ステータスコード：400

ThrottlingException

TPS は、意図的なまたは意図的でない、大量のリクエストを防ぐために制限されています。

HTTP ステータスコード：400

ValidationException

検証エラーが発生したため、操作は成功しませんでした。

HTTP ステータスコード：400

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutHypervisorPropertyMappings

サービス: AWS Backup gateway

このアクションは、指定されたハイパーバイザーのプロパティマッピングを設定します。ハイパーバイザープロパティマッピングは、ハイパーバイザーから利用可能なエンティティプロパティと、 で利用可能なプロパティとの関係を表示します AWS。

リクエストの構文

```
{
   "HypervisorArn": "string",
   "IamRoleArn": "string",
   "VmwareToAwsTagMappings": [
      {
         "AwsTagKey": "string",
         "AwsTagValue": "string",
         "VmwareCategory": "string",
         "VmwareTagName": "string"
      }
   ]
}
```

リクエストパラメータ

すべてのアクションに共通のパラメータの詳細については、「共通パラメータ」を参照してください。

リクエストは以下の JSON 形式のデータを受け入れます。

HypervisorArn

ハイパーバイザーの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。500 の最大長。

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必須：はい

IamRoleArn

IAM ロールの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 20 です。最大長は 2,048 です。

Pattern: ^arn:(aws|aws-cn|aws-us-gov):iam::([0-9]+):role/(\S+)$

必須：はい

VmwareToAwsTagMappings

このアクションは VMware タグと AWS タグとのマッピングをリクエストします。

型: VmwareToAwsTagMapping オブジェクトの配列

必須: はい

レスポンスの構文

```
{
   "HypervisorArn": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

HypervisorArn

ハイパーバイザーの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。500 の最大長。

パターン：^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

権限が不足しているため、操作を続行できません。

HTTP ステータスコード：400

ConflictException

サポートされていないため、操作を続行できません。

HTTP ステータスコード：400

InternalServerException

内部エラーが発生したために操作は成功しませんでした。後ほどもう一度試してください。」

HTTP ステータスコード：500

ResourceNotFoundException

アクションに必要なリソースが見つかりませんでした。

HTTP ステータスコード：400

ThrottlingException

TPS は、意図的なまたは意図的でない、大量のリクエストを防ぐために制限されています。

HTTP ステータスコード：400

ValidationException

検証エラーが発生したため、操作は成功しませんでした。

HTTP ステータスコード：400

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutMaintenanceStartTime

サービス: AWS Backup gateway

ゲートウェイのメンテナンス開始時間を設定します。

リクエストの構文

```
{
   "DayOfMonth": number,
   "DayOfWeek": number,
   "GatewayArn": "string",
   "HourOfDay": number,
   "MinuteOfHour": number
}
```

リクエストパラメータ

すべてのアクションに共通のパラメータの詳細については、「共通パラメータ」を参照してください。

リクエストは以下の JSON 形式のデータを受け入れます。

DayOfMonth

ゲートウェイでメンテナンスを開始する月の日。

有効な値の範囲は Sunday ~ Saturday です。

タイプ : 整数

有効な範囲: 最小値 は 1 です。最大値は 31 です。

必須: いいえ

DayOfWeek

ゲートウェイのメンテナンスを開始する曜日。

タイプ: 整数

有効な範囲: 最小値 は 0 です。最大値は 6 です。

必須: いいえ

GatewayArn

メンテナンス開始時刻を指定するために使用するゲートウェイの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。最大長は 180 です。

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必須 : はい

HourOfDay

ゲートウェイでメンテナンスを開始する時間。

タイプ: 整数

有効な範囲: 最小値 は 0 です。最大値は 23 です。

必須: はい

MinuteOfHour

ゲートウェイでメンテナンスを開始する時間の分。

タイプ: 整数

有効な範囲: 最小値 は 0 です。最大値は 59 です。

必須: はい

レスポンスの構文

```
{
   "GatewayArn": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

GatewayArn

メンテナンス開始時間を設定したゲートウェイの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。最大長は 180 です。

パターン：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

ConflictException

サポートされていないため、操作を続行できません。

HTTP ステータスコード：400

InternalServerException

内部エラーが発生したために操作は成功しませんでした。後ほどもう一度試してください。」

HTTP ステータスコード：500

ResourceNotFoundException

アクションに必要なリソースが見つかりませんでした。

HTTP ステータスコード：400

ThrottlingException

TPS は、意図的なまたは意図的でない、大量のリクエストを防ぐために制限されています。

HTTP ステータスコード：400

ValidationException

検証エラーが発生したため、操作は成功しませんでした。

HTTP ステータスコード：400

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

StartVirtualMachinesMetadataSync

サービス: AWS Backup gateway

このアクションは、指定された仮想マシン間でメタデータを同期するリクエストを送信します。

リクエストの構文

```
{
   "HypervisorArn": "string"
}
```

リクエストパラメータ

すべてのアクションに共通のパラメータの詳細については、「共通パラメータ」を参照してください。

リクエストは以下の JSON 形式のデータを受け入れます。

HypervisorArn

ハイパーバイザーの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。500 の最大長。

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必須：はい

レスポンスの構文

```
{
   "HypervisorArn": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

HypervisorArn

ハイパーバイザーの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。500 の最大長。

パターン：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

権限が不足しているため、操作を続行できません。

HTTP ステータスコード：400

InternalServerException

内部エラーが発生したために操作は成功しませんでした。後ほどもう一度試してください。」

HTTP ステータスコード：500

ResourceNotFoundException

アクションに必要なリソースが見つかりませんでした。

HTTP ステータスコード：400

ThrottlingException

TPS は、意図的なまたは意図的でない、大量のリクエストを防ぐために制限されています。

HTTP ステータスコード：400

ValidationException

検証エラーが発生したため、操作は成功しませんでした。

HTTP ステータスコード：400

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

TagResource

サービス: AWS Backup gateway

リソースをタグ付け。

リクエストの構文

```
{
   "ResourceARN": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

リクエストパラメータ

すべてのアクションに共通のパラメータの詳細については、「共通パラメータ」を参照してください。

リクエストは以下の JSON 形式のデータを受け入れます。

ResourceARN

タグに対するのリソースの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。500 の最大長。

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必須 : はい

Tags

リソースに割り当てるタグのリスト。

型: Tag オブジェクトの配列

必須: はい

レスポンスの構文

```
{
   "ResourceARN": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

ResourceARN

タグ付けした リソースの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。500 の最大長。

パターン：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InternalServerException

内部エラーが発生したために操作は成功しませんでした。後ほどもう一度試してください。」

HTTP ステータスコード：500

ResourceNotFoundException

アクションに必要なリソースが見つかりませんでした。

HTTP ステータスコード：400

ThrottlingException

TPS は、意図的なまたは意図的でない、大量のリクエストを防ぐために制限されています。

HTTP ステータスコード：400

ValidationException

検証エラーが発生したため、操作は成功しませんでした。

HTTP ステータスコード：400

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

TestHypervisorConfiguration

サービス: AWS Backup gateway

ハイパーバイザー構成をテストして、バックアップゲートウェイがハイパーバイザーとそのリソースに接続できることを確認します。

リクエストの構文

```
{
   "GatewayArn": "string",
   "Host": "string",
   "Password": "string",
   "Username": "string"
}
```

リクエストパラメータ

すべてのアクションに共通のパラメータの詳細については、「共通パラメータ」を参照してください。

リクエストは以下の JSON 形式のデータを受け入れます。

GatewayArn

テストするハイパーバイザーへのゲートウェイの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。最大長は 180 です。

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必須：はい

Host

ハイパーバイザーのサーバーホスト。これは、IP アドレスまたは完全修飾ドメイン名 (FQDN) のいずれかです。

型: 文字列

長さの制限: 最小長は 3 です。最大長は 128 です。

パターン: ^.+$

必須：はい

Password

ハイパーバイザーのパスワード。

型: 文字列

長さの制限: 最小長は 1 です。最大長は 100 です。

Pattern: ^[-~]+$

必須: いいえ

Username

ハイパーバイザーのユーザー名。

型: 文字列

長さの制限: 最小長は 1 です。最大長は 100 です。

Pattern: ^[-\.0-\[\]-~]*[!-\.0-\[\]-~][-\.0-\[\]-~]*$

必須：いいえ

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 200 レスポンスを返します。

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

ConflictException

サポートされていないため、操作を続行できません。

HTTP ステータスコード：400

InternalServerException

内部エラーが発生したために操作は成功しませんでした。後ほどもう一度試してください。」

HTTP ステータスコード：500

ResourceNotFoundException

アクションに必要なリソースが見つかりませんでした。

HTTP ステータスコード：400

ThrottlingException

TPS は、意図的なまたは意図的でない、大量のリクエストを防ぐために制限されています。

HTTP ステータスコード：400

ValidationException

検証エラーが発生したため、操作は成功しませんでした。

HTTP ステータスコード：400

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UntagResource

サービス: AWS Backup gateway

リソースからタグを削除します。

リクエストの構文

```
{
   "ResourceARN": "string",
   "TagKeys": [ "string" ]
}
```

リクエストパラメータ

すべてのアクションに共通のパラメータの詳細については、「共通パラメータ」を参照してください。

リクエストは以下の JSON 形式のデータを受け入れます。

ResourceARN

タグを削除するリソースの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。500 の最大長。

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必須：はい

TagKeys

削除するタグを指定するタグキーのリスト。

型: 文字列の配列

長さの制限：最小長は 1 です。最大長は 128 です。

パターン: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

必須：はい

レスポンスの構文

```
{
   "ResourceARN": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

ResourceARN

タグを削除するリソースの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。500 の最大長。

パターン：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InternalServerException

内部エラーが発生したために操作は成功しませんでした。後ほどもう一度試してください。」

HTTP ステータスコード：500

ResourceNotFoundException

アクションに必要なリソースが見つかりませんでした。

HTTP ステータスコード：400

ThrottlingException

TPS は、意図的なまたは意図的でない、大量のリクエストを防ぐために制限されています。

HTTP ステータスコード：400

ValidationException

検証エラーが発生したため、操作は成功しませんでした。

HTTP ステータスコード：400

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateGatewayInformation

サービス: AWS Backup gateway

ゲートウェイの名前を更新します。リクエストのゲートウェイの Amazon リソースネーム (ARN) を使用して、更新するゲートウェイを指定します。

リクエストの構文

```
{
   "GatewayArn": "string",
   "GatewayDisplayName": "string"
}
```

リクエストパラメータ

すべてのアクションに共通のパラメータの詳細については、「共通パラメータ」を参照してください。

リクエストは以下の JSON 形式のデータを受け入れます。

GatewayArn

更新するゲートウェイの Amazon リソースネーム (ARN)

型: 文字列

長さの制限: 最小長は 50 です。最大長は 180 です。

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必須：はい

GatewayDisplayName

ゲートウェイの更新された表示名。

型: 文字列

長さの制限: 最小長は 1 です。最大長は 100 です。

Pattern: `^[a-zA-Z0-9-]*$`

必須: いいえ

レスポンスの構文

```
{
   "GatewayArn": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

GatewayArn

更新したゲートウェイの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。最大長は 180 です。

パターン：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

ConflictException

サポートされていないため、操作を続行できません。

HTTP ステータスコード：400

InternalServerException

内部エラーが発生したために操作は成功しませんでした。後ほどもう一度試してください。」

HTTP ステータスコード：500

ResourceNotFoundException

アクションに必要なリソースが見つかりませんでした。

HTTP ステータスコード：400

ThrottlingException

TPS は、意図的なまたは意図的でない、大量のリクエストを防ぐために制限されています。

HTTP ステータスコード：400

ValidationException

検証エラーが発生したため、操作は成功しませんでした。

HTTP ステータスコード：400

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateGatewaySoftwareNow

サービス: AWS Backup gateway

ゲートウェイ仮想マシン (VM) ソフトウェアを更新します。リクエストはただちにソフトウェアの更新をトリガーします。

> **Note**
>
> このリクエストを行うと、すぐに 200 OK 成功のレスポンスが返されます。ただし、更新が完了するまでにしばらくかかります。

リクエストの構文

```
{
   "GatewayArn": "string"
}
```

リクエストパラメータ

すべてのアクションに共通のパラメータの詳細については、「共通パラメータ」を参照してください。

リクエストは以下の JSON 形式のデータを受け入れます。

GatewayArn

更新するゲートウェイの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。最大長は 180 です。

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必須：はい

レスポンスの構文

```
{
```

```
   "GatewayArn": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

GatewayArn

更新したゲートウェイの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。最大長は 180 です。

パターン：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

InternalServerException

内部エラーが発生したために操作は成功しませんでした。後ほどもう一度試してください。」

HTTP ステータスコード：500

ResourceNotFoundException

アクションに必要なリソースが見つかりませんでした。

HTTP ステータスコード：400

ThrottlingException

TPS は、意図的なまたは意図的でない、大量のリクエストを防ぐために制限されています。

HTTP ステータスコード：400

ValidationException

検証エラーが発生したため、操作は成功しませんでした。

HTTP ステータスコード：400

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateHypervisor

サービス: AWS Backup gateway

ホスト、ユーザー名、パスワードなどのハイパーバイザーメタデータを更新します。リクエストのハイパーバイザーの Amazon リソースネーム (ARN) を使用して、更新するハイパーバイザーを指定します。

リクエストの構文

```
{
   "Host": "string",
   "HypervisorArn": "string",
   "LogGroupArn": "string",
   "Name": "string",
   "Password": "string",
   "Username": "string"
}
```

リクエストパラメータ

すべてのアクションに共通のパラメータの詳細については、「共通パラメータ」を参照してください。

リクエストは以下の JSON 形式のデータを受け入れます。

Host

ハイパーバイザーの更新されたホスト。これは、IP アドレスまたは完全修飾ドメイン名 (FQDN) のいずれかです。

型: 文字列

長さの制限: 最小長は 3 です。最大長は 128 です。

Pattern: ^.+$

必須: いいえ

HypervisorArn

更新するハイパーバイザーの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。500 の最大長。

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必須 : はい

LogGroupArn

リクエストされたログ内のゲートウェイグループの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 0 です。最大長は 2,048 です。

パターン: `^$|^arn:(aws|aws-cn|aws-us-gov):logs:([a-zA-Z0-9-]+):([0-9]+):log-group:[a-zA-Z0-9_\-\/\.]+:\*$`

必須: いいえ

Name

ハイパーバイザーの更新された名前。

型: 文字列

長さの制限: 最小長は 1 です。最大長は 100 です。

Pattern: `^[a-zA-Z0-9-]*$`

必須: いいえ

Password

ハイパーバイザーの更新されたパスワード。

型: 文字列

長さの制限: 最小長は 1 です。最大長は 100 です。

Pattern: `^[ -~]+$`

必須: いいえ

Username

ハイパーバイザーの更新されたユーザー名。

型: 文字列

長さの制限: 最小長は 1 です。最大長は 100 です。

Pattern: ^[-\.0-\[\]-~]*[!-\.0-\[\]-~][-\.0-\[\]-~]*$

必須: いいえ

レスポンスの構文

```
{
   "HypervisorArn": "string"
}
```

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

HypervisorArn

更新したハイパーバイザーの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。500 の最大長。

パターン：^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$

エラー

すべてのアクションに共通のエラーについては、「共通エラー」を参照してください。

AccessDeniedException

権限が不足しているため、操作を続行できません。

HTTP ステータスコード：400

ConflictException

サポートされていないため、操作を続行できません。

HTTP ステータスコード：400

InternalServerException

内部エラーが発生したために操作は成功しませんでした。後ほどもう一度試してください。」

HTTP ステータスコード：500

ResourceNotFoundException

アクションに必要なリソースが見つかりませんでした。

HTTP ステータスコード：400

ThrottlingException

TPS は、意図的なまたは意図的でない、大量のリクエストを防ぐために制限されています。

HTTP ステータスコード：400

ValidationException

検証エラーが発生したため、操作は成功しませんでした。

HTTP ステータスコード：400

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS コマンドラインインターフェイス
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for PHP V3

- AWS SDK for Python
- AWS SDK for Ruby V3

データ型

以下のデータタイプが AWS Backup によってサポートされています。

- AdvancedBackupSetting
- BackupJob
- BackupJobSummary
- BackupPlan
- BackupPlanInput
- BackupPlansListMember
- BackupPlanTemplatesListMember
- BackupRule
- BackupRuleInput
- BackupSelection
- BackupSelectionsListMember
- BackupVaultListMember
- CalculatedLifecycle
- Condition
- ConditionParameter
- Conditions
- ControlInputParameter
- ControlScope
- CopyAction
- CopyJob
- CopyJobSummary
- DateRange
- Framework
- FrameworkControl

- KeyValue
- LegalHold
- Lifecycle
- ProtectedResource
- ProtectedResourceConditions
- RecoveryPointByBackupVault
- RecoveryPointByResource
- RecoveryPointCreator
- RecoveryPointMember
- RecoveryPointSelection
- ReportDeliveryChannel
- ReportDestination
- ReportJob
- ReportPlan
- ReportSetting
- RestoreJobCreator
- RestoreJobsListMember
- RestoreJobSummary
- RestoreTestingPlanForCreate
- RestoreTestingPlanForGet
- RestoreTestingPlanForList
- RestoreTestingPlanForUpdate
- RestoreTestingRecoveryPointSelection
- RestoreTestingSelectionForCreate
- RestoreTestingSelectionForGet
- RestoreTestingSelectionForList
- RestoreTestingSelectionForUpdate

以下のデータタイプが AWS Backup gateway によってサポートされています。

- BandwidthRateLimitInterval

- Gateway
- GatewayDetails
- Hypervisor
- HypervisorDetails
- MaintenanceStartTime
- Tag
- VirtualMachine
- VirtualMachineDetails
- VmwareTag
- VmwareToAwsTagMapping

AWS Backup

以下のデータタイプが AWS Backup によってサポートされています。

- AdvancedBackupSetting
- BackupJob
- BackupJobSummary
- BackupPlan
- BackupPlanInput
- BackupPlansListMember
- BackupPlanTemplatesListMember
- BackupRule
- BackupRuleInput
- BackupSelection
- BackupSelectionsListMember
- BackupVaultListMember
- CalculatedLifecycle
- Condition
- ConditionParameter
- Conditions
- ControlInputParameter

- ControlScope
- CopyAction
- CopyJob
- CopyJobSummary
- DateRange
- Framework
- FrameworkControl
- KeyValue
- LegalHold
- Lifecycle
- ProtectedResource
- ProtectedResourceConditions
- RecoveryPointByBackupVault
- RecoveryPointByResource
- RecoveryPointCreator
- RecoveryPointMember
- RecoveryPointSelection
- ReportDeliveryChannel
- ReportDestination
- ReportJob
- ReportPlan
- ReportSetting
- RestoreJobCreator
- RestoreJobsListMember
- RestoreJobSummary
- RestoreTestingPlanForCreate
- RestoreTestingPlanForGet
- RestoreTestingPlanForList
- RestoreTestingPlanForUpdate
- RestoreTestingRecoveryPointSelection

- RestoreTestingSelectionForCreate
- RestoreTestingSelectionForGet
- RestoreTestingSelectionForList
- RestoreTestingSelectionForUpdate

AdvancedBackupSetting

サービス: AWS Backup

各リソースタイプのバックアップオプション。

内容

BackupOptions

選択したリソースのバックアップオプションを指定します。このオプションは、Windows VSS バックアップジョブでのみ有効です。

有効値:

`"WindowsVSS":"enabled"` に設定すると、`WindowsVSS` のバックアップオプションが有効になり、Windows VSS バックアップが作成されます。

`"WindowsVSS":"disabled"` に設定すると、定期的にバックアップを作成します。`WindowsVSS` のオプションはデフォルトでは、有効ではありません。

無効なオプションを指定すると、`InvalidParameterValueException` の例外が発生します。

Windows VSS バックアップの詳細については、VSS 対応の Windows Backup の作成を参照してください。

型: 文字列から文字列へのマッピング

キーパターン: `^[a-zA-Z0-9\-\_\.]{1,50}$`

値パターン:`^[a-zA-Z0-9\-\_\.]{1,50}$`

必須: いいえ

ResourceType

リソースタイプとバックアップオプションを含むオブジェクトを指定します。サポートされているリソースタイプは、Windows Volume Shadow Copy Service (VSS)を使用した Amazon EC2 インスタンスのみです。 CloudFormation 例については、「 ユーザーガイド」の「Windows VSS を有効にするサンプル CloudFormation テンプレート AWS Backup 」を参照してください。

有効な値: `EC2`。

型: 文字列

パターン：^[a-zA-Z0-9\-_\.]{1,50}$

必須: いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupJob

サービス: AWS Backup

バックアップジョブに関する詳細情報が含まれています。

内容

AccountId

バックアップジョブを所有する アカウント ID です。

型: 文字列

パターン：^[0-9]{12}$

必須: いいえ

BackupJobId

リソースをバックアップ AWS Backup する へのリクエストを一意に識別します。

タイプ: 文字列

必須: いいえ

BackupOptions

選択したリソースのバックアップオプションを指定します。このオプションは、Windows ボリュームシャドウコピーサービス (VSS) バックアップジョブでのみ使用できます。

