ONTAPサイバーボールトによるデータ保護

NetApp data management solutions

NetApp
August 18, 2025

目次

ONTAPサイバーボールトによるデータ保護

ONTAPサイバーボールトの概要

サイバー金庫の実装を必要とする主な脅威は、サイバー攻撃、特にランサムウェアとデータ侵害の蔓延と巧妙化の進行です。"フィッシングの増加に伴い"認証情報の窃盗方法がますます巧妙化しているため、ランサムウェア攻撃を開始するために使用された認証情報は、インフラストラクチャ システムへのアクセスに使用される可能性があります。このような場合、強化されたインフラストラクチャ システムであっても攻撃を受けるリスクがあります。侵害されたシステムに対する唯一の防御策は、データを保護してサイバー金庫に隔離することです。

NetApp のONTAPベースのサイバー ボールトは、組織に最も重要なデータ資産を保護するための包括的かつ柔軟なソリューションを提供します。 ONTAP、強力な強化手法による論理エアギャップを活用することで、進化するサイバー脅威に耐性のある、安全で分離されたストレージ環境を構築できます。 ONTAPを使用すると、ストレージ インフラストラクチャの俊敏性と効率性を維持しながら、データの機密性、整合性、可用性を確保できます。

> 2024年7月以降、これまでPDFで公開されていたテクニカル レポートの内容がONTAPの製品ドキュメントに統合されました。さらに、このドキュメントのような新しい技術レポート (TR) には、TR 番号が付与されなくなります。

サイバーボールトとは何ですか?

サイバー ボールトは、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。

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与える脅威の影響を受けない、「エアギャップ」、不変、*消去不可能*なデータリポジトリです。サイバー金庫は、*不変*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。

NetAppのサイバーボールトへのアプローチ

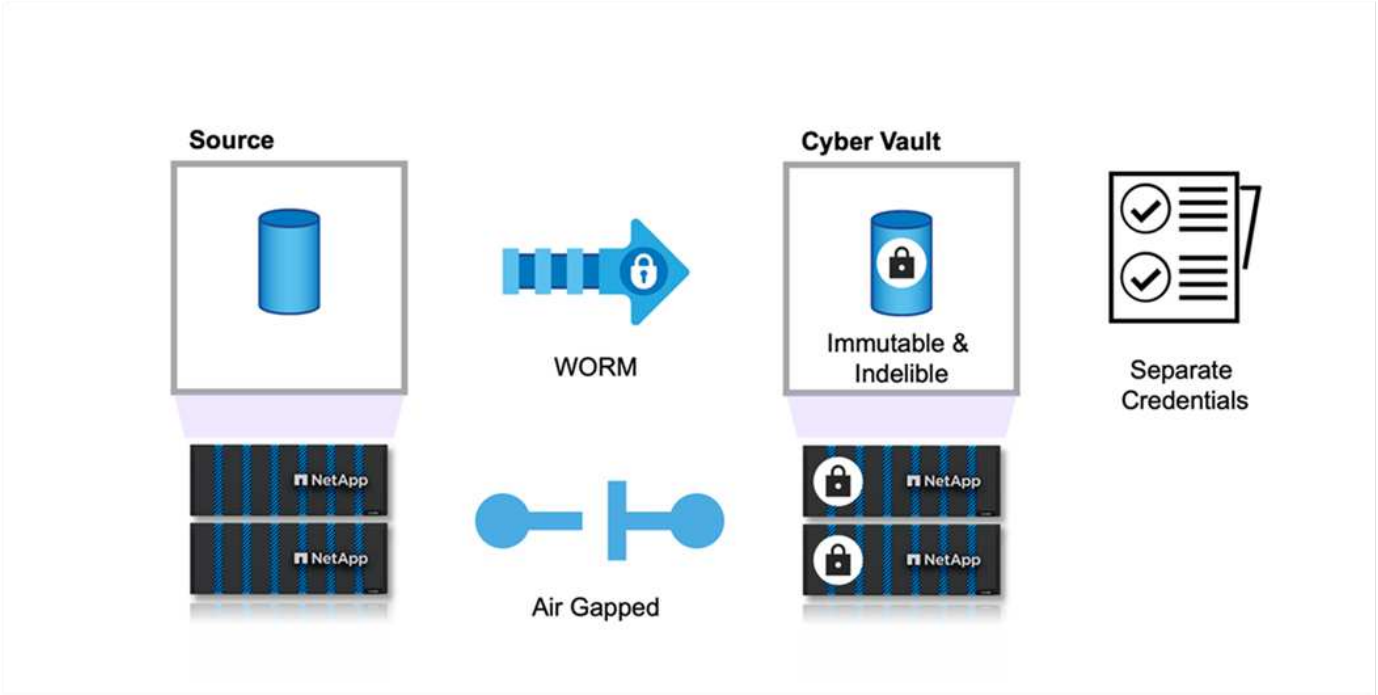
サイバー ボールト向けNetAppリファレンス アーキテクチャの主な機能は次のとおりです。

