



Amazon FSx for NetApp ONTAP

を使用します

Amazon FSx for NetApp ONTAP

NetApp
February 11, 2026

目次

Amazon FSx for NetApp ONTAP を使用します	1
NetApp Workload Factory で FSx for ONTAPのコスト削減を検討	1
電卓オプション	1
カスタマイズによるコスト削減の詳細	1
検出されたストレージ環境の削減効果を確認する	3
FSx for ONTAPファイルシステムの導入	6
NetApp Workload Factoryでリソースのコストを追跡する	6
リンクを使用	7
NetApp Workload Factoryのリンクについて学ぶ	7
LambdaリンクでFSx for ONTAPファイルシステムに接続	9
ワークロードファクトリーのリンクを管理する	15
Workload Factory でキャッシュボリュームを検出する	18
ボリュームの管理	19
Workload Factory で FSx for ONTAPボリュームを作成する	19
FSx for ONTAPのファイルシステムデータへのアクセス	25
ブロックストレージリソースを作成する	26
NetApp Workload Factory でファイルシステムのイニシエータグループを作成する	26
NetApp Workload Factoryでファイルシステム用のブロックデバイスを作成する	27
FSx for ONTAPファイルシステム用Storage VMの作成	29
Storage VM を作成	29
データを保護	30
NetApp Workload Factoryにおけるデータ保護の種類	30
スナップショットを使用する	32
オブジェクトストレージへのバックアップを使用する	36
レプリケーションを使用する	38
AIを搭載したNetAppの自律型ランサムウェア保護でデータを保護	42
NetApp Workload Factoryでボリュームをクローンする	46
NetApp Workload Factory でオンプレミスのONTAPクラスタ データを使用する	46
サイバーボルトでデータを保護	50

Amazon FSx for NetApp ONTAP を使用します

NetApp Workload Factory で FSx for ONTAPのコスト削減を検討

Amazon Elastic Block Store (EBS) 、 Elastic File System (EFS) 、 FSx for Windows ファイルサーバを使用するストレージワークロードと FSx for NetApp ONTAPを使用するストレージワークロードの削減効果をご確認ください。

NetApp Workload Factory には、 Amazon ストレージ環境と FSx for ONTAPを比較するためのストレージ節約計算ツールが含まれています。 AWS 認証情報の提供の有無にかかわらず節約を検討し、ストレージ環境の構成設定をカスタマイズできます。 AWS 認証情報を提供すると、たとえば Amazon Elastic Block Store のインスタンスを 1 つ以上選択し、 Workload Factory に自動的に比較させることができます。手動でも自動でも、計算機はストレージのニーズに対してどのストレージ サービスが最も低コストであるかを決定します。

ストレージ計算ツールによって最もコスト効率の高いストレージが FSx for ONTAPであることが判明した場合は、 Workload Factory に付与する権限に関係なく、 FSx for ONTAP構成を作成または保存し、 Codebox を使用して Infrastructure-as-Code テンプレートを生成できます。

電卓オプション

お客様のシステムとFSx for ONTAPのコストを比較するために、 Amazonストレージ環境のカスタマイズと自動検出という2つの計算ツールオプションが用意されています。

カスタマイズによる削減効果の詳細：ストレージ環境の構成設定（ユースケース、 リージョン、 ボリュームまたはファイルシステムの数、 ストレージ容量、 Snapshotの頻度、 Snapshotあたりの変更量、 プロビジョニングされたIOPS、 スループットなど）を指定できます。

検出されたストレージ環境の節約を検討: Workload Factory は既存の AWS ストレージ環境にリンクし、 詳細を計算ツールに取り込んで自動的に比較します。自動モードを使用するには、自動化権限を付与する必要があります。ユースケースは変更できますが、 その他のすべての詳細は計算で自動的に決定されます。

さらに、 計算機分析の精度を向上させることができます "[AWS クレデンシャルを追加](#)"。を選択します。 [クレデンシャルの追加] ページにリダイレクトされます。クレデンシャルを追加したら、 **FSx for ONTAP** と比較する既存のリソースを選択し、 [削減効果を確認する]*を選択します。

カスタマイズによるコスト削減の詳細

タブに表示されるストレージの選択手順に従います。

Amazon Elastic Block Store (EBS)

手順

1. いずれかを使用してログインし"コンソールエクスペリエンス"ます。
2. メニューを選択  次に*ストレージ*を選択します。
3. [ストレージ] メニューから [節約の検討] を選択し、[Amazon Elastic Block Store (EBS)] タブを選択します。
4. Storage Savings Calculatorで、次の詳細を入力します。
 - a. ユースケース：必須。ドロップダウンメニューからユースケースを選択します。選択したユースケースに基づいて、FSx for ONTAPファイルシステムの特性を比較します。
 - b. リージョン：オプション。ドロップダウンメニューからEBS設定のリージョンを選択します。
 - c. * EBSボリュームタイプを選択*：オプション。構成に使用するEBSボリュームタイプを選択します。
 - d. ボリューム数：オプション。EBS構成内のボリューム数を入力します。
 - e. ボリュームあたりのストレージ容量 (TiB)：オプション。ボリュームあたりのストレージ容量をTiB単位で入力します。
 - f. * Snapshotの頻度*：オプション。EBS構成のスナップショット頻度を選択します。
 - g. * Snapshotあたりの変更量 (GiB) *：オプション。Snapshotストレージの場合のみ。Snapshotあたりの変更量をGiB単位で入力します。
 - h. *ボリュームあたりのプロビジョニングIOPS *：オプション。gp3、io1、およびio2ボリュームの場合。ボリュームあたりのプロビジョニングIOPSを入力します。
 - i. スループット (MiB/秒)：オプション。gp3ボリュームの場合のみ。ボリュームあたりのスループット (MiB/秒) を入力します。

Amazon FSx for Windows ファイルサーバ

手順

1. いずれかを使用してログインし"コンソールエクスペリエンス"ます。
2. メニューを選択  次に*ストレージ*を選択します。
3. [ストレージ] メニューから [節約の検討] を選択し、[Amazon Elastic Block Store (EBS)] タブを選択します。
4. Storage Savings Calculatorで、次の詳細を入力します。
 - a. ユースケース：必須。ドロップダウンメニューからユースケースを選択します。選択したユースケースに基づいて、FSx for ONTAPファイルシステムの特性を比較します。
 - b. リージョン：オプション。FSx for Windowsファイルサーバ構成のリージョンをドロップダウンメニューから選択します。
 - c. 導入タイプ：オプション。または[複数のアベイラビリティゾーン]*を選択します。
 - d. ストレージタイプ：SSDストレージタイプがデフォルトで選択されています。
 - e. ストレージ容量 (TiB)：オプション。構成のストレージ容量を入力します。
 - f. 重複排除による削減量 (%)：オプション。重複排除によって削減できる容量の割合を入力しま

す。

- g. * Snapshotの頻度*：オプション。構成に応じたスナップショットの頻度を選択します。
- h. * Snapshotあたりの変更量 (GiB) *：オプション。Snapshotストレージの場合のみ。Snapshotあたりの変更量をGiB単位で入力します。
- i. *プロビジョニングされたSSD IOPS *：オプション。[Provisioned SSD IOPS]を入力します。
- j. スループット (**MiB/秒**)：オプション。スループットをMiB/秒単位で入力します。

Amazon Elastic File System (EFS)

手順

1. いずれかを使用してログインし "[コンソールエクスペリエンス](#)" ます。
2. メニューを選択  次に*ストレージ*を選択します。
3. [ストレージ] メニューから [節約の検討] を選択し、[Amazon Elastic Block Store (EBS)] タブを選択します。
4. Storage Savings Calculatorで、次の詳細を入力します。
 - a. ユースケース：必須。ドロップダウンメニューからユースケースを選択します。選択したユースケースに基づいて、FSx for ONTAPファイルシステムの特性を比較します。
 - b. リージョン：オプション。FSx for Windowsファイルサーバ構成のリージョンをドロップダウンメニューから選択します。
 - c. ファイルシステムタイプ：オプション。地域*または* 1ゾーン*を選択します。
 - d. ストレージ容量 (**TiB**)：オプション。EFS構成のストレージ容量を入力します。
 - e. アクセス頻度の高いデータ (%)：オプション。アクセス頻度の高いデータの割合を入力します。
 - f. スループットモード：オプション。または[弹性スループット]*を選択します。
 - g. スループット (**MiB/秒**)：オプション。スループットをMiB/秒単位で入力します。

ストレージシステム構成の詳細を指定したら、ページに表示される計算方法と推奨事項を確認します。

さらに、次のいずれかを選択して、ページの一番下までスクロールしてレポートを表示します。

- * PDFのエクスポート*
- 電子メールで送信
- 計算結果を表示

FSx for ONTAPに切り替えるには、の手順に従います [FSx for ONTAPファイルシステムの導入](#)。

検出されたストレージ環境の削減効果を確認する

開始する前に

Workload FactoryがAWSアカウント内のAmazon Elastic Block Store (EBS)、Elastic File System (EFS)、およびFSx for Windows File Serverストレージ環境を検出するには、次のことを確認してください。["表示、計画、分析の権限を付与する" AWS アカウント](#)で。



この計算ツールオプションでは、EBSスナップショットとFSx for Windows File Serverシャドウコピーの計算はサポートされていません。カスタマイズによるコスト削減を検討する場合は、EBSとFSx for Windows File Serverスナップショットの詳細を提供できます。

タブに表示されるストレージの選択手順に従います。

Amazon Elastic Block Store (EBS)

手順

1. いざれかを使用してログインし"コンソールエクスペリエンス"ます。
2. メニューを選択  次に*ストレージ*を選択します。
3. [ストレージ] メニューから [節約の検討] を選択し、[Amazon Elastic Block Store (EBS)] タブを選択します。
4. タブで、**FSx for ONTAP**と比較するインスタンスを選択し、[Explore savings]*を選択します。
5. Storage Savings Calculatorが表示されます。選択したインスタンスに基づいて、ストレージシステムの次の特性が事前に入力されています。
 - a. ユースケース：構成のユースケース。必要に応じてユースケースを変更できます。
 - b. 選択したボリューム：EBS構成内のボリュームの数
 - c. 合計ストレージ容量 (**TiB**)：ボリュームあたりのストレージ容量 (TiB)
 - d. *合計プロビジョニングIOPS *：gp3、io1、およびio2のボリューム
 - e. 合計スループット (**MiB/秒**)：gp3ボリュームのみ

Amazon FSx for Windows ファイルサーバー

手順

1. いざれかを使用してログインし"コンソールエクスペリエンス"ます。
2. メニューを選択  次に*ストレージ*を選択します。
3. [ストレージ] メニューから [節約の検討] を選択し、[Amazon FSx for Windows ファイル サーバー] タブを選択します。
4. [Amazon FSx for Windows File Server*]タブで、FSx for ONTAPと比較するインスタンスを選択し、*[Explore savings]*を選択します。
5. Storage Savings Calculatorが表示されます。選択したインスタンスの導入タイプに基づいて、ストレージシステムの次の特性があらかじめ設定されています。
 - a. ユースケース：構成のユースケース。必要に応じてユースケースを変更できます。
 - b. 選択されたファイルシステム
 - c. 合計ストレージ容量 (**TiB**)
 - d. *プロビジョニングされたSSD IOPS *
 - e. スループット (**MiB/秒**)

Amazon Elastic File System (EFS)

手順

1. いざれかを使用してログインし"コンソールエクスペリエンス"ます。
2. メニューを選択  次に*ストレージ*を選択します。
3. [ストレージ] メニューから [節約の検討] を選択し、[Amazon Elastic File System (EFS)] タブを選択します。

4. [Elastic File System (EFS)]タブで、FSx for ONTAPと比較するインスタンスを選択し、*[Explore savings (削減効果を確認)]*を選択します。
5. Storage Savings Calculatorが表示されます。選択したインスタンスに基づいて、ストレージシステムの次の特性が事前に入力されています。
 - a. ユースケース：構成のユースケース。必要に応じてユースケースを変更できます。
 - b. ファイル・システムの総数
 - c. 合計ストレージ容量 (TiB)
 - d. 合計プロビジョニングスループット (MiB/秒)
 - e. 弾性スループットの合計-読み取り (GiB)
 - f. 合計柔軟性に優れたスループット-書き込み (GiB)

ストレージシステム構成の詳細を指定したら、ページに表示される計算方法と推奨事項を確認します。

さらに、次のいずれかを選択して、ページの一番下までスクロールしてレポートを表示します。

- * PDFのエクスポート*
- 電子メールで送信
- 計算結果を表示

FSx for ONTAPファイルシステムの導入

コスト削減を実現するためにFSx for ONTAPに切り替えたい場合は、FSx for ONTAPファイルシステムの作成ウィザードからファイルシステムを直接作成する場合は*作成*を選択し、推奨構成を後で保存する場合は*保存*を選択します。

導入方法

`automate` モードでは、Workload Factory から FSx for ONTAPファイルシステムを直接デプロイできます。また、Codebox ウィンドウからコンテンツをコピーし、Codebox メソッドのいずれかを使用してシステムを展開することもできます。

`_basic_mode`では、Codebox ウィンドウからコンテンツをコピーし、いずれかのCodeboxメソッドを使用してFSx for ONTAPファイルシステムを導入できます。

NetApp Workload Factoryでリソースのコストを追跡する

NetApp Workload Factoryを使用して、FSx for ONTAPファイルシステムのコストと使用状況を統合ビューで追跡します。コストデータは、予算を管理し、リソースを効率的に最適化するのに役立ちます。AWS Cost Explorer はコストデータを提供します。

タスクの内容

FSx for ONTAPファイルシステムリソースのコストと使用状況データは、次の権限を使用して AWS Cost Explorer から抽出されます。

- `ce:GetCostAndUsage`

- ce:GetTags

開始する前に

"_表示、計画、分析_権限ポリシーで資格情報を付与します"Workload Factory で FSx for ONTAPのコストを追跡します。

手順

1. いざれかを使用してログインし"コンソールエクスペリエンス"ます。
2. メニューを選択  次に*ストレージ*を選択します。
3. ストレージメニューから*コスト*を選択します。
4. [コスト] ページで、次の情報を入力して、FSx for ONTAPリソースのコストと容量データをフィルタリングします。
 - a. AWS アカウント: コストデータを表示するアカウントを選択します。
 - b. 資格情報: _表示、計画、および分析_権限を持つ資格情報を選択します。
 - c. リージョン: コストデータを表示する AWS リージョンを選択します。
 - d. コスト データ範囲: 表示するコスト データの期間を選択します。
5. FSx for ONTAPリソースの コストの詳細 を表示します。

リンクを使用

NetApp Workload Factoryのリンクについて学ぶ

NetApp Workload Factory リンクは、Workload Factory アカウントと 1 つ以上の FSx for ONTAPファイルシステムの間に信頼関係と接続を作成します。これにより、Amazon FSx for ONTAP API では利用できない特定のファイルシステム機能を、ONTAP REST API 呼び出しから直接監視および管理できるようになります。

Workload Factory の使用を開始するためにリンクは必要ありませんが、場合によっては、Workload Factory のすべての機能とワークロード機能のロックを解除するためにリンクを作成する必要があります。

リンクが有益な理由

リンクを使用すると、Workload Factory がAmazon FSx for ONTAP API を通じてネイティブに利用できない操作を実行できるようになるため、便利です。リンクにより、高度なONTAP機能と自動化が可能になり、FSx for ONTAPファイルシステムの管理が強化されます。

リンクを使用する利点は次のとおりです。

- このリンクにより、NetAppコンソールはONTAPコマンドを FSx for ONTAPファイルシステムに直接送信できるようになり、AWS がネイティブに提供する機能を超える高度なONTAP機能が利用できるようになります。
- リンクはAWS Lambdaを活用してイベントに応答するコードを実行します。このサーバーレスアプローチにより、VPC内で実行されるインスタンスへの依存が排除されます。

リンクの仕組み

リンクはAWS Lambdaを利用します。Lambdaはイベントに応じてコードを実行し、そのコードに必要なコンピューティングリソースを自動的に管理します。作成したリンクはNetAppアカウントの一部であり、AWSアカウントに関連付けられています。