有効な値:"WindowsVSS":"enabled" に設定してWindowsVSS バックアップオプションをを有効にし、Windows VSS バックアップを作成します。"WindowsVSS":"disabled" に設定すると、定期的にバックアップを作成します。無効なオプションを指定すると、InvalidParameterValueException の例外が発生します。

型: 文字列から文字列へのマッピング

キーパターン: ^[a-zA-Z0-9\-_\.]{1,50}$

値パターン:^[a-zA-Z0-9\-_\.]{1,50}$

必須: いいえ

BackupSizeInBytes

バックアップのサイズはバイト単位です。

型: Long

必須: いいえ

BackupType

バックアップジョブのバックアップのタイプを表します。

タイプ: 文字列

必須: いいえ

BackupVaultArn

arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVaultなどのバックアップボールトを一意に識別する Amazon リソースネーム (ARN)。

タイプ: 文字列

必須: いいえ

BackupVaultName

バックアップを保存する論理コンテナの名前。バックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先の AWS リージョンに一意の名前で識別されます。

型: 文字列

パターン：^[a-zA-Z0-9\-_]{2,50}$

必須: いいえ

BytesTransferred

ジョブステータスの照会時にバックアップボールトに転送されたバイト単位のサイズ。

型: Long

必須: いいえ

CompletionDate

バックアップジョブを作成するジョブが完了した日時 をUnix 形式および協定世界時 (UTC)で表示します。CompletionDate の値は、ミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

CreatedBy

バックアップジョブの作成に使用されたバックアッププランの BackupPlanArn,BackupPlanId,BackupPlanVersion, およびBackupRuleId 含む、バックアップジョブの作成に関する識別情報がまれています。

タイプ：RecoveryPointCreator オブジェクト

必須: いいえ

CreationDate

バックアップジョブが作成された日時をUnix形式および協定世界時 (UTC) で表示します。CreationDate の値は、ミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

ExpectedCompletionDate

リソースのバックアップを行うジョブが完了する予定の日時を、Unix形式および協定世界時 (UTC) で表示します。ExpectedCompletionDate の値は,ミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

IamRoleArn

対象となるリカバリーポイントの作成に使用する IAM ロール ARN を指定します。デフォルトロール以外の IAM ロールには、ロール名に AWSBackup または AwsBackup のいずれかを含める必要があります。例えば arn:aws:iam::123456789012:role/AWSBackupRDSAccess です。これらの文字列のないロール名には、バックアップジョブを実行する権限がありません。

タイプ: 文字列

必須: いいえ

InitiationDate

バックアップジョブが開始された日付。

型: タイムスタンプ

必須: いいえ

IsParent

これは、これが親 (複合) バックアップジョブであることを示すブール値です。

型: ブール値

必須: いいえ

MessageCategory

このパラメータは、指定されたメッセージカテゴリのジョブ数です。

文字列の例としては `AccessDenied`、`SUCCESS`、`AGGREGATE_ALL`、および `INVALIDPARAMETERS` があります。 MessageCategory 文字列のリストについては、「モニタリング」を参照してください。

値 ANY は、すべてのメッセージカテゴリの数を返します。

`AGGREGATE_ALL` は、すべてのメッセージカテゴリのジョブ数を集計し、その合計を返します。

タイプ: 文字列

必須: いいえ

ParentJobId

これは、リソースをバックアップするための AWS Backup へのリクエストを一意に識別します。戻り値は親 (複合) ジョブ ID になります。

タイプ: 文字列

必須: いいえ

PercentDone

ジョブのステータスが照会された時点でのジョブの完了見込み率が含まれます。

タイプ: 文字列

必須: いいえ

RecoveryPointArn

リカバリーポイントを一意に識別する ARN、たとえば、arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45 です。

タイプ: 文字列

必須: いいえ

ResourceArn

リソースを一意に識別するためのARN。ARN の形式は、リソースタイプによって異なります。

タイプ: 文字列

必須: いいえ

ResourceName

指定されたバックアップに属するリソースの一意でない名前。

タイプ: 文字列

必須: いいえ

ResourceType

バックアップする AWS リソースのタイプ。Amazon Elastic Block Store (Amazon EBS) ボリュームや Amazon Relational Database Service (Amazon RDS) データベースなど。Windows Volume Shadow Copy Service (VSS) バックアップでは、サポートされているリソースタイプは Amazon EC2 のみです。

型: 文字列

パターン：^[a-zA-Z0-9\-_\.]{1,50}$

必須: いいえ

StartBy

バックアップジョブがキャンセルされる前に開始しなければならない時刻を Unix 形式および協定世界時 (UTC)) で指定します。この値は、スケジュールされた時刻に開始ウィンドウを追加して計算されます。そのため、予定時刻が午後6時でスタートウィンドウが2時間であれ

ば、StartBy時刻は指定された日付の午後 8:00 になります。StartByの値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

State

バックアップジョブの現在の状態です。

型: 文字列

有効な値 : CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL

必須 : いいえ

StatusMessage

リソースをバックアップするジョブのステータスを説明する詳細なメッセージ。

タイプ: 文字列

必須: いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupJobSummary

サービス: AWS Backup

過去 30 日以内に作成または実行されたジョブの概要です。

返される概要には、リージョン、アカウント、状態、 RestourceType MessageCategory、StartTime EndTime、含まれるジョブの数が含まれます。

内容

AccountId

概要に含まれるジョブを所有するアカウント ID。

型: 文字列

パターン：`^[0-9]{12}$`

必須: いいえ

Count

概要に含まれるジョブの数を示す値。

タイプ: 整数

必須: いいえ

EndTime

ジョブの終了時刻を数値形式で表した時間の値。

この値は、Unix 形式、協定世界時 (UTC) で、ミリ秒単位の精度です。例えば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

MessageCategory

このパラメータは、指定されたメッセージカテゴリのジョブ数です。

文字列の例としては `AccessDenied`、`Success`、および `InvalidParameters` があります。MessageCategory 文字列のリストについては、「モニタリング」を参照してください。

値 ANY は、すべてのメッセージカテゴリの数を返します。

AGGREGATE_ALL は、すべてのメッセージカテゴリのジョブ数を集計し、その合計を返します。

タイプ: 文字列

必須: いいえ

Region

ジョブ概要内の AWS リージョン。

タイプ: 文字列

必須: いいえ

ResourceType

この値は、指定されたリソースタイプのジョブ数です。リクエスト GetSupportedResourceTypes は、サポートされているリソースタイプの文字列を返します。

型: 文字列

パターン：^[a-zA-Z0-9\-_\.]{1,50}$

必須: いいえ

StartTime

ジョブの開始時刻を数値形式で表した時間の値。

この値は、Unix 形式、協定世界時 (UTC) で、ミリ秒単位の精度です。例えば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

State

この値は、指定された状態のジョブのジョブ数です。

型: 文字列

有効な値：CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL | AGGREGATE_ALL | ANY

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupPlan

サービス: AWS Backup

バックアップ計画の表示名 (省略可能) と BackupRule オブジェクトの配列が含まれます。各オブジェクトがバックアップルールを指定します。バックアップ計画の各ルールは、個別にスケジュールされるタスクであり、異なる AWS リソースの選択をバックアップすることができます。

内容

BackupPlanName

バックアッププランの表示名。1～50 の英数字または 「-_」 を含める必要があります。。

型: 文字列

必須: はい

Rules

BackupRule オブジェクトの配列。各オブジェクトは、選択したリソースのバックアップに使用される、スケジュールされたタスクを指定します。

型: BackupRule オブジェクトの配列

必須: はい

AdvancedBackupSettings

リソースタイプごとにBackupOptions リストが含まれます。。

型: AdvancedBackupSetting オブジェクトの配列

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupPlanInput

サービス: AWS Backup

バックアップ計画の表示名 (省略可能) と BackupRule オブジェクトの配列が含まれます。各オブジェクトがバックアップルールを指定します。バックアップ計画の各ルールは、個別のスケジュールタスクです。

内容

BackupPlanName

バックアッププランの表示名。1～50 の英数字または 「-_」 を含める必要があります。。

型: 文字列

必須: はい

Rules

BackupRule オブジェクトの配列。各オブジェクトは、選択したリソースのバックアップに使用される、スケジュールされたタスクを指定します。

型: BackupRuleInput オブジェクトの配列

必須: はい

AdvancedBackupSettings

リソースタイプごとに BackupOptions のリストを指定します。これらの設定は、Windows Volume Shadow Copy Service (VSS) バックアップジョブでのみで有効です。

型: AdvancedBackupSetting オブジェクトの配列

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2

- AWS SDK for Ruby V3

BackupPlansListMember

サービス: AWS Backup

バックアップ計画に関するメタデータが含まれます。

内容

AdvancedBackupSettings

リソースタイプの BackupOptions のリストが含まれます。

型: AdvancedBackupSetting オブジェクトの配列

必須: いいえ

BackupPlanArn

例えば、arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50 などのバックアップ計画を一意に識別する Amazon リソースネーム (ARN) です。

タイプ: 文字列

必須: いいえ

BackupPlanId

バックアップ計画を一意に識別します。

タイプ: 文字列

必須: いいえ

BackupPlanName

保存されたバックアップ計画の表示名。

タイプ: 文字列

必須: いいえ

CreationDate

リソースのバックアップ計画が作成された日時をUnix 形式および協定世界時 (UTC)で表示します。CreationDate の値は、ミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

CreatorRequestId

リクエストを識別するための一意の文字列で、失敗したリクエストを再試行する際に、オペレーションを2回実行するリスクを回避することができます。このパラメータはオプションです。

使用する場合、このパラメータには 1～50 文字の英数字または「-_」を含める必要があります 。

タイプ: 文字列

必須: いいえ

DeletionDate

バックアップ計画が削除される日時は、Unix 形式および協定世界時 (UTC)で表示されます。DeletionDateの値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

LastExecutionDate

このバックアッププランが最後に実行された時刻。日時は、Unix 形式および協定世界時 (UTC) です。LastExecutionDateの値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

VersionId

一意のランダムに生成された UTF-8 エンコード Unicode 文字列 (最大 1,024 バイト長)。バージョン ID を編集することはできません。

タイプ: 文字列

必須: いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupPlanTemplatesListMember

サービス: AWS Backup

バックアップ計画テンプレートに関連するメタデータを指定するオブジェクトです。

内容

BackupPlanTemplateId

保存されているバックアップ計画テンプレートを一意に識別します。

タイプ: 文字列

必須: いいえ

BackupPlanTemplateName

バックアップ計画テンプレートのオプション表示名です。

タイプ: 文字列

必須: いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupRule

サービス: AWS Backup

選択したリソースをバックアップするスケジュールタスクを指定します。

内容

RuleName

バックアップルールの表示名。1～50 の英数字または 「-_」 を含める必要があります。。

型: 文字列

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

必須：はい

TargetBackupVaultName

バックアップを保存する論理コンテナの名前。バックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先の AWS リージョンに一意の名前で識別されます。

型: 文字列

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

必須：はい

CompletionWindowMinutes

バックアップジョブが正常に開始されてから完了するまで、または AWS Backupによってキャンセルされるまでの分単位の値です。この値はオプションです。

型: Long

必須: いいえ

CopyActions

`CopyAction` オブジェクトの配列で、コピーオペレーションの詳細を含みます。

型: CopyAction オブジェクトの配列

必須: いいえ

EnableContinuousBackup

が継続的バックアップ AWS Backup を作成するかどうかを指定します。True の場合 AWS Backup 、 は point-in-time 復元可能な継続的バックアップ (PITR) を作成します。False (または指定なし) の場合 AWS Backup 、 はスナップショットバックアップを作成します。

型: ブール値

必須: いいえ

Lifecycle

ライフサイクルは、保護されたリソースがコールドストレージに移行するタイミングと、期限切れになるタイミングを定義します。 は、定義したライフサイクルに従ってバックアップを自動的に AWS Backup 移行および期限切れにします。

コールドストレージに移行されたバックアップは、そこに最低 90 日保存される必要があります。したがって、「保持期間」の設定は、「コールドへの移行 (日数)」設定から 90 日以上あける必要があります。バックアップがコールドに移行された後で、「コールドへの移行 (日数)」設定を変更することはできません。

コールドストレージに移行できるリソースタイプは、「リソース別の機能の可用性」の表に記載されています。他のリソースタイプでは、この式は AWS Backup 無視されます。

タイプ : Lifecycle オブジェクト

必須: いいえ

RecoveryPointTags

バックアップから復元されたときに、このルールに関連付けられているリソースに割り当てられるタグ。

型: 文字列間のマッピング

必須: いいえ

RuleId

選択したリソースのバックアップをスケジュールに入れるために使用されるルールを一意に識別します。

タイプ: 文字列

必須: いいえ

ScheduleExpression

がバックアップジョブ AWS Backup を開始するタイミングを指定する UTC の cron 式。 AWS cron 式の詳細については、「Amazon Events ユーザーガイド」の「ルールのスケジュール式」を参照してください。 CloudWatch AWS cron 式の 2 つの例は、 `15 * ? * * *` (1 時間ごとに 15 分後にバックアップを取る) と `0 12 * * ? *` (毎日正午 UTC にバックアップを取る) です。例のテーブルについては、前のリンクをクリックし、ページを下にスクロールします。

タイプ: 文字列

必須: いいえ

ScheduleExpressionTimezone

スケジュール式が設定されているタイムゾーン。デフォルトでは、 ScheduleExpressions は UTC です。これを、指定したタイムゾーンに変更できます。

タイプ: 文字列

必須: いいえ

StartWindowMinutes

バックアップが予定されてから、ジョブが正常に開始されない場合にキャンセルされるまでの時間を分単位で指定する値です。この値はオプションです。この値を含める場合、エラーを避けるために少なくとも 60 分必要です。

開始ウィンドウ中、バックアップジョブのステータスは、正常に開始されるか、開始ウィンドウの時間がなくなるまで `CREATED` ステータスのままになります。開始ウィンドウ時間内にジョブの再試行を許可するエラー AWS Backup を受け取った場合、 AWS Backup は、バックアップが正常に開始 (ジョブステータスが に変わる`RUNNING`) するか、ジョブステータスが に変わる `EXPIRED` (開始ウィンドウ時間が終了すると発生することが予想される) まで、少なくとも 10 分ごとにジョブの開始を自動的に再試行します。

型: Long

必須: いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupRuleInput

サービス: AWS Backup

選択したリソースをバックアップするスケジュールタスクを指定します。

内容

RuleName

バックアップルールの表示名。1～50 の英数字または 「-_」 を含める必要があります。。

型: 文字列

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

必須：はい

TargetBackupVaultName

バックアップを保存する論理コンテナの名前。バックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先の AWS リージョンに一意の名前で識別されます。

型: 文字列

Pattern: `^[a-zA-Z0-9\-\_]{2,50}$`

必須：はい

CompletionWindowMinutes

バックアップジョブが正常に開始されてから完了するまで、または AWS Backupによってキャンセルされるまでの分単位の値です。この値はオプションです。

型: Long

必須: いいえ

CopyActions

`CopyAction` オブジェクトの配列で、コピーオペレーションの詳細を含みます。

型: CopyAction オブジェクトの配列

必須: いいえ

EnableContinuousBackup

が継続的バックアップ AWS Backup を作成するかどうかを指定します。True の場合 AWS Backup 、 は point-in-time 復元可能な継続的バックアップ (PITR) を作成します。False (または指定なし) の場合 AWS Backup 、 はスナップショットバックアップを作成します。

型: ブール値

必須: いいえ

Lifecycle

ライフサイクルは、保護されたリソースがコールドストレージに移行するタイミングと有効期限を定義します。 AWS Backup は、定義したライフサイクルに従ってバックアップを自動的に移行して期限切れにします。

コールドストレージに移行されたバックアップは、そこに最低 90 日保存される必要があります。したがって、「保持期間」の設定は、「コールドへの移行 (日数)」設定から 90 日以上あける必要があります。バックアップをコールドストレージに移行した後は、「数日後にコールドに移行」設定を変更することはできません。

コールドストレージに移行できるリソースタイプは、「リソース別の機能の可用性」の表に記載されています。他のリソースタイプでは、この式は AWS Backup 無視されます。

このパラメータの最大値は 100 年 (36,500 日) です。

タイプ : Lifecycle オブジェクト

必須: いいえ

RecoveryPointTags

リソースに割り当てるタグ。

型: 文字列間のマッピング

必須: いいえ

ScheduleExpression

がバックアップジョブ AWS Backup を開始するタイミングを指定する UTC の CRON 式。

タイプ: 文字列

必須: いいえ

ScheduleExpressionTimezone

スケジュール式が設定されているタイムゾーン。デフォルトでは、 ScheduleExpressions は UTC です。これを、指定したタイムゾーンに変更できます。

タイプ: 文字列

必須: いいえ

StartWindowMinutes

バックアップが予定されてから、ジョブが正常に開始されない場合にキャンセルされるまでの時間を分単位で指定する値です。この値はオプションです。この値を含める場合、エラーを避けるために少なくとも 60 分必要です。

このパラメータの最大値は 100 年 (52,560,000 分) です。

開始ウィンドウ中、バックアップジョブのステータスは、正常に開始されるか、開始ウィンドウの時間がなくなるまで CREATED ステータスのままになります。開始ウィンドウ時間内にジョブの再試行を許可するエラー AWS Backup を受け取った場合、 AWS Backup は、バックアップが正常に開始 (ジョブステータスが に変わるRUNNING) するか、ジョブステータスが に変わる EXPIRED (開始ウィンドウ時間が終了すると発生することが予想される) まで、少なくとも 10 分ごとにジョブの開始を自動的に再試行します。

型: Long

必須: いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupSelection

サービス: AWS Backup

バックアップ計画にリソースのセットを指定するために使用します。

含める、または除外する条件、タグ、またはリソースを指定することをお勧めします。そうしないと、バックアップはサポートされているすべてのストレージリソースとオプトインされたストレージリソースを選択しようとします。これは、意図しないコストに影響する可能性があります。

詳細については、「プログラムによるリソースの割り当て」を参照してください。

内容

IamRoleArn

ターゲットリソースのバックアップ時に が認証 AWS Backup に使用する IAM ロールの ARN。例えば、`arn:aws:iam::123456789012:role/S3Access`。

型: 文字列

必須: はい

SelectionName

リソース選択ドキュメントの表示名。1～50 の英数字または 「-_」 を含める必要があります。。

型: 文字列

Pattern: `^[a-zA-Z0-9\-\_\.]{1,50}$`

必須：はい

Conditions

タグを使用してバックアッププランにリソースを割り当てるために定義する条件。例えば `"StringEquals": { "ConditionKey": "aws:ResourceTag/CreatedByCryo", "ConditionValue": "true" }` です。

`Conditions` は、`StringEquals`、`StringLike`、`StringNotEquals`、および をサポートしますStringNotLike。条件演算子では、大文字と小文字が区別されます。

複数の条件を指定すると、リソースはすべての条件 (AND ロジック) とほぼ一致します。

タイプ：Conditions オブジェクト

必須: いいえ

ListOfTags

タグを使用してバックアッププランにリソースを割り当てるために定義する条件。例えば `"StringEquals": { "ConditionKey": "aws:ResourceTag/CreatedByCryo", "ConditionValue": "true"}` です。

`ListOfTags` は のみをサポートします`StringEquals`。条件演算子では、大文字と小文字が区別されます。

複数の条件を指定すると、リソースはどの条件 (OR ロジック) にもよく一致します。

型: Condition オブジェクトの配列

必須: いいえ

NotResources

バックアッププランから除外するリソースの Amazon ARNs)。ARN の最大数は、ワイルドカードを使用しない場合は 500、またはワイルドカードを使用する場合は 30 の ARN です。

バックアップ計画から多くのリソースを除外する必要がある場合は、1 つまたは少数のリソースタイプのみを割り当てるか、タグを使用してリソース選択を調整するなど、異なるリソース選択戦略を検討してください。

タイプ：文字列の配列

必須: いいえ

Resources

バックアッププランに割り当てるリソースの Amazon ARNs)。ARN の最大数は、ワイルドカードを使用しない場合は 500、またはワイルドカードを使用する場合は 30 ARNです。

バックアッププランに多数のリソースを割り当てる必要がある場合は、リソースタイプのすべてのリソースを割り当てるか、タグを使用してリソース選択を調整するなど、異なるリソース選択戦略を検討してください。

複数の ARNs、リソースはどの ARNsにもよく一致します。

タイプ：文字列の配列

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupSelectionsListMember

サービス: AWS Backup

`BackupSelection` オブジェクトに関するメタデータが含まれます。

内容

BackupPlanId

バックアップ計画を一意に識別します。

タイプ: 文字列

必須: いいえ

CreationDate

バックアップ計画が作成された日時は、Unix 時刻形式および協定世界時 (UTC)で表示されています。`CreationDate`の値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

CreatorRequestId

リクエストを識別するための一意の文字列で、失敗したリクエストを再試行する際に、オペレーションを2回実行するリスクを回避することができます。このパラメータはオプションです。