- 安全で分離されたストレージ インフラストラクチャ (例: エアギャップ ストレージ システム)
- データのコピーは例外なく*不変*かつ*消去不可能*でなければならない
- 厳格なアクセス制御と多要素認証
- 迅速なデータ復元機能

ONTAPを搭載したNetAppストレージを、エアギャップ型サイバーボールトとして活用することができます。"SnapLock Complianceによる Snapshot コピーの WORM 保護" 。 Cyber vault では、 SnapLock

Compliance のすべての基本的なタスクを実行できます。一度設定すると、Cyber vault ボリュームは自動的に保護されるため、スナップショット コピーを手動で WORM にコミットする必要がなくなります。論理的エアギャップに関する詳細は、こちらをご覧ください。"ブログ"

SnapLock Compliance は、銀行および金融規制 SEC 70-a-4(f)、FINRA 4511(c)、CFTC 1.31(c)-(d) に準拠するために使用されます。これらの規制に準拠していることは Cohasset Associates によって認定されています (監査レポートはリクエストに応じて入手可能)。この認証を備えたSnapLock Complianceを使用すると、銀行記録の保持と取得を確実にするために世界最大の金融機関が信頼している、データのエアギャップのための強化されたメカニズムが得られます。



Cyber Vault ONTAP用語

これらは、サイバー ボールト アーキテクチャでよく使用される用語です。

自律型ランサムウェア保護 **(ARP)** - 自律型ランサムウェア保護 (ARP) 機能は、NAS (NFS および SMB) 環境のワークロード分析を使用して、ランサムウェア攻撃の兆候となる可能性のある異常なアクティビティをプロアクティブにリアルタイムで検出し、警告します。攻撃の疑いが検出された場合、定期的なSnapshotコピーによる既存の保護に加えて、新しいSnapshotコピーも作成されます。詳細については、"自律型ランサムウェア保護に関するONTAPドキュメント"

エアギャップ（論理） - ONTAPでNetAppストレージを論理エアギャップサイバーボールトとして構成することができます。"SnapLock Complianceによる Snapshot コピーの WORM 保護"

エアギャップ **(物理)** - 物理的なエアギャップ システムにはネットワーク接続がありません。テープ バックアップを使用すると、イメージを別の場所に移動できます。 SnapLock Compliance の論理エアギャップは、物理的なエアギャップ システムと同様に堅牢です。

要塞ホスト - 攻撃に耐えられるように構成された、隔離されたネットワーク上の専用コンピューター。

不変のスナップショット コピー - 例外なく変更できないスナップショット コピー (サポート組織やストレージ システムを低レベル フォーマットする機能を含む)。

削除できないスナップショット コピー - 例外なく削除できないスナップショット コピー (サポート組織やストレージ システムを低レベル フォーマットする機能を含む)。

改ざん防止スナップショット コピー - 改ざん防止スナップショット コピーは、 SnapLock Complianceクロック機能を使用して、指定された期間、スナップショット コピーをロックします。これらのロックされたスナップショットは、どのユーザーまたはNetAppサポートでも削除できません。ランサムウェア攻撃、マルウェア、ハッカー、不正な管理者、または誤った削除によってボリュームが侵害された場合は、ロックされたスナップショット コピーを使用してデータを回復できます。詳細については、"改ざん防止スナップショットコピーに関するONTAPドキュメント"