リンクを作成したら、それを1つまたは複数のFSx for ONTAPファイルシステムに関連付けることができます。各ファイルシステムは、同じNetAppアカウント内の1つのリンクにのみ関連付けることができます。複数のNetAppアカウントがある場合は、1つのファイルシステムを別々のNetAppアカウントの下にある追加のリンクに関連付けることができます。

Workload Factory のストレージワーククロードからリンクを作成し、関連付けます。

Workload Factory 認証情報サービスに保存されている認証情報、またはAWS Secrets Manager に保存されている認証情報を使用してリンクを認証できます。ワークロードファクトリーは認証モードの変更をサポートしていません。

コスト

Lambdaが実行するトランザクションごとに料金が発生します。Lambdaは2つのシステム間のプロキシとして機能するため、Lambdaがファイルシステム上のONTAP REST APIにリクエストを送信するとき、および応答をWorkload Factoryに返すときに料金が発生します。

["AWS Lambdaの使用に関するコストの詳細を確認する"](#)

リンクが必要な場合

ワークロードファクトリーでは、情報を表示したりタスクを実行したりするためのリンクが必要です。リンクを必要とする操作を実行しようとしたが、FSx for ONTAPファイルシステムにリンクが関連付けられていない場合、Workload Factoryは操作にリンクが必要であることを通知します。

リンクが必要な機能は次のとおりです。

- プロアクティブなメンテナンス、信頼性、コストパフォーマンスの最適化を実現するFSx for ONTAPファイルシステム構成の適切なアーキテクチャの状態
- ONTAP EMSイベント監視とアラート
- NetApp自律型ランサムウェア保護(ARP/AI)
- FSx for ONTAPファイルシステム全体の容量の総合的な観測性が強化されました
- ボリュームおよびストレージVMデータのレプリケーション、管理、および監視
- SMB/CIFS共有およびNFSエクスポートポリシーのプロビジョニングと管理
- FSx for ONTAPファイルシステムでのiSCSIボリュームの管理
- カスタム保護SLAのスナップショットポリシーの作成と管理
- 自動容量管理のためのiノード管理の強化
- 弾力的なスケーリングのためのボリューム自動拡張
- クローンの作成と管理により、即時にインプレースでデータのクローンを作成できます。
- ONTAPバージョンなどの追加メトリックをONTAPから直接表示する

方法をご確認ください["FSx for ONTAPファイルシステムへのリンクを接続する"。](#)

LambdaリンクでFSx for ONTAPファイルシステムに接続

高度なONTAP管理操作を実行するには、Workload Factory アカウントと 1つ以上のFSx for ONTAPファイルシステム間の接続を設定します。これには、新しいLambdaリンクと既存のLambdaリンクの関連付けと、リンクの認証が含まれます。リンクの関連付けにより、Amazon FSx for ONTAP API 経由では利用できない特定の機能を FSx for ONTAPファイルシステムから直接監視および管理できます。

"リンクの詳細"です。

タスクの内容

リンクはAWS Lambdaを利用してイベントに応じてコードを実行し、そのコードに必要なコンピューティングリソースを自動的に管理します。作成したリンクはNetAppアカウントの一部であり、AWSアカウントに関連付けられています。

FSx for ONTAPファイルシステムを定義するときに、アカウントにリンクを作成できます。リンクはそのファイルシステムに使用され、他のFSx for ONTAPファイルシステムにも使用できます。後でファイルシステムのリンクを関連付けることもできます。

リンクには認証が必要です。Workload Factory 認証情報サービスに保存されている認証情報、またはAWS Secrets Managerに保存されている認証情報を使用してリンクを認証できます。リンクごとに1つの認証方法のみがサポートされます。たとえば、AWS Secrets Managerを使用したリンク認証を選択した場合、後で認証方法を変更することはできません。



コンソールエージェントを使用する場合、AWS Secrets Managerはサポートされません。

新しいリンクの関連付け

新しいリンクの関連付けには、リンクの作成と関連付けが含まれます。

このワークフローでリンクを作成するには、自動または手動の2つのオプションがあります。リンクを作成するには、AWSアカウントでAWS CloudFormationスタックを起動する必要があります。

- 自動: Workload Factory 経由で自動登録してリンクを作成します。自動的に作成されたリンクには、Workload Factory自動化用のトークンが必要であり、CloudFormationコードの有効期間は短くなります。最大6時間までしか使用できません。
- 手動: CodeboxからCloudFormationまたはTerraformを使用して手動で登録し、リンクを作成します。コードが存続し、操作を完了するための時間が延長されます。これは、セキュリティやDevOpsなどのさまざまなチームと連携して作業する場合に便利です。これらのチームには、リンクの作成を完了するために必要な権限を最初に付与する必要があります。

開始する前に

- どのリンク作成オプションを使用するかを検討する必要があります。
- Workload Factoryには少なくとも1つのFSx for ONTAPファイルシステムが必要です。FSx for ONTAPファイルシステムを検出するには、FSx for ONTAPインスタンスに対する権限を持つAWSアカウントが必要です。["Workload Factoryに資格情報を追加する"ストレージ管理の_表示、計画、および分析_権限を持ちます。](#)

- ・リンク接続のために、FSx for ONTAP ファイルシステムに関連付けられたセキュリティ グループで次のポートが開いている必要があります。
 - Workload Factory コンソールの場合: ポート 443 (HTTPS)
 - CloudShell および FSx for ONTAP緊急管理システム (EMS) イベント分析の場合: ポート 22 (SSH)
- ・リンクは次のエンドポイントに接続できる必要があります: <https://api.workloads.netapp.com>.Webベースのコンソールは、このエンドポイントに接続して Workload Factory API と対話し、FSx for ONTAPワークロードを管理および操作します。
- ・CloudFormationスタックを使用してリンクを追加する場合は、AWSアカウントで次の権限が必要です。

```

"cloudformation:GetTemplateSummary",
"cloudformation>CreateStack",
"cloudformation>DeleteStack",
"cloudformation:DescribeStacks",
"cloudformation>ListStacks",
"cloudformation:DescribeStackEvents",
"cloudformation>ListStackResources",
"ec2:DescribeSubnets",
"ec2:DescribeSecurityGroups",
"ec2:DescribeVpcs",
"iam>ListRoles",
"iam:GetRolePolicy",
"iam:GetRole",
"iam:DeleteRolePolicy",
"iam>CreateRole",
"iam:DetachRolePolicy",
"iam:PassRole",
"iam:PutRolePolicy",
"iam:DeleteRole",
"iam:AttachRolePolicy",
"lambda:AddPermission",
"lambda:RemovePermission",
"lambda:InvokeFunction",
"lambda:GetFunction",
"lambda>CreateFunction",
"lambda:DeleteFunction",
"lambda:TagResource",
"codestar-connections:GetSyncConfiguration",
"ecr:BatchGetImage",
"ecr:GetDownloadUrlForLayer"

```

自動作成

CloudFormation を使用して、Workload Factory 内でリンクを自動的に作成して登録します。

手順

1. いずれかを使用してログインし"コンソールエクスペリエンス"ます。
2. メニューを選択  次に*ストレージ*を選択します。
3. [ストレージ] メニューから、**FSx for ONTAP** を選択します。
4. *FSx for ONTAP*から、リンクを関連付けるファイルシステムのアクションメニューを選択し、*リンクの関連付け*を選択します。
5. [リンクの関連付け]ダイアログで、[新しいリンクの作成]*を選択し、[続行]*を選択します。
6. [Create Link]ページで、次の情報を指定します。
 - a. リンク名：このリンクに使用する名前を入力します。名前はアカウント内で一意である必要があります。
 - b. **AWS Secrets Manager**: オプション。Workload Factory が AWS Secrets Manager から FSx for ONTAP アクセス認証情報を取得できるようにします。

リンク デプロイメント スタックは、次のデフォルトのシークレット マネージャー ARN 正規表現を Lambda アクセス許可ポリシーに自動的に追加します。

`arn:aws:secretsmanager:<link_deployment_region>:<link_deployment_account_id>:secret:FSxSecret*`

デフォルトの権限に合わせてシークレットを作成するか、リンクポリシーにカスタムの権限を割り当てることができます。

- VPCプライベートエンドポイントをAWS Secrets Managerに設定*はデフォルトで無効になっています。このオプションを選択すると、シークレットはローカルではなくVPCプライベートエンドポイントを使用して格納されます。
- c. リンクの権限: リンクの権限について、次のいずれかのオプションを選択します。
 - 自動: このオプションを選択すると、AWS CloudFormation コードによって Lambda アクセス許可ポリシーと実行ロールが自動的に作成されます。
 - ユーザー指定: 指定したLambda実行ロールとそれに紐付けられたポリシーをLambdaリンクに割り当てるには、このオプションを選択します。Lambdaには以下の権限が必要です。`secretsmanager:GetSecretValue` AWS Secrets Manager を有効にした場合にのみ、権限が必要です。

```
"ec2:CreateNetworkInterface",
"ec2:DescribeNetworkInterfaces",
"ec2>DeleteNetworkInterface",
"ec2:AssignPrivateIpAddresses",
"ec2:UnassignPrivateIpAddresses",
"secretsmanager:GetSecretValue"
```

テキストボックスに Lambda 実行ロール ARN を入力します。

- d. タグ: 必要に応じて、リソースをより簡単に分類できるように、このリンクに関連付けるタグを追加します。たとえば、FSx for ONTAPファイルシステムでこのリンクが使用されていることを示すタグを追加できます。

ワークロードファクトリーは、FSx for ONTAPファイルシステムに基づいて、AWS アカウント、場所、セキュリティグループを自動的に取得します。

7. 「* Create *」を選択します。

「CloudFormation にリダイレクト」ダイアログが表示され、AWS CloudFormation サービスからリンクを作成する方法が説明されます。

8. [続行]*を選択して AWS 管理コンソールを開き、この FSx for ONTAP ファイルシステムの AWS アカウントにログインします。

9. [Quick create stack] ページの [Capabilities] で、*[I acknowledge that AWS CloudFormation might create IAM resources]*を選択します。

CloudFormation テンプレートを起動すると、Lambda に 3 つの権限が付与されます。Workload Factory では、リンクの使用時にこれらの権限が使用さ

```
"lambda:InvokeFunction",
"lambda:GetFunction",
"lambda:UpdateFunctionCode"
```

10. を選択し、[続行]*を選択します。

リンク作成ステータスはイベント ページで監視できます。これには 5 分もかかりません。

11. Workload Factory インターフェイスに戻ると、リンクが FSx for ONTAP ファイルシステムに関連付けられていることがわかります。

手動で作成

Codebox の 2 つの Infrastructure-as-Code (IaC) ツール、CloudFormation または Terraform を使用してリンクを作成できます。このオプションを使用すると、AWS CloudFormation からリンクの ARN を抽出し、ここで報告します。ワークロード ファクトリーがリンクを手動で登録します。

手順

1. いずれかを使用してログインし "コンソールエクスペリエンス" ます。
2. メニューを選択  次に *ストレージ* を選択します。
3. [ストレージ] メニューから、**FSx for ONTAP** を選択します。
4. *FSx for ONTAP* から、リンクを関連付けるファイルシステムのアクション メニューを選択し、*リンクの関連付け* を選択します。
5. [リンクの関連付け] ダイアログで、【新しいリンクの作成】*を選択し、[続行]*を選択します。
6. [リンクの作成] ページで、コードボックスから CloudFormation または Terraform を選択し、次の情報を入力します。

- a. リンク名：このリンクに使用する名前を入力します。名前はアカウント内で一意である必要があります。
- b. **AWS Secrets Manager**: オプション。 Workload Factory が AWS Secrets Manager から FSx for ONTAPアクセス認証情報を取得できるようにします。

リンク デプロイメント スタックは、次のデフォルトのシークレット マネージャー ARN 正規表現を Lambda アクセス許可ポリシーに自動的に追加します。

```
arn:aws:secretsmanager:<link_deployment_region>:<link_deployment_account_id>:secret:FSxSecret*
```

デフォルトの権限に合わせてシークレットを作成するか、リンクポリシーにカスタムの権限を割り当てることができます。

- VPCプライベートエンドポイントをAWS Secrets Managerに設定*はデフォルトで無効になっています。このオプションを選択すると、シークレットはローカルではなくVPCプライベートエンドポイントを使用して格納されます。
- c. リンクの権限: リンクの権限について、次のいずれかのオプションを選択します。
 - 自動: このオプションを選択すると、AWS CloudFormation コードによって Lambda アクセス許可ポリシーと実行ロールが自動的に作成されます。
 - ユーザー指定: 指定したLambda実行ロールとそれに紐付けられたポリシーをLambdaリンクに割り当てるには、このオプションを選択します。Lambdaには以下の権限が必要です。
secretsmanager:GetSecretValue AWS Secrets Manager を有効にした場合にのみ、権限が必要です。

```
"ec2:CreateNetworkInterface",
"ec2:DescribeNetworkInterfaces",
"ec2:DeleteNetworkInterface",
"ec2:AssignPrivateIpAddresses",
"ec2:UnassignPrivateIpAddresses"
"secretsmanager:GetSecretValue"
```

テキストボックスに Lambda 実行ロール ARN を入力します。

- d. タグ: 必要に応じて、リソースをより簡単に分類できるように、このリンクに関連付けるタグを追加します。たとえば、FSx for ONTAPファイルシステムでこのリンクが使用されていることを示すタグを追加できます。
- e. リンクの登録: リンクの登録方法については、CloudFormation または Terraform を選択し、指示に従います。

CloudFormationテンプレートを起動すると、Lambdaに3つの権限が付与されます。Workload Factoryでは、リンクの使用時にこれらの権限が使用さ

```
"lambda:InvokeFunction",
"lambda:GetFunction",
"lambda:UpdateFunctionCode"
```

- + スタックが正常に作成されたら、テキストボックスにLambda ARNを貼り付けます。
- a. ワークロードファクトリーは、FSx for ONTAPファイルシステムに基づいて、AWS アカウント、場所、セキュリティグループを自動的に取得します。
 7. 「* Create *」を選択します。
- リンク作成ステータスはイベント ページで監視できます。これには 5 分もかかりません。
8. Workload Factory インターフェイスに戻ると、リンクが FSx for ONTAPファイル システムに関連付けられていることがわかります。

結果

ワークロード ファクトリーは、リンクを FSx for ONTAPファイル システムに関連付けます。高度なONTAP操作を実行できます。

既存のリンクを**FSx for ONTAP**ファイルシステムに関連付ける

リンクを作成したら、1つ以上のFSx for ONTAPファイルシステムに関連付けます。

手順

1. いずれかを使用してログインし"コンソールエクスペリエンス"ます。
2. メニューを選択  次に*ストレージ*を選択します。
3. [ストレージ] メニューから、**FSx for ONTAP** を選択します。
4. *FSx for ONTAP*から、リンクを関連付けるファイルシステムのアクションメニューを選択し、*リンクの関連付け*を選択します。
5. [リンクの関連付け]ページで*を選択し、リンクを選択して[続行]*を選択します。
6. 認証モードを選択します。
 - Workload Factory：パスワードを2回入力します。
 - AWS Secrets Manager：シークレットARNを入力します。

filesystemID はオプションですが、シークレット ARN に次の有効なキー ペアが含まれていることを確認します。

- *filesystemID* = FSx_filesystem_id (オプション)
- ユーザー = FSx_user
- password = user_password



AWS Secrets Manager を使用した認証には、指定した *FSx_user* または FSx for ONTAPファイルシステムで作成された別のユーザーが必要です。デフォルトのユーザーは `fsxadmin` ユーザーを指定しない場合は、