使用する場合、このパラメータには 1～50 文字の英数字または「-_」を含める必要があります 。

タイプ: 文字列

必須: いいえ

IamRoleArn

ターゲットリカバリーポイントを作成する IAM ロール Amazon Resource Name (ARN) を指定します。たとえば `arn:aws:iam::123456789012:role/S3Access` 。

タイプ: 文字列

必須: いいえ

SelectionId

バックアップ計画に一連のリソースを割り当てるためのリクエストを一意に識別します。

タイプ: 文字列

必須: いいえ

SelectionName

リソース選択ドキュメントの表示名。

型: 文字列

パターン：`^[a-zA-Z0-9\-\_\.]{1,50}$`

必須: いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

BackupVaultListMember

サービス: AWS Backup

バックアップボールトに関するメタデータが含まれます。

内容

BackupVaultArn

arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVaultなどのバックアップボールトを一意に識別する Amazon リソースネーム (ARN)。

タイプ: 文字列

必須: いいえ

BackupVaultName

バックアップを保存する論理コンテナの名前。バックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先の AWS リージョンに一意の名前で識別されます。

型: 文字列

パターン：^[a-zA-Z0-9\-_]{2,50}$

必須: いいえ

CreationDate

リソースのバックアップが作成された日時は、Unix形式および、協定世界時 (UTC) で表示されています。CreationDate の値は、ミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

CreatorRequestId

リクエストを識別するための一意の文字列で、失敗したリクエストを再試行する際に、オペレーションを2回実行するリスクを回避することができます。このパラメータはオプションです。

使用する場合、このパラメータには 1 ~ 50 文字の英数字または「-_」を含める必要があります 。

タイプ: 文字列

必須: いいえ

EncryptionKeyArn

フル AWS Backup 管理をサポートするサービスからのバックアップを暗号化するために指定できるサーバー側の暗号化キー。例えば、`arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`。キーを指定する場合は、エイリアスではなく ARN を指定する必要があります。キーを指定しない場合、 AWS Backup はデフォルトで KMS キーを作成します。

フル AWS Backup 管理をサポートしている AWS Backup サービス、およびフル をサポートしていないサービスからのバックアップの暗号化を が AWS Backup 処理する方法については AWS Backup、「 でのバックアップの暗号化 AWS Backup」を参照してください。

タイプ: 文字列

必須: いいえ

LockDate

AWS Backup ボールトロック設定がイミュータブルになった日時。つまり、変更または削除することはできません。

ロック日を指定せずにボールトロックをボールトに適用した場合は、いつでもボールトロックの設定を変更したり、ボールトからボールトロックを完全に削除したりできます。

この値は、Unix 形式、協定世界時 (UTC) 、ミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

Locked

AWS Backup ボールトロックが選択したバックアップボールトに適用されるかどうかを示すブール値。`true` の場合は、ボールトロックにより、選択したボールト内のリカバリーポイントに対する削除および更新操作ができなくなります。

型: ブール値

必須: いいえ

MaxRetentionDays

AWS Backup ボールトが復旧ポイントを保持する最大保持期間を指定するボールトロック設定。このパラメータを指定しない場合、Vault Lock はボールト内のリカバリポイントに最大保持期間を強制しません (無期限ストレージを許可)。

指定した場合、ボールトへのバックアップジョブもしくはコピージョブには、保存期間が最大保存期間と同等もしくは以下のライフサイクル・ポリシーを持つ必要があります。ジョブの保持期間がその最大保存期間よりも長い場合、ボールトはバックアップジョブもしくはコピージョブに失敗するため、ライフサイクル設定を変更するか、別のボールトを使用する必要があります。ボールトロックの前にボールトにすでに格納されているリカバリポイントは影響を受けません。

型: Long

必須: いいえ

MinRetentionDays

AWS Backup ボールトが復旧ポイントを保持する最小保持期間を指定するボールトロック設定。このパラメータを指定しない場合、ボールトロックは最小保持期間を強制しません。

指定した場合、ボールトへのバックアップジョブまたはコピージョブには、最小保存期間以上の保存期間を持つライフサイクルポリシーが必要です。ジョブの保持期間がその最小保存期間より短い場合、ボールトはバックアップジョブまたはコピージョブに失敗するため、ライフサイクル設定を変更するか、別のボールトを使用する必要があります。ボールトロックの前にボールトにすでに格納されているリカバリポイントは影響を受けません。

型: Long

必須: いいえ

NumberOfRecoveryPoints

バックアップボールトに保存されているリカバリーポイントの数です。

型: Long

必須: いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CalculatedLifecycle

サービス: AWS Backup

リカバリーポイントのライフサイクルを指定するために使用される `DeleteAt` および `MoveToColdStorageAt`のタイムスタンプが含まれています。

ライフサイクルは、保護されたリソースがコールドストレージに移行するタイミングと、期限切れになるタイミングを定義します。 は、定義したライフサイクルに従ってバックアップを自動的に AWS Backup 移行および期限切れにします。

コールドストレージに移行されたバックアップは、そこに最低 90 日保存される必要があります。したがって、「保持期間」の設定は、「コールドへの移行 (日数)」設定から 90 日以上あける必要があります。バックアップがコールドに移行された後で、「コールドへの移行 (日数)」設定を変更することはできません。

コールドストレージに移行できるリソースタイプは、「リソース別の機能の可用性」の表に記載されています。他のリソースタイプでは、この式は AWS Backup 無視されます。

内容

DeleteAt

リカバリーポイントを削除するタイミングを指定するタイムスタンプです。

型: タイムスタンプ

必須: いいえ

MoveToColdStorageAt

リカバリーポイントをコールドストレージに移行するタイミングを指定するタイムスタンプです。

型: タイムスタンプ

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Condition

サービス: AWS Backup

条件タイプ (StringEquals など)、キー、および値で構成されるトリプレットの配列を含みます。タグを使用してリソースをフィルタリングし、バックアッププランに割り当てるために使用します。大文字と小文字の区別があります。

内容

ConditionKey

キーと値のペアのキー。たとえば、タグでは Department: Accounting,Department がキーです。

型: 文字列

必須: はい

ConditionType

バックアップ計画にリソースを割り当てるために使用されるキーと値のペアに適用される操作です。条件は、StringEqualsのみサポートします。StringLike、および、バックアッププランからリソースを除外する機能を含む、より柔軟な割り当てオプションについては、BackupSelection に Conditions（末尾に「s」を付けて）お使いください。

型: 文字列

有効な値：STRINGEQUALS

必須: はい

ConditionValue

キーと値のペアの値。たとえば、タグでは Department: Accounting,Accounting が値です。

型: 文字列

必須: はい

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ConditionParameter

サービス: AWS Backup

タグ付きリソースをバックアップ計画に割り当てるときに定義したタグに関する情報が含まれています。

タグに プレフィックスを含めaws:ResourceTagます。例えば "aws:ResourceTag/TagKey1": "Value1" です。

内容

ConditionKey

キーと値のペアのキー。たとえば、タグでは Department: Accounting,Department がキーです。

タイプ: 文字列

必須: いいえ

ConditionValue

キーと値のペアの値。たとえば、タグでは Department: Accounting,Accounting が値です。

タイプ: 文字列

必須: いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Conditions

サービス: AWS Backup

タグを使用してバックアップ計画に含める、または除外するリソースに関する情報が含まれています。条件キーは大文字と小文字が区別されます。

内容

StringEquals

タグ付きリソースの値を、同じ値でタグ付けしたリソースに対してのみフィルタリングします。 「完全一致」とも呼ばれます。

型: ConditionParameter オブジェクトの配列

必須: いいえ

StringLike

タグ付きリソースの値をフィルタリングして、文字列内の任意の場所でワイルドカード文字 (*) を使用してタグ値を一致させます。 たとえば、「prod*」または「*rod*」はタグ値「production」と一致します。

型: ConditionParameter オブジェクトの配列

必須: いいえ

StringNotEquals

タグ付きリソースの値を、同じ値を持たないタグ付きリソースに対してのみフィルタリングします。 「否定マッチング」とも呼ばれます。

型: ConditionParameter オブジェクトの配列

必須: いいえ

StringNotLike

文字列の任意の場所にワイルドカード文字 (*) を使用して、タグ付きリソースの値に一致しないタグ値をフィルタリングします。

型: ConditionParameter オブジェクトの配列

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ControlInputParameter

サービス: AWS Backup

コントロールのパラメータ。コントロールには、0、1、または複数のパラメーターを含めることができます。2 つのパラメーターを持つコントロールの例は、「バックアップ計画の頻度は少なくとも daily で、保存期間は、少なくとも 1 year である」があげられます。最初のパラメータは daily です。2番目のパラメータは 1 year です。

内容

ParameterName

パラメータの名前は、たとえば、BackupPlanFrequency 。

タイプ: 文字列

必須: いいえ

ParameterValue

パラメーターの値は、たとえば、hourly 。

タイプ: 文字列

必須: いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ControlScope

サービス: AWS Backup

フレームワークは、1 つまたは、複数のコントロールで構成されます。各コントロールには独自のコントロールスコープがあります。　コントロールスコープには、1 つ以上のリソースタイプ、タグキーと値の組み合わせ、または 1 つのリソースタイプと 1 つのリソース ID の組み合わせを含めることができます。スコープが指定されていない場合は、レコーディンググループ内のいずれかのリソースの設定が変更されたときにルールの評価が行われます。

> **Note**
>
> 特定のリソースをすべて含むコントロールスコープを設定するには、`ControlScope` を空にするか、`CreateFramework` を呼び出し時にそれを渡さないようにします。

内容

ComplianceResourceIds

コントロールスコープに含める唯一の AWS リソースの ID。

タイプ：文字列の配列

配列メンバー: 最小数は 1 項目です。最大数は 100 項目です。

必須: いいえ

ComplianceResourceTypes

コントロールスコープに `EFS` または `RDS` などのリソースが含まれているかどうかを記述します。

タイプ：文字列の配列

必須: いいえ

Tags

ルールの評価をトリガーする AWS リソースに適用されるタグのキーと値のペア。最大 1 つのキーと値のペアを指定できます。タグ値はオプションですが、コンソールからフレームワークを作成または編集する場合、空の文字列にすることはできません (ただし、 CloudFormation テンプレートに含める場合は空の文字列にすることができます) 。

タグを割り当てる構造は次のとおりです。`[{"Key":"string","Value":"string"}]` 。

型: 文字列間のマッピング

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CopyAction

サービス: AWS Backup

コピーオペレーションの詳細です。

内容

DestinationBackupVaultArn

コピーされたバックアップの送信先バックアップボールトを一意に識別する Amazon リソースネーム (ARN)。例えば `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault` です。

タイプ: 文字列

必須: はい

Lifecycle

復旧ポイントがコールドストレージに移行するか、削除されるまでの時間を日数で指定します。

コールドストレージに移行されたバックアップは、そこに最低 90 日保存される必要があります。したがって、コンソールでは、保持設定は、日数設定後のコールドへの移行よりも 90 日長くする必要があります。バックアップがコールドに移行した後、日数設定をコールドに移行することはできません。

コールドストレージに移行できるリソースタイプは、「リソース別の機能の可用性」の表に記載されています。他のリソースタイプでは、この式は AWS Backup 無視されます。

既存のライフサイクルと保持期間を削除し、復旧ポイントを無期限に保持するには、`MoveToColdStorageAfterDays`と に -1 を指定します`DeleteAfterDays`。

タイプ : Lifecycle オブジェクト

必須: いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

CopyJob

サービス: AWS Backup

コピージョブに関する詳細情報が含まれます。

内容

AccountId

コピージョブを所有するアカウント IDです。

型: 文字列

パターン：`^[0-9]{12}$`

必須: いいえ

BackupSizeInBytes

コピージョブのサイズをバイト単位で表します。

型: Long

必須: いいえ

ChildJobsInState

これにより、含まれている子 (ネストされた) コピージョブの統計が返されます。

タイプ: 文字列を long にマッピング

有効なキー: `CREATED | RUNNING | COMPLETED | FAILED | PARTIAL`

必須: いいえ

CompletionDate

コピージョブが完了した日時をUnix 形式および協定世界時 (UTC)で表示します。`CompletionDate` の値は、ミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

CompositeMemberIdentifier

複合 (親) スタックに属するネストされた (子) 復旧ポイントなど、複合グループ内のリソースの識別子。ID はスタック内の論理 ID から転送されます。

タイプ: 文字列

必須: いいえ

CopyJobId

コピージョブを一意に識別します。

タイプ: 文字列

必須: いいえ

CreatedBy

復旧ポイントのバックアップを開始するために が AWS Backup 使用したバックアッププランとルールに関する情報が含まれています。

タイプ : RecoveryPointCreator オブジェクト

必須: いいえ

CreationDate

コピージョブが作成された日時をUnix形式、および協定世界時 (UTC) で表示します。CreationDate の値は、ミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

DestinationBackupVaultArn

コピー先のボールトを一意に識別する Amazon Resource Name (ARN) 、たとえば、arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault です。

タイプ: 文字列

必須: いいえ

DestinationRecoveryPointArn

宛先リカバリポイントを一意に識別するARN。例えば、 `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`。

タイプ: 文字列

必須: いいえ

IamRoleArn

ターゲットリカバリポイントのコピーに使用する IAM ロール ARN を指定します。たとえば、`arn:aws:iam::123456789012:role/S3Access` です。

タイプ: 文字列

必須: いいえ

IsParent

これは、これが親 (複合) バックアップジョブであることを示すブール値です。

型: ブール値

必須: いいえ

MessageCategory

このパラメータは、指定されたメッセージカテゴリのジョブ数です。

文字列の例としては `AccessDenied`、`SUCCESS`、`AGGREGATE_ALL`、および `InvalidParameters` があります。 MessageCategory 文字列のリストについては、「モニタリング」を参照してください。

値 ANY は、すべてのメッセージカテゴリの数を返します。

`AGGREGATE_ALL` は、すべてのメッセージカテゴリのジョブ数を集計し、その合計を返します。

タイプ: 文字列

必須: いいえ

NumberOfChildJobs

子 (ネストされた) コピージョブの数。

型: Long

必須: いいえ

ParentJobId

これは、リソースをコピーするための AWS Backup へのリクエストを一意に識別します。戻り値は親 (複合) ジョブ ID になります。

タイプ: 文字列

必須: いいえ

ResourceArn

コピーする AWS リソース。Amazon Elastic Block Store (Amazon EBS) ボリュームや Amazon Relational Database Service (Amazon RDS) データベースなど。

タイプ: 文字列

必須: いいえ

ResourceName

指定されたバックアップに属するリソースの一意でない名前。

タイプ: 文字列

必須: いいえ

ResourceType

コピーする AWS リソースのタイプ。Amazon Elastic Block Store (Amazon EBS) ボリュームや Amazon Relational Database Service (Amazon RDS) データベースなど。

型: 文字列

パターン：`^[a-zA-Z0-9\-\_\.]{1,50}$`

必須: いいえ

SourceBackupVaultArn

コピー元のボールトを一意に識別するAmazon Resource Name（ARN）、たとえば、`arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.です。

タイプ: 文字列

必須: いいえ

SourceRecoveryPointArn

ソースリカバリーポイントを一意に識別する ARN、たとえば、arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45 です。

タイプ: 文字列

必須: いいえ

State

コピージョブの現在の状態です。

型: 文字列

有効な値：CREATED | RUNNING | COMPLETED | FAILED | PARTIAL

必須：いいえ

StatusMessage

リソースをコピーするジョブの状態を説明する詳細なメッセージです。

タイプ: 文字列

必須: いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CopyJobSummary

サービス: AWS Backup

過去 30 日以内に作成または実行されたコピージョブの概要です。

返される概要には、リージョン、アカウント、状態 RestourceType、 MessageCategory、StartTime EndTime、含まれるジョブの数が含まれます。

内容

AccountId

概要に含まれるジョブを所有するアカウント ID。

型: 文字列

パターン：`^[0-9]{12}$`

必須: いいえ

Count

概要に含まれるジョブの数を示す値。

タイプ: 整数

必須: いいえ

EndTime

ジョブの終了時刻を数値形式で表した時間の値。

この値は、Unix 形式、協定世界時 (UTC) で、ミリ秒単位の精度です。例えば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

MessageCategory

このパラメータは、指定されたメッセージカテゴリのジョブ数です。

文字列の例としては `AccessDenied`、`Success`、および `InvalidParameters` があります。MessageCategory 文字列のリストについては、「モニタリング」を参照してください。

値 ANY は、すべてのメッセージカテゴリの数を返します。

AGGREGATE_ALL は、すべてのメッセージカテゴリのジョブ数を集計し、その合計を返します。

タイプ: 文字列

必須: いいえ

Region

ジョブ概要内の AWS リージョン。

タイプ: 文字列

必須: いいえ

ResourceType

この値は、指定されたリソースタイプのジョブ数です。リクエスト GetSupportedResourceTypes は、サポートされているリソースタイプの文字列を返します。

型: 文字列

パターン：^[a-zA-Z0-9\-_\.]{1,50}$

必須: いいえ

StartTime

ジョブの開始時刻を数値形式で表した時間の値。

この値は、Unix 形式、協定世界時 (UTC) で、ミリ秒単位の精度です。例えば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

State

この値は、指定された状態のジョブのジョブ数です。

型: 文字列

有効な値 : CREATED | RUNNING | ABORTING | ABORTED | COMPLETING | COMPLETED | FAILING | FAILED | PARTIAL | AGGREGATE_ALL | ANY

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DateRange

サービス: AWS Backup

これは、: と FromDate： DateTime を含むリソースフィルターです ToDate DateTime。両方の値とも必須です。将来の DateTime 値は許可されません。

日時は、Unix 形式および協定世界時 (UTC) で、ミリ秒単位の精度です (ミリ秒はオプション)。例えば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

内容

FromDate

この値は、開始日で、その日付も含みます。

日時は、Unix 形式および協定世界時 (UTC) で、ミリ秒単位の精度です (ミリ秒はオプション)。

型: タイムスタンプ

必須: はい

ToDate

この値は、終了日 (その日付を含む) です。

日時は、Unix 形式および協定世界時 (UTC) で、ミリ秒単位の精度です (ミリ秒はオプション)。

型: タイムスタンプ

必須：はい

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Framework

サービス: AWS Backup

フレームワークに関する詳細情報が含まれます。フレームワークには、バックアップイベントとリソースを評価して報告するコントロールが含まれています。フレームワークは、毎日のコンプライアンスの結果を生成します。

内容

CreationTime

フレームワークが作成された日付と時刻を ISO 8601 で表したものです。`CreationTime` の値は、ミリ秒単位の精度です。例えば、2020-07-10T15:00:00.000-08:00 は 2020 年 7 月 10 日午後 3 時 (UTC から 8 時間遅れ) を表します。

型: タイムスタンプ

必須: いいえ

DeploymentStatus

フレームワークのデプロイステータス。ステータスは次のとおりです。

`CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED | FAILED`

タイプ: 文字列

必須: いいえ

FrameworkArn

リソースを一意に識別する Amazon リソースネーム (ARN)。ARN の形式は、リソースタイプによって異なります。

タイプ: 文字列

必須: いいえ

FrameworkDescription

最大 1,024 文字のフレームワークの説明 (オプション)。

型: 文字列

長さの制限: 最小長は 0 です。最大長は 1,024 です。

パターン: `.*\S.*`

必須: いいえ

FrameworkName

フレームワークの一意の名前です。この名前は、文字で始まり、文字 (a~z、A~Z)、数字 (0~9)、およびアンダースコア (_) を含む 1 から 256 文字で構成されます。

型: 文字列

長さの制限：最小長は 1 です。最大長は 256 です。

パターン：`[a-zA-Z][_a-zA-Z0-9]*`

必須: いいえ

NumberOfControls

フレームワークに含まれるコントロールの数です。

タイプ: 整数

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FrameworkControl

サービス: AWS Backup

フレームワークのすべてのコントロールに関する詳細情報が含まれています。各フレームワークには、少なくとも 1 つのコントロールを含める必要があります。

内容

ControlName

コントロールの名前です。この名前は1～256文字です。

型: 文字列

必須: はい

ControlInputParameters

名前と値のペア。

型: ControlInputParameter オブジェクトの配列

必須: いいえ

ControlScope

コントロールのスコープ。コントロールスコープは、コントロールが評価する内容を定義します。　コントロールスコープの 3 つの例は、特定のバックアップ計画、特定のタグを持つすべてのバックアップ計画、またはすべてのバックアップ計画です。

詳細については、「ControlScope」を参照してください。

タイプ：ControlScope オブジェクト

必須: いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2

- AWS SDK for Ruby V3

KeyValue

サービス: AWS Backup

関連する 2 つの文字列のペアです。使用できる文字は、UTF-8 で表現できる文字、スペース、数字、および + - = . _ : / です。

内容

Key

タグキー (文字列)。キーのスタートを aws: にすることはできません。

長さの制限：最小長は 1 です。最大長は 128 です。

パターン: ^(?![aA]{1}[wW]{1}[sS]{1}:)([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$