- SnapLock* - SnapLock は、規制やガバナンスの目的で WORM ストレージを使用してファイルを変更されていない形式で保持する組織向けの高性能コンプライアンス ソリューションです。詳細については、"SnapLockに関するONTAPドキュメント" 。
- SnapMirror* - SnapMirror は、データを効率的に複製するように設計された災害復旧レプリケーション テクノロジーです。 SnapMirror は、オンプレミスまたはクラウド内のセカンダリ システムにミラー (またはデータの正確なコピー)、ボールト (スナップショット コピーの保持期間が長いデータのコピー)、またはその両方を作成できます。これらのコピーは、災害、クラウドへのバースト、サイバー ボールト (ボールト ポリシーを使用してボールトをロックする場合) など、さまざまな目的に使用できます。詳細については、"SnapMirrorに関するONTAPドキュメント"
- SnapVault* - ONTAP 9.3 では、 SnapVault は廃止され、vault または mirror-vault ポリシーを使用してSnapMirrorを構成することが推奨されます。この用語は現在でも使われていますが、あまり使われなくなっています。詳細については、 "SnapVaultに関するONTAPドキュメント" 。

ONTAPによるサイバーボールトのサイジング

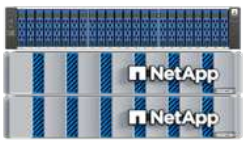
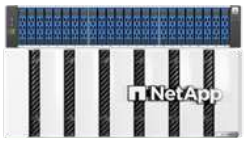
サイバー ボールトのサイズを決定するには、特定の復旧時間目標 (RTO) 内に復元する必要があるデータの量を把握する必要があります。適切な規模のサイバー ボールト ソリューションを適切に設計するには、多くの要素が関係します。サイバー ボールトのサイズを決定する際には、パフォーマンスと容量の両方を考慮する必要があります。

パフォーマンスサイジングの考慮事項

1. ソース プラットフォーム モデル (FAS 、 AFF A シリーズ、 AFF C シリーズ) は何ですか?
2. ソースとサイバー ボールト間の帯域幅と遅延はどれくらいですか?
3. ファイルサイズはどれくらいですか、またファイル数はいくつですか?
4. 回復時間の目標は何ですか?
5. RTO 内にどれだけのデータを回復する必要がありますか?
6. サイバー ボールトはいくつのSnapMirrorファンイン関係を取り込みますか?
7. 回復は 1 つだけ、または複数が同時に発生しますか?
8. これらの複数の回復は同じプライマリに対して発生しますか?
9. ボールトからのリカバリ中に、 SnapMirror はボールトにレプリケートしますか?

サイズ例

さまざまなサイバー ボールトの構成の例を次に示します。

Platform	AFF A1K	AFF C400	AFF C250	FAS70
Estimated RTO (100TB)	5 HR	18 HR	24 HR	24> HR
Relative cost	High	Moderate	Low	Ultra Low

容量サイジングの考慮事項

ONTAPサイバー ボールトの宛先ボリュームに必要なディスク領域の量はさまざまな要因によって異なりますが、最も重要なのはソース ボリュームのデータの変更率です。宛先ボリュームのバックアップ スケジュールとスナップショット スケジュールは両方とも宛先ボリュームのディスク使用量に影響し、ソース ボリュームの変更率は一定にならない可能性があります。エンドユーザーやアプリケーションの動作の将来的な変化に対応するために必要な容量に加えて、追加のストレージ容量のバッファーを用意しておくことをお勧めします。

ONTAPで 1 か月間の保持関係のサイズを決定するには、プライマリ データセットのサイズ、データ変更率（日次変更率）、重複排除と圧縮による節約（該当する場合）など、いくつかの要素に基づいてストレージ要件を計算する必要があります。

手順は次のとおりです。

最初のステップは、サイバー ボールトで保護しているソース ボリュームのサイズを確認することです。これは、サイバー ボールトの宛先に最初に複製されるデータの基本量です。次に、データセットの毎日の変化率を推定します。これは毎日変更されるデータの割合です。データがどれだけ動的であるかをよく理解することが重要です。

例えば：

- プライマリデータセットのサイズ = 5TB
- 日次変化率 = 5% (0.05)
- 重複排除と圧縮効率 = 50% (0.50)