7. * 適用 * を選択します。

結果

リンクはFSx for ONTAPファイルシステムに関連付けられています。高度なONTAP処理を実行できます。

AWS Secrets Managerのリンク認証に関する問題のトラブルシューティング

問題

リンクにシークレットを取得する権限がありません。

解決策：リンクがアクティブになった後に権限を追加します。AWSコンソールにログインし、Lambdaリンクを見つけて、添付されている権限ポリシーを編集します。

問題

その秘密は見つからない。

解決策：正しいシークレットARNを指定します。

問題

その秘密は正しい形式ではない。

解決方法：AWS Secrets Managerに移動して形式を編集します。

シークレットには、次のキー有効なペアが含まれている必要があります。

- filesystemID = fsx_filesystem_id
- ユーザー名 = FSx_user
- password = user_password

問題

シークレットに、ファイルシステム認証用の有効なONTAPクレデンシャルが含まれていません。

解決方法：AWS Secrets ManagerでFSx for ONTAPファイルシステムを認証するためのクレデンシャルを指定します。

ワークロードファクトリーのリンクを管理する

Workload Factory アカウントに関連付けたリンクを管理します。 FSx for ONTAPファイルシステムに関連付けられているリンクを表示したり、リンク認証に使用するパスワードを指定したり、Workload Factory コンソールからリンクを削除したりできます。

"リンクの詳細" または "リンクを作成して関連付ける"。

アカウントに関連付けられているリンクを表示する

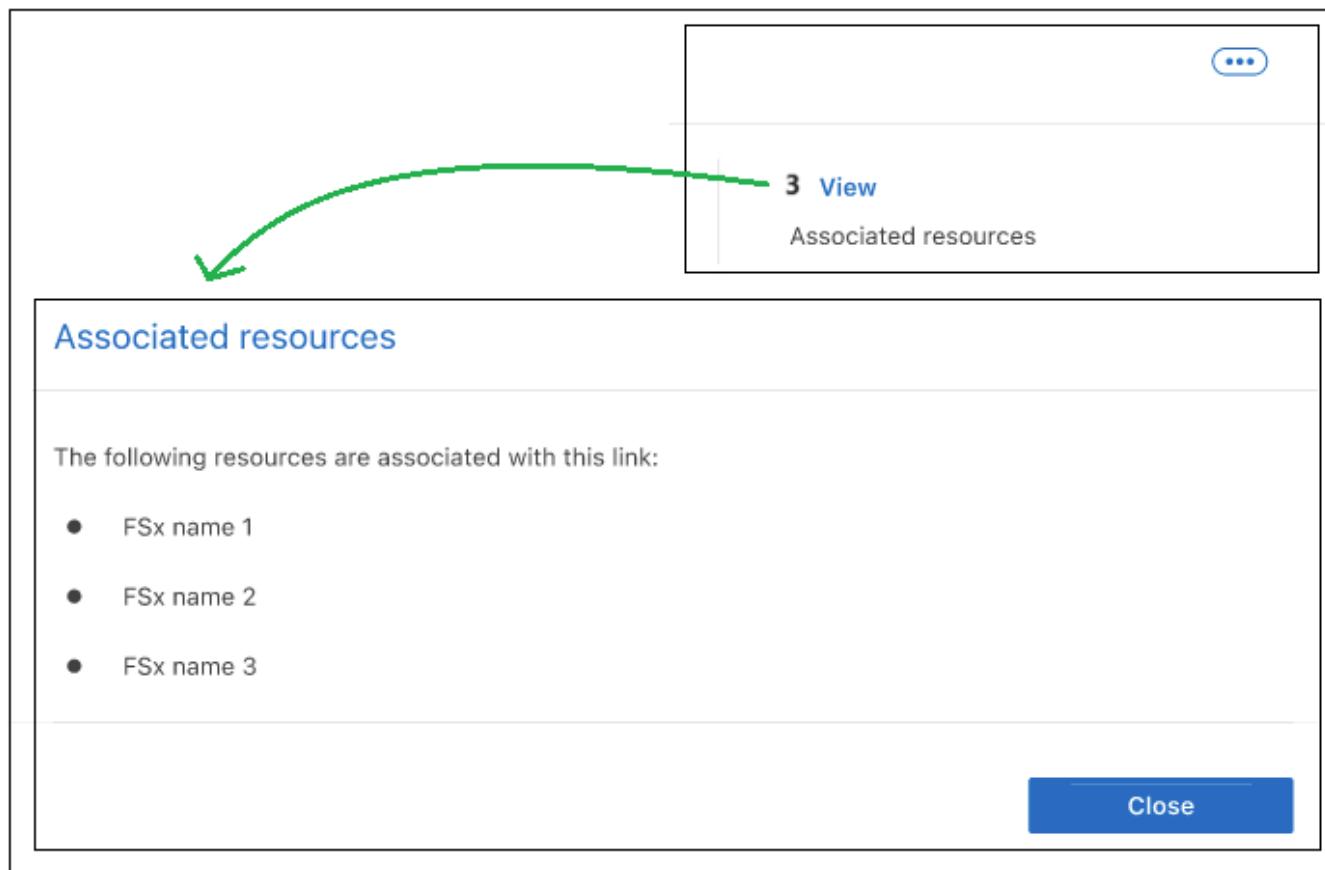
現在アカウントに関連付けられているリンクを表示できます。

手順

1. いずれかを使用してログインし"コンソールエクスペリエンス"ます。
2. ストレージメニューから、*管理*を選択し、次に*リンク*を選択します。

既存のリンクは「リンク」ページに表示されます。

3. リンクに関連付けられているFSx for ONTAPファイルシステムを表示するには、[関連リソース]セクションで*[表示]*ボタンを選択します。



4. リンクにAmazon Resource Name (ARN) が必要な場合は、ARNフィールドの横にある_COPY_ICONを選択します。

リンクの編集

Workload Factory インターフェースからリンクを編集することはできません。リンクを変更する必要がある場合は、新しいリンクを作成し、そのリンクをファイルシステムに関連付ける必要があります。



AWSコンソールを使用してLambdaネットワーク構成（VPC、サブネット、セキュリティグループなど）を編集すると、変更がリンク管理UIに反映されますが、これらの変更によってLambdaとONTAP間の接続の問題が発生する可能性があるため、推奨されません。

リンクの認証

リンクを FSx for ONTAPファイルシステムに接続するには、Workload Factory 認証情報の管理ユーザーパスワードまたは AWS Secrets Manager シークレット ARN を指定します。

コンソールエージェントを使用する場合、AWS Secrets Manager はサポートされません。



1つのリンクでサポートされる認証方式は1つだけです。たとえば、[Link authentication with AWS Secrets Manager]を選択した場合、あとで認証方法を変更することはできません。

手順

1. いざれかを使用してログインし"コンソールエクスペリエンス"ます。
2. メニューを選択  次に*ストレージ*を選択します。
3. [ストレージ] メニューから、**FSx for ONTAP** を選択します。
4. *FSx for ONTAP*から、リンクを関連付けるファイルシステムのアクションメニューを選択し、*管理*を選択します。
5. ファイルシステムの概要で、*[リンクの認証]*を選択します。
6. [Authenticate]リンクページで、認証モードを選択します。
 - Workload Factory : パスワードを2回入力します。
 - AWS Secrets Manager : シークレットARNを入力します。
7. * 適用 * を選択します。

結果

リンクが認証され、高度なONTAP処理を実行できます。

リンク認証用のパスワードを更新する

管理パスワードが無効な場合は、パスワードを更新してFSx for ONTAPファイルシステムへのリンクを接続します。

手順

1. いざれかを使用してログインし"コンソールエクスペリエンス"ます。
2. メニューを選択  次に*ストレージ*を選択します。
3. [ストレージ] メニューから、**FSx for ONTAP** を選択します。
4. *FSx for ONTAP*から、リンクを関連付けるファイルシステムのアクションメニューを選択し、*管理*を選択します。
5. ファイルシステムの概要で、*[パスワードの更新]*を選択します。
6. [Authenticate]リンクページで、新しいパスワードを2回入力します。
7. * 適用 * を選択します。

結果

パスワードが更新され、FSx for ONTAPファイルシステムにリンクが接続されました。

リンクの削除

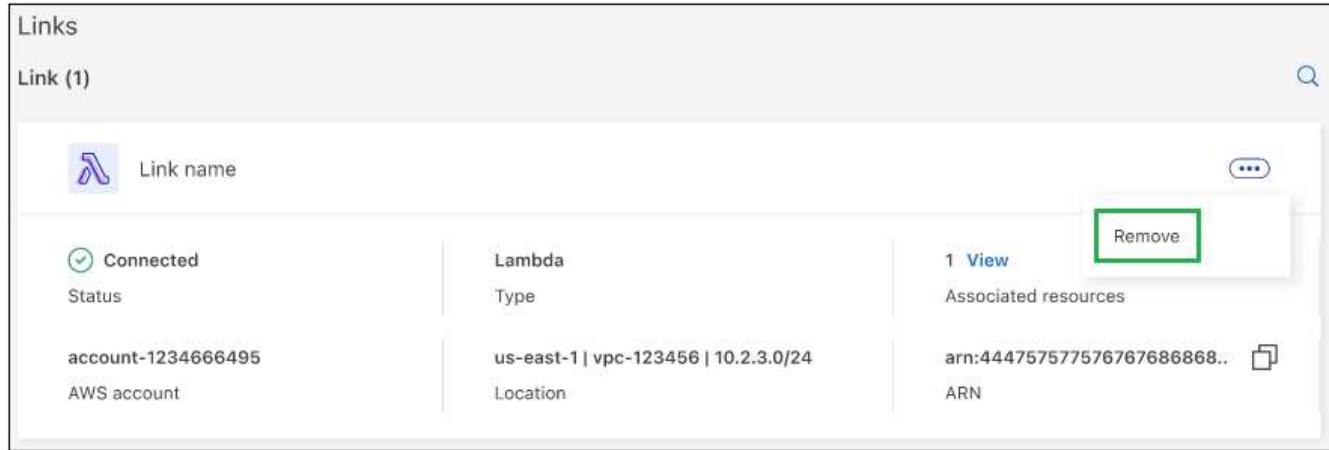
環境で使用しなくなったリンクを削除できます。リンクを使用していたFSx for ONTAPファイルシステムやその他のリソースは、リンクを削除すると特定の機能を使用できなくなります。

リンクは Workload Factory からのみ削除され、AWS 環境からは削除されないことに注意してください。Workload Factory のリンクを削除した後、AWS アカウントから Lambda 関数を削除する必要があります。

手順

1. いざれかを使用してログインし"コンソールエクスペリエンス"ます。

2. メニューを選択  次に*ストレージ*を選択します。
 3. ストレージメニューから、*管理*を選択し、次に*リンク*を選択します。
- 既存のリンクは「リンク」ページに表示されます。
4. 「リンク」ページで、削除するリンクのアクションメニューを選択し、「削除」を選択します。



The screenshot shows the AWS Lambda 'Links' page. It displays a single link entry for 'Lambda'. The link details are as follows:

Link name	Type	Associated resources
account-1234666495	Lambda us-east-1 vpc-123456 10.2.3.0/24	arn:44475757575767686868..
AWS account	Location	ARN

The 'Remove' button in the top right corner of the link row is highlighted with a green box.

5. 確認する場合は、*[削除]*をもう一度選択します。

AWSのドキュメントを参照してください ["Lambda関数の削除"](#)。

Workload Factory でキャッシュボリュームを検出する

NetApp Workload Factory コンソールを離れることなく、キャッシュ関係に関連付けられたキャッシュ ボリュームを検出して表示します。キャッシュ関係は、ONTAP FlexCache関係とも呼ばれます。Workload Factory は、FlexCacheテクノロジーを使用して既存のキャッシュ関係を検出します。FlexCache テクノロジーは、データ アクセスを高速化し、WAN の遅延、帯域幅、および読み取り集中型ワークロードのコストを削減するNetApp ONTAP のリモート キャッシュ機能であり、特にクライアントが同じデータに繰り返しアクセスする必要がある場合に効果を発揮します。

["FlexCacheを使用したデータの複製について詳しく説明します。"](#)

タスクの内容

キャッシュ関係を検出するには、リンクの関連付けが必要です。

キャッシュ関係は、1つの FSx for ONTAPファイル システムと1つのCloud Volumes ONTAPシステムなど、2つのONTAPシステム上のボリューム間に存在する場合があります。キャッシュ関係は、ボリュームからボリュームまで、単一の FSx for ONTAPファイル システム内に存在することもできます。

開始する前に

始める前に次の点を考慮してください。

- ファイル システム上のキャッシュ関係を検出するには、リンクを関連付ける必要があります。["既存のリンクを関連付ける方法、または新しいリンクを作成して関連付ける方法を学びます"](#)。リンクが関連付け

られたら、この操作に戻ります。

- 既存のキャッシング関係が必要です。

手順

- いずれかを使用してログインし"コンソールエクスペリエンス"ます。
- メニューを選択  次に*ストレージ*を選択します。
- [ストレージ] メニューから、**FSx for ONTAP** を選択します。
- *FSx for ONTAP*から、*キャッシング関係*タブを選択します。
- キャッシング ボリュームがテーブルに表示されます。表には、各キャッシング ボリュームに関する次の情報が含まれています。
 - 元のクラスター: FlexCache関係の元のクラスター。
 - 元のボリューム: FlexCache関係の元のボリューム。
 - 元のストレージ VM: ボリュームの元の、つまりソースのストレージ VM。
 - キャッシング ボリューム: FlexCache関係のキャッシング、つまりターゲット ボリューム。
 - キャッシング ストレージ VM: ボリュームのキャッシング、つまりターゲット ストレージ VM。
 - ステータス: FlexCache関係のステータス。
 - キャッシング上の使用可能なストレージ: キャッシュ ボリューム上の使用可能なストレージの量。
 - キャッシング ファイル システム: キャッシュ ボリュームのファイル システム。
 - 書き込みモード: FlexCache関係の書き込みモード。
 - DR キャッシュ:** FlexCache関係が災害復旧 (DR) キャッシュであるかどうかを示します。
 - エクスポート ポリシー: キャッシュ ボリュームのエクスポート ポリシー。

関連情報

["キャッシングボリュームを管理する"](#)

ボリュームの管理

Workload Factory で FSx for ONTAPボリュームを作成する

FSx for ONTAPファイル システムを設定したら、データをグループ化するための仮想リソースとして、Workload Factory に FSx for ONTAPボリュームを作成します。

タスクの内容

FSx for ONTAP ボリュームはデータを仮想的にグループ化し、データの保存方法を決定し、データへのアクセスの種類を決定します。ボリュームはファイルシステムのストレージ容量を消費しません。ボリュームに格納されたデータは、主にSSDストレージを消費します。ボリュームの階層化ポリシーによっては、データが容量プールのストレージを消費する場合もあります。ボリュームのサイズは作成時に設定します。あとで変更することもできます。

ボリュームには次のプロトコルが使用されます。

- SMB/CIFS: Windows オペレーティング システム用のファイルストレージ プロトコル
- NFS : UNIXオペレーティングシステム用のファイルストレージプロトコル
- iSCSI : ブロックストレージプロトコル

S3 エンドポイントは FSx for ONTAPボリュームに接続できます。S3 アクセスポイントを使用すると、AWS S3 API を介して SMB/CIFS または NFS ボリューム上にあるファイルデータにアクセスできます。これにより、既存のデータを、S3 アクセスポイントをサポートする AWS サービスの GenAI、ML、分析と統合できます。

音量設定の詳細

変更不可能なファイル

この機能はSnapLockとも呼ばれ、デフォルトでは無効になっています。不变ファイルを有効にすると、一定期間データの削除や上書きが防止されます。この機能を有効にできるのは、ボリュームの作成時のみです。機能を有効にすると、無効にすることはできません。これは、追加料金がかかる FSx for ONTAPのプレミアム機能です。詳細については、["SnapLockの仕組み"](#) Amazon FSx for NetApp ONTAP ドキュメント。

- 保持モード: エンタープライズ または コンプライアンス の 2 つの保持モードから選択できます。
 - _ENTERPRISE_MODEでは、管理者は変更不可のファイル (SnapLock) を保持期間中にファイルを削除できます。
 - _Compliance_modeでは、WORMファイルは保持期間が終了するまで削除できません。同様に、変更不可のボリュームは、ボリューム内のすべてのファイルの保持期間が終了するまで削除できません。
- 保持期間: 保持期間には、保持ポリシーと保持期間の 2 つの設定があります。保持ポリシーは、ファイルを不变の WORM 状態で保持する期間を定義します。独自の保持ポリシーを指定することも、デフォルトの保持ポリシー (未指定) (30 年) を使用することもできます。最小および最大の_保持期間_は、ファイルのロックに許可される時間の範囲を定義します。