型: 文字列

必須: はい

Value

キーの値です。

長さの制限：最大長は 256 です。

パターン：^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$

型: 文字列

必須: はい

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

LegalHold

サービス: AWS Backup

リーガルホールドは、ホールド中にバックアップが削除されないようにする管理ツールです。ホールドが実施されている場合は、ホールド状態にあるバックアップは削除できず、バックアップステータスを変更するライフサイクルポリシー (コールドストレージへの移行など) は、リーガルホールドが削除されるまで延期されます。1 つのバックアップについて、リーガルホールドが複数ある場合があります。リーガルホールドは 1 つ以上のバックアップ (復旧ポイントとも呼ばれます) に適用されます。これらのバックアップは、リソースタイプとリソース ID でフィルタリングできます。

内容

CancellationDate

リーガルホールドがキャンセルされた時刻。

型: タイムスタンプ

必須: いいえ

CreationDate

リーガルホールドが作成された時刻。

型: タイムスタンプ

必須: いいえ

Description

リーガルホールドの説明。

タイプ: 文字列

必須: いいえ

LegalHoldArn

リーガルホールドの Amazon リソースネーム (ARN)。例えば、`arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`。

タイプ: 文字列

必須: いいえ

LegalHoldId

リーガルホールドの ID。

タイプ: 文字列

必須: いいえ

Status

リーガルホールドのステータス。

型: 文字列

有効な値 : `CREATING | ACTIVE | CANCELING | CANCELED`

必須 : いいえ

Title

リーガルホールドのタイトル。

タイプ: 文字列

必須: いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Lifecycle

サービス: AWS Backup

復旧ポイントがコールドストレージに移行するか、削除されるまでの時間を日数で指定します。

コールドストレージに移行されたバックアップは、そこに最低 90 日保存される必要があります。したがって、コンソールでは、保持設定は、日数設定後のコールドへの移行よりも 90 日長くする必要があります。バックアップがコールドに移行した後、日数設定をコールドに移行することはできません。

コールドストレージに移行できるリソースタイプは、「リソース別の機能の可用性」の表に記載されています。他のリソースタイプでは、この式は AWS Backup 無視されます。

既存のライフサイクルと保持期間を削除し、復旧ポイントを無期限に保持するには、`MoveToColdStorageAfterDays`と に -1 を指定します`DeleteAfterDays`。

内容

DeleteAfterDays

作成後、復旧ポイントが削除された日数。この値は、 で指定された日数から 90 日以上経過している必要があります`MoveToColdStorageAfterDays`。

型: Long

必須: いいえ

MoveToColdStorageAfterDays

作成後、復旧ポイントがコールドストレージに移動される日数。

型: Long

必須: いいえ

OptInToArchiveForSupportedResources

値が true の場合、バックアッププランは、ライフサイクル設定に従って、サポートされているリソースをアーカイブ (コールド) ストレージ階層に移行します。

型: ブール値

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ProtectedResource

サービス: AWS Backup

バックアップされたリソースに関する情報を含む構造体です。

内容

LastBackupTime

リソースが最後にバックアップされた日時 はUnix 形式および協定世界時 (UTC)で表示されます。`LastBackupTime` の値は、ミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

LastBackupVaultArn

最新のバックアップ復旧ポイントを含むバックアップボールトの ARN (Amazon リソースネーム) 。

タイプ: 文字列

必須: いいえ

LastRecoveryPointArn

最新の復旧ポイントの ARN (Amazon リソースネーム) 。

タイプ: 文字列

必須: いいえ

ResourceArn

リソースを一意に識別する Amazon リソースネーム (ARN)。ARN の形式は、リソースタイプによって異なります。

タイプ: 文字列

必須: いいえ

ResourceName

指定されたバックアップに属するリソースの一意でない名前。

タイプ: 文字列

必須: いいえ

ResourceType

AWS リソースのタイプ。Amazon Elastic Block Store (Amazon EBS) ボリュームや Amazon Relational Database Service (Amazon RDS) データベースなど。Windows Volume Shadow Copy Service (VSS) バックアップでは、サポートされているリソースタイプは Amazon EC2 のみです。

型: 文字列

パターン：`^[a-zA-Z0-9\-\_\.]{1,50}$`

必須: いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ProtectedResourceConditions

サービス: AWS Backup

タグを使用して復元テストプランのリソースに定義する条件。

例えば `"StringEquals": { "Key": "aws:ResourceTag/CreatedByCryo", "Value": "true" },` です。条件演算子では、大文字と小文字が区別されます。

内容

StringEquals

タグ付きリソースの値を、同じ値でタグ付けしたリソースに対してのみフィルタリングします。「完全一致」とも呼ばれます。

型: KeyValue オブジェクトの配列

必須: いいえ

StringNotEquals

タグ付きリソースの値を、同じ値を持たないタグ付きリソースに対してのみフィルタリングします。「否定マッチング」とも呼ばれます。

型: KeyValue オブジェクトの配列

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RecoveryPointByBackupVault

サービス: AWS Backup

バックアップボールトに保存されているリカバリーポイントに関する詳細情報が含まれています。

内容

BackupSizeInBytes

バックアップのサイズはバイト単位です。

型: Long

必須: いいえ

BackupVaultArn

バックアップボールトを一意に識別するARN、たとえば、`arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault` です。

タイプ: 文字列

必須: いいえ

BackupVaultName

バックアップを保存する論理コンテナの名前。バックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先の AWS リージョンに一意の名前で識別されます。

型: 文字列

パターン：`^[a-zA-Z0-9\-\_]{2,50}$`

必須: いいえ

CalculatedLifecycle

`DeleteAt` および `MoveToColdStorageAt` のタイムスタンプを含む `CalculatedLifecycle` オブジェクト。

タイプ：CalculatedLifecycle オブジェクト

必須: いいえ

CompletionDate

復旧ポイントの復元ジョブが完了した日時は、Unix 形式および協定世界時 (UTC)で表しています。CompletionDate の値は、ミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

CompositeMemberIdentifier

複合 (親) スタックに属するネストされた (子) 復旧ポイントなど、複合グループ内のリソースの識別子。ID はスタック内の論理 ID から転送されます。

タイプ: 文字列

必須: いいえ

CreatedBy

リカバリーポイントの作成に使用されるバックアッププランのBackupPlanArn、BackupPlanId、BackupPlanVersion、およびBackupRuleIdを含む、リカバリポイントの作成に関する識別情報が含まれています。

タイプ : RecoveryPointCreator オブジェクト

必須: いいえ

CreationDate

リカバリーポイントが作成された日時をUnix形式、および協定世界時 (UTC) で表しています。CreationDate の値は、ミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

EncryptionKeyArn

たとえば、arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab などのバックアップを保護するために使用されるサーバー側の暗号化キーです。

型: 文字列

必須: いいえ

IamRoleArn

ターゲット復旧ポイントの作成に使用する IAM ロール ARN を指定します。例えば、arn:aws:iam::123456789012:role/S3Accessです。

タイプ: 文字列

必須: いいえ

IsEncrypted

指定されたリカバリーポイントが暗号化されている場合は TRUE 、リカバリーポイントが暗号化されていない場合は FALSE として返されるブール値です。

型: ブール値

必須: いいえ

IsParent

これは親 (複合) 復旧ポイントであることを示すブール値です。

型: ブール値

必須: いいえ

LastRestoreTime

リカバリーポイントが最後に復元された日時をUnix 形式および協定世界時 (UTC)で表しています。LastRestoreTime 値は、ミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

Lifecycle

ライフサイクルは、保護されたリソースがコールドストレージに移行するタイミングと、期限切れになるタイミングを定義します。 は、定義したライフサイクルに従ってバックアップを自動的に AWS Backup 移行および期限切れにします。

コールドストレージに移行されたバックアップは、そこに最低 90 日保存される必要があります。したがって、「保持期間」の設定は、「コールドへの移行 (日数)」設定から 90 日以上あける必要があります。バックアップがコールドに移行された後で、「コールドへの移行 (日数)」設定を変更することはできません。

コールドストレージに移行できるリソースタイプは、「リソース別の機能の可用性」の表に記載されています。他のリソースタイプでは、この式は AWS Backup 無視されます。

タイプ：Lifecycle オブジェクト

必須: いいえ

ParentRecoveryPointArn

親 (複合) 復旧ポイントの Amazon リソースネーム (ARN)。

タイプ: 文字列

必須: いいえ

RecoveryPointArn

バックアップボールトを一意に識別する Amazon リソースネーム (ARN) 、たとえば、`arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45` です。

タイプ: 文字列

必須: いいえ

ResourceArn

リソースを一意に識別するためのARN。ARN の形式は、リソースタイプによって異なります。

タイプ: 文字列

必須: いいえ

ResourceName

指定されたバックアップに属するリソースの一意でない名前。

タイプ: 文字列

必須: いいえ

ResourceType

復旧ポイントとして保存された AWS リソースのタイプ。Amazon Elastic Block Store (Amazon EBS) ボリュームや Amazon Relational Database Service (Amazon RDS) データベースなど。Windows Volume Shadow Copy Service (VSS) バックアップでは、サポートされているリソースタイプは Amazon EC2 のみです。

型: 文字列

パターン：`^[a-zA-Z0-9\-\_\.]{1,50}$`

必須: いいえ

SourceBackupVaultArn

リカバリーポイントのコピー元のバックアップボールト。リカバリーポイントが同じアカウントに復元された場合、この値は `null` です。

タイプ: 文字列

必須: いいえ

Status

リカバリーポイントの状態を指定するステータスコードです。

型: 文字列

有効な値：`COMPLETED | PARTIAL | DELETING | EXPIRED`

必須：いいえ

StatusMessage

復旧ポイントの現在のステータスを説明するメッセージ。

タイプ: 文字列

必須: いいえ

VaultType

記述された復旧ポイントが保存されるボールトのタイプ。

型: 文字列

有効な値：BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RecoveryPointByResource

サービス: AWS Backup

保存されたリカバリーポイントに関する詳細情報が含まれています。

内容

BackupSizeBytes

バックアップのサイズはバイト単位です。

型: Long

必須: いいえ

BackupVaultName

バックアップを保存する論理コンテナの名前。バックアップボールトは、これらのボールトを作成するために使用されたアカウントと作成先の AWS リージョンに一意の名前で識別されます。

型: 文字列

パターン：`^[a-zA-Z0-9\-\_]{2,50}$`

必須: いいえ

CreationDate

リカバリーポイントが作成された日時をUnix形式、および協定世界時 (UTC) で表しています。`CreationDate` の値は、ミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

EncryptionKeyArn

たとえば、`arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab` などのバックアップを保護するために使用されるサーバー側の暗号化キーです。

型: 文字列

必須: いいえ

IsParent

これは親 (複合) 復旧ポイントであることを示すブール値です。

型: ブール値

必須: いいえ

ParentRecoveryPointArn

親 (複合) 復旧ポイントの Amazon リソースネーム (ARN)。

タイプ: 文字列

必須: いいえ

RecoveryPointArn

バックアップボールトを一意に識別する Amazon リソースネーム (ARN) 、たとえば、`arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45` です。

タイプ: 文字列

必須: いいえ

ResourceName

指定されたバックアップに属するリソースの一意でない名前。

タイプ: 文字列

必須: いいえ

Status

リカバリーポイントの状態を指定するステータスコードです。

型: 文字列

有効な値：`COMPLETED | PARTIAL | DELETING | EXPIRED`

必須：いいえ

StatusMessage

復旧ポイントの現在のステータスを説明するメッセージ。

タイプ: 文字列

必須: いいえ

VaultType

記述された復旧ポイントが保存されるボールトのタイプ。

型: 文字列

有効な値：BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RecoveryPointCreator

サービス: AWS Backup

復旧ポイントのバックアップを開始するために が AWS Backup 使用したバックアッププランとルールに関する情報が含まれています。

内容

BackupPlanArn

例えば、arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50 などのバックアップ計画を一意に識別する Amazon リソースネーム (ARN) です。

タイプ: 文字列

必須: いいえ

BackupPlanId

バックアップ計画を一意に識別します。

タイプ: 文字列

必須: いいえ

BackupPlanVersion

バージョンIDは、一意のランダムに生成されたUnicode、UTF-8でエンコードされた文字列で、最大1,024バイトの長さです。編集することはできません。

タイプ: 文字列

必須: いいえ

BackupRuleId

選択したリソースのバックアップを予定するために使用されるルールを一意に識別します。

タイプ: 文字列

必須: いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RecoveryPointMember

サービス: AWS Backup

これは親 (複合) 復旧ポイントの子 (ネストされた) 復旧ポイントである復旧ポイントです。これらの復旧ポイントは、親 (複合) 復旧ポイントとの関連付けを解除できます。その場合、これらの復旧ポイントはメンバーではなくなります。

内容

BackupVaultName

バックアップボールトの名前 (バックアップが保存されている論理コンテナ) 。

型: 文字列

パターン：`^[a-zA-Z0-9\-\_]{2,50}$`

必須: いいえ

RecoveryPointArn

親 (複合) 復旧ポイントの Amazon リソースネーム (ARN)。

タイプ: 文字列

必須: いいえ

ResourceArn

保存されたリソースを一意に識別する Amazon リソースネーム (ARN)。

タイプ: 文字列

必須: いいえ

ResourceType

復旧ポイントとして保存される AWS リソースタイプ。

型: 文字列

パターン：`^[a-zA-Z0-9\-\_\.]{1,50}$`

必須: いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RecoveryPointSelection

サービス: AWS Backup

これは、リソースタイプやバックアップボールトなど、リソースセットを割り当てる基準を指定します。

内容

DateRange

これは、: と FromDate： DateTime を含むリソースフィルターです ToDate DateTime。両方の値とも必須です。将来の DateTime 値は許可されません。

日時は、Unix 形式および協定世界時 (UTC) で、ミリ秒単位の精度です (ミリ秒はオプション)。例えば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

タイプ：DateRange オブジェクト

必須: いいえ

ResourceIdentifiers

これらはリソース選択に含まれるリソースです (リソースのタイプやボールトを含む)。

タイプ：文字列の配列

必須: いいえ

VaultNames

これらは、選択した復旧ポイントが含まれているボールトの名前です。

タイプ：文字列の配列

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2

- AWS SDK for Ruby V3

ReportDeliveryChannel

サービス: AWS Backup

レポートを配信する場所について、具体的には Amazon S3 バケット名、S3 キープレフィックス、レポートの形式に関するレポートプランの情報が含まれています。

内容

S3BucketName

レポートを受け取る S3 バケットの一意の名前です。

型: 文字列

必須: はい

Formats

レポートの形式: CSV、JSON、またはその両方。指定されなかった場合、デフォルト値は CSV です。

タイプ : 文字列の配列

必須: いいえ

S3KeyPrefix

AWS Backup Audit Manager がレポートを Amazon S3 に配信する のプレフィックス。プレフィックスは、次のパスのこの部分です: s3://your-bucket-name/prefix/Backup/us-west-2/year/month/day/report-name 。指定しない場合、プレフィックスはありません。

タイプ: 文字列

必須: いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2

- AWS SDK for Ruby V3

ReportDestination

サービス: AWS Backup

レポートジョブからのレポート送信先に関する情報が含まれます。

内容

S3BucketName

レポートを受け取る Amazon S3 バケットの一意の名前です。

タイプ: 文字列

必須: いいえ

S3Keys

S3バケット内のレポートを一意に識別するためのオブジェクトキーです。

タイプ：文字列の配列

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ReportJob

サービス: AWS Backup

レポートジョブに関する詳細情報が含まれています。レポートジョブは、レポートプランに基づいてレポートをコンパイルし、Amazon S3 にパブリッシュします。

内容

CompletionTime

レポートジョブが完了した日時をUnix 形式および協定世界時 (UTC)で表しています。CompletionTime の値は、ミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

CreationTime

ドメインリストが作成された日時をUnix 時刻形式および協定世界時 (UTC)で表しています。CreationTime の値は、ミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

ReportDestination

レポートジョブがレポートを発行する宛先の S3 バケット名と S3 キーです。

タイプ：ReportDestination オブジェクト

必須: いいえ

ReportJobId

レポートジョブの識別子です。一意で、ランダムに生成された、Unicode、UTF-8でエンコードされた、最大で1,024バイトの長さの文字列です。レポートジョブ ID を編集することはできません。

タイプ: 文字列

必須: いいえ

ReportPlanArn

リソースを一意に識別する Amazon リソースネーム (ARN)。ARN の形式は、リソースタイプによって異なります。

タイプ: 文字列

必須: いいえ

ReportTemplate

レポートのレポートテンプレートを識別します。レポートは、レポートテンプレートを使用して構築されます。レポートテンプレートは次のとおりです。

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

タイプ: 文字列

必須: いいえ

Status

レポートジョブのステータスです。ステータスは次のとおりです。

`CREATED | RUNNING | COMPLETED | FAILED`

`COMPLETED` は、指定された目的地でレポートを確認できることを意味します。ステータスが `FAILED` の場合は、その理由を `StatusMessage` で確認してください。

タイプ: 文字列

必須: いいえ

StatusMessage

レポートジョブのステータスを説明するメッセージです。

タイプ: 文字列

必須: いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ReportPlan

サービス: AWS Backup

レポートプランに関する詳細情報が含まれています。

内容

CreationTime

レポートプランが作成された日時をUnix形式、および協定世界時 (UTC) で表しています。CreationTimeの値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

DeploymentStatus

レポートプランの展開状況。ステータスは次のとおりです。

CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED

タイプ: 文字列

必須: いいえ

LastAttemptedExecutionTime

このレポートプランに関連付けられたレポートジョブが最後に実行しようとした日時はUnix 形式および協定世界時 (UTC)で表しています。LastAttemptedExecutionTime の値は、ミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

LastSuccessfulExecutionTime

このレポートプランに関連付けられたレポートジョブが最後に正常に実行された日時をUnix 形式および協定世界時 (UTC)で表しています。LastSuccessfulExecutionTime の値は、ミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

ReportDeliveryChannel

レポートを配信する場所と方法に関する情報、具体的にはAmazon S3バケット名、S3キーのプレフィックス、レポートの形式などが含まれています。

タイプ：ReportDeliveryChannel オブジェクト

必須: いいえ

ReportPlanArn

リソースを一意に識別する Amazon リソースネーム (ARN)。ARN の形式は、リソースタイプによって異なります。

タイプ: 文字列

必須: いいえ

ReportPlanDescription

最大 1,024 文字のレポートプランの説明（オプション）。

型: 文字列

長さの制限: 最小長は 0 です。最大長は 1,024 です。

パターン: `.*\S.*`

必須: いいえ

ReportPlanName

レポートプランの一意の名前です。この名前は、アルファベットで始まり、アルファベット(a-z, A-Z)、数字(0-9)、アンダースコア(_)で構成される1～256文字です。

型: 文字列

長さの制限：最小長は 1 です。最大長は 256 です。

パターン：`[a-zA-Z][_a-zA-Z0-9]*`

必須: いいえ

ReportSetting

レポートのレポートテンプレートを識別します。レポートは、レポートテンプレートを使用して構築されます。レポートテンプレートは次のとおりです。

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

レポートテンプレートが `RESOURCE_COMPLIANCE_REPORT`または の場合`CONTROL_COMPLIANCE_REPORT`、この API リソースは AWS リージョン および フレームワークによるレポートカバレッジも記述します。

タイプ : ReportSetting オブジェクト

必須: いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ReportSetting

サービス: AWS Backup

レポート設定に関する詳細情報が含まれています。

内容

ReportTemplate

レポートのレポートテンプレートを識別します。レポートは、レポートテンプレートを使用して構築されます。レポートテンプレートは次のとおりです。

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

型: 文字列

必須: はい

Accounts

これらはレポートに含まれるアカウントです。

すべての組織単位を含めるROOTには、 の文字列値を使用します。

タイプ : 文字列の配列

必須: いいえ

FrameworkArns

レポートがカバーするフレームワークの Amazon リソースネーム (ARN)。

タイプ : 文字列の配列

必須: いいえ

NumberOfFrameworks

レポートがカバーするフレームワークの数。

タイプ: 整数

必須: いいえ

OrganizationUnits

これらはレポートに含まれる組織単位です。

タイプ：文字列の配列

必須: いいえ

Regions

これらはレポートに含まれるリージョンです。

ワイルドカードを文字列値として使用して、すべてのリージョンを含めます。

タイプ：文字列の配列

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreJobCreator

サービス: AWS Backup

復元ジョブを開始するために AWS Backup で使用された復元テストプランに関する情報が含まれます。

内容

RestoreTestingPlanArn

復元テストプランを一意に識別する Amazon リソースネーム (ARN)。

タイプ: 文字列

必須: いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreJobsListMember

サービス: AWS Backup

復元ジョブに関するメタデータが含まれます。

内容

AccountId

復元ジョブを所有するアカウントIDです。

型: 文字列

パターン：`^[0-9]{12}$`

必須: いいえ

BackupSizeInBytes

復元されたリソースのサイズは、バイト単位で表します。

型: Long

必須: いいえ

CompletionDate

復旧ポイントの復元ジョブが完了した日時は、Unix 形式および協定世界時 (UTC)で表しています。`CompletionDate` の値は、ミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