それでは計算を見てみましょう。

- 毎日のデータ変化率を計算します。

```
Changed data per day = 5000 * 5% = 250GB
```

- 30 日間の変更されたデータの合計を計算します。

```
Total changed data in 30 days = 250 GB * 30 = 7.5TB
```

- 必要な合計ストレージを計算します。

```
TOTAL = 5TB + 7.5TB = 12.5TB
```

- 重複排除と圧縮による節約を適用します。

```
EFFECTIVE = 12.5TB * 50% = 6.25TB
```

ストレージニーズの概要

- 効率性がなければ、サイバー ボールト データの 30 日分を保存するには **12.5 TB** が必要になります。
- 効率が 50% の場合: 重複排除と圧縮後に **6.25 TB** のストレージが必要になります。

スナップショット コピーではメタデータによる追加のオーバーヘッドが発生する可能性がありますが、通常はそれほど大きくありません。

1 日に複数のバックアップが作成される場合は、1 日に作成される Snapshot コピーの数に応じて計算を調整します。

時間の経過に伴うデータの増加を考慮して、サイズが将来にも対応できることを確認します。

ONTAPでサイバーボールトを作成

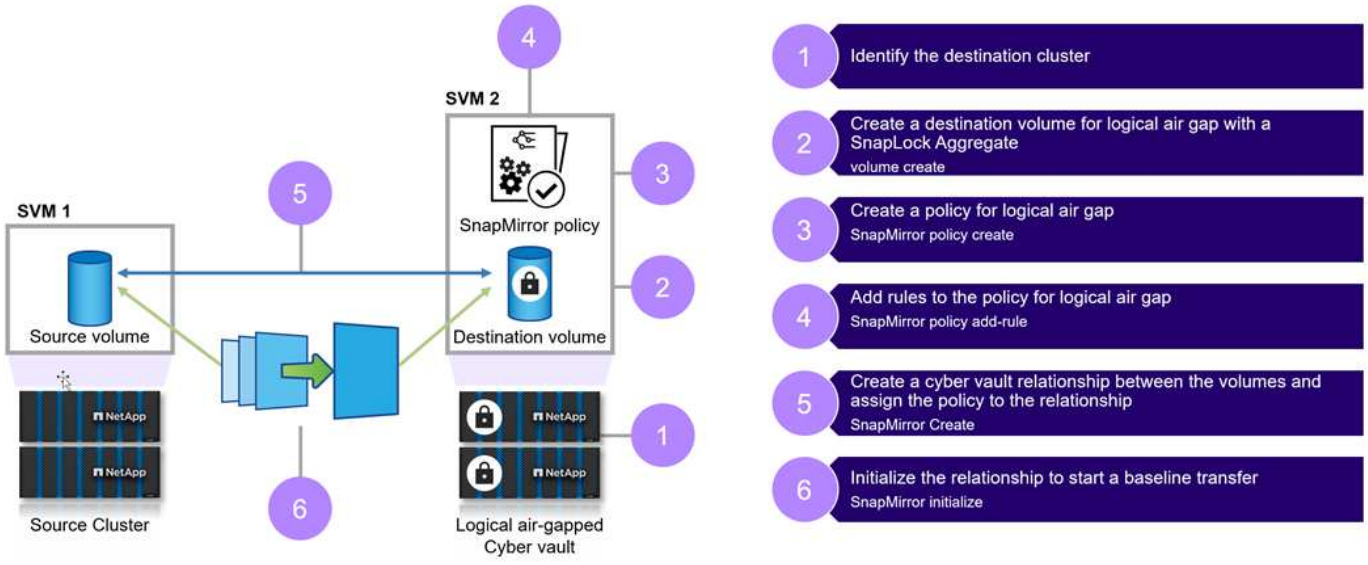
以下の手順は、 ONTAPを使用したサイバー ボールトの作成に役立ちます。

開始する前に

- ソース クラスタはONTAP 9 以降を実行している必要があります。
- ソース アグリゲートとデスティネーション アグリゲートはどちらも64ビットである必要があります。
- ピアSVMを含むピア クラスタにソース ボリュームとデスティネーション ボリュームを作成する必要があります。詳細については、以下を参照してください。 "クラスタ ピアリング" 。
- ボリュームの自動拡張が無効になっている場合は、デスティネーション ボリュームに、ソース ボリュームで使用されているスペースよりも少なくとも5%多い空きスペースが必要です。