保持期間が経過したあともWORMファイルを変更することはできません。削除するか、新しい保持期間を設定してWORM保護を再度有効にすることしかできません。

- 自動コミット: 自動コミット機能を有効にするオプションがあります。自動コミット機能は、ファイルが自動コミット期間中に変更されなかった場合、SnapLockボリューム上のファイルを WORM 状態にコミットします。デフォルトでは、自動コミット機能は無効になっています。自動コミットするファイルがSnapLockボリューム上に存在していることを確認する必要があります。
- 特権削除: SnapLock管理者は、SnapLock Enterpriseボリュームで特権削除をオンにして、ファイルの保持期間が終了する前にファイルを削除できるようにすることができます。この機能はデフォルトで無効になっています。
- ボリューム追加モード: WORM で保護されたファイル内の既存のデータを変更することはできません。ただし、不变ファイルでは、WORM 追加可能ファイルを使用して既存のデータの保護を維持することができます。たとえば、ログ ファイルを生成したり、増分的にデータを書き込むときにオーディオまたはビデオのストリーミング データを保持したりできます。["ボリュームアペンドモードに関する詳細情報"](#) Amazon FSx for NetApp ONTAP ドキュメント。

開始する前に

ボリュームを作成する前に、次の前提条件を確認してください。

- Workload Factory コンソールに FSx for ONTAPファイル システムが必要です。

- Storage VMが必要です。
- プロトコルアクセスの場合は、次の手順を実行します。
 - ボリュームへのアクセスを構成するには、リンクを関連付ける必要があります。"既存のリンクを関連付ける方法、または新しいリンクを作成して関連付ける方法を学びます"です。リンクが関連付けられたら、この操作に戻ります。
 - 選択したプロトコル (SMB/CIFS、NFS、または iSCSI) のアクセスを構成する必要があります。

ボリュームの作成

Codeboxで使用可能なREST API、CloudFormation、Terraformの各ツールを使用してボリュームを作成できます。"Codeboxを使用して自動化する方法"です。



CodeboxからTerraformを使用すると、コピーまたはダウンロードしたコードが非表示になり、パスワードが表示され `fsxadmin` `vsadmin` ます。コードを実行するときは、パスワードを再入力する必要があります。

手順

- いずれかを使用してログインし"コンソールエクスペリエンス"ます。
- メニューを選択 次に*ストレージ*を選択します。
- [ストレージ] メニューから、**FSx for ONTAP** を選択します。
- *FSx for ONTAP*から、ボリュームを作成するファイルシステムのアクションメニューを選択し、*ボリュームの作成*を選択します。
- [Create volume]ページの[General details]で、次の詳細を指定します。
 - ボリューム名：ボリュームの名前を入力します。
 - * Storage VM名*：必要に応じて、Storage VM名を入力します。
 - ボリュームスタイル：* FlexVol または FlexGroup * volumeを選択します。

FlexVolボリュームの形式はデフォルトで選択されています。

FlexGroup ボリュームのサイズは構成要素の数によって異なり、構成要素ごとに 100 GiB が必要です。

- ボリュームサイズ：ボリュームサイズと単位を入力します。

必要に応じて、ボリュームの自動拡張を有効にします。このオプションは、ボリュームアクセスタイルとして*ファイルアクセス*を選択した場合に使用できます。

- ボリュームの自動拡張：オプションでボリュームの自動拡張を有効にすると、ボリュームが最大サイズに達するまでボリューム容量が自動的に拡張されます。この機能は、データ使用量の増加に対応し、中断のない運用を保証します。

ボリュームの最大拡張サイズと単位を指定します。最大拡張サイズを現在のボリュームサイズより小さく設定することはできません

- タグ:オプションで、最大50個のタグを追加できます。

- [Access] (リンクが関連付けられているファイルシステムの場合のみ) で、次の詳細を指定します。

- a. アクセスタイプ：*ファイルアクセス*または*ブロックアクセス*を選択します。ボリュームアクセスを設定するための追加フィールドは、選択内容によって異なります。
- ファイルアクセス：SMB / CIFS、NFS、またはデュアル（SMB / NFS）プロトコルを使用して、許可された複数のユーザとデバイスにボリュームへのアクセスを許可します。
- 次のフィールドに値を入力して、ボリュームへのファイルアクセスを設定します。
- b. * NFSエクスポートポリシー*：NFSアクセスを提供するには、次の詳細を指定してください：
- i. アクセス制御：ドロップダウンメニューから*、[既存のエクスポートポリシー]、または[ボリュームへのアクセスなし]*を選択します。
 - ii. エクスポートポリシー名：
- カスタムエクスポートポリシーを選択した場合は、ドロップダウンメニューから既存のポリシー名を選択します。
- 既存のエクスポートポリシーを選択した場合は、新しいポリシー名を入力します。
- i. エクスポートポリシールールの追加：必要に応じて、カスタムエクスポートポリシーの場合、エクスポートポリシールールをポリシーに追加できます。
- c. **SMB/CIFS 共有**: 以下を指定します。
- i. 名前: アクセスを提供するための SMB/CIFS 共有名を入力します。
 - ii. 権限：[フルコントロール]、[読み取り/書き込み]、[読み取り]、または[アクセスなし]を選択し、ユーザまたはグループをセミコロン（;）で区切って入力します。ユーザまたはグループでは大文字と小文字が区別されます。ユーザのメインは「domain\username」の形式で指定する必要があります。
- d. セキュリティ形式：デュアルプロトコルボリュームの場合は、UNIXまたはNTFSのいずれかのセキュリティ形式を選択します。UNIXは、デュアルプロトコルボリュームのデフォルトのセキュリティ形式です。このコンテキストでのユーザマッピングの詳細なガイダンスについては、AWSブログ記事を参照して["Amazon FSx for NetApp ONTAPでマルチプロトコルワークLOADを実現"](#)ください。
- ブロックアクセス：重要なビジネスアプリケーションを実行しているホストがiSCSIプロトコルを使用してボリュームにアクセスできるようにします。ブロックアクセスは、ファイルシステムのスケールアウト構成のHAペアが6つ以下の場合にのみ使用できます。
- ボリュームへのブロックアクセスを設定するには、次のフィールドに値を入力します。
- A. * iSCSIの設定*：ボリュームへのブロックアクセス用にiSCSIを設定するには、以下の詳細を指定してください。
- I. または[既存のイニシエータグループをマッピングする]*を選択します。
 - II. ドロップダウンメニューから*[ホストオペレーティングシステム]*を選択します。
 - III. 新しいイニシエータグループの*イニシエータグループ名*を入力します。
 - IV. [Host Initiators]で、1つ以上のiSCSI Qualified Name (IQN) ホストイニシエータを追加します。
- e. **S3 アクセス ポイント**: オプションで、S3 アクセス ポイントを接続して、AWS S3 API 経由で NFS または SMB/CIFS ボリューム上にある FSx for ONTAPファイル システム データにアクセスします。ファイル アクセス タイプのみがサポートされます。以下の詳細を提供します:

- **S3 アクセス ポイント名:** S3 アクセス ポイントの名前を入力します。
 - **ユーザー:** ボリュームへのアクセス権を持つ既存のユーザーを選択するか、新しいユーザーを作成します。
 - **ユーザー タイプ:** ユーザー タイプとして **UNIX** または **Windows** を選択します。
 - **ネットワーク構成:** インターネット または **仮想プライベート クラウド (VPC)** を選択します。選択するネットワークの種類によって、アクセス ポイントがインターネットからアクセスできるか、特定の VPC に制限されるかが決まります。
 - **メタデータを有効にする:** メタデータを有効になると、S3 アクセス ポイントからアクセスできるすべてのオブジェクトを含む S3 テーブルが作成され、監査、ガバナンス、自動、分析、最適化に使用できるようになります。メタデータを有効になると追加の AWS コストが発生します。詳細については、["Amazon S3 価格設定ドキュメント"](#)を参照してください。
- f. **S3 アクセス ポイント タグ:** オプションで、最大 50 個のタグを追加したり、タグを削除したりできます。

7. [Efficiency and protection]で、次の詳細を指定します。

- a. **ストレージ効率:** デフォルトで有効になっています。この機能を無効にするには選択します。

ONTAPは、重複排除機能と圧縮機能を活用してストレージ効率を実現します。重複排除機能は重複するデータブロックを排除し、データ圧縮機能はデータブロックを圧縮することで、必要な物理ストレージ容量を削減します。

- b. * **Snapshotポリシー*** : Snapshotポリシーを選択して、Snapshotの頻度と保持を指定します。

以下は AWS のデフォルトポリシーです。既存のスナップショットポリシーを表示するには、["リンクの関連付け"](#)。

default

このポリシーでは、次のスケジュールでSnapshotが自動的に作成され、新しいコピー用のスペースを確保するために最も古いSnapshotコピーが削除されます。

- 最大6つの時間単位のスナップショットが毎時5分に作成されます。
- 最大2つの日次スナップショットが月曜日から土曜日の午前0時10分に作成されます。
- 最大2つの週単位Snapshotが毎週日曜日の午前0時15分に作成されます。



Snapshotの時間はファイルシステムのタイムゾーンに基づいており、デフォルトは協定世界時 (UTC) です。タイムゾーンの変更については、NetAppのサポートドキュメントのを参照してください ["システムのタイムゾーンの表示と設定"](#)。

default-1weekly

このポリシーはポリシーと同様に機能し `default` ますが、週次スケジュールのSnapshotが1つだけ保持されます。

none

このポリシーではスナップショットは作成されません。このポリシーをボリュームに割り当てるごとに、自動Snapshotが作成されないようにすることができます。

c. 階層化ポリシー：ボリュームに格納されているデータの階層化ポリシーを選択します。

バランス(自動)は、Workload Factory コンソールを使用してボリュームを作成するときのデフォルトの階層化ポリシーです。ボリューム階層化ポリシーの詳細については、以下を参照してください。["ボリュームのストレージ容量" AWS FSx for NetApp ONTAP ドキュメント](#)。Workload Factory では、階層化ポリシーに Workload Factory コンソールでユースケースベースの名前が使用され、括弧内に FSx for ONTAP 階層化ポリシー名が含まれていることに注意してください。

d. 不変ファイル: 不変ファイル機能を有効にすると、このボリューム内のファイルが不变の WORM(write-once-read-many) 状態に永続的にコミットされます。以下の詳細を入力してください。

i. 選択すると、* SnapLockを使用した変更不可ファイル*が有効になります。

ii. 同意して続行するには、ボックスを選択してください。

iii. [有効]を選択します。

iv. 保持モード：*エンタープライズ*または*コンプライアンス*モードを選択します。

v. 保持期間：

▪ 保持ポリシーを選択します。

▪ 未指定：保持ポリシーを30年に設定します。

▪ 期間の指定：独自の保持ポリシーを設定する秒数、分数、時間数、日数、月数、または年数を入力します。

▪ 最小保持期間と最大保持期間を選択します。

▪ 最小：最小保持期間を設定する秒数、分数、時間数、日数、月数、または年数を入力します。

▪ 最大：最大保持期間を設定する秒数、分数、時間数、日数、月数、または年数を入力します。

vi. * autocommit *：自動コミットを無効または有効にします。自動コミットを有効にする場合は、自動コミット期間を設定します。

vii. 特権削除：無効または有効。特権削除を有効にすると、SnapLock管理者は保存期間が終了する前にファイルを削除できます。

viii. ボリュームアpendモード：無効または有効にします。WORMファイルに新しいコンテンツを追加できます。

e. ARP/AI: リンクがファイルシステムに関連付けられている場合、NetApp Autonomous Ransomware Protection with AI (ARP/AI) はデフォルトで有効になります。["ARP/AIについて詳しくはこちら"](#)です。続行するには、ステートメントを受け入れます。

機能が利用できない場合は、次のいずれかの理由が考えられます。

▪ リンクはファイルシステムに関連付けられていません。["既存のリンクを関連付ける方法、または新しいリンクを作成して関連付ける方法を学びます"](#)です。リンクが関連付けられたら、この操作に戻ります。

▪ 不変のファイルを含むボリューム、および iSCSI および NVMe プロトコルを含むボリュームは、ARP/AI ではサポートされません。

▪ ファイルシステムには既に ARP/AI ポリシーがあります。

8. [Advance configuration]で、次の情報を指定します。

- a. ジャンクションパス：ボリュームをマウントするStorage VMのネームスペース内の場所を入力します。デフォルトのジャンクションパスはです /<volume-name>。
 - b. アグリゲートリスト：FlexGroupボリュームのみ。アグリゲートを追加または削除します。アグリゲートの最小数は1です。
 - c. コンステイチュエントの数：FlexGroupボリュームの場合のみ。アグリゲートあたりのコンステイチュエントの数を入力します。コンステイチュエントあたり100GiBが必要です。
9. 「* Create *」を選択します。

関連情報

- "[Workload Factoryでボリューム容量を調整する](#)"
- "[Workload Factory でボリューム階層化ポリシーを変更する](#)"
- "[Workload Factory で S3 アクセス ポイントを管理する](#)"

FSx for ONTAPのファイルシステムデータへのアクセス

NASクライアントのボリュームをマウントし、SANクライアントのiSCSI LUNをマウントすることで、FSx for ONTAPファイルシステムにオンプレミスからアクセスできます。

["データへのアクセス"](#) Amazon FSx for NetApp ONTAPのドキュメントには、参照用にデータにアクセスする方法に関するトピックが記載されています。

NetApp Workload Factory でボリュームのマウント ポイントを取得することもできます。

NetApp Workload Factory のボリュームのマウント ポイントを取得する

CIFS共有またはNFSクライアントに共有をマウントするボリュームのマウントポイントを取得します。

手順

1. いずれかを使用してログインし"[コンソールエクスペリエンス](#)"ます。
2. メニューを選択  次に*ストレージ*を選択します。
3. *FSx for ONTAP*から、ボリュームを含むファイルシステムのアクションメニューを選択し、*管理*を選択します。
4. ファイルシステムの概要で、*[ボリューム]*タブを選択します。
5. [ボリューム] タブから、ボリュームのアクション メニューを選択し、基本アクション、マウント コマンドの表示 を選択します。
6. [コマンドのマウント]ダイアログで*[コピー]*を選択し、NFSマウントポイントまたはCIFS共有のコマンドをコピーします。コピーしたコマンドを端末に入力します。
7. [閉じる (Close)]を選択します。

NASクライアントへの接続

- "[Linuxクライアントへのボリュームのマウント](#)"
- "[Windowsクライアントへのボリュームのマウント](#)"

- "macOSクライアントへのボリュームのマウント"

SANクライアントへの接続

- "LinuxクライアントへのiSCSI LUNのマウント"
- "WindowsクライアントへのiSCSI LUNのマウント"

ブロックストレージリソースを作成する

NetApp Workload Factory でファイルシステムのイニシエータグループを作成する

NetApp Workload Factoryを使用して、イニシエータ グループを作成し、SANブロックデバイスへのホスト アクセスを管理します。

タスクの内容

イニシエータ グループ (igroup) は、ブロック デバイス (LUN) を、それらへのアクセスが許可されているコンピューティング リソースに接続します。ボリュームが広範囲にアクセス可能で、ユーザー権限によってアクセスが制御される NFS や CIFS とは異なり、ブロック ストレージの権限はマシン レベルで動作します。通常、一度にブロック デバイスにアクセスできるのは 1 つのシステムだけです。

igroupは、ブロックストレージの権限レイヤーとして機能します。サーバーがストレージシステムに接続すると、iSCSI認定 (IQN) ホストイニシエーターを使用してサーバー自体を識別します。そのIQNが1つ以上のigroupに属している場合、サーバーはそれらのigroupに関連付けられているすべてのLUNにアクセスできるようになります。iSCSIが適切に機能するには、igroupとiSCSIホスト接続の両方が必要です。

開始する前に

igroupを作成するには、リンクを関連付ける必要があります。["既存のリンクを関連付ける方法、または新しいリンクを作成して関連付ける方法を学びます"](#)。リンクを関連付けたら、この操作に戻ります。