CreatedBy

復元ジョブの作成に関する識別情報が含まれます。

タイプ：RestoreJobCreator オブジェクト

必須: いいえ

CreatedResourceArn

リソースを一意に識別する Amazon リソースネーム (ARN)。ARN の形式は、リソースタイプによって異なります。

タイプ: 文字列

必須: いいえ

CreationDate

復元ジョブが作成された日付と時刻は、Unix形式、および協定世界時 (UTC) で表示されます。CreationDate 値は、ミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

DeletionStatus

復元テストで生成されたデータのステータスを示します。ステータスは、Deleting、Failed、または Successful です。

型: 文字列

有効な値 : DELETING | FAILED | SUCCESSFUL

必須 : いいえ

DeletionStatusMessage

復元ジョブの削除ステータスを示します。

タイプ: 文字列

必須: いいえ

ExpectedCompletionTimeMinutes

リカバリーポイントを復元するジョブに要する予想される分単位の時間です。

型: Long

必須: いいえ

IamRoleArn

ターゲット復旧ポイントの作成に使用する IAM ロール ARN を指定します。例えば、arn:aws:iam::123456789012:role/S3Accessです。

タイプ: 文字列

必須: いいえ

PercentDone

ジョブのステータスが照会された時点でのジョブの完了見込み率が含まれます。

タイプ: 文字列

必須: いいえ

RecoveryPointArn

リカバリーポイントを一意に識別する ARN、たとえば、`arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45` です。

タイプ: 文字列

必須: いいえ

RecoveryPointCreationDate

復旧ポイントが作成された日付です。

型: タイムスタンプ

必須: いいえ

ResourceType

リストされた復元ジョブのリソースタイプ、たとえば、Amazon Elastic Block Store（Amazon EBS）ボリュームまたはAmazon Relational Database Service（Amazon RDS）データベースなどです。。Windows ボリュームシャドウコピーサービス (VSS) バックアップでは、サポートされているリソースタイプは Amazon EC2 のみです。

型: 文字列

パターン：`^[a-zA-Z0-9\-\_\.]{1,50}$`

必須: いいえ

RestoreJobId

リカバリーポイントを復元するジョブを一意に識別します。

タイプ: 文字列

必須: いいえ

Status

リカバリポイントを復元 AWS Backup するために によって開始されたジョブの状態を指定するステータスコード。

型: 文字列

有効な値：PENDING | RUNNING | COMPLETED | ABORTED | FAILED

必須：いいえ

StatusMessage

復旧ポイントを復元するジョブのステータスを説明する詳細なメッセージです。

タイプ: 文字列

必須: いいえ

ValidationStatus

指定された復元ジョブで実行された検証のステータス。

型: 文字列

有効な値：FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING

必須：いいえ

ValidationStatusMessage

指定された復元ジョブで実行された検証のステータスの説明です。

タイプ: 文字列

必須: いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreJobSummary

サービス: AWS Backup

過去 30 日以内に作成または実行された復元ジョブの概要です。

返される概要には、リージョン、アカウント、状態 ResourceType、 MessageCategory、 StartTime EndTime、含まれるジョブの数が含まれます。

内容

AccountId

概要に含まれるジョブを所有するアカウント ID。

型: 文字列

パターン：`^[0-9]{12}$`

必須: いいえ

Count

概要に含まれるジョブの数を示す値。

タイプ: 整数

必須: いいえ

EndTime

ジョブの終了時刻を数値形式で表した時間の値。

この値は、Unix 形式、協定世界時 (UTC) で、ミリ秒単位の精度です。例えば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

Region

ジョブ概要内の AWS リージョン。

タイプ: 文字列

必須: いいえ

ResourceType

この値は、指定されたリソースタイプのジョブ数です。リクエスト GetSupportedResourceTypes は、サポートされているリソースタイプの文字列を返します。

型: 文字列

パターン：^[a-zA-Z0-9\-_\.]{1,50}$

必須: いいえ

StartTime

ジョブの開始時刻を数値形式で表した時間の値。

この値は、Unix 形式、協定世界時 (UTC) で、ミリ秒単位の精度です。例えば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

State

この値は、指定された状態のジョブのジョブ数です。

型: 文字列

有効な値：CREATED | PENDING | RUNNING | ABORTED | COMPLETED | FAILED | AGGREGATE_ALL | ANY

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreTestingPlanForCreate

サービス: AWS Backup

復元テストプランに関するメタデータが含まれます。

内容

RecoveryPointSelection

RecoveryPointSelection には 5 つのパラメータがあります (3 つは必須、2 つはオプション) 。指定した値によって、復元テストに含まれる復旧ポイントが決まります。内で最新の復旧ポイントが必要Algorithmかどうか SelectionWindowDays、またはランダムな復旧ポイントが必要かどうかを示す必要があります。また、どのボールト IncludeVaultsから復旧ポイントを選択できるかを示す必要があります。

Algorithm (必須) 有効な値：LATEST_WITHIN_WINDOW「」または RANDOM_WITHIN_WINDOW「」。

Recovery point types (必須) 有効な値：SNAPSHOT「」および/または CONTINUOUS「」。スナップショット復旧ポイントのみを復元 SNAPSHOTするには を含め、継続的復旧ポイント (ポイントインタイム復元/PITR) を復元 CONTINUOUSするには を含めます。スナップショットまたは継続的復旧ポイントのいずれかを復元するには、両方を使用します。復旧ポイントは、 の値によって決まります Algorithm。

IncludeVaults (必須) 。1 つ以上のバックアップボールトを含める必要があります。ワイルドカード ["*"] または特定の ARNs。

SelectionWindowDays (オプション) 値は 1～365 の整数 (日単位) である必要があります。含まれていない場合、値はデフォルトで になります 30。

ExcludeVaults (オプション) 。1 つ以上の特定のバックアップボールト ARNs を入力して、それらのボールトの内容を復元資格から除外できます。または、セレクタのリストを含めることもできます。このパラメータとその値が含まれていない場合、デフォルトで空のリストになります。

型: RestoreTestingRecoveryPointSelection オブジェクト

必須: はい

RestoreTestingPlanName

RestoreTestingPlanName は、復元テストプランの名前である一意の文字列です。これは作成後に変更できず、英数字とアンダースコアのみで構成されている必要があります。

型: 文字列

必須: はい

ScheduleExpression

復元テストプランが実行されるときを示す、指定されたタイムゾーンの CRON 式。

型: 文字列

必須: はい

ScheduleExpressionTimezone

オプション。これは、スケジュール式が設定されるタイムゾーンです。デフォルトでは、ScheduleExpressions は UTC です。これを、指定したタイムゾーンに変更できます。

タイプ: 文字列

必須: いいえ

StartWindowHours

デフォルトは 24 時間です。

復元テストがスケジュールされてから、ジョブが正常に開始されない場合にキャンセルされるまでの時間を時間単位で示す値。この値はオプションです。この値を含める場合、このパラメータの最大値は 168 時間 (1 週間) になります。

タイプ: 整数

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreTestingPlanForGet

サービス: AWS Backup

復元テストプランに関するメタデータが含まれます。

内容

CreationTime

復元テストプランが作成された日時を Unix 形式、および協定世界時 (UTC) で表しています。`CreationTime` の値は、ミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: はい

RecoveryPointSelection

復元ポイントタイプやバックアップボールトなど、リソースのセットを割り当てるために指定された条件。

型: RestoreTestingRecoveryPointSelection オブジェクト

必須: はい

RestoreTestingPlanArn

復元テストプランを一意に識別する Amazon リソースネーム (ARN)。

型: 文字列

必須: はい

RestoreTestingPlanName

復元テストプラン名。

型: 文字列

必須: はい

ScheduleExpression

復元テストプランが実行されるときを示す、指定されたタイムゾーンの CRON 式。

型: 文字列

必須: はい

CreatorRequestId

リクエストを識別し、失敗したリクエストを再試行する際に、オペレーションを 2 回実行するリスクを回避することができます。リクエストに既存のバックアッププランと一致する CreatorRequestId が含まれる場合、そのプランが返されます。このパラメータはオプションです。

使用する場合、このパラメータには 1～50 文字の英数字または「-_」を含める必要があります 。

タイプ: 文字列

必須: いいえ

LastExecutionTime

指定した復元テストプランで復元テストを最後に実行した日時。日時は、Unix 形式および協定世界時 (UTC) です。LastExecutionDateの値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

LastUpdateTime

復元テストプランが更新された日時。この更新日時は Unix 形式および協定世界時 (UTC) です。LastUpdateTimeの値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

ScheduleExpressionTimezone

オプション。これは、スケジュール式が設定されるタイムゾーンです。デフォルトでは、ScheduleExpressions は UTC です。これを、指定したタイムゾーンに変更できます。

タイプ: 文字列

必須: いいえ

StartWindowHours

デフォルトは 24 時間です。

復元テストがスケジュールされてから、ジョブが正常に開始されない場合にキャンセルされるまでの時間を時間単位で示す値。この値はオプションです。この値を含める場合、このパラメータの最大値は 168 時間 (1 週間) になります。

タイプ: 整数

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreTestingPlanForList

サービス: AWS Backup

復元テストプランに関するメタデータが含まれます。

内容

CreationTime

復元テストプランが作成された日時を Unix 形式、および協定世界時 (UTC) で表しています。`CreationTime` の値は、ミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: はい

RestoreTestingPlanArn

復元テストプランを一意に識別する Amazon リソースネーム (ARN)。

型: 文字列

必須: はい

RestoreTestingPlanName

復元テストプラン名。

型: 文字列

必須: はい

ScheduleExpression

復元テストプランが実行されるときを示す、指定されたタイムゾーンの CRON 式。

型: 文字列

必須: はい

LastExecutionTime

指定した復元テストプランで復元テストを最後に実行した日時。日時は、Unix 形式および協定世界時 (UTC) です。`LastExecutionDate`の値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

LastUpdateTime

復元テストプランが更新された日時。この更新日時は Unix 形式および協定世界時 (UTC) です。LastUpdateTimeの値はミリ秒単位の精度です。たとえば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前12:11:30.087 を表します。

型: タイムスタンプ

必須: いいえ

ScheduleExpressionTimezone

オプション。これは、スケジュール式が設定されるタイムゾーンです。デフォルトでは、ScheduleExpressions は UTC です。これを、指定したタイムゾーンに変更できます。

タイプ: 文字列

必須: いいえ

StartWindowHours

デフォルトは 24 時間です。

復元テストがスケジュールされてから、ジョブが正常に開始されない場合にキャンセルされるまでの時間を時間単位で示す値。この値はオプションです。この値を含める場合、このパラメータの最大値は 168 時間 (1 週間) になります。

タイプ: 整数

必須 : いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreTestingPlanForUpdate

サービス: AWS Backup

復元テストプランに関するメタデータが含まれます。

内容

RecoveryPointSelection

必須: `Algorithm`、`RecoveryPointTypes`、`IncludeVaults` (1 つ以上)。

オプション: SelectionWindowDays (指定されていない場合は「30」) 、 `ExcludeVaults` (リストされていない場合はデフォルトで空のリストになります) 。

タイプ : RestoreTestingRecoveryPointSelection オブジェクト

必須: いいえ

ScheduleExpression

復元テストプランが実行されるときを示す、指定されたタイムゾーンの CRON 式。

タイプ: 文字列

必須: いいえ

ScheduleExpressionTimezone

オプション。これは、スケジュール式が設定されるタイムゾーンです。デフォルトでは、ScheduleExpressions は UTC です。これを、指定したタイムゾーンに変更できます。

タイプ: 文字列

必須: いいえ

StartWindowHours

デフォルトは 24 時間です。

復元テストがスケジュールされてから、ジョブが正常に開始されない場合にキャンセルされるまでの時間を時間単位で示す値。この値はオプションです。この値を含める場合、このパラメータの最大値は 168 時間 (1 週間) になります。

タイプ: 整数

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreTestingRecoveryPointSelection

サービス: AWS Backup

RecoveryPointSelection には 5 つのパラメータがあります (3 つは必須、2 つはオプション) 。指定した値によって、復元テストに含まれる復旧ポイントが決まります。内で最新の復旧ポイントが必要Algorithmかどうか SelectionWindowDays、またはランダムな復旧ポイントが必要かどうかを示す必要があります。また、どのボールト IncludeVaultsから復旧ポイントを選択できるかを示す必要があります。

Algorithm (必須) 有効な値：LATEST_WITHIN_WINDOW「」または RANDOM_WITHIN_WINDOW「」。

Recovery point types (必須) 有効な値：SNAPSHOT「」および/または CONTINUOUS「」。スナップショット復旧ポイントのみを復元 SNAPSHOT するには を含め、継続的復旧ポイント (ポイントインタイム復元/PITR) を復元 CONTINUOUS するには を含めます。スナップショットまたは継続的復旧ポイントのいずれかを復元するには、両方を使用します。復旧ポイントは、 の値によって決まります Algorithm。

IncludeVaults (必須) 。1 つ以上のバックアップボールトを含める必要があります。ワイルドカード ["*"] または特定の ARNs。

SelectionWindowDays (オプション) 値は 1 ~ 365 の整数 (日単位) である必要があります。含まれていない場合、値はデフォルトで になります 30。

ExcludeVaults (オプション) 。1 つ以上の特定のバックアップボールト ARNs を入力して、それらのボールトの内容を復元資格から除外できます。または、セレクタのリストを含めることもできます。このパラメータとその値が含まれていない場合、デフォルトで空のリストになります。

内容

Algorithm

使用できる値は、「LATEST_WITHIN_WINDOW」または「RANDOM_WITHIN_WINDOW」です。

型: 文字列

有効な値：LATEST_WITHIN_WINDOW | RANDOM_WITHIN_WINDOW

必須：いいえ

ExcludeVaults

使用できる値は、特定の ARN または選択項目のリストです。リストされていない場合はデフォルトで空のリストになります。

タイプ：文字列の配列

必須: いいえ

IncludeVaults

使用できる値は、ワイルドカード ["*"]、特定の ARN、ワイルドカードで置き換えた ARN ["arn:aws:backup:us-west-2:123456789012:backup-vault:asdf", ...] ["arn:aws:backup:*:*:backup-vault:asdf-*", ...] です。

タイプ：文字列の配列

必須: いいえ

RecoveryPointTypes

復旧ポイントのタイプです。

スナップショット復旧ポイントのみを復元SNAPSHOTするには を含め、継続的復旧ポイント (ポイントインタイム復元/PITR) を復元CONTINUOUSするには を含めます。スナップショットまたは継続的復旧ポイントのいずれかを復元するには、両方を使用します。復旧ポイントは、 の値によって決まりますAlgorithm。

タイプ：文字列の配列

有効な値: CONTINUOUS | SNAPSHOT

必須：いいえ

SelectionWindowDays

使用できる値は 1～365 の整数です。

タイプ: 整数

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreTestingSelectionForCreate

サービス: AWS Backup

特定の復元テスト選択に関するメタデータが含まれます。

ProtectedResourceType は、Amazon EBS や Amazon EC2 などに必要です。

これは、RestoreTestingSelectionName、ProtectedResourceType と、以下のいずれかで構成されます。

- ProtectedResourceArns
- ProtectedResourceConditions

保護対象リソースのタイプごとに値を 1 つ設定できます。

復元テスト選択には、ProtectedResourceArns のワイルドカード値 (「*」) を ProtectedResourceConditions と併せて含めることができます。または、ProtectedResourceArns に保護対象リソースの ARN を最大 30 個まで含めることもできます。

ProtectedResourceConditions の例には、StringEquals や StringNotEquals があります。

内容

IamRoleArn

ターゲットリソースを作成するために AWS Backup で使用する IAM ロールの Amazon リソースネーム (ARN)。例えば、arn:aws:iam::123456789012:role/S3Access です。

型: 文字列

必須: はい

ProtectedResourceType

復元テスト選択に含まれる AWS リソースのタイプ。Amazon EBS ボリュームや Amazon RDS データベースなど。

サポートされているリソースタイプは以下のとおりです。

- Amazon Aurora 用の Aurora

- Amazon DocumentDB (MongoDB 互換性) 用の `DocumentDB`
- Amazon DynamoDB 用の `DynamoDB`
- Amazon Elastic Block Store 用の `EBS`
- Amazon Elastic Compute Cloud 用の `EC2`
- Amazon Elastic File System 用の `EFS`
- Amazon FSx の場合 用の `FSx`
- Amazon Neptune の場合 用の `Neptune`
- Amazon Relational Database Service 用の `RDS`
- Amazon S3 の場合は `S3`

型: 文字列

必須: はい

RestoreTestingSelectionName

関連する復元テストプランに属する復元テスト選択の一意の名前。

型: 文字列

必須: はい

ProtectedResourceArns

保護対象の各リソースは、特定の ARN (例: `ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]`) またはワイルドカード (例: `ProtectedResourceArns: ["*"]`) でフィルタリングできますが、両方でフィルタリングすることはできません。

タイプ：文字列の配列

必須: いいえ

ProtectedResourceConditions

にワイルドカードを含めた場合は ProtectedResourceArns、 などのリソース条件を含めることができます`ProtectedResourceConditions: { StringEquals: [{ key: "XXXX", value: "YYYY" }]`。

タイプ：ProtectedResourceConditions オブジェクト

必須: いいえ

RestoreMetadataOverrides

`RestoreTestingSelection` の本文にパラメータ `RestoreMetadataOverrides` を含めることで、特定の復元メタデータのキーを上書きできます。キー値では大文字と小文字が区別されません。

復元テストの推定メタデータの全リストを参照してください。

型: 文字列間のマッピング

必須: いいえ

ValidationWindowHours

データに対して検証スクリプトを実行するのにかかる時間 (1 ~ 168 時間) です。データは、検証スクリプトの完了時または指定した保持期間の終了時 (どちらか早い方) に削除されます。

タイプ: 整数

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreTestingSelectionForGet

サービス: AWS Backup

復元テスト選択に関するメタデータが含まれます。

内容

CreationTime

復元テスト選択が作成された日時を Unix 形式、および協定世界時 (UTC) で表しています。CreationTime の値は、ミリ秒単位の精度です。例えば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前 12:11:30.087 を表します。

型: タイムスタンプ

必須: はい

IamRoleArn

ターゲットリソースを作成するために AWS Backup で使用する IAM ロールの Amazon リソースネーム (ARN)。例えば、arn:aws:iam::123456789012:role/S3Access です。

型: 文字列

必須: はい

ProtectedResourceType

AWS リソーステスト選択に含まれるリソースのタイプ。Amazon EBS ボリュームや Amazon RDS データベースなど。

型: 文字列

必須: はい

RestoreTestingPlanName

RestoreTestingPlanName は、復元テストプランの名前である一意の文字列です。

型: 文字列

必須: はい

RestoreTestingSelectionName

関連する復元テストプランに属する復元テスト選択の一意の名前。

型: 文字列

必須: はい

CreatorRequestId

リクエストを識別し、失敗したリクエストを再試行する際に、オペレーションを 2 回実行するリスクを回避することができます。リクエストに既存のバックアッププランと一致する CreatorRequestId が含まれる場合、そのプランが返されます。このパラメータはオプションです。

使用する場合、このパラメータには 1～50 文字の英数字または「-_」を含める必要があります 。

タイプ: 文字列

必須: いいえ

ProtectedResourceArns

特定の ARN (例: ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]) またはワイルドカード (例: ProtectedResourceArns: ["*"]) を含めることができますが、両方を含めることはできません。

タイプ：文字列の配列

必須: いいえ

ProtectedResourceConditions

復元テスト選択でこのパラメータを使用する場合、StringEquals や StringNotEquals などの特定の条件でフィルタリングできます。

タイプ：ProtectedResourceConditions オブジェクト

必須: いいえ

RestoreMetadataOverrides

RestoreTestingSelection の本文にパラメータ RestoreMetadataOverrides を含めることで、特定の復元メタデータのキーを上書きできます。キー値では大文字と小文字が区別されません。

復元テストの推定メタデータの全リストを参照してください。

型: 文字列間のマッピング

必須: いいえ

ValidationWindowHours

データに対して検証スクリプトを実行するのにかかる時間 (1 ~ 168 時間) です。データは、検証スクリプトの完了時または指定した保持期間の終了時 (どちらか早い方) に削除されます。

タイプ: 整数

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreTestingSelectionForList

サービス: AWS Backup

復元テスト選択に関するメタデータが含まれます。

内容

CreationTime

復元テスト選択が作成された日時を Unix 形式、および協定世界時 (UTC) で表しています。`CreationTime` の値は、ミリ秒単位の精度です。例えば、1516925490.087 の値は、2018 年 1 月 26 日 (金) 午前 12:11:30.087 を表します。

型: タイムスタンプ

必須: はい

IamRoleArn

ターゲットリソースを作成するために AWS Backup で使用する IAM ロールの Amazon リソースネーム (ARN)。例えば、`arn:aws:iam::123456789012:role/S3Access` です。