タスク概要

次の図は、 SnapLock Complianceボールト関係を初期化する手順を示しています。



手順

1. エアギャップ データを受信するサイバー ボールトとなる宛先アレイを特定します。
2. 宛先アレイでサイバー金庫を準備するには、"ONTAP Oneライセンスをインストールする" 、"コンプライアンスクロックを初期化する"また、9.10.1より前のONTAPリリースを使用している場合は、"SnapLock Complianceアグリゲートを作成する" 。
3. 宛先アレイで、タイプ DP のSnapLock Compliance宛先ボリュームを作成します。

   ```
   volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name
   -snaplock-type compliance|enterprise -type DP -size size
   ```

4. ONTAP 9.10.1以降では、SnapLockボリュームと非SnapLockボリュームを同じアグリゲートに配置できるため、ONTAP 9.10.1を使用している場合はSnapLockアグリゲートを別々に作成する必要はありません。ボリュームを使う `-snaplock-type`コンプライアンスの種類を指定するオプション。 ONTAP 9.10.1 より前のONTAPリリースでは、 SnapLockモードのコンプライアンスはアグリゲートから継承されます。バージョンに依存しないデスティネーション ボリュームはサポートされません。デスティネーション ボリュームの言語設定とソース ボリュームの言語設定が一致している必要があります。

   次のコマンドは、2 GBのSnapLock Complianceボリュームを作成します。 `dstvolB`で `SVM2`合計で`node01_aggr`：

   ```
   cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate node01_aggr
   -snaplock-type compliance -type DP -size 2GB
   ```

5. 宛先クラスタでエアギャップを作成するには、デフォルトの保存期間を設定します。"デフォルトの保持期間の設定" 。バックアップ デスティネーションであるSnapLockボリュームには、デフォルトの保持期間が割り当てられます。この期間の値は、最初は最小 0 年、最大 100 年に設定されます (ONTAP 9.10.1 以降)。以前のONTAPリリースでは、値は 0 ～ 70 です。)各NetApp Snapshotコピーは、最初はこのデフォルトの保持期間でコミットされます。デフォルトの保存期間を変更する必要があります。保存期間は必要に応じて後で延長できますが、短縮することはできません。詳細については、以下を参照してください。 "保持時間の設定の概要" 。

   > ⓘ サービスプロバイダーは、保持期間を決定する際に顧客の契約終了日を考慮する必要があります。たとえば、サイバーボールトの保存期間が 30 日間で、保存期間が終了する前に顧客の契約が終了した場合、保存期間が終了するまでサイバーボールト内のデータは削除できません。

6. "新しいレプリケーション関係を作成する"非SnapLockソースと手順 3 で作成した新しいSnapLock宛先の間。

   この例では、XDPDefault ポリシーを使用して宛先SnapLockボリューム dstvolB との新しいSnapMirror関係を作成し、毎日および毎週のラベルが付けられた Snapshot コピーを時間単位のスケジュールで保管します。

   ```
   cluster2::> snapmirror create -source-path SVM1:srcvolA -destination-path
   SVM2:dstvolB -vserver SVM2 -policy XDPDefault -schedule hourly
   ```

   "カスタム レプリケーション ポリシーの作成"または"カスタムスケジュール"利用可能なデフォルトが適切でない場合。

7. デスティネーションSVMで、手順5で作成したSnapVault関係を初期化します。

   ```
   snapmirror initialize -destination-path destination_path
   ```

8. 次のコマンドは、SVM1 上のソース ボリューム srcvolA と SVM2 上の宛先ボリューム dstvolB 間の関係を初期化します。

```
cluster2::> snapmirror initialize -destination-path SVM2:dstvolB
```

9. 関係が初期化されアイドル状態になったら、宛先で snapshot show コマンドを使用して、複製された Snapshot コピーに適用されたSnapLock の有効期限を確認します。

この例では、 SnapMirrorラベルとSnapLock有効期限を持つボリューム dstvolB 上の Snapshot コピーを一覧表示します。

```
cluster2::> snapshot show -vserver SVM2 -volume dstvolB -fields snapmirror-
label, snaplock-expiry-time
```