手順

1. いずれかを使用してログインし["コンソールエクスペリエンス"](#)ます。
2. ストレージ タイルで、[ストレージへ移動] を選択します。
3. [ストレージ] メニューから、**FSx for ONTAP** を選択します。
4. **FSx for ONTAP***から、*ブロック デバイス タブを選択します。
5. リソース タイプ **Create initiator group** を選択し、**Create igrup** を選択します。
6. イニシエーター グループの作成 ダイアログで、次の操作を行います：
 - **igroup name:** イニシエーター グループの名前を入力します。
 - **igroup description :** (オプション) イニシエーター グループの説明を入力します。
 - ストレージ VM 名：イニシエーター グループのストレージ VM を選択します。
 - **Block device name :** イニシエーター グループに関連付ける 1 つ以上のブロック デバイスを選択します。リストされているブロック デバイスは、まだホスト イニシエーターにマップされていないデバイスです。
 - オペレーティング システムの種類：オペレーティング システムの種類として、Linux、VMware、または Windows を選択します。

- ホスト イニシエーター：1つ以上の iSCSI 認定（IQN）ホスト イニシエーターをイニシエーター グループに追加します。

7. 「* Create *」を選択します。

関連情報

["FSx for ONTAP ファイルシステムの igrup を管理する"](#)

NetApp Workload Factoryでファイルシステム用のブロックデバイスを作成する

基幹業務 (LOB) アプリケーション要件をサポートするブロック デバイスを作成します。

タスクの内容

NetApp Workload Factoryのブロック デバイスでは、FlexVolボリュームのみがサポートされます。iSCSI プロトコルを使用してブロック デバイスを作成できます。

ブロック サイズは、使用可能なFlexVol volumeよりも小さくする必要があります。

開始する前に

- ブロック デバイスを作成するには、リンクを関連付ける必要があります。["既存のリンクを関連付ける方法、または新しいリンクを作成して関連付ける方法を学びます"](#)。リンクを関連付けたら、この操作に戻ります。

手順

- いずれかを使用してログインし["コンソールエクスペリエンス"](#)ます。
- ストレージ タイルで、[ストレージへ移動] を選択します。
- [ストレージ] メニューから、**FSx for ONTAP** を選択します。
- FSx for ONTAP***から、*ブロック デバイス タブを選択します。
- *ブロックデバイスの作成*を選択します。
- *ボリュームの詳細*で、次の操作を行います。
 - ボリューム名: 次のいずれかのオプションを選択します。
 - 新しいボリュームを作成し、ボリュームの名前を入力します。
 - 既存のボリュームを選択します。
 - ストレージ VM: ストレージ VM を選択します。
 - ボリューム スタイル: デフォルトのボリューム スタイルは * FlexVol* です。
 - ボリューム サイズ: ボリュームのサイズを入力し、単位を選択します。FlexVol volumeあたりの最大サイズは 100 TiB です。
 - ボリュームの自動拡張: オプションで、ボリュームの自動拡張を有効にして、ボリュームが容量に達したときにサイズが自動的に増加するようにします。最大拡張サイズは 300 TiB です。
 - タグ: オプションで、ブロックデバイスを整理および分類するためにタグを追加します。
- *ブロックデバイスの詳細*で、次の操作を行います。
 - ブロックデバイス名: ブロックデバイスの名前を入力します。
 - ブロック デバイス サイズ: ブロック デバイスのサイズを入力し、単位を選択します。ブロック デバイ

スのサイズは、使用可能なボリューム サイズよりも小さくする必要があります。

8. アクセス で、次の操作を行います。

a. **iSCSI** 構成: 次のいずれかのオプションを選択します。

- 新しいイニシエーター グループの作成: ホスト オペレーティング システム、イニシエーター グループ名を指定し、1つ以上の iSCSI 修飾名 (IQN) ホスト イニシエーターを追加します。
- 既存のイニシエーター グループのマップ: 既存のイニシエーター グループを選択し、ホスト オペレーティング システムを指定して、1つ以上の iSCSI 修飾名 (IQN) ホスト イニシエーターを選択します。

9. *効率と保護*の下で、次の操作を行います。

a. ストレージ効率: デフォルトで有効になっています。この機能を無効にするには選択します。

ONTAPは、重複排除機能と圧縮機能を活用してストレージ効率を実現します。重複排除機能は重複するデータブロックを排除し、データ圧縮機能はデータブロックを圧縮することで、必要な物理ストレージ容量を削減します。

b. * Snapshotポリシー* : Snapshotポリシーを選択して、Snapshotの頻度と保持を指定します。

以下は AWS のデフォルトポリシーです。既存のスナップショットポリシーを表示するには、[xref:.."リンクの関連付け](#)。

default

このポリシーでは、次のスケジュールでSnapshotが自動的に作成され、新しいコピー用のスペースを確保するために最も古いSnapshotコピーが削除されます。

- 最大6つの時間単位のスナップショットが毎時5分に作成されます。
- 最大2つの日次スナップショットが月曜日から土曜日の午前0時10分に作成されます。
- 最大2つの週単位Snapshotが毎週日曜日の午前0時15分に作成されます。



Snapshotの時間はファイルシステムのタイムゾーンに基づいており、デフォルトは協定世界時 (UTC) です。タイムゾーンの変更については、NetAppのサポートドキュメントのを参照してください ["システムのタイムゾーンの表示と設定"](#)。

default-1weekly

このポリシーはポリシーと同様に機能し default ますが、週次スケジュールのSnapshotが1つだけ保持されます。

none

このポリシーではスナップショットは作成されません。このポリシーをボリュームに割り当てるごとに、自動Snapshotが作成されないようにすることができます。

c. 階層化ポリシー：ボリュームに格納されているデータの階層化ポリシーを選択します。

バランス (自動) は、Workload Factory コンソールを使用してボリュームを作成するときのデフォルトの階層化ポリシーです。ボリューム階層化ポリシーの詳細については、以下を参照してください。["ボリュームのストレージ容量"](#) AWS FSx for NetApp ONTAP ドキュメント。Workload Factory では、階層化ポリシーに Workload Factory コンソールでユースケース ベースの名前が使用され、括弧内に

FSx for ONTAP階層化ポリシー名が含まれていることに注意してください。

- d. **ARP/AI:** リンクがファイル システムに関連付けられている場合、NetApp Autonomous Ransomware Protection with AI (ARP/AI) はデフォルトで有効になります。"ARP/AIについて詳しくはこちら"です。続行するには、ステートメントを受け入れます。

機能が利用できない場合は、次のいずれかの理由が考えられます。

- リンクはファイル システムに関連付けられていません。"既存のリンクを関連付ける方法、または新しいリンクを作成して関連付ける方法を学びます"です。リンクが関連付けられたら、この操作に戻ります。
- 不変ファイルを含むボリュームと NVMe プロトコルを使用するボリュームは、ARP/AI ではサポートされません。
- ファイル システムには既に ARP/AI ポリシーがあります。

10. 「* Create *」を選択します。

関連情報

"FSx for ONTAPファイルシステムのブロックデバイスを管理する"

FSx for ONTAPファイルシステム用Storage VMの作成

FSx for ONTAPファイル システム用のストレージ VM (SVM) を作成し、NetApp Workload Factory のワークロードのストレージおよびデータ サービスに仮想的にアクセスします。

タスクの内容

ストレージ VM は、ワークロード ファクトリー ストレージ内の各ワークロードのデータにアクセスするために使用できる分離されたファイル サーバーです。各 SVM には、データの管理とアクセスを行うための独自の管理資格情報とエンドポイントがあります。

SVMを使用している場合、FSx for ONTAPのデータにアクセスすると、SVMのエンドポイント（IPアドレス）を使用して、SVMによってホストされているボリューム、CIFS / SMB共有、またはiSCSI LUNがクライアントやワークステーションにマウントされます。

開始する前に

ファイルシステムあたりのサポートされるStorage VM数を確認します。ファイルシステムあたりのSVMの最大数については、AWSのドキュメントのを参照してください "FSx for ONTAP Storage Virtual Machineの管理"。

Storage VM を作成

Workload Factory コンソールからストレージ VM を作成できます。Codebox で利用可能な REST API 、CloudFormation、Terraform などのツールも使用できます。"Codeboxを使用して自動化する方法"。



CodeboxからTerraformを使用すると、コピーまたはダウンロードしたコードが非表示になり、パスワードが表示され fsxadmin vsadmin ます。コードを実行するときは、パスワードを再入力する必要があります。

手順

1. いざれかを使用してログインし"コンソールエクスペリエンス"ます。
2. メニューを選択  次に*ストレージ*を選択します。
3. [ストレージ] メニューから、**FSx for ONTAP** を選択します。
4. *FSx for ONTAP*から、ファイルシステムのアクションメニューを選択し、*管理*を選択します。
5. ストレージ VM のファイルシステムの概要で、*ストレージ VM の作成*を選択します。
6. [ストレージ VM の作成] ページの [ストレージ VM 構成] で、次の情報を入力します。
 - a. 名前 : Storage VMの名前を入力します。
 - b. * Storage VM クレデンシャル* : このStorage VMのユーザのパスワードを指定する vsadmin か、ファイルシステムのユーザクレデンシャルを使用して fsxadmin ください。
 - c. ルートボリュームのセキュリティ形式 : データにアクセスするクライアントのタイプ (UNIX (Linux クライアント) 、 NTFS (Windowsクライアント) 、 Mixed) に応じて、ルートボリュームのセキュリティ形式を選択します。
 - d. タグ:オプションで、最大50個のタグを追加できます。
7. 「* Create *」を選択します。

データを保護

NetApp Workload Factoryにおけるデータ保護の種類

FSx for ONTAP は、データ保護のためにスナップショット、AI を搭載したNetApp Autonomous Ransomware Protection、レプリケーション、バックアップをサポートしています。避けられない事態に備え、データを保護するために、複数のデータ保護タイプを組み合わせて使用することをお勧めします。

データホゴノシュルイ

ワークロードのデータ保護は、データ損失からいつでもリカバリできるようにします。使用する機能を選択する前に、データ保護の種類について説明します。

スナップショット

Snapshotは、ソースボリューム内のボリュームのポイントインタイムイメージをSnapshotコピーとして読み取り専用で作成します。Snapshotコピーを使用して、個々のファイルをリカバリしたり、ボリュームの内容全体をリストアしたりできます。Snapshotは、すべてのバックアップ方法の基礎となります。ボリュームに作成されたSnapshotコピーを使用して、レプリケートされたボリュームとバックアップファイルがソースボリュームに加えられた変更と同期された状態に維持されます。

NetApp のAI を活用した自律型ランサムウェア防御

NetApp Autonomous Ransomware Protection with AI (ARP/AI) は、NAS (NFS/SMB) 環境でのワークロード分析を使用して、ランサムウェア攻撃の可能性がある異常なアクティビティを検出し、警告します。攻撃が疑われる場合、ARP/AI は、スケジュールされたスナップショットによって提供される既存の保護に加えて、新しい不变のスナップショットも作成します。

レプリケーション

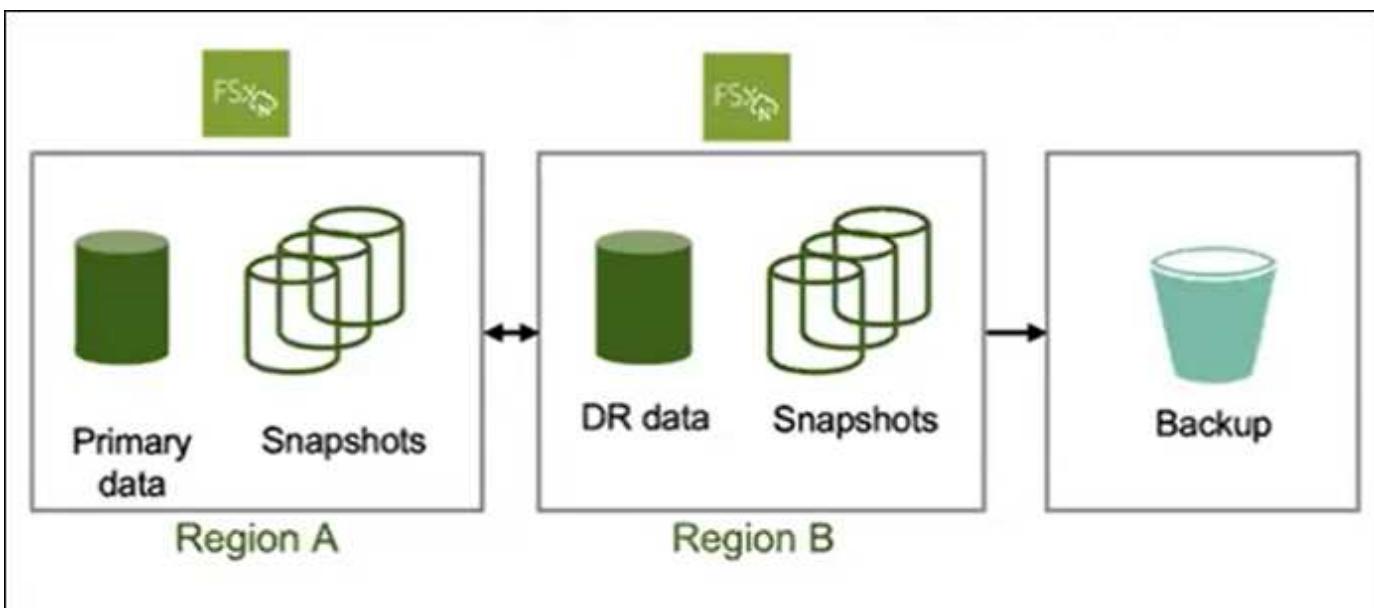
レプリケーションでは、別のFSx for ONTAPファイルシステムにデータのセカンダリコピーが作成され、セカンダリデータが継続的に更新されます。データは最新の状態に維持され、ディザスタリカバリなど、必要なときにいつでも利用できます。

レプリケートされたボリュームを別のFSx for ONTAPファイルシステムに作成し、バックアップファイルをクラウドに作成することもできます。または、レプリケートされたボリュームまたはバックアップファイルを作成するだけを選択できます。

バックアップ

保護や長期保持のために、データのバックアップをクラウドに作成できます。必要に応じて、ボリューム、フォルダ、または個々のファイルをバックアップから同じ、または別の作業ファイルシステムにリストアできます。

次の図は、Snapshot、リージョン間のレプリケーション、オブジェクトストレージへのバックアップを使用したFSx for ONTAPストレージのデータ保護を視覚的に表したものです。



ワークロードデータを保護するためのベストプラクティス

FSx for ONTAPには、複数のデータ保護オプションが用意されています。これらのオプションを組み合わせることで、選択した目標復旧時点と時間を達成できます。最大限の保護を実現するには、ボリュームSnapshotとボリュームバックアップの両方を使用することを推奨します。

Recovery Point Objective (RPO ; 目標復旧時点) は、データの最新のコピーをどのくらいの期間確実に保持できるかを表します。この値は、コピーが作成される頻度によって異なります。Recovery Time Objective (RTO ; 目標復旧時間) は、データのリストアにかかる時間を定義します。

Snapshotでワークロードデータを保護

Snapshotは、スケジュールに基づいて作成されるボリュームの仮想ポイントインタイムバージョンです。スナップショットには、標準のファイルシステムコマンドを使用してアクセスできます。SnapshotによるRPOはわずか1時間です。RTOはリストアするデータ量に依存し、主にボリュームのスループット制限によって制限されます。Snapshotを使用すると、特定のファイルやディレクトリをリストアできるため、RTOをさらに短縮できます。Snapshotは、ボリュームに加えられた変更に対してのみ、追加のボリュームスペースを消費します。

NetApp Autonomous Ransomware Protection with AI でワークロード データを保護

NetApp Autonomous Ransomware Protection with AI (ARP/AI) は、ウイルス対策ソフトウェアが侵入を検出できなかった場合に、重要な追加の防御層として機能します。ARP/AI ポリシーを設定すると、すべてのストレージ VM と、既存および新しく作成されたすべてのボリュームに対して有効になります。有効にすると、ARP/AI はすべてのボリュームとストレージ VM を検出して保護します。ファイル拡張子が異常としてフラグ付けされている場合は、アラートを評価する必要があります。