型: 文字列

必須: はい

ProtectedResourceType

復元テスト選択に含まれる AWS リソースのタイプ。Amazon EBS ボリュームや Amazon RDS データベースなど。

型: 文字列

必須: はい

RestoreTestingPlanName

復元テストプランの名前を表す一意の文字列です。

作成後にこの名前を変更することはできません。名前には英数字とアンダースコアのみを使用できます。最大長は 50 文字です。

型: 文字列

必須: はい

RestoreTestingSelectionName

復元テスト選択の一意の名前。

型: 文字列

必須: はい

ValidationWindowHours

この値は、オプションの検証を実施するために復元テスト後にデータを保持する時間 (時間単位) です。

使用できる値は 0 から 168 (7 日間に相当する時間) の整数です。

タイプ: 整数

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RestoreTestingSelectionForUpdate

サービス: AWS Backup

復元テスト選択に関するメタデータが含まれます。

内容

IamRoleArn

ターゲットリソースを作成するために AWS Backup で使用する IAM ロールの Amazon リソースネーム (ARN)。例えば、`arn:aws:iam::123456789012:role/S3Access` です。

タイプ: 文字列

必須: いいえ

ProtectedResourceArns

特定の ARN のリスト (例: `ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]`) またはワイルドカード (例: `ProtectedResourceArns: ["*"]`) を含めることができますが、両方を含めることはできません。

タイプ : 文字列の配列

必須: いいえ

ProtectedResourceConditions

タグを使用して復元テストプランでリソースに定義する条件。

例えば `"StringEquals": { "Key": "aws:ResourceTag/CreatedByCryo", "Value": "true" },` です。条件演算子では、大文字と小文字が区別されます。

タイプ : ProtectedResourceConditions オブジェクト

必須: いいえ

RestoreMetadataOverrides

`RestoreTestingSelection` の本文にパラメータ `RestoreMetadataOverrides` を含めることで、特定の復元メタデータのキーを上書きできます。キー値では大文字と小文字が区別されません。

復元テストの推定メタデータの全リストを参照してください。

型: 文字列間のマッピング

必須: いいえ

ValidationWindowHours

この値は、オプションの検証を実施するために復元テスト後にデータを保持する時間 (時間単位) です。

使用できる値は 0 から 168 (7 日間に相当する時間) の整数です。

タイプ: 整数

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AWS Backup gateway

以下のデータタイプが AWS Backup gateway によってサポートされています。

- BandwidthRateLimitInterval
- Gateway
- GatewayDetails
- Hypervisor
- HypervisorDetails
- MaintenanceStartTime
- Tag
- VirtualMachine
- VirtualMachineDetails

- VmwareTag
- VmwareToAwsTagMapping

BandwidthRateLimitInterval

サービス: AWS Backup gateway

ゲートウェイの帯域幅レート制限間隔を記述します。帯域幅レート制限スケジュールは、帯域幅レート制限間隔で構成されます。帯域幅レート制限間隔は、1 週間のうちの 1 日以上の期間を定義して、その間にアップロード、ダウンロード、またはその両方に対して帯域幅レート制限が指定されるものです。

内容

DaysOfWeek

帯域幅レート制限間隔を構成する曜日単位は、0 ~ 6 の序数で表されます。0 は日曜日、6 は土曜日を表します。

タイプ: 整数の配列

配列メンバー : 最小数は 1 項目です。最大数は 7 項目です。

有効な範囲: 最小値 は 0 です。最大値は 6 です。

必須: はい

EndHourOfDay

帯域幅レート制限間隔を終了する時刻のうちの時間。

タイプ: 整数

有効な範囲: 最小値 は 0 です。最大値は 23 です。

必須: はい

EndMinuteOfHour

帯域幅レート制限間隔が終了する時刻のうちの分。

> **Important**
> 帯域幅レート制限間隔は、この 1 分間の最後に終了します。1 時間の終わりに間隔を終了するには、値 59 を使用します。

タイプ: 整数

有効な範囲: 最小値 は 0 です。最大値は 59 です。

必須: はい

StartHourOfDay

帯域幅レート制限間隔を開始する時刻のうちの時間。

タイプ: 整数

有効な範囲: 最小値 は 0 です。最大値は 23 です。

必須: はい

StartMinuteOfHour

帯域幅レート制限期間を開始する時間のうちの分。間隔はその 1 分間の開始時から始まります。間隔の開始時刻を、その時間の開始時から正確に開始するには、値 `0` を使用します。

タイプ: 整数

有効な範囲: 最小値 は 0 です。最大値は 59 です。

必須: はい

AverageUploadRateLimitInBitsPerSec

帯域幅レート制限間隔の平均アップロード速度制限単位 (ビット/秒)。アップロード速度制限が設定されていない場合、このフィールドはレスポンスに表示されません。

型: 長整数

有効な範囲: 最小値 は 51200 です。最大値は 8000000000000 です。

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Gateway

サービス: AWS Backup gateway

ゲートウェイは、 AWS クラウドのバックアップストレージへのシームレスな接続を提供するために、お客様のネットワーク上で実行される AWS Backup ゲートウェイアプライアンスです。

内容

GatewayArn

ゲートウェイの Amazon リソースネーム (ARN)。ListGateways オペレーションを使用して、アカウント と のゲートウェイのリストを返します AWS リージョン。

型: 文字列

長さの制限: 最小長は 50 です。最大長は 180 です。

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必須: いいえ

GatewayDisplayName

ゲートウェイの表示名です。

型: 文字列

長さの制限: 最小長は 1 です。最大長は 100 です。

Pattern: `^[a-zA-Z0-9-]*$`

必須: いいえ

GatewayType

ゲートウェイのタイプ。

型: 文字列

有効な値：`BACKUP_VM`

必須：いいえ

HypervisorId

ゲートウェイのハイパーバイザー IDです。

型: 文字列

長さの制限: 最小長は 1 です。最大長は 100 です。

必須: いいえ

LastSeenTime

AWS Backup ゲートウェイが最後にゲートウェイと通信した時刻を Unix 形式および UTC 時間で表します。

型: タイムスタンプ

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

GatewayDetails

サービス: AWS Backup gateway

ゲートウェイの詳細です。

内容

GatewayArn

ゲートウェイの Amazon リソースネーム (ARN)。ListGateways 操作を使用して、アカウントと AWS リージョンのリストを返します。

型: 文字列

長さの制限: 最小長は 50 です。最大長は 180 です。

Pattern: ^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$

必須: いいえ

GatewayDisplayName

ゲートウェイの表示名です。

型: 文字列

長さの制限: 最小長は 1 です。最大長は 100 です。

Pattern: ^[a-zA-Z0-9-]*$

必須: いいえ

GatewayType

ゲートウェイタイプのタイプ。

型: 文字列

有効な値：BACKUP_VM

必須：いいえ

HypervisorId

ゲートウェイのハイパーバイザー IDです。

型: 文字列

長さの制限: 最小長は 1 です。最大長は 100 です。

必須: いいえ

LastSeenTime

AWS Backup ゲートウェイが最後にクラウドと通信した時刻を Unix 形式および UTC 時間で示す詳細。

型: タイムスタンプ

必須: いいえ

MaintenanceStartTime

曜日と時刻を含むゲートウェイの週次メンテナンス開始時刻を返します。値はゲートウェイのタイムゾーンを基準としていることに注意してください。週単位でも月単位でもかまいません。

タイプ：MaintenanceStartTime オブジェクト

必須: いいえ

NextUpdateAvailabilityTime

ゲートウェイの次回の更新可能時間を示す詳細。

型: タイムスタンプ

必須: いいえ

VpcEndpoint

ゲートウェイがバックアップゲートウェイ用のクラウドへの接続に使用する仮想プライベートクラウド (VPC) エンドポイントの DNS 名。

型: 文字列

長さの制限：最小長は 1 です。最大長は 255 です。

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Hypervisor

サービス: AWS Backup gateway

ゲートウェイが接続するハイパーバイザーの権限を表します。

ハイパーバイザーは、仮想マシンを作成および管理し、それらにリソースを割り当てるハードウェア、ソフトウェア、またはファームウェアです。

内容

Host

ハイパーバイザーのサーバーホストです。これは、IP アドレスまたは完全修飾ドメイン名 (FQDN) のいずれかです。

型: 文字列

長さの制限: 最小長は 3 です。最大長は 128 です。

Pattern: `^.+$`

必須: いいえ

HypervisorArn

ハイパーバイザーの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。500 の最大長。

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必須: いいえ

KmsKeyArn

ハイパーバイザーの暗号化 AWS Key Management Service に使用される の Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。500 の最大長。

Pattern: ^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$

必須: いいえ

Name

ハイパーバイザーの名前。

型: 文字列

長さの制限: 最小長は 1 です。最大長は 100 です。

Pattern: ^[a-zA-Z0-9-]*$

必須: いいえ

State

ハイパーバイザーの状態です。

型: 文字列

有効な値：PENDING | ONLINE | OFFLINE | ERROR

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

HypervisorDetails

サービス: AWS Backup gateway

これは、指定されたハイパーバイザーの詳細です。ハイパーバイザーは、仮想マシンを作成および管理し、それらにリソースを割り当てるハードウェア、ソフトウェア、またはファームウェアです。

内容

Host

ハイパーバイザーのサーバーホストです。これは、IP アドレスまたは完全修飾ドメイン名 (FQDN) のいずれかです。

型: 文字列

長さの制限: 最小長は 3 です。最大長は 128 です。

Pattern: `^.+$`

必須: いいえ

HypervisorArn

ハイパーバイザーの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 50 です。500 の最大長。

Pattern: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必須: いいえ

KmsKeyArn

ハイパーバイザーの暗号化に AWS KMS 使用する Amazon リソースネーム (ARN)です。

型: 文字列

長さの制限: 最小長は 50 です。500 の最大長。

Pattern: `^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

必須: いいえ

LastSuccessfulMetadataSyncTime

これは、メタデータの同期が最後に成功した時刻です。

型: タイムスタンプ

必須: いいえ

LatestMetadataSyncStatus

これは、指定したメタデータ同期の最新のステータスです。

型: 文字列

有効な値：CREATED | RUNNING | FAILED | PARTIALLY_FAILED | SUCCEEDED

必須：いいえ

LatestMetadataSyncStatusMessage

これは、指定したメタデータ同期の最新のステータスです。

タイプ: 文字列

必須: いいえ

LogGroupArn

リクエストされたログ内のゲートウェイグループの Amazon リソースネーム (ARN)。

型: 文字列

長さの制限: 最小長は 0 です。最大長は 2,048 です。

パターン: `^$|^arn:(aws|aws-cn|aws-us-gov):logs:([a-zA-Z0-9-]+):([0-9]+):log-group:[a-zA-Z0-9_\-\/\.]+:\*$`

必須: いいえ

Name

これは、指定されたハイパーバイザーの名前です。

型: 文字列

長さの制限: 最小長は 1 です。最大長は 100 です。

Pattern: ^[a-zA-Z0-9-]*$

必須: いいえ

State

これは、指定されたハイパーバイザーの現在の状態です。

可能な状態は、PENDING、ONLINE、OFFLINE または ERROR です。

型: 文字列

有効な値 : PENDING | ONLINE | OFFLINE | ERROR

必須 : いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

MaintenanceStartTime

サービス: AWS Backup gateway

これは、曜日と時刻を含むゲートウェイの週次メンテナンス開始時刻です。値はゲートウェイのタイムゾーンを基準としていることに注意してください。週単位でも月単位でもかまいません。

内容

HourOfDay

メンテナンス開始時間の時間単位は hh で表されます。hh は時間 (0 ~ 23) です。時間は、ゲートウェイのタイムゾーンで表示されます。

タイプ: 整数

有効な範囲: 最小値 は 0 です。最大値は 23 です。

必須: はい

MinuteOfHour

メンテナンス開始時間の分単位は mm で表されます。mm は分 (0 ~ 59) です。時刻のうちの分は、ゲートウェイのタイムゾーンで表示されます。

タイプ: 整数

有効な範囲: 最小値 は 0 です。最大値は 59 です。

必須: はい

DayOfMonth

メンテナンス開始時刻の日単位は、1 ~ 28 の序数で表されます。ここで、1 は月の最初の日、28 は月の最終日を表します。

タイプ : 整数

有効な範囲: 最小値 は 1 です。最大値は 31 です。

必須: いいえ

DayOfWeek

曜日を表す 0 ~ 6 の序数。0 は日曜日、6 は土曜日を表します。曜日は、ゲートウェイのタイムゾーンで表示されます。

タイプ: 整数

有効な範囲: 最小値 は 0 です。最大値は 6 です。

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Tag

サービス: AWS Backup gateway

リソースの管理、フィルタリング、検索に使用できるキーと値のペアです。使用可能な文字は、UTF-8の文字、数字、スペース、および以下の文字です。+ - = . _ : /。

内容

Key

タグのキーと値のペアのキー部分です。キーのスタートを aws: にすることはできません。

型: 文字列

長さの制限: 最小長は 1 です。最大長は 128 です。

パターン: ^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$

必須：はい

Value

タグのキーと値のペアの値部分です。

型: 文字列

長さの制限: 最小長は 0 です。最大長は 256 です。

パターン：^[^\x00]*$

必須：はい

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

VirtualMachine

サービス: AWS Backup gateway

ハイパーバイザー上にある仮想マシンです。

内容

HostName

仮想マシンのホスト名です。

型: 文字列

長さの制限: 最小長は 1 です。最大長は 100 です。

Pattern: ^[a-zA-Z0-9-]*$

必須: いいえ

HypervisorId

仮想マシンのハイパーバイザーの IDです。

タイプ: 文字列

必須: いいえ

LastBackupDate

仮想マシンがバックアップされた最新の日付は Unix 形式および UTC 時刻で表しています。

型: タイムスタンプ

必須: いいえ

Name

仮想マシンの名前。

型: 文字列

長さの制限: 最小長は 1 です。最大長は 100 です。

Pattern: ^[a-zA-Z0-9-]*$

必須: いいえ

Path

仮想マシンのパスです。

型: 文字列

長さの制限：最小長は 1 です。最大長は 4,096 です。

パターン: ^[^\x00]+$

必須: いいえ

ResourceArn

仮想マシンの Amazon リソースネーム (ARN)です。例えば arn:aws:backup-gateway:us-west-1:0000000000000:vm/vm-0000ABCDEFGIJKL です。

タイプ: 文字列

長さの制限: 最小長は 50 です。500 の最大長。

Pattern: ^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$

必須: いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

VirtualMachineDetails

サービス: AWS Backup gateway

Amazon リソースネーム (ARN) の順序が付けられた、`VirtualMachine` オブジェクトです。

内容

HostName

仮想マシンのホスト名です。

型: 文字列

長さの制限: 最小長は 1 です。最大長は 100 です。

Pattern: `^[a-zA-Z0-9-]*$`

必須: いいえ

HypervisorId

仮想マシンのハイパーバイザーの IDです。

タイプ: 文字列

必須: いいえ

LastBackupDate

仮想マシンがバックアップされた最新の日付は Unix 形式および UTC 時刻で表しています。

型: タイムスタンプ

必須: いいえ

Name

仮想マシンの名前。

型: 文字列

長さの制限: 最小長は 1 です。最大長は 100 です。

Pattern: `^[a-zA-Z0-9-]*$`

必須: いいえ

Path

仮想マシンのパスです。

型: 文字列

長さの制限：最小長は 1 です。最大長は 4,096 です。

パターン: ^[^\x00]+$

必須: いいえ

ResourceArn

仮想マシンの Amazon リソースネーム (ARN)です。例えば arn:aws:backup-gateway:us-west-1:0000000000000:vm/vm-0000ABCDEFGIJKL です。

タイプ: 文字列

長さの制限: 最小長は 50 です。500 の最大長。

Pattern: ^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$

必須: いいえ

VmwareTags

これは、指定された仮想マシンに関連付けられている VMware タグの詳細です。

型: VmwareTag オブジェクトの配列

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

VmwareTag

サービス: AWS Backup gateway

VMware タグは、特定の仮想マシンにアタッチされたタグです。タグは、リソースの管理、フィルタリング、検索に使用できるキーと値のペアです。

VMware タグの内容はタグと照合できます AWS 。

内容

VmwareCategory

これは、VMware のカテゴリです。

型: 文字列

長さの制限：最小長は 1 です。最大長は 80 です。

必須: いいえ

VmwareTagDescription

これは、VMware タグについてのユーザーが定義した説明です。

タイプ: 文字列

必須: いいえ

VmwareTagName

これは、VMware タグについてのユーザーが定義した名前です。

型: 文字列

長さの制限：最小長は 1 です。最大長は 80 です。

必須：いいえ

その他の参照資料

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++

- AWS SDK for Java V2
- AWS SDK for Ruby V3

VmwareToAwsTagMapping

サービス: AWS Backup gateway

これにより、VMware タグと対応する AWS タグのマッピングが表示されます。

内容

AwsTagKey

AWS タグのキーと値のペアのキー部分。

型: 文字列

長さの制限: 最小長は 1 です。最大長は 128 です。

パターン: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

必須：はい

AwsTagValue

AWS タグのキーと値のペアの値部分。

型: 文字列

長さの制限: 最小長は 0 です。最大長は 256 です。

パターン：`^[^\x00]*$`

必須：はい

VmwareCategory

これは、VMware のカテゴリです。

型: 文字列

長さの制限：最小長は 1 です。最大長は 80 です。

必須: はい

VmwareTagName

これは、VMware タグについてのユーザーが定義した名前です。

型: 文字列

長さの制限：最小長は 1 です。最大長は 80 です。

必須：はい

以下の資料も参照してください。

言語固有の AWS SDKs のいずれかでこの API を使用する方法の詳細については、以下を参照してください。

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

共通パラメータ

次のリストには、すべてのアクションが署名バージョン 4 リクエストにクエリ文字列で署名するために使用するパラメータを示します。アクション固有のパラメータは、アクションのトピックに示されています。Signature Version 4 の詳細については、「IAM ユーザーガイド」の「AWS API リクエストの署名」を参照してください。

Action

実行するアクション。

型: 文字列

必須: はい

Version

リクエストが想定している API バージョンである、YYYY-MM-DD 形式で表示されます。

型: 文字列

必須: はい

X-Amz-Algorithm

リクエストの署名を作成するのに使用したハッシュアルゴリズム。

条件: HTTP 認証ヘッダーではなくクエリ文字列に認証情報を含める場合は、このパラメータを指定します。

型: 文字列

有効な値: AWS4-HMAC-SHA256

必須: 条件による

X-Amz-Credential

認証情報スコープの値で、アクセスキー、日付、対象とするリージョン、リクエストしているサービス、および終了文字列 ("aws4_request") を含む文字列です。値は次の形式で表現されます。[access_key/YYYYYYYYMMDD/リージョン/サービス/aws4_request]

詳細については、「IAM ユーザーガイド」の「署名付きAWS API リクエストの作成」を参照してください。

条件: HTTP 認証ヘッダーではなくクエリ文字列に認証情報を含める場合は、このパラメータを指定します。

型: 文字列

必須: 条件による

X-Amz-Date

署名を作成するときに使用する日付です。形式は ISO 8601 基本形式の YYYYMMDD'T'HHMMSS'Z' でなければなりません。例えば、日付 20120325T120000Z は、有効な X-Amz-Date の値です。

条件: X-Amz-Date はすべてのリクエストに対してオプションです。署名リクエストで使用する日付よりも優先される日付として使用できます。ISO 8601 ベーシック形式で日付ヘッダーが指定されている場合、X-Amz-Date は必要ありません。X-Amz-Date を使用すると、常に Date ヘッダーの値よりも優先されます。詳細については、「IAM ユーザーガイド」の「AWS API リクエスト署名の要素」を参照してください。

タイプ: 文字列

必須: 条件による

X-Amz-Security-Token

AWS Security Token Service (AWS STS) へのを呼び出しで取得された一時的なセキュリティトークン。AWS STS の一時的なセキュリティ認証情報をサポートするサービスのリストについては、「IAM ユーザーガイド」の「IAM と連携するAWS のサービス」を参照してください。

条件:AWS STS の一時的なセキュリティ認証情報を使用する場合、セキュリティトークンを含める必要があります。

タイプ: 文字列

必須: 条件による

X-Amz-Signature

署名する文字列と派生署名キーから計算された 16 進符号化署名を指定します。

条件: HTTP 認証ヘッダーではなくクエリ文字列に認証情報を含める場合は、このパラメータを指定します。

型: 文字列

必須: 条件による

X-Amz-SignedHeaders

正規リクエストの一部として含まれていたすべての HTTP ヘッダーを指定します。署名付きヘッダーの指定に関する詳細については、「IAM ユーザーガイド」の「署名付き AWS API リクエストの作成」を参照してください。

条件: HTTP 認証ヘッダーではなくクエリ文字列に認証情報を含める場合は、このパラメータを指定します。

型: 文字列

必須: 条件による

共通エラー

このセクションでは、AWS のすべてのサービスの API アクションに共通のエラーを一覧表示しています。このサービスの API アクションに固有のエラーについては、その API アクションのトピックを参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 400