サイバー金庫の強化

これらは、 ONTAPサイバー ボールトを強化するための追加の推奨事項です。詳細な推奨事項と手順については、以下のONTAP強化ガイドを参照してください。

サイバー金庫の強化に関する推奨事項

- サイバー金庫の管理プレーンを分離する
- 宛先クラスタでデータLIFを有効にしないでください。これは追加の攻撃ベクトルとなるためです。
- 宛先クラスタで、サービス ポリシーを使用してソース クラスタへのクラスタ間 LIF アクセスを制限します。
- サービス ポリシーと要塞ホストを使用して、宛先クラスタの管理 LIF をセグメント化し、アクセスを制限します。
- ソースクラスタからサイバーボールトへのすべてのデータトラフィックを制限し、 SnapMirrorトラフィックに必要なポートのみを許可します。
- 可能であれば、 ONTAP内の不要な管理アクセス方法を無効にして、攻撃対象領域を減らします。
- 監査ログとリモートログストレージを有効にする
- 複数の管理者による検証を有効にし、通常のストレージ管理者以外の管理者（CISO スタッフなど）による検証を要求します。
- ロールベースのアクセス制御を実装する
- システムマネージャとSSHに管理多要素認証を要求する
- スクリプトとREST API呼び出しにトークンベースの認証を使用する

詳細は"ONTAP強化ガイド"、"マルチ管理者認証 - 概要"そして"ONTAP多要素認証ガイド"これらの強化手順を実行する方法について説明します。

サイバー金庫の相互運用性

ONTAPハードウェアとソフトウェアを使用して、サイバー ボールト構成を作成できます。

ONTAPハードウェアの推奨事項

すべてのONTAP統合物理アレイは、サイバー ボールトの実装に使用できます。

- FASハイブリッド ストレージは、最もコスト効率の高いソリューションを提供します。
- AFF C シリーズは、最も効率的な電力消費と密度を提供します。
- AFF A シリーズは、最高の RTO を提供する最高パフォーマンスのプラットフォームです。最近発表された最新のAFF A シリーズにより、このプラットフォームはパフォーマンスを犠牲にすることなく最高のストレージ効率を提供します。

ONTAPソフトウェアの推奨事項

ONTAP 9.14.1以降では、SnapMirror関係のSnapMirrorポリシーで特定のSnapMirrorラベルの保持期間を指定することで、ソース ボリュームからデスティネーション ボリュームにレプリケートされたSnapshotコピーを、ルールで指定した保持期間にわたって保持できます。保持期間を指定しない場合は、デスティネーション ボリュームのデフォルトの保持期間が使用されます。

ONTAP 9.13.1 以降では、snaplock-type オプションを「non-snaplock」に設定してFlexCloneを作成し、SnapLockクローン作成操作を実行するときに Snapshot コピーを「parent-snapshot」として指定することで、 SnapLockボールト関係の宛先 SnapLock ボリューム上のロックされた Snapshot コピーを瞬時にリストアできます。詳細はこちら"SnapLockタイプのFlexCloneボリュームを作成する" 。

MetroCluster構成

MetroCluster構成の場合は、次の点に注意してください。

- SnapVault関係は、同期元のSVM間でのみ作成できます。同期元のSVMと同期先のSVMの間では作成できません。
- 同期元のSVMのボリュームからデータ提供用のSVMへのSnapVault関係を作成できます。
- データ提供用のSVMのボリュームから同期元のSVMのDPボリュームへのSnapVault関係を作成できます。

サイバーボールトに関するよくある質問

この FAQ は、 NetApp の顧客とパートナーを対象としています。 NetApp のONTAPベースのサイバー ボールト リファレンス アーキテクチャに関するよくある質問に回答します。

NetAppサイバー ボールトとは何ですか?

サイバー ボールトは、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 ボールトは、マルウェア、ランサムウェア、内部脅威など、プライマリ データに影響を与える脅威の影響を受けない、「エアギャップ」型の不変かつ消去不可能なデータ リポジトリです。サイバー ボールトは、変更不可能なNetApp ONTAP Snapshot コピーを使用して実現でき、 NetApp SnapLock Complianceによって消去不能になります。 SnapLock Compliance保護下にある間