ボリュームレプリケーションでワークロードデータを保護

ボリュームレプリケーションでは、別のリージョンにあるすべてのSnapshotを含むボリュームの最新データのコピーが作成されます。ボリュームバックアップからボリュームのフルリストア処理のRTOを数時間短縮できない場合は、ボリュームレプリケーションの実行を検討してください。ボリュームレプリケーションを使用すると、最新のデータを別のリージョンで使用できるようになりますが、他のリージョンのボリュームを使用するようにクライアントを調整する必要があります。

バックアップでワークロードデータを保護

ボリュームのバックアップは、ボリュームの独立したポイントインタイムコピーを提供します。古いバックアップを保存し、データの必要な2つ目のコピーを提供するために使用できます。日次、週次、月次のバックアップスケジュールでは、1日からRPOを設定できます。ボリュームのバックアップは全体としてのみリストアできます。バックアップからのボリュームの作成 (RTO) には、バックアップのサイズによって数時間から数日かかることがあります。

ワークロードデータの保護に関する推奨事項

ワークロードデータを保護するために、次の推奨事項を考慮してください。

- ・ 災害復旧にはボリューム レプリケーションを使用します。アプリケーションで低い RTO が必要な場合は、ボリューム レプリケーションを使用してデータを別のリージョンに複製することを検討してください。
- ・ ボリュームバックアップとSnapshotの併用：2つの機能を併用すると、Snapshotからファイルをリストアしたり、バックアップを使用してボリュームが失われた場合にフルリストアを実行したりできます。
- ・ ボリュームのバックアップポリシーを定義する：バックアップポリシーがバックアップの期間と頻度に関する企業の要件を満たしていることを確認します。ボリュームごとに最低2つの日次バックアップを保持することを推奨します。
- ・ Snapshotスケジュールを定義：古いSnapshotがデータのリストアに使用される可能性が低くなります。スナップショット容量の追加コストと比較して、古いスナップショットを保持することによる収益の減少を考慮したスナップショットスケジュールを定義することをお勧めします。
- ・ ファイル システムまたは個々のボリュームに対して ARP/AI ポリシーを有効にして、保護層を追加し、ランサムウェア攻撃からデータを保護します。

スナップショットを使用する

FSx for ONTAPボリュームの手動スナップショットの作成

NetApp Workload Factory で FSx for ONTAPボリュームの手動スナップショットを作成します。スナップショットは、ボリュームのコンテンツの特定時点のバージョンです。

Snapshotはボリュームのリソースであり、変更されたデータのためだけにスペースを消費するデータを瞬時

にキャプチャします。データは時間の経過とともに変化するため、Snapshotは通常、古くなるにつれてより多くのスペースを消費します。

FSx for ONTAPボリュームではジャストインタイムのcopy-on-writeが使用されるため、Snapshot内の変更されていないファイルがボリュームの容量を消費することはありません。



スナップショットはデータのコピーではありません。データのコピーを作成する場合は、FSx for ONTAPのバックアップ機能やボリュームレプリケーション機能の使用を検討してください。

開始する前に

ボリュームの手動スナップショットを作成するには、リンクを関連付ける必要があります。["既存のリンクを関連付ける方法、または新しいリンクを作成して関連付ける方法を学びます"](#)です。リンクが関連付けられたら、この操作に戻ります。

手順

1. いずれかを使用してログインし["コンソールエクスペリエンス"](#)ます。
2. メニューを選択 次に*ストレージ*を選択します。
3. [ストレージ] メニューから、**FSx for ONTAP** を選択します。
4. *FSx for ONTAP*から、スナップショットを作成するボリュームを含むファイルシステムのアクションメニューを選択し、*管理*を選択します。
5. ファイルシステムの概要で、*[ボリューム]*タブを選択します。
6. ボリューム タブから、スナップショットで保護するボリュームのアクション メニューを選択します。
7. *データ保護アクション*を選択し、*スナップショットの管理*を選択します。
8. スナップショットの管理ページで、*スナップショットの作成*を選択します。
9. [スナップショットの作成] ダイアログで、次の操作を行います。
 - a. スナップショット名 フィールドにスナップショット名を入力します。
 - b. 必要に応じて、ラベルを選択するか、新しいラベルを作成します。
 - c. [Retention Period]*に、時間、日、月、または年数を設定します。
 - d. オプション: このスナップショットを不变にすることで、保持期間中にスナップショットが削除されるのを防ぎます。
- 変更不可のスナップショットに関するステートメントを受け入れます。
10. 「* Create *」を選択します。

Workload Factory でストレージ VM のスナップショット ポリシーを作成する

スナップショットの作成と保持を管理するには、Workload Factory でストレージ VM のカスタム スナップショット ポリシーを作成します。スナップショット ポリシーは、システムがストレージ VM のスナップショットを作成する方法を定義します。FSx for ONTAPファイルシステム内のストレージ VM のスナップショット ポリシーを作成できます。複数のストレージ VM 間でポリシーを共有することもできます。

タスクの内容

FSx for ONTAPに組み込まれている3つのスナップショットポリシーとは異なるカスタムスナップショットポリシーを作成できます。

- default
- default-1weekly
- none

デフォルトでは、すべてのボリュームがファイルシステムのSnapshotポリシーに関連付けられ default です。ほとんどのワークロードでこのポリシーを使用することを推奨します。

ポリシーをカスタマイズすると、スナップショットを作成するタイミング、保持するコピーの数、およびスナップショットに名前を付ける方法を指定できます。

開始する前に

- Snapshotポリシーを作成したあとでStorage VMとの関連付けを変更することはできませんが、ポリシーはボリュームに対して追加または削除できます。
- Snapshotを使用する前に、Snapshotの容量について次の点を考慮してください。
 - ほとんどのデータセットでは、20%の容量を追加すれば、Snapshotを最大4週間保持できます。データが古くなるにつれて、リストアに使用される可能性は低くなります。
 - Snapshot内のすべてのデータを上書きすると、ボリューム容量が大量に消費されます。これは、ボリューム容量のプロビジョニングに影響します。
- カスタム スナップショット ポリシーを作成するには、リンクを関連付ける必要があります。 "[既存のリンクを関連付ける方法、または新しいリンクを作成して関連付ける方法を学びます](#)"です。リンクが関連付けられたら、この操作に戻ります。

手順

1. いざれかを使用してログインし"[コンソールエクスペリエンス](#)"ます。
 2. メニューを選択  次に*ストレージ*を選択します。
 3. [ストレージ] メニューから、**FSx for ONTAP** を選択します。
 4. *FSx for ONTAP*から、ボリュームを含むファイルシステムのアクションメニューを選択し、*管理*を選択します。
 5. ファイルシステムの概要で、*[Storage VMs]*タブを選択します。
 6. ストレージ VM タブから、スケジュールされたスナップショットで保護するボリュームのアクション メニューを選択し、詳細アクションを選択して、スナップショット ポリシーの管理を選択します。
 7. Snapshotポリシーの管理ページで、* Snapshotポリシーの作成*を選択します。
 8. Snapshotポリシーネーム*フィールドに、Snapshotポリシーの名前を入力します。
 9. 必要に応じて、Snapshotポリシーの説明を入力します。
 10. [ポリシーのスケジュールとコピー]*で、Snapshotを作成するタイミングを選択します。たとえば、毎分、毎時などです。
- 複数の周波数を選択できます。

11. [コピー数]*で、保持するコピー数を入力します。

コピーの最大数は1、023です。

12. オプション：[命名規則]*で、ポリシーの*プレフィックス*を入力します。

13. *保持ラベル*は自動的に入力されます。

このラベルは、ソースファイルシステムからターゲットファイルシステムへのレプリケーション用に指定されたSnapshotのみを選択するために使用されるSnapMirror（レプリケーションラベル）を示します。

14. オプション：必要なスケジュールについて*変更不可のスナップショット*を有効にするには、スケジュールごとに*保持期間*を設定し、このステートメントを受け入れて続行します。

変更不可のSnapshotを有効にすると、このSnapshotポリシー内のすべてのSnapshotがロックされ、保持期間中にSnapshotが削除されないようになります。

15. * Storage VM間で共有*：デフォルトで有効になっています。有効にすると、Snapshotポリシーがファイルシステム内のすべてのStorage VMで共有されます。単一のStorage VMのSnapshotポリシーを作成する場合は無効にしてください。

16. 「* Create *」を選択します。

Workload Factory のスナップショットからボリュームを復元する

Workload Factory では、スナップショットから既存のボリュームまたは新しいボリュームにデータを復元できます。復元操作により、ボリュームに削除されたファイルまたは破損したファイルが含まれている場合に、ポイントインタイムリカバリが可能になります。

タスクの内容

スナップショットから既存のボリュームまたは新しいボリュームにデータを復元するオプションがあります。

スナップショットから新しいボリュームを作成すると、ボリュームのサイズに関係なく、数秒以内にボリューム全体のコピーが作成されます。新しく作成されたコピーは新しいボリュームを表します。

開始する前に

Snapshotからボリュームを作成する前に、次の制限事項を考慮してください。

- Snapshotからボリュームをリストアできるのは、ボリュームの既存のSnapshotコピーがある場合のみです。
- 権限モデルの変更：この処理を使用してNetwork-Attached Storage (NAS；ネットワーク接続型ストレージ) プロトコルタイプを切り替えると、セキュリティ形式で提供される権限モデルも切り替える可能性があります。ファイルアクセス権限の問題が発生する可能性があります。この問題は、NASクライアントツールを使用して権限の設定を行う管理者アクセスでのみ手動で修正できます。

手順

1. いずれかを使用してログインし"コンソールエクスペリエンス"ます。

2. メニューを選択  次に*ストレージ*を選択します。

3. [ストレージ] メニューから、**FSx for ONTAP** を選択します。

4. *FSx for ONTAP*から、ボリュームを含むファイルシステムのアクションメニューを選択し、*管理*を選択します。
5. ファイルシステムの概要で、*[ボリューム]*タブを選択します。
6. ボリューム タブから、スナップショットから復元するボリュームのアクション メニューを選択します。
7. *データ保護アクション*を選択し、*スナップショットの管理*を選択します。
8. [スナップショットの管理] ページで、復元するスナップショットのアクション メニューを選択し、[復元] を選択します。
9. スナップショットからボリュームを復元するダイアログで、次のオプションから選択します。
 - *新しいボリュームとして復元*を選択して切り替えます。

[リストアされたボリューム名]*フィールドに、リストアするボリュームの一意の名前を入力します。

◦ スナップショットから既存のボリュームにデータを復元します。この操作により、スナップショットの作成時間以降に変更されたデータはすべて完全に削除されます。
10. [* Restore] を選択します。

オブジェクトストレージへのバックアップを使用する

NetApp Workload Factory でボリュームの手動バックアップを作成する

NetApp Workload Factory で、定期的にスケジュールされたバックアップ以外でボリュームの手動バックアップを作成します。

タスクの内容

FSx for ONTAPのバックアップはボリューム単位で行われるため、各バックアップには特定のボリューム内のデータのみが含まれます。

FSx for ONTAPバックアップは増分バックアップです。つまり、最新のバックアップ後に変更されたボリューム上のデータのみが保存されます。これにより、バックアップの作成に必要な時間とバックアップに必要なストレージを最小限に抑えることができ、データを複製しないことでストレージコストを削減できます。

開始する前に

ボリュームのバックアップを作成するには、ボリュームとファイルシステムの両方に、バックアップ Snapshotを格納するための十分なSSDストレージ容量が必要です。バックアップスナップショットの作成時に、スナップショットによって消費される追加のストレージ容量によって、ボリュームのSSDストレージ利用率が98%を超えることはありません。この場合、バックアップは失敗します。

手順

1. いずれかを使用してログインし"コンソールエクスペリエンス"ます。
2. メニューを選択  次に*ストレージ*を選択します。
3. [ストレージ] メニューから、**FSx for ONTAP** を選択します。
4. *FSx for ONTAP*から、ボリュームを含むファイルシステムのアクションメニューを選択し、*管理*を選

択します。

5. ファイルシステムの概要で、*[ボリューム]*タブを選択します。
6. *ボリューム*タブから、バックアップするボリュームのアクションメニューを選択します。
7. データ保護アクション、* FSx for ONTAPバックアップ*、*手動バックアップ*の順に選択します。
8. [Manual backup]ダイアログで、バックアップの名前を入力します。
9. [バックアップ]*を選択します。

NetApp Workload Factory でバックアップからボリュームを復元する

NetApp Workload Factory では、バックアップから AWS アカウント内の任意の FSx for ONTAPファイルシステムにボリュームを復元できます。

リストアに十分な容量があるかどうかはワークロード工場で確認され、十分でない場合はSSDストレージ階層の容量を自動的に追加できます。

手順

1. いずれかを使用してログインし"コンソールエクスペリエンス"ます。
2. メニューを選択  次に*ストレージ*を選択します。
3. [ストレージ] メニューから、**FSx for ONTAP** を選択します。
4. *FSx for ONTAP*から、ボリュームを含むファイルシステムのアクションメニューを選択し、*管理*を選択します。
5. ファイルシステムの概要で、*[ボリューム]*タブを選択します。
6. *ボリューム*タブから、バックアップから復元するボリュームのアクションメニューを選択します。
7. データ保護アクション、* FSx for ONTAPバックアップ*、*バックアップからのリストア*の順に選択します。
8. [Restore from a backup]ダイアログで、次の情報を指定します。
 - a. ターゲットファイルシステム: ドロップダウンメニューからターゲットファイルシステムを選択します。
 - b. *ターゲット Storage VM *: ドロップダウンメニューからターゲット Storage VMを選択します。
 - c. バックアップ名: ドロップダウンメニューからバックアップ名を選択します。
 - d. リストアされたボリューム名: リストアされたボリュームの名前を入力します。
9. リストア処理に必要なファイルシステムの容量を確認します。

ファイルシステムの容量が制限されると、次のような状況が発生する可能性があります。

- 復元により、使用済み容量が指定したしきい値を超える可能性があります。復元操作を完了できません。考慮する"手動によるSSDストレージ階層の容量の追加"または、Workload Factory を選択して、SSD ストレージ層の容量を自動的に追加します。
- 復元には追加の SSD 容量が必要です。続行するには、Workload Factory が SSD ストレージ層の容量を自動的に追加するように選択する必要があります。

10. [* Restore] を選択します。

レプリケーションを使用する

NetApp Workload Factoryでレプリケーション関係を作成する

予期しない災害が発生した場合のデータ損失を回避するために、NetApp Workload FactoryでFSx for ONTAPファイルシステムのレプリケーション関係を作成します。レプリケーションは、2つのFSx for ONTAPファイルシステム間、およびオンプレミスのONTAPシステムとFSx for ONTAPファイルシステム間でサポートされています。

タスクの内容

災害が地域に影響を及ぼした場合には、レプリケーションによってデータが保護されます。

この操作は、FSx for ONTAP ファイルシステムまたはオンプレミス ONTAP システムのソースボリュームのレプリケーション関係を作成します。

ターゲットファイルシステム内のレプリケートされたボリュームは、データ保護 (DP) ボリュームであり、命名形式はです。 {OriginalVolumeName}_copy

不変ファイルを含むソース ボリュームをレプリケートすると、ソース ボリューム内の不変ファイルの保持期間が終了するまで、ターゲット ボリュームとファイル システムはロックされたままになります。不変ファイル機能は、Amazon FSx for NetApp ONTAP ファイル システムの["ボリュームを作成する"](#)ときに使用できます。

- iSCSI または NVMe プロトコルを使用するブロック ボリュームでは、レプリケーションはサポートされていません。
- 1つのソース（読み取り/書き込み）ボリュームまたは1つのデータ保護 (DP) ボリュームをレプリケートできます。カスケードレプリケーションはサポートされていますが、3番目のホップはサポートされていません。詳細については、をご覧ください ["カスケードレプリケーション"](#)。