IncompleteSignature

リクエストの署名が AWS 基準に適合しません。

HTTP ステータスコード: 400

InternalFailure

リクエストの処理が、不明なエラー、例外、または障害により実行できませんでした。

HTTP ステータスコード: 500

InvalidAction

リクエストされたアクション、またはオペレーションは無効です。アクションが正しく入力されていることを確認します。

HTTP ステータスコード: 400

InvalidClientTokenId

指定された x.509 証明書、または AWS アクセスキー ID が見つかりません。

HTTP ステータスコード: 403

NotAuthorized

このアクションを実行するにはアクセス許可が必要です。

HTTP ステータスコード: 400

OptInRequired

サービスを利用するためには、AWS アクセスキー ID を取得する必要があります。

HTTP ステータスコード: 403

RequestExpired

リクエストの日付スタンプの 15 分以上後またはリクエストの有効期限 (署名付き URL の場合など) の 15 分以上後に、リクエストが到着しました。または、リクエストの日付スタンプが現在より 15 分以上先です。

HTTP ステータスコード: 400

ServiceUnavailable

リクエストは、サーバーの一時的障害のために実行に失敗しました。

HTTP ステータスコード: 503

ThrottlingException

リクエストは、制限が必要なために実行が拒否されました。

HTTP ステータスコード: 400

ValidationError

入力が、AWS サービスで指定された制約を満たしていません。

HTTP ステータスコード: 400

のドキュメント履歴 AWS Backup

- API バージョン: 2023 年 12 月 6 日
- ドキュメントの最終更新日: 2024 年 6 月 3 日

次の表は、2019 年 1 月のサービス AWS Backup 開始から現在までのすべての起動を示しています。このドキュメントの更新に関するお知らせをするために、RSS フィードをサブスクライブすることができます。

変更	説明	日付
AWS Backup 機能リージョンの拡張	AWS Backup Amazon EBS スナップショットアーカイブ階層のサポートが、次のリージョンで利用可能になりました。 • 中国 (北京) • 中国 (寧夏) • AWS GovCloud （米国西部） • AWS GovCloud （米国東部）	2024 年 6 月 3 日
AWS 管理ポリシーの更新	AWS Backup は、以下の マネージドポリシー`backup:TagResource` にアクセス許可を追加しました。 • AWSBackupServiceRolePolicyForBackup • AWSBackupServiceRolePolicyForS3Backup • AWSBackupServiceLinkedRolePolicyForBackup	2024 年 5 月 17 日

変更	説明	日付
	詳細については、「ポリシーの更新」を参照してください。	
AWS Backup がカナダ西部 (カルガリー) リージョンで利用可能に	多くのリソースタイプのバックアップと復元が AWS リージョン カナダ西部 (カルガリー) で利用可能になりました。 互換性のあるバックアップ機能については、「 による機能の可用性 AWS リージョン」を参照してください。 サポートされているリソースタイプについては、「 がサポートするサービス AWS リージョン」を参照してください。	2024 年 3 月 14 日
管理ポリシーにアクセス許可を追加	AWS Backup は、復元テスト機能内の追加のリソースタイプをサポートするアクセス許可を追加AWSServiceRolePolicyForBackupRestoreTestingすることで、ポリシーを更新しました。 追加された特定のアクセス許可の詳細については、「ポリシーの更新」を参照してください。	2024 年 2 月 14 日

変更	説明	日付
FSx for ONTAP FlexGroup ボリュームのバックアップと復元のサポート	AWS Backup は、ほとんどので FSx for ONTAP FlexGroup ボリュームのバックアップと復元をサポートするようになりました AWS リージョン。 詳細については、「FSx ファイルシステムの復元」を参照してください。 .	2024 年 1 月 10 日
SAP HANA HA のバックアップと復元のサポート	AWS Backup は、Amazon EC2 のバックアップと復元で SAP HANA High Availability データベースをサポートするようになりました。 詳細については、「Amazon EC2 インスタンス上の SAP HANA データベースのバックアップ」と、「Amazon EC2 インスタンスで SAP HANA データベースを復元する」を参照してください。	2023 年 12 月 21 日

変更	説明	日付
AWS Backup 復元テストの Audit Manager コントロール	AWS Backup Audit Manager は、リソースがターゲットを満たすための復元時間の制御を提供し、復元時間のモニタリングをサポートするようになりました。このコントロールは、リソースの復元時間が目標を満たしているかどうかをチェックします。 詳細については、「コントロールと修正」および「復元テストの監査」を参照してください。	2023 年 12 月 18 日
Amazon EBS コールドストレージのサポート	AWS Backup で、EBS バックアップのウォームストレージからコールドストレージへの移行がサポートされるようになりました。詳細については、以下を参照してください。 • コールドストレージ用の Amazon EBS アーカイブ階層 • ライフサイクルとストレージ階層 • バックアッププランの作成	2023 年 11 月 27 日

変更	説明	日付
復元テストの導入	AWS Backup では復元テストが導入されています。これにより、復元の実行可能性を自動的かつ定期的に評価し、復元ジョブの所要時間をモニタリングできます。 詳細については、「復元テスト」を参照してください。	2023 年 11 月 27 日

変更	説明	日付
AWS 管理ポリシーの更新	AWS Backup は、アクセス許可 `ec2:DescribeSnapshotTierStatus` と `ec2:ModifySnapshotTier` を マネージドポリシー `AWSBackupServiceRolePolicyForBackups` とに追加しました`AWSBackupServiceLinkedRolePolicyForBackup` 。AWS Backup また、 は、アクセス許可 `ec2:DescribeSnapshotTierStatus` と `ec2:RestoreSnapshotTier` を マネージドポリシー に追加しました`AWSBackupServiceRolePolicyForRestores` 。 これらのアクセス許可は、 に保存されている Amazon EBS リソースを AWS Backup アーカイブストレージに移行したり、アーカイブストレージ階層からリソースを復元したりするためのオプションをユーザーが持つために必要です。 詳細については、「ポリシーの更新」を参照してください。	2023 年 11 月 27 日

変更	説明	日付
復元テストをサポートするためのパスロール許可を追加	AWS Backup が IamPassRolePermissions と restore-testing.backup.amazonaws.com に追加されましたIamCreateServiceLinkedRolePermissions 。この追加は、 がお客様に代わって復元テストを実行する AWS Backup ために必要です。	2023 年 11 月 27 日

変更	説明	日付
新しいサービスリンクロールを追加	AWS Backup は、 という名前の新しいサービスにリンクされたロールを追加しました。このロールは`AWSServiceRoleForBackupRestoreTesting`、復元テストを実行するためのバックアップアクセス許可を提供します。 この新しいサービスにリンクされたロールは AWS Backup 、復元テストを実行するために必要なアクセス許可を提供します。アクセス許可には、Aurora 、DocumentDB、DynamoDB、Amazon EBS、Amazon EC2、Amazon EFS、FSx for Lustre、FSx for Windows File Server、FSx for ONTAP、FSx for OpenZFS、Amazon Neptune、Amazon RDS、Amazon S3 といったサービスを復元テストに含めるための、`list, read, and write` アクションが含まれます。	2023 年 11 月 27 日

変更	説明	日付
AWS Backup コンソールの新しいジョブメトリクスダッシュボード	AWS Backup コンソールにジョブダッシュボードが表示されるようになりました。これにより、新しいビジュアルユーザーインターフェイスと、 でサポートされているサービスの集約されたバックアップ、コピー、復元メトリクスを使用して、大規模なバックアップヘルスモニタリングを簡素化できます AWS Backup。 ジョブダッシュボードは、AWS Backup Audit Manager が利用可能なすべてのリージョンで使用できます。 リストにないリージョンは、引き続きCloudWatch ダッシュボード にアクセスできます。 詳細については、「AWS Backup コンソールダッシュボード」を参照してください。	2023 年 11 月 15 日

変更	説明	日付
ネストされたスタックのバックアップのサポート	AWS Backup は、 AWS CloudFormation リソースのバックアップのサポートを拡張しました。ネストされたスタックがある CloudFormation アプリケーションスタックは、バックアップに含めることができます。 詳細については、「CloudFormation スタックのバックアップ」を参照してください。	2023 年 11 月 8 日
中国 (北京) および中国 (寧夏) での Amazon S3 のサポート。	AWS Backup Amazon S3 のサポートが、中国 (北京) および中国 (寧夏) リージョンで利用可能になりました。 詳細については、「リージョンごとの機能の可用性」を参照してください。	2023 年 10 月 26 日
Amazon Aurora の継続的バックアップと Point-in-time 復元のサポート	AWS Backup は、Aurora リソースの継続的バックアップと point-in-time 復元 (PITR) をサポートするようになりました。 詳細については、「継続的バックアップ」と「P oint-in-time リカバリ」を参照してください。	2023 年 9 月 7 日

変更	説明	日付
AWS CloudFormation スタックは リソースの除外をサポートします	AWS Backup では、選択したリソースを AWS CloudFormation スタックから除外するオプションがサポートされるようになりました。 詳細については、「AWS CloudFormation スタックのバックアップ」を参照してください。	2023 年 9 月 6 日
バックアッププランのルールでのタイムゾーンの柔軟性向上	AWS Backup プランルールで、バックアップウィンドウのタイムゾーンを指定できるようになりました。 詳細については、「バックアッププランの管理」を参照してください。	2023 年 8 月 28 日
AWS Backup がイスラエル (テルアビブ) リージョンで利用可能に	新しいイスラエル (テルアビブ) リージョンで多くの AWS Backup 機能が利用できるようになりました。 サポートされているリソースについては、「AWS リージョンごとの機能の可用性」をご覧ください。	2023 年 8 月 22 日

変更	説明	日付
AWS Backup Audit Manager が委任管理者アカウントをサポートするようになりました	AWS Backup Audit Manager のレポート生成に、委任された管理者アカウントがアクセスできるようになりました。詳細については、以下を参照してください。 • AWS Backup Audit Manager を使用してバックアップを監査し、レポートを作成する • 監査レポートの使用 • 委任された管理者	2023 年 8 月 16 日
論理的に工アギャップのあるバックアップボールトのプレビュー	AWS Backup では、データ保護オペレーションを補完するために、新しいタイプのバックアップボールトのプレビューが提供されるようになりました。 詳細については、「論理工アギャップボールト (プレビュー)」を参照してください。	2023 年 8 月 8 日
AWS Backup で Amazon S3 バックアップを強化	AWS Backup では、S3 バケットバックアップのパフォーマンス、サイズ、速度の機能が向上しました。 詳細については、「Amazon S3 のバックアップ」を参照してください。	2023 年 8 月 1 日

変更	説明	日付
復元機能のタグが中国リージョンで利用可能に	中国 (北京) または中国 (寧夏) リージョンで復元ジョブを作成するときに、バックアップに含まれるタグをコピーできるようになりました。 詳細については、「復元時のタグのコピー」を参照してください。	2023 年 7 月 17 日
AWS Backup が追加のリージョンで Amazon S3 をサポートするようになりました	AWS Backup Amazon S3 のサポートが、欧州 (スペイン)、欧州 (チューリッヒ)、アジアパシフィック (ハイデラバード)、およびアジアパシフィック (メルボルン) の各リージョンで利用可能になりました。 詳細については、「リージョンごとの機能の可用性」を参照してください。	2023 年 7 月 6 日

変更	説明	日付
クロスアカウントコピーに関するリージョンの追加	AWS Backup では、アジアパシフィック (ジャカルタ) 、中東 (バーレーン) 、アジアパシフィック (香港) 、アフリカ (ケープタウン) 、欧州 (ミラノ) 、アジアパシフィック (大阪) 、中東 (アラブ首長国連邦) 、欧州 (スペイン) 、欧州 (チューリッヒ) 、アジアパシフィック (ハイデラバード) 、アジアパシフィック (メルボルン) の各リージョンで、ほとんどの リソースのクロスアカウントバックアップコピーがサポートされるようになりました。 詳細については、「リージョンごとの機能の可用性」を参照してください。	2023 年 7 月 5 日
Backup Audit Manager が GovCloud リージョンで利用可能に	AWS Backup は AWS Backup Audit Manager を AWS GovCloud （米国東部) と AWS GovCloud （米国西部) に拡張しました。 詳細については、「リージョンごとの機能の可用性」を参照してください。	2023 年 6 月 29 日

変更	説明	日付
クロスアカウント管理が GovCloud リージョンで利用可能に	AWS Backup で、 AWS GovCloud （米国東部) および AWS GovCloud （米国西部) でのリソースのクロスアカウント管理がサポートされるようになりました。 詳細については、「複数の AWS アカウントにまたがる AWS Backup リソースの管理」を参照してください。	2023 年 6 月 29 日
Amazon Aurora のクロスリージョンコピーのサポート対象のリージョン追加	AWS Backup では、アジアパシフィック (ジャカルタ）、中東 (バーレーン）、アジアパシフィック (香港）、アフリカ (ケープタウン）、欧州 (ミラノ）、中東 (アラブ首長国連邦）、欧州 (スペイン）、欧州 (チューリッヒ）、アジアパシフィック (ハイデラバード）、アジアパシフィック (メルボルン) の各リージョンとの間で Aurora クラスターのクロスリージョンバックアップコピーがサポートされるようになりました。	2023 年 6 月 5 日

変更	説明	日付
復元時のタグのコピー	復元ジョブの作成時に、バックアップの一部であるタグをコピーできるようになりました。 詳細については、「復元時のタグのコピー」を参照してください。	2023 年 5 月 22 日
AWS Backup と AWS ユーザー通知の統合	バックアップ、コピー、復元のイベントに関する通知をAWS ユーザー通知コンソールから受信する選択ができるようになりました。 詳細については、AWS 「ユーザー通知の開始方法」を参照してください。	2023 年 5 月 10 日
クロスリージョンバックアップが新たに 4 つのリージョンで利用可能に	AWS Backup は、中東 (アラブ首長国連邦) リージョン、欧州 (スペイン) リージョン、欧州 (チューリッヒ) リージョン、およびアジアパシフィック (ハイデラバード) リージョンでのクロスリージョンバックアップをサポートするようになりました。	2023 年 4 月 28 日

変更	説明	日付
クロスリージョン AWS Backup コピーのサポートを拡張	Amazon EFS、VMware、DynamoDB リソースのクロスリージョンバックアップが、以下のリージョンで実行可能になりました: アジアパシフィック (ジャカルタ)、中東 (バーレーン)、アジアパシフィック (香港),アフリカ (ケープタウン)、および欧州 (ミラノ) です。	2023 年 4 月 28 日
南米 (サンパウロ) リージョンでの Amazon S3 のバックアップおよび復元	AWS Backup Amazon S3 (Amazon Simple Storage Service) のサポートが南米 (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、「Amazon S3 のバックアップ」を参照してください。	2023 年 4 月 20 日
AWS Backup がアジアパシフィック (メルボルン) リージョンに拡張	AWS Backup がアジアパシフィック (メルボルン) リージョンで利用可能になりました。 詳細については、「リージョン別の機能の可用性 AWS」を参照してください。	2023 年 4 月 20 日

変更	説明	日付
Amazon S3 サポートのリージョン拡大	AWS Backup Amazon S3 (Amazon Simple Storage Service) のサポートが、 AWS GovCloud （ 米国東部) および AWS GovCloud （ 米国西部) リージョンで利用可能になりました 詳細については、「Amazon S3 のバックアップ」を参照してください。	2023 年 4 月 19 日
Amazon EC2 インスタンス上の SAP HANA データベースのバックアップと復元	AWS Backup では、ほとんどの リージョンで Amazon EC2 インスタンスで実行されている SAP HANA データベースをバックアップおよび復元できるようになりました。 詳細については、「Amazon EC2 インスタンス上の SAP HANA データベースのバックアップ」を参照してください。	2023 年 4 月 17 日

変更	説明	日付
AWS Backup が欧州 (スペイン)、欧州 (チューリッヒ)、アジアパシフィック (ハイデラバード) の各リージョンで利用可能に	AWS Backup サポートは、欧州 (スペイン)、欧州 (チューリッヒ)、アジアパシフィック (ハイデラバード) などの新しい リージョンに拡張されました。サポートされるリソースは、これらのリージョンでバックアップと復元ができます。 詳細については、「リージョン別の機能の可用性 AWS」を参照してください。	2023 年 4 月 13 日
AWS 管理ポリシーの更新 `AWSBackupAuditAccess`	AWS マネージドポリシーを更新 AWS Backup しましたAWSBackupAuditAccess。 API 内のリソース選択をワイルドカードリソース`config:DescribeComplianceByConfigRule` に置き換えました。 詳細については、「AWS Backupポリシーの更新」を参照してください。	2023 年 4 月 11 日

変更	説明	日付
Amazon CloudWatch Logs を使用したハイパーバイザー	AWS Backup ゲートウェイユーザーは、ハイパーバイザーを CloudWatch ログと統合してログを維持できるようになりました。詳細については、「ハイパーバイザー設定の編集」および CloudWatch「ログ」を参照してください。	2023 年 3 月 29 日
Amazon S3 サポートのリージョン拡大	AWS Backup Amazon S3 のサポートが、アジアパシフィック (ジャカルタ) および中東 (アラブ首長国連邦) リージョンで利用可能になりました。	2023 年 3 月 22 日
仮想マシンの増分バックアップの強化	CBT (変更ブロックトラッキング) データの問題が発生した VMware VM (仮想マシン) バックアップに、修正とトラブルシューティングに役立つ追加情報が含まれるようになりました。 詳細については、「VM の増分バックアップ」と「仮想マシンのトラブルシューティング」を参照してください。	2023 年 3 月 15 日

変更	説明	日付
AWS Backup 複数のネットワークアダプタのサポート	AWS Backup ゲートウェイが複数のネットワークアダプタの設定をサポートするようになりました ネットワークアダプタの設定の詳細については、「AWS Backup デベロッパーガイド」の「VMware での複数の NIC 用のゲートウェイの設定」を参照してください。	2023 年 3 月 8 日
AWS Backup vSphere 8 のサポート	AWS Backup は、VMware vSphere 8 で実行される仮想マシンのバックアップと復元をサポートするようになりました。 サポートされている VMware オプションの詳細については、「AWS Backup デベロッパーガイド」の「サポートされている VM」を参照してください。	2023 年 3 月 8 日

変更	説明	日付
AWS Backup Audit Manager が Amazon RDS マルチ AZ バックアップをサポート	Backup Audit Manager は、Amazon Relational Database Service マルチアベイラビリティーゾーンバックアップをサポートするようになりました。 詳細については、「Audit Manager を使用してバックアップを監査し、レポートを作成する方法 AWS Backup」を参照してください。	2023 年 2 月 1 日
AWS Backup は Amazon Timestream テーブルの増分バックアップを提供します	AWS Backup で Timestream バックアップのバックアップ機能が拡張されました。バックアッププランで、増分バックアップを実行して、Timestream リソースのバックアップに必要な時間を短縮し、ストレージコストを削減できるようになりました。 詳細については、「Amazon Timestream のバックアップ」を参照してください。	2023 年 1 月 23 日
AWS Backup がドバイで利用可能に	AWS Backup が中東 (UAE) リージョンに拡張されました。サポートされるリソースは、このリージョンでバックアップと復元ができます。	2023 年 1 月 17 日

変更	説明	日付
クロスリージョンコピーの利用可能なリージョンが追加	AWS Backup では、ほとんどのリソースについて、アジアパシフィック (ジャカルタ) リージョン、中東 (バーレーン) リージョン、アジアパシフィック (香港) リージョン、アフリカ (ケープタウン) リージョン、欧州 (ミラノ) リージョンでクロスリージョンバックアップが提供されるようになりました。 詳細については、「AWS リージョン間でのバックアップコピーの作成」を参照してください。	2022 年 12 月 21 日

変更	説明	日付
バックアップゲートウェイの帯域幅の制限とスロットリング	AWS Backup ゲートウェイでは、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 AWS Backup ために、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できるようになりました。 この機能をサポートするために、 AWS Backup は やなどの 管理ポリシー を作成AWSBackupFullAccess および更新しました AWSBackupOperatorAccess 。 詳細については、「バックアップゲートウェイの帯域幅のスロットリング」を参照してください。	2022 年 12 月 15 日

変更	説明	日付
バックアップゲートウェイ VMware タグのサポート	AWS Backup Gateway で VMware タグがサポートされるようになりました。ユーザーは、仮想マシンに使用される AWS タグと一致するタグを作成するための柔軟性が高まります。 この機能をサポートするために、 AWS Backup は、、、 などの 管理ポリシー AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync を作成AWSBackupFullAccess および更新しましたAWSBackupOperatorAccess 。 詳細については、「VMware タグ」を参照してください。	2022 年 12 月 15 日
AWS Backup Amazon Timestream のサポート	AWS Backup で Amazon Timestream テーブルのバックアップと復元がサポートされるようになりました。詳細については「Amazon Timestream のバックアップ」を参照してください。	2022 年 12 月 13 日

変更	説明	日付
AWS Backup がリーガルホールドを提供	AWS Backup は、リーガルホールドを通じて復旧ポイントを保護するための新しいツールを導入しました。詳細については、「リーガルホールド」を参照してください。	2022 年 11 月 27 日
AWS Backup Audit Manager のクロスリージョンおよびクロスアカウントレポート	AWS Backup Audit Manager は、コンプライアンスレポートとジョブレポートに追加の機能を提供します。ユーザーは、複数のリージョンおよび複数のアカウントを組み込んだレポートを生成できます。 詳細については、「監査レポートの使用」を参照してください。	2022 年 11 月 27 日
AWS Backup が Amazon Redshift をサポート	AWS Backup では、Amazon Redshift クラスターのバックアップと Amazon Redshift クラスターとテーブルの復元がサポートされるようになりました。詳細については、「Amazon Redshift バックアップ」を参照してください。	2022 年 11 月 27 日