開始する前に

開始する前に、これらの要件を確認してください。

- レプリケーション関係のターゲットに使用するFSx for ONTAPファイル システムが1つ必要です。
- レプリケーション関係に使用する FSx for ONTAP ファイル システムには、関連付けられたリンクが必要です。["既存のリンクを関連付ける方法、または新しいリンクを作成して関連付ける方法を学びます"](#)。リンクを関連付けたら、この操作に戻ります。
- オンプレミス ONTAP システムから FSx for ONTAP ファイルシステムへのレプリケーションの場合は、オンプレミス ONTAP システムが検出されていることを確認してください。

ファイル システム内の特定のボリュームまたはすべてのボリュームを複製するには、次の手順に従います。

手順

1. いずれかを使用してログインし["コンソールエクスペリエンス"](#)ます。
2. メニューを選択  次に*ストレージ*を選択します。
3. [ストレージ] メニューから、**FSx for ONTAP** を選択します。

4. *FSx for ONTAP*から、複製するボリュームを含むファイルシステムのアクションメニューを選択し、*管理*を選択します。
 5. ファイルシステム内のすべてのボリュームをレプリケートするか、選択したボリュームをレプリケートします。
 - ファイルシステム内のすべてのボリュームをレプリケートするには、ファイルシステムの概要で*Replicate data*を選択します。
 - 選択したボリュームをレプリケートするには：ファイルシステムの概要で*[ボリューム]*タブを選択します。
 6. [ボリューム]テーブルで1つ以上のボリュームを選択し、*[データのレプリケート]*を選択します。
- a. 使用ケース: レプリケーションの次の使用ケースのいずれかを選択します。選択したユースケースに応じて、Workload Factory はベストプラクティスに従って推奨値をフォームに入力します。フォームに入力する際に、推奨値を受け入れることも、変更することもできます。
- 移行：ターゲットのFSx for ONTAPファイルシステムにデータを転送
 - ホットディザスタリカバリ：重要なワークロードの高可用性と迅速なディザスタリカバリを実現
 - コールド/アーカイブのディザスタリカバリ：
 - コールドディザスタリカバリ：目標復旧時間（RTO）とオブジェクト復旧時点（RPO）を長くしてコストを削減
 - アーカイブ：長期的なストレージとコンプライアンスのためにデータをレプリケート
 - その他
- さらに、ユースケースの選択によって、レプリケーションポリシー（SnapMirrorポリシー（ONTAP））も決まります。レプリケーションポリシーを説明するために使用される用語は、から来て["ONTAP 9 のドキュメント"](#)います。
- 移行などの場合、レプリケーションポリシーは_MirrorAllSnapshots_です。_MirrorAllSnapshots_は、すべてのSnapshotと最新のアクティブファイルシステムをミラーリングする非同期ポリシーです。
 - ホット、コールド、またはアーカイブのディザスタリカバリの場合、レプリケーションポリシーは_MirrorAndVault_と呼ばれます。_MirrorAndVault_は、最新のアクティブファイルシステムと日単位および週単位のSnapshotをミラーリングするための非同期バックアップポリシーです。
- すべてのユースケースで、Snapshotの長期保持を有効にすると、デフォルトのレプリケーションポリシーは_MirrorAndVault_です。
- b. * FSx for ONTAPファイルシステム*：対象となるFSx for ONTAPファイルシステムのクレデンシャル、リージョン、FSx for ONTAPファイルシステム名を選択します。
 - c. * Storage VM名*：ドロップダウンメニューからStorage VMを選択します。選択したストレージ VMは、このレプリケーション関係で選択されたすべてのボリュームのターゲットになります。
 - d. ボリューム名：ターゲットボリューム名は次の形式で自動的に生成されます {OriginalVolumeName}_copy。自動生成されたボリューム名を使用するか、別のボリューム名を入力できます。

- e. 階層化ポリシー：ターゲットボリュームに格納されているデータの階層化ポリシーを選択します。階層化ポリシーは、選択したユースケースに応じた推奨される階層化ポリシーにデフォルトで設定されます。

バランス (自動) は、Workload Factory コンソールを使用してボリュームを作成するときのデフォルトの階層化ポリシーです。ボリューム階層化ポリシーの詳細については、以下を参照してください。["ボリュームのストレージ容量" AWS FSx for NetApp ONTAP ドキュメント](#)。ワークロード ファクトリーは、ワークロード ファクトリー コンソールで階層化ポリシーにユースケース ベースの名前を使用し、括弧内に FSx for ONTAP 階層化ポリシー名を含めることに注意してください。

移行ユースケースを選択した場合、Workload Factory はソース ボリュームの階層化ポリシーをターゲット ボリュームにコピーすることを自動的に選択します。階層化ポリシーのコピーの選択を解除し、レプリケーション対象として選択したボリュームに適用する階層化ポリシーを選択できます。

- a. 最大転送速度：* Limited *を選択し、最大転送速度をMB/秒単位で入力します。または、*無制限*を選択します。

制限がないと、ネットワークとアプリケーションのパフォーマンスが低下する可能性があります。また、FSx for ONTAP ファイルシステムは、主にディザスタリカバリに使用されるワークロードなど、重要なワークロードには無制限の転送速度を推奨します。

7. [Replication settings]で、次の情報を指定します。

- a. レプリケーション間隔：ソースボリュームからターゲットボリュームにSnapshotを転送する頻度を選択します。
- b. 長期保存：オプションで、長期保存用のスナップショットを有効にします。長期保存により、サイト全体に障害が発生してもビジネスサービスの運用を継続できるため、アプリケーションをセカンダリ コピーを使用して透過的にフェイルオーバーできます。

長期保存のないレプリケーションでは、*MirrorAllSnapshots* ポリシーが使用されます。長期保存を有効にすると、レプリケーションに *MirrorAndVault* ポリシーが割り当てられます。

長期保持を有効にする場合は、既存のポリシーを選択するか、新しいポリシーを作成して、レプリケートするSnapshotと保持する数を定義します。



長期保存には、ソースラベルとターゲットラベルを一致させる必要があります。必要に応じて、Workload Factoryで不足しているラベルが作成することができます。

- 既存のポリシーを選択：ドロップダウンメニューから既存のポリシーを選択します。
 - 新しいポリシーを作成：*ポリシー名*を入力します。
- c. 不変のスナップショット: オプション。このポリシーで作成されたSnapshotが保持期間中に削除されないようにするには、[変更不可のSnapshotを有効にする]*を選択します。
- [Retention Period]*を時間、日、月、または年数で設定します。
 - * Snapshotポリシー*：表で、Snapshotポリシーの頻度と保持するコピーの数を選択します。Snapshotポリシーは複数選択できます。
- d. S3 アクセス ポイント: オプションで、S3 アクセス ポイントを接続して、AWS S3 API 経由で NFS または SMB/CIFS ボリューム上にある FSx for ONTAP ファイル システム データにアクセスします。ファイル アクセス タイプのみがサポートされます。以下の詳細を提供します:
- S3 アクセス ポイント名: S3 アクセス ポイントの名前を入力します。

- ユーザー: ボリュームへのアクセス権を持つ既存のユーザーを選択するか、新しいユーザーを作成します。
 - ユーザー タイプ: ユーザー タイプとして **UNIX** または **Windows** を選択します。
 - ネットワーク構成: インターネット または 仮想プライベート クラウド (**VPC**) を選択します。選択するネットワークの種類によって、アクセス ポイントがインターネットからアクセスできるか、特定の VPC に制限されるかが決まります。
 - メタデータを有効にする: メタデータを有効になると、S3 アクセス ポイントからアクセスできるすべてのオブジェクトを含む S3 テーブルが作成され、監査、ガバナンス、自動、分析、最適化に使用できるようになります。メタデータを有効になると追加の AWS コストが発生します。詳細については、["Amazon S3 價格設定ドキュメント"](#)を参照してください。
- e. **S3** アクセス ポイント タグ: オプションで、最大 50 個のタグを追加できます。

8. 「* Create *」を選択します。

結果

レプリケーション関係は、ターゲットのFSx for ONTAPファイルシステムの*レプリケーション関係*タブに表示されます。

NetApp Workload Factoryでレプリケーション関係を初期化する

ソース ボリュームとターゲット ボリューム間のレプリケーション関係を初期化して、スナップショットとNetApp Workload Factory 内のすべてのデータ ブロックを転送します。

タスクの内容

初期化では、_baseline_transferが実行されます。ソースボリュームのSnapshotが作成され、そのSnapshotおよびSnapshotが参照するすべてのデータブロックがターゲットボリュームに転送されます。

開始する前に

この処理をいつ完了するかを検討してください。初期化には時間がかかる場合があります。ベースライン転送はオフピークの時間帯に実行することを推奨します。

手順

1. いずれかを使用してログインし["コンソールエクスペリエンス"](#)ます。
2. メニューを選択  次に*ストレージ*を選択します。
3. [ストレージ] メニューから、**FSx for ONTAP** を選択します。
4. *FSx for ONTAP*から、更新するファイルシステムのアクションメニューを選択し、*管理*を選択します。
5. ファイルシステムの概要で、*[レプリケーション関係]*タブを選択します。
6. レプリケーション関係タブで、初期化するレプリケーション関係のアクション メニューを選択します。
7. [初期化]*を選択します。
8. [Initialize relationship]ダイアログで、*[Initialize]*を選択します。

AIを搭載したNetAppの自律型ランサムウェア保護でデータを保護

NetApp Autonomous Ransomware Protection with AI (ARP/AI) でデータを保護します。これは、NAS (NFS/SMB) 環境でのワークロード分析を使用して、ランサムウェア攻撃の可能性がある異常なアクティビティを検出し、警告する機能です。攻撃が疑われる場合、ARP/AI はデータを復元できる新しい不变のスナップショットも作成します。

タスクの内容

ARP/AI を使用して、身代金が支払われるまで攻撃者がデータを保持するサービス拒否攻撃から保護します。ARP/AI は、以下に基づいてリアルタイムのランサムウェア検出を提供します。

- 受信データを暗号化またはプレーンテキストとして識別します。
- 以下を検出する分析：
 - **Entropy**：ファイル内のデータのランダム性の評価
 - ファイル拡張子タイプ：通常の拡張子タイプと一致しない拡張子
 - ファイル**IOPS**：データ暗号化による異常なボリュームアクティビティの急増

ARP/AI は、少数のファイルが暗号化されただけでほとんどのランサムウェア攻撃の拡散を検出し、データを保護するためのアクションを自動的に実行し、疑わしい攻撃が発生していることを警告します。

ARP/AI 機能は、Amazon FSx for NetApp ONTAPが実行するONTAPバージョンに応じて自動的に更新されるため、手動で更新する必要はありません。

学習モードとアクティブモード

ARP/AI は最初に 学習モード で動作し、その後自動的に アクティブ モード に切り替わります。

- 学習モード: ARP/AI を有効にすると、学習モード で実行されます。学習モードでは、FSx for ONTAP ファイルシステムは、エントロピー、ファイル拡張子の種類、ファイル IOPS などの分析領域に基づいてアラート プロファイルを作成します。ファイル システムが ARP/AI を学習モードで十分な時間実行し、ワークロードの特性を評価した後、Workload Factory は自動的に ARP/AI を アクティブ モード に切り替え、データの保護を開始します。
- アクティブ モード: ARP/AI が アクティブ モード に切り替わると、脅威が検出された場合に FSx for ONTAP はデータを保護するために ARP/AI スナップショットを作成します。

アクティブモードで、ファイル拡張子が異常としてフラグされている場合は、アラートを評価する必要があります。アラートに対処してデータを保護したり、アラートを誤検出としてマークしたりできます。アラートをfalse positiveとしてマークすると、アラートプロファイルが更新されます。たとえば、新しいファイル拡張子によってアラートがトリガーされ、アラートをfalse positiveとしてマークした場合、次回そのファイル拡張子が監視されたときにアラートは受信されません。

ブロック デバイスを含むFlexVolボリュームは、ARP/AI をアクティブ モードで起動します。

サポートされない構成

次の構成では、ARP/AI の使用はサポートされません。

- iSCSI ボリューム
- NVMeボリューム

ファイルシステムまたはボリュームのARP/AIを有効にする

ファイル システムに対して ARP/AI を有効にすると、既存の NAS および新しく作成された NAS (NFS/SMB) ボリュームすべてに自動的に保護が追加されます。個々のボリュームに対して ARP/AI を有効にすることもできます。

ARP/AI を有効にした後、攻撃が発生し、それが実際の攻撃であると判断された場合、Workload Factory は 4 時間ごとに最大 6 個のスナップショットを取得するスナップショット ポリシーを自動的に設定します。各スナップショットは 2 ~ 5 日間ロックされます。

開始する前に

ファイル システムまたはボリュームに対して ARP/AI を有効にするには、リンクを関連付ける必要があります。["既存のリンクを関連付ける方法、または新しいリンクを作成して関連付ける方法を学びます"](#)。リンクが関連付けられたら、この操作に戻ります。

ファイルシステムの**ARP/AI**を有効にする

手順

1. いずれかを使用してログインし"**コンソールエクスペリエンス**"ます。
2. メニューを選択  次に*ストレージ*を選択します。
3. [ストレージ] メニューから、**FSx for ONTAP** を選択します。
4. *FSx for ONTAP*から、ファイルシステムのアクションメニューを選択してARP/AIを有効にし、*管理*を選択します。
5. [情報] の下で、[Autonomous Ransomware Protection] の横にある鉛筆アイコンを選択します。**Autonomous Ransomware Protection** 行の上にマウスを置くと、矢印の横に鉛筆アイコンが表示されます。
6. NetApp Autonomous Ransomware Protection with AI (ARP/AI) ページから、次の操作を行います。
 - a. 機能を有効または無効にします。
 - b. 自動スナップショット作成: 保持するスナップショットの最大数と、スナップショットを取得する間隔を選択します。デフォルトでは、4時間ごとに6回のスナップショットが作成されます。
 - c. 不変スナップショット: 不変スナップショットを保持するデフォルトの保持期間（時間単位）と最大日数を選択します。このオプションを有効にすると、指定された保持期間が終了するまでスナップショットを削除または変更できなくなります。
 - d. 検出: オプションで、次のいずれかのパラメータを選択して、自動的にスキャンし、異常を検出します。
7. 続行するには、ステートメントを受け入れます。
8. [適用]*を選択して変更を保存します。

ボリュームの**ARP/AI**を有効にする

手順

1. いずれかを使用してログインし"**コンソールエクスペリエンス**"ます。
2. メニューを選択  次に*ストレージ*を選択します。
3. [ストレージ] メニューから、**FSx for ONTAP** を選択します。
4. *FSx for ONTAP*から、ファイルシステムのアクションメニューを選択してARP/AIを有効にし、*管理*を選択します。
5. [ボリューム] タブから、ARP/AI を有効にするボリュームのアクション メニューを選択し、次にデータ保護アクション、**ARP/AI** の管理 を選択します。
6. ARP/AI の管理ダイアログで、次の操作を行います。
 - a. 機能を有効または無効にします。
 - b. 検出: オプションで、次のいずれかのパラメータを選択して、自動的にスキャンし、異常を検出します。
7. 続行するには、ステートメントを受け入れます。
8. [適用]*を選択して変更を保存します。

ランサムウェア攻撃を検証

攻撃が誤ったアラームであるか、本物のランサムウェアインシデントであるかを特定

手順

1. いざれかを使用してログインし"コンソールエクスペリエンス"ます。
2. メニューを選択  次に*ストレージ*を選択します。
3. [ストレージ] メニューから、**FSx for ONTAP** を選択します。
4. *FSx for ONTAP*から、ランサムウェア攻撃を検証するファイル システムを選択します。
5. ファイルシステムの概要で、*[ボリューム]*タブを選択します。
6. [Autonomous Ransomware Protection] タイルで[Analyze Attacks]*を選択します。
7. 攻撃イベントレポートをダウンロードして、ファイルやフォルダが侵害されていないかどうかを確認し、攻撃が発生したかどうかを判断します。
8. 攻撃が発生していない場合は、テーブル内のボリュームに対して* False alarm を選択し、 Close *を選択します。
9. 攻撃が発生した場合は、表のボリュームに対して* Real Attack を選択します。 [**Restore compromised volume data**] ダイアログが開きます。すぐに進むか、[閉じる]*を選択して後でリカバリプロセスを完了することができます [データをリカバリ](#)。

ランサムウェア攻撃のあとにデータをリカバリ

攻撃の疑いが検出されると、システムはその時点のボリュームSnapshotを作成し、そのコピーをロックします。後で攻撃が確認された場合は、ARP/AI スナップショットを使用して、影響を受けたファイルまたはボリューム全体を復元できます。

ロックされたSnapshotは保持期間が終了するまで削除できません。ただし、後で攻撃をfalse positiveとしてマークすると、ロックされたコピーは削除されます。

影響を受けるファイルと攻撃時間を把握していれば、ボリューム全体をSnapshotの1つに戻すだけでなく、さまざまなSnapshotから影響を受けるファイルを選択してリカバリできます。

手順

1. いざれかを使用してログインし"コンソールエクスペリエンス"ます。
2. メニューを選択  次に*ストレージ*を選択します。
3. [ストレージ] メニューから、**FSx for ONTAP** を選択します。
4. *FSx for ONTAP*から、データを回復するファイルシステムを選択します。
5. ファイルシステムの概要で、*[ボリューム]*タブを選択します。
6. [Autonomous Ransomware Protection] タイルで[Analyze Attacks]*を選択します。
7. 攻撃が発生した場合は、表のボリュームに対して* Real Attack *を選択します。
8. [**Restore compromised volume data**] ダイアログで、指示に従って、ファイルレベルまたはボリュームレベルでリストアします。ほとんどの場合、ボリューム全体ではなくファイルをリストアします。
9. リストアが完了したら、*[閉じる]*を選択します。

結果

侵害されたデータが復元されました。

NetApp Workload Factoryでボリュームをクローンする

NetApp Workload Factory でボリュームのクローンを作成し、テスト用に元のボリュームの読み取り/書き込みボリュームを作成します。

クローンには、データの現在のポイントインタイムの状態が反映されます。クローンを使用すると、追加のユーザに本番環境のデータへのアクセスを許可することなく、データへのアクセスを許可することもできます。

タスクの内容

ボリュームクローニングは、FlexCloneボリュームでのみサポートされます。

ボリュームがクローニングされると、親ボリュームのSnapshotへの参照を使用して書き込み可能なボリュームが作成されます。クローンの作成は数秒で完了します。クローニングされたデータはボリュームクローンには格納されず、親ボリュームに格納されます。クローン作成後にボリュームに書き込まれた新しいデータは、クローン上に格納されます。

クローンボリュームに親ボリュームのすべてのデータと、作成後にクローンに追加された新しいデータを格納するには、親ボリュームからを実行する必要が "クローンをスプリットする" あります。また、親ボリュームにクローンがある場合は削除できません。親ボリュームを削除するには、クローンをスプリットする必要があります。

手順

1. いずれかを使用してログインし"コンソールエクスペリエンス"ます。
2. メニューを選択  次に*ストレージ*を選択します。
3. [ストレージ] メニューから、**FSx for ONTAP** を選択します。
4. **FSx for ONTAP** から、クローンを作成するボリュームが含まれている FSx for ONTAPファイル システムのアクション メニューを選択し、管理を選択します。
5. ファイルシステムの[概要]タブで、*[ボリューム]*タブを選択します。
6. 「ボリューム」タブで、クローンを作成するボリュームのアクション メニューを選択します。
7. を選択し、[ボリュームのクローニング]*を選択します。
8. [Clone volume]ダイアログで、ボリュームクローンの名前を入力します。
9. 「* Clone *」を選択します。

NetApp Workload Factory でオンプレミスのONTAPクラスタ データを使用する

NetApp Workload Factory でオンプレミスのONTAPデータを検出して複製し、AI ナレッジ ベースの強化に使用できるようにします。

タスクの内容

オンプレミスのONTAPクラスタのデータを使用するには、まずオンプレミスのONTAPクラスタを検出する必要があります。オンプレミスのONTAPクラスタを検出したら、次のいずれかのユースケースでデータを使用できます。

ユースケース

生成AIワークロードの主なユースケースは、この一連のタスクの焦点です。

- 生成AIワークロード：オンプレミスのONTAPボリュームのデータをFSx for ONTAPファイルシステムにレプリケートして、データを使用できるようにし "AIナレッジベースの充実" ます。
- クラウドへのバックアップと移行：オンプレミスのONTAPボリュームデータをFSx for ONTAPファイルシステムにレプリケートし、クラウド内のバックアップとして使用できます。
- データ階層化：レプリケーション後、アクセス頻度の低いオンプレミスのONTAPボリュームデータを、SSDストレージ階層から容量プールストレージ階層に階層化できます。

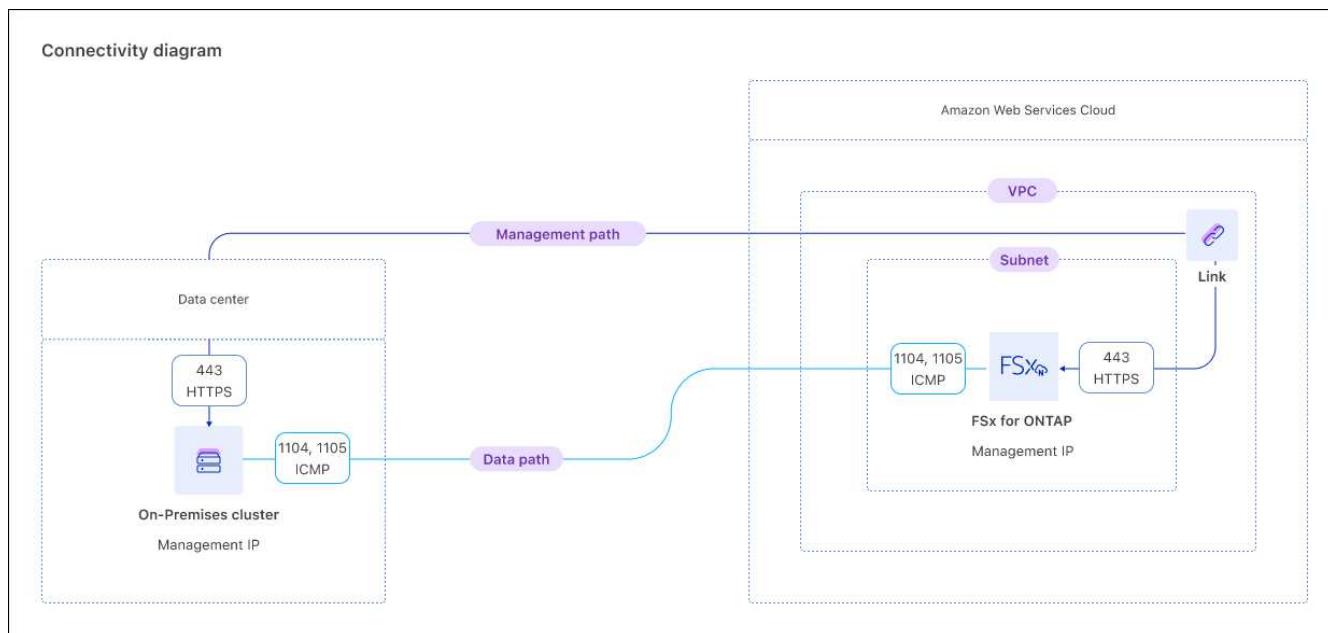
オンプレミスの ONTAP クラスタを検出

NetApp Workload Factory でオンプレミスのONTAPクラスターを検出し、Amazon FSx for NetApp ONTAPファイルシステムにデータを複製できるようにします。

開始する前に

作業を開始する前に、次の情報が揃っていることを確認してください。

- レプリケーションのためのFSx for ONTAPファイルシステム。
- 検出されたオンプレミスクラスタに関する接続リンク。リンクがない場合は、リンクをクリックする必要があります "作成" ます。
- 必要な権限を持つONTAPユーザクレデンシャル。
- オンプレミスのONTAPバージョン9.8以降。
- 次の図に示すように接続します。



手順

- いずれかを使用してログインし "コンソールエクスペリエンス" ます。
- メニューを選択 次に *ストレージ* を選択します。

3. [On-Premises ONTAP *]タブを選択します。
4. [検出]*を選択します。
5. 前提条件を確認し、* Next *を選択します。
6. [Discover ONTAP on-premise]ページの*[Cluster configuration]*で、次の情報を指定します。
 - a. リンク: リンクを選択します。リンクはオンプレミス クラスターに関連付けられ、クラスターと Workload Factory 間の接続が作成されます。
リンクを作成していない場合は、指示に従って操作に戻り、リンクを選択します。
 - b. クラスタIPアドレス: レプリケートするオンプレミスのONTAPクラスタのIPアドレスを指定します。
 - c. * ONTAPクレデンシャル*: オンプレミスのONTAPクラスタのONTAPクレデンシャルを入力します。ユーザに必要な権限があることを確認します。
7. 検出プロセスを開始するには、*[検出]*を選択します。

結果

オンプレミスのONTAPクラスタが検出され、* On-Premises ONTAP *タブに表示されます。

オンプレミスのONTAPクラスタとのデータを表示できるようになりまし[FSx for ONTAPファイルシステムにデータをレプリケート](#)た。

オンプレミスのONTAPクラスタからボリュームデータをレプリケート

オンプレミスのONTAPクラスタからFSx for ONTAPファイルシステムにボリュームデータをレプリケートします。レプリケーション後は、データを使用してAIのナレッジベースを充実させることができます。

開始する前に

- ・ボリュームデータをレプリケートするには、オンプレミスのONTAPクラスタを検出する必要があります。
- ・レプリケーションのターゲットとして使用できるFSx for ONTAPファイルシステムが必要です。
- ・レプリケーション関係に使用するオンプレミスのONTAPクラスタとFSx for ONTAPファイルシステムの両方に、リンクが関連付けられている必要があります。["既存のリンクを関連付ける方法、または新しいリンクを作成して関連付ける方法を学びます"](#)です。リンクが関連付けられたら、この操作に戻ります。

手順

1. いずれかを使用してログインし["コンソールエクスペリエンス"](#)ます。
2. メニューを選択  次に*ストレージ*を選択します。
3. [ストレージ] メニューから、[オンプレミスONTAP] を選択します。
4. Storage VMでボリュームを検索するには、ドロップダウンから*[Storage VMの選択]*を選択します。
5. レプリケートするボリュームを1つ以上選択し、*[レプリケート]*を選択します。
6. [Create replication]ページの[Replication target]で、次の情報を指定します。
 - a. * FSx for ONTAPファイルシステム* : 対象となるFSx for ONTAPファイルシステムのクレデンシャル、リージョン、FSx for ONTAPファイルシステム名を選択します。
 - b. * Storage VM名* : ドロップダウンメニューからStorage VMを選択します。

- c. ボリューム名：ターゲットボリューム名は次の形式で自動的に生成されます
`{OriginalVolumeName}_copy`。自動生成されたボリューム名を使用するか、別のボリューム名を入力できます。
- d. データの階層化：ターゲットボリュームに格納されているデータの階層化ポリシーを選択します。
 - 自動: Workload Factory FSx for ONTAPユーザー インターフェイスを使用してボリュームを作成するときのデフォルトの階層化ポリシー。特定の期間、ユーザー データとスナップショットを含むすべてのコールド データを容量プールのストレージ層に階層化します。
 - * Snapshotのみ*: スナップショットデータのみを容量プールストレージ階層に階層化します。
 - なし：ボリュームのすべてのデータをプライマリストレージ階層に保持します。
 - * all *：すべてのユーザデータとSnapshotデータをコールドとしてマークし、容量プールストレージ階層に格納します。

一部の階層化ポリシーには、最小クーリング期間が関連付けられています。最小クーリング期間は、ボリューム内のアクセス頻度の低いユーザデータが「コールド」とみなされて大容量プールストレージ階層に移動されるまでの時間 (*cooling days*) を設定します。クーリング期間は、データがディスクに書き込まれた時点から開始されます。

ボリューム階層化ポリシーの詳細については、AWS FSx for NetApp ONTAP ドキュメントのを参照してください ["ボリュームのストレージ容量"](#)。

- a. 最大転送速度：* Limited *を選択し、最大転送速度をMiB/秒で入力します。または、*無制限*を選択します。

制限がないと、ネットワークとアプリケーションのパフォーマンスが低下する可能性があります。また、FSx for ONTAPファイルシステムは、主にディザスタリカバリに使用されるワークロードなど、重要なワークロードには無制限の転送速度を推奨します。

7. [Replication settings]で、次の情報を指定します。

- a. レプリケーション間隔：ソースボリュームからターゲットボリュームにSnapshotを転送する頻度を選択します。
- b. 長期保存：オプションで、長期保存用のスナップショットを有効にします。

長期保持を有効にする場合は、既存のポリシーを選択するか、新しいポリシーを作成して、レプリケートするSnapshotと保持する数を定義します。

- 既存のポリシーの場合は、*[既存のポリシーを選択]*を選択し、ドロップダウンメニューから既存のポリシーを選択します。
- 新しいポリシーの場合は、*[新しいポリシーを作成する]*を選択し、次の情報を指定します。
 - ポリシーナー：ポリシーナーを入力します。
 - * Snapshotポリシー*：表で、Snapshotポリシーの頻度と保持するコピーの数を選択します。Snapshotポリシーは複数選択できます。

8. 「* Create *」を選択します。

結果

レプリケーション関係は、ターゲットのFSx for ONTAPファイルシステムの*レプリケーション関係*タブに表示されます。

NetApp Workload Factory からオンプレミスのONTAPクラスタを削除する

必要に応じて、オンプレミスのONTAPクラスターをNetApp Workload Factory から削除します。

開始する前に

解除された関係が残らないようにするために、クラスタを削除する前にオンプレミスのONTAPクラスタ内のボリュームを対象にする必要があります"既存のレプリケーション関係をすべて削除する"。

手順

1. いざれかを使用してログインし"コンソールエクスペリエンス"ます。
2. メニューを選択  次に*ストレージ*を選択します。
3. [ストレージ] メニューから、[オンプレミスONTAP] を選択します。
4. 削除するオンプレミスのONTAPクラスタを選択します。
5. アクション メニューを選択し、ワーカロード ファクトリーから削除 を選択します。

結果

オンプレミスのONTAPクラスターがNetApp Workload Factory から削除されます。

サイバーボルトでデータを保護

サイバーボルト ボリュームは、データのバックアップ コピーを保存し、ランサムウェア攻撃やその他のサイバー脅威からデータを保護するために使用する、隔離された安全なストレージの場所です。ボルト作成の一環として、サイバーボルト ボリュームを作成し、すべてのクライアント プロトコルを無効にし、ソース ボリュームとサイバーボルト ボリューム間のレプリケーション関係を設定し、サイバーボルト ボリューム上に不变のスナップショットを作成します。

サイバーボルトとは何ですか？

サイバーボルトは、主要な IT インフラストラクチャとは別の隔離された環境に重要なデータを保存する特定のデータ保護技術です。

サイバーボルトは、マルウェア、ランサムウェア、さらには内部脅威など、メイン ネットワークに影響を及ぼす脅威の影響を受けない、「エアギャップ」された、変更不可能で消去不可能なデータ リポジトリです。サイバーボルトは、変更不可能かつ消去不可能なスナップショットによって実現できます。

従来の方法を使用するエアギャップ バックアップでは、スペースを作成し、プライマリ メディアとセカンダリ メディアを物理的に分離する必要があります。メディアをオフサイトに移動したり、接続を切断したりすることで、悪意のある人物がデータにアクセスできなくなります。これによりデータは保護されますが、回復時間が遅くなる可能性があります。

ONTAPサイバーボルト向け FSx

Amazon FSx for NetApp ONTAP は、サイバーボルトのソースおよびターゲットとしてサポートされています。

導入

Workload Factory は、サイバーボルト アーキテクチャの作成を支援します。NetAppに連絡してサイバーボルトの実装に関心があることを伝えると、NetApp のスペシャリストがお客様に連絡して要件について話

し合います。

開始するには、ng-FSx-CyberVault@netapp.com に電子メールを送信してください。

関連情報

サイバー金庫とこのアーキテクチャの設定方法の詳細については、["ONTAPサイバー ポートのドキュメント"](#)。

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を隨時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5225.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。