変更	説明	日付
AWS Backup はアプリケーション AWS CloudFormation スタックのバックアップをサポート	AWS Backup は、スタックをバックアップ CloudFormation し、スタック内のリソースを復元することで、複数のリソースを含むアプリケーションをバックアップおよび復元する機能を提供します。 詳細については、「アプリケーションスタックのバックアップ」を参照してください。	2022 年 11 月 27 日
AWS Backup は、委任された管理者アカウントとバックアップポリシーの委任を提供します。	AWS Backup に登録されている アカウント AWS Organizations は、メンバーアカウントを委任管理者アカウントとして指定できます。 詳細については、「 による複数のアカウントの管理 AWS Organizations」を参照してください。	2022 年 11 月 27 日

変更	説明	日付
Amazon EC2 インスタンス上の SAP HANA のバックアップと復元のパブリックプレビュー	AWS Backup と AWS Backint は、EC2 インスタンスで SAP HANA データベースをバックアップおよび復元するための機能の統合されたパブリックプレビューを提供しています。 詳細については、「Amazon EC2 インスタンス上の SAP HANA のパブリックプレビュー」を参照してください。 このプレビューをサポートするために、 AWS Backup では、これらの機能に関するポリシーの更新と新しいAWS管理ポリシーが提供されました。	2022 年 11 月 20 日
Amazon EC2 インスタンスでの VMware 復元	AWS Backup では、EBS、VMware、VMware Cloud on および VMware AWS VMware Cloud on にマシンを復元する機能に加えて、仮想マシンを Amazon EC2 インスタンスに復元できるようになりました AWS Outposts。 詳細については、 AWS Backup コンソールを使用して仮想マシン復旧ポイント を復元する方法に関するドキュメントを参照してください。	2022 年 11 月 9 日

変更	説明	日付
AWS Backup ボールトロック機能の拡張	AWS Backup ボールトロックをガバナンスモードで作成して IAM 保護を追加したり、コンプライアンスモードで作成してイミュータビリティを確保できるようになりました。 詳しくは、「AWS Backup ボールトロック」をご覧ください。	2022 年 10 月 4 日
AWS Backup Audit Manager がアフリカ (ケープタウン) リージョンおよび欧州 (ミラノ) リージョンで利用可能に	AWS Backup Audit Manager は、アフリカ (ケープタウン) リージョンと欧州 (ミラノ) リージョンに拡張されました。Backup Audit Manager の詳細については、「Audit Manager によるバックアップの監査とレポートの作成 AWS Backup」を参照してください。	2022 年 9 月 14 日
AWS Backup は Amazon CloudWatch メトリクスを Backup コンソールダッシュボードに持ち込む	AWS Backup は、バックアップコンソールダッシュボードを強化し、バックアップジョブと復元ジョブの統合 Amazon CloudWatch メトリクスを表示して、モニタリング機能と柔軟性を高めます。	2022 年 9 月 8 日
Amazon EBS 暗号化の復元時に新たな柔軟性をサポート	AWS Backup では、Amazon EBS スナップショットの復元中に暗号化の追加オプションが提供されるようになりました。	2022 年 9 月 1 日

変更	説明	日付
AWS Backup で Amazon S3 クロスアカウントおよびクロスリージョンバックアップコピーをサポート	AWS Backup で、Amazon S3 バックアップのクロスリージョンおよびクロスアカウントバックアップコピーが提供されるようになりました。 詳細については、「Amazon S3 のバックアップ」を参照してください。	2022 年 7 月 28 日
AWS Backup Audit Manager が FSx for ONTAP の追加コントロールサポートを提供	AWS Backup Audit Manager は、バックアップリソースがバックアッププランと最後に作成された復旧ポイントによって保護されているなど、FSx for ONTAP ボリュームのモニタリングと監査をサポートする追加のコントロールを提供するようになりました。https://docs.aws.amazon.com/aws-backup/latest/devguide/controls-and-remediation.html#last-recovery-point-created-control 詳細については、「AWS Backup Audit Manager の制御と改善」を参照してください。	2022 年 7 月 22 日

変更	説明	日付
AWS Backup が PostgreSQL および MySQL クラスターの Amazon RDS マルチ AZ クラスターのバックアップと復元のサポートを追加	AWS Backup は、1 つのプライマリデータベースインスタンスと 2 つの読み取り可能なスタンバイデータベースインスタンスを持つマルチアベイラビリティーゾーンクラスターのバックアップおよび復元オプションを追加しました。 詳細については、「Amazon RDS マルチ AZ バックアップ」を参照してください。	2022 年 7 月 20 日
AWS Backup Audit Manager が復旧ポイント作成の新しいコントロールを追加	AWS Backup Audit Manager は、コンプライアンスサポートを強化するための新しい監査コントロールを提供します。 `Last recovery point created` は、指定された期間内に復旧ポイントが作成されるようにするためのオプションの追加コントロールです。 詳細については、「最後に作成された復旧ポイントのコントロール」を参照してください。	2022 年 1 月 29 日

変更	説明	日付
AWS Backup ゲートウェイエンドポイントのサンプルを追加	AWS Backup Gateway は、ユーザーが VPNs (仮想プライベートネットワーク) に接続する際に役立つサンプルエンドポイントを提供しました。詳細については、AWS Backup「VPC エンドポイントの作成」を参照してください。	2022 年 6 月 14 日
AWS Backup が VMware 用の Amazon VPC エンドポイントの提供を開始	AWS Backup で VMware の Amazon VPC エンドポイントがサポートされるようになりました。これにより、VMware 環境と AWS 間の仮想プライベートネットワークを で使用できます AWS PrivateLink。 詳細については、「ゲートウェイ の作成」と「AWS Backup および AWS PrivateLink」を参照してください。	2022 年 6 月 1 日
AWS Backup Audit Manager が Amazon S3 の追加コントロールサポートを提供	Backup Audit Manager は、S3 リソースタイプの「バックアッププランによって保護されたバックアップリソース」のコンプライアンスコントロールをサポートするようになりました。 詳細については、「AWS Backup Audit Manager の制御と改善」を参照してください。	2022 年 5 月 25 日

変更	説明	日付
AWS Backup Audit Manager が Storage Gateway の追加コントロールサポートを提供	Backup Audit Manager で、Storage Gateway の「リソースタイプのバックアッププランによって保護されたバックアップリソース」のコンプライアンスコントロールをサポートするようになりました。 詳細については、「AWS Backup Audit Manager の制御と改善」を参照してください。	2022 年 5 月 25 日
Amazon FSx for OpenZFS 向けサポート	AWS Backup では、FSx for OpenZFS ファイルシステムのバックアップと復元のためのデータ保護の管理が追加されました。	2022 年 5 月 18 日
AWS Backup VMware の Audit Manager サポート	AWS Backup で Backup Audit Manager のコントロールと修復における仮想マシンのサポートが提供されるようになりました。詳細については、「AWS Backup Audit Manager の制御と改善」を参照してください。	2022 年 5 月 11 日

変更	説明	日付
Amazon FSx がアジアパシフィック (大阪) リージョンで利用開始	AWS Backup では、アジアパシフィック (大阪) リージョンでの Amazon FSx のバックアップと、アジアパシフィック (大阪) リージョンとのクロスリージョンコピーの提供を開始しました。	2022 年 4 月 26 日
Amazon FSx for Lustre Persistent_2 向けサポート	AWS Backup では、Amazon FSx for Lustre の一般提供が開始されました。これは、Persistent_1 ファイルシステムと比較して、ストレージユニットあたりのスループットレベルが高くなります。	2022 年 4 月 5 日
VMware の強化	AWS Backup では、Amazon EBS ボリュームへの復元、ディスクレベルの復元、VMware VMware on のサポートが提供されるようになりました AWS Outposts。詳細については、「仮想マシンの復元」を参照してください。	2022 年 3 月 31 日
AWS Backup アジアパシフィック (ジャカルタ) の可用性	AWS Backup が、アジアパシフィック (ジャカルタ) リージョンのお客様にご利用いただけるようになりました。	2022 年 3 月 17 日

変更	説明	日付
AWS Backup Audit Manager の新しいコントロール	AWS Backup Audit Manager は、クロスリージョンコピー、クロスアカウントコピー、バックアップボールトロックの 3 つの新しい監査コントロールを導入しました。詳細については、「AWS Backup Audit Manager の制御と改善」を参照してください。	2022 年 3 月 17 日
のサポート AWS PrivateLink	for を使用すると AWS Backup、パブリックインターネット経由で接続するのではなく、 AWS PrivateLink VPC のインターフェイスエンドポイント AWS Backup を使用して に直接接続できます。インターフェイスエンドポイントは、オンプレミスまたは別の AWS リージョンにあるアプリケーションから直接アクセスできます。詳細については、「AWS Backup と AWS PrivateLink」を参照してください。	2022 年 2 月 28 日

変更	説明	日付
Amazon Simple Storage Service (Amazon S3) 向けサポート	Amazon S3 AWS Backup のの一般提供 AWS リージョン は、中国 (北京) リージョン、中国 (寧夏) リージョン、 AWS GovCloud （米国西部）、 AWS GovCloud および (米国東部) リージョンを除き、すべての で利用できます。詳細については、「Amazon S3 データの使用」を参照してください。	2022 年 2 月 14 日
AWS 中国リージョンでの高度な DynamoDB バックアップのサポート	高度な DynamoDB バックアップは、中国 (北京) リージョンおよび中国 (寧夏) リージョンで利用可能になりました。詳細については、「高度な DynamoDB バックアップ」を参照してください。	2022 年 1 月 18 日
Amazon S3 のサポートのプレビュー公開	AWS Backup は、Amazon S3 バックアップのパブリックプレビューを提供します。詳細については、「Amazon S3 データの操作」を参照してください。	2021 年 11 月 30 日
VMware 仮想マシン (VM) のサポート	AWS Backup を使用して VMware VMs を自動的にバックアップできるようになりました。詳細については、「仮想マシンのバックアップ」を参照してください。	2021 年 11 月 30 日

変更	説明	日付
高度な DynamoDB バックアップ向けサポート	を使用して AWS Backup 、作成したすべての新しい DynamoDB テーブルのバックアップで、コールドストレージ階層化、コスト配分タグ付け、クロスリージョンコピー、クロスアカウントコピー、従属暗号化、ソース DynamoDB テーブルからのタグのコピーなどの機能を実行できるようになりました。詳細については、アドバンスト DynamoDB バックアップ「Amazon DynamoDB デベロッパーガイド」の「」およびDynamoDB AWS Backup での の使用」を参照してください。	2021 年 11 月 23 日
AWS 中国リージョンでの AWS Backup リソース割り当ての強化のサポート	AWS Backup リソース割り当ての機能強化が、中国 (北京) リージョンおよび中国 (寧夏) リージョンで利用可能になりました。詳細については、「バックアッププランへのリソース割り当て」を参照してください。	2021 年 11 月 16 日

変更	説明	日付
AWS Backup リソース割り当ての機能強化の起動	バックアップリソース割り当ての強化により、数十万の AWS リソースを保護するバックアッププランをデプロイするための、きめ細かなコントロールと新しい合理化されたプロセスが追加されます。この機能を使用すると、 AWS Backupを使用してデータを保護する際のスピード、柔軟性、精度を向上させることができます。詳細については、「バックアッププランへのリソース割り当て」を参照してください。	2021 年 11 月 10 日
Amazon Neptune のサポート	AWS Backup を使用して Amazon Neptune クラスター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、「AWS Backupとは?」を参照してください。	2021 年 11 月 5 日
Amazon DocumentDB のサポート	AWS Backup を使用して Amazon DocumentDB クラスター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、「AWS Backupとは?」を参照してください。	2021 年 11 月 5 日

変更	説明	日付
AWS 中国リージョンでの AWS Backup ボールトロックのサポート	AWS Backup ボールトロックが中国 (北京) リージョンと中国 (寧夏) リージョンで利用可能になりました。詳細については、「AWS Backup ボールトロック」を参照してください。	2021 年 11 月 3 日
AWS Backup ボールトロックの起動	AWS Backup ボールトロックを使用すると、バックアップボールトに保存されている AWS Backup バックアップの削除を防ぐことができます。詳細については、「AWS Backup ボールトロック」を参照してください。	2021 年 10 月 7 日
AWS Backup Audit Manager コンプライアンスレポートの起動	コンプライアンスレポートを使用すると、 AWS Backup Audit Manager フレームワークで定義したコントロールに対するバックアップアクティビティとリソースのコンプライアンスに関する日次レポートを生成できます。詳細については、「コンプライアンスレポートのテンプレート」を参照してください。	2021 年 10 月 5 日

変更	説明	日付
AWS CloudFormation AWS Backup Audit Manager のサポート	では AWS CloudFormation、AWS Backup Audit Manager のフレームワーク、コントロール、レポートプランを安全かつ反復可能な方法で大規模にデプロイできるようになりました。詳細については、「Audit Manager による監査とレポートのバックアップ AWS Backup」を参照してください。	2021 年 10 月 4 日
AWS Backup Audit Manager の起動	AWS Backup Audit Manager では、バックアップアクティビティとリソースのコントロールを定義し、コントロールに準拠していないアクティビティとリソースを特定できるようになりました。 AWS Backup Audit Manager を使用して、定義したコントロールのコンプライアンスの証拠となる日次レポートとオンデマンドレポートを生成することもできます。詳細については、「Audit Manager による監査とレポートのバックアップ AWS Backup」を参照してください。	2021 年 8 月 24 日

変更	説明	日付
新しい非同期の復旧ポイントオペレーションのサポート	AWS Backup は、元の IAM ロールを変更または削除した場合に備えて、バックアップライフサイクルルールを管理するサービスにリンクされたロールを引き受けるようになりました。詳細については、「バックアップの削除」を参照してください。	2021 年 8 月 23 日
Amazon EBS マルチボリュームのクラッシュコンシステントバックアップのサポート	これで、 AWS Backup を使用して Amazon EC2 インスタンスを保護すると、 AWS Backup はデフォルトで各 Amazon EC2 インスタンスにアタッチされているすべての Amazon EBS ボリュームのマルチボリュームのクラッシュコンシステントバックアップを取得します。詳細については、「Amazon EBS マルチボリューム、クラッシュコンシステントバックアップの作成」を参照してください。	2021 年 6 月 14 日

変更	説明	日付
追加での Amazon FSx のサポート AWS リージョン	AWS Backup を使用して、次のリージョンで Amazon FSx ファイルシステムを保護することができるようになりました。 AWS GovCloud (US)、欧州 (ミラノ) リージョン、アフリカ (ケープタウン) リージョン、中東 (バーレーン) リージョン。詳細については、AWS Backup 全般のリファレンスの「AWS エンドポイントとクォータ」を参照してください。	2021 年 4 月 15 日
Amazon FSx クロスリージョンおよびクロスアカウントバックアップのサポート	を使用して AWS Backup 、および アカウント間で AWS リージョン Amazon FSx バックアップをコピーできるようになりました。詳細については、「バックアップコピーの作成」を参照してください。 カスタマー管理ポリシーを使用する場合は、既存のバックアップジョブが失敗しないように、新しいアクセス権限 `fsx:CopyBackup` を追加する必要があります。そのアクセス権限については、「カスタマー管理ポリシー」の「Amazon FSx バックアップポリシー」の最後のステートメントを参照してください。	2021 年 4 月 12 日

変更	説明	日付
Amazon EFS バックアップのコスト配分タグのサポート	コスト配分タグを使用して、Amazon EFS バックアップのコストを詳細レベルで追跡し、 を使用してそれらのタグを表示およびフィルタリングできるようになりましたAWS Cost Explorer。詳細については、「コスト配分タグの使用」を参照してください。	2021 年 4 月 7 日
FedRAMP High 認証	AWS Backup は、FedRAMP High ワークロードをサポートすることが承認されました。詳細については、「コンプライアンスプログラムによる対象範囲内のAWS サービス」を参照してください。	2021 年 3 月 25 日
新規 AWS リージョン	AWS Backup がアジアパシフィック (大阪) リージョンで利用可能になりました。このリージョンで、 AWS Backup は現在 Storage Gateway、Amazon FSx、クロスアカウントバックアップは、このリージョンでサポートされていません。詳細については、AWS Backup 全般のリファレンスの「AWS エンドポイントとクォータ」を参照してください。	2021 年 3 月 25 日

変更	説明	日付
復旧ポイントのバッチ操作のサポート	AWS Backup コンソールを使用してバッチオペレーションを自動化し、バックアップボールトの復旧ポイントをクリーンアップできるようになりました。詳細については、「バックアップの削除」を参照してください。	2021 年 3 月 23 日
Amazon EFS ワンゾーンストレージクラスへの復元をサポート	Amazon EFS バックアップを Amazon EFS ワンゾーンストレージクラスに復元できるようになりました。詳細については、「Amazon EFS ファイルシステムの復元」を参照してください。	2021 年 3 月 12 日
Amazon Relational Database Service point-in-time の復元と継続的バックアップのサポート	スナップショットバックアップのオーケストレーションに加えて、 AWS Backup を使用して Amazon RDS の継続的バックアップを自動化し、point-in-time 復元 (PITR) を実行できるようになりました。詳細については、「リカバリを使用した指定された時刻への point-in-time 復元」を参照してください。	2021 年 3 月 10 日

変更	説明	日付
Amazon のサポート CloudWatch	CloudWatch を使用して AWS Backup メトリクスをモニタリングできるようになりました。詳細については、「Amazon と Amazon によるイベント CloudWatch とメトリクスのモニタリング EventBridge」を参照してください。	2021 年 2 月 3 日
Amazon のサポート EventBridge	EventBridge を使用して AWS Backup イベントをモニタリングできるようになりました。詳細については、「Amazon と Amazon によるイベント CloudWatch とメトリクスのモニタリング EventBridge」を参照してください。	2021 年 2 月 3 日
クロスアカウントバックアップのサポート	を使用して AWS Backup 、複数の にまたがるリソースをバックアップできるようになりました AWS アカウント。詳細については、AWS 「アカウント間でのバックアップコピーの作成」を参照してください。	2020 年 11 月 18 日
Amazon FSx ファイルシステムのバックアップおよび復元サポート	AWS Backup を使用して Amazon FSx ファイルシステム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、「Amazon FSx ファイルシステムの操作」を参照してください。	2020 年 11 月 9 日

変更	説明	日付
新規 AWS リージョン	AWS Backup がアフリカ (ケープタウン) および欧州 (ミラノ) で利用可能になりました AWS リージョン。詳細については、「AWS 全般のリファレンス」の「AWS Backup エンドポイントとクォータ」を参照してください。	2020 年 10 月 21 日
VSS 対応 Windows バックアップのサポート	Amazon EC2 インスタンスで実行されている VSS (Volume Shadow Copy Service) 対応の Windows アプリケーションをバックアップおよび復元できるようになりました。詳細については、「Windows VSS バックアップの作成」を参照してください。	2020 年 9 月 22 日
Amazon EFS 自動バックアップのサポート	AWS Backup を使用して Amazon EFS ファイルシステムを自動的にバックアップできるようになりました。詳細については、「使用開始 4: Amazon EFS 自動バックアップの作成」を参照してください。	2020 年 7 月 16 日
新規 AWS リージョン	AWS Backup が で利用可能になりました AWS GovCloud (US) Region。詳細については、「AWS 全般のリファレンス」の「AWS Backup エンドポイントとクォータ」を参照してください。	2020 年 6 月 24 日

変更	説明	日付
複数の にまたがるバックアップの管理のサポート AWS アカウント	を使用して、複数の にまた AWS アカウント がるバックアップを管理できるようになりましたAWS Organizations。詳細については、「クロスアカウント管理の仕組み」を参照してください。	2020 年 6 月 24 日
Amazon Aurora のサポートが に追加されました AWS Backup	Amazon Aurora のリソースをバックアップ AWS Backup するように を設定できるようになりました。詳細については、Amazon Aurora のユーザーガイドの「Aurora DB クラスターのバックアップと復元の概要」を参照してください。	2020 年 6 月 10 日
と連携するサービスの設定のサポート AWS Backup	特定の AWS サービスのリソースをバックアップ AWS Backup するように を設定できるようになりました。詳細については、「 で のサービスの管理にオプトインする AWS Backup」を参照してください。	2020 年 5 月 20 日
Amazon EC2 インスタンスのバックアップをサポート、およびリージョン間のバックアップのサポートも追加	Amazon EC2 インスタンス全体をバックアップし、 AWS リージョン間でのリソースもコピーできるようになりました。詳細については、「AWS リージョン間でのバックアップコピーの作成」を参照してください。	2020 年 1 月 13 日

変更	説明	日付
新規ガイド	AWS は AWS Backup と AWS Backup デベロッパーガイドを起動します。	2019 年 1 月 15 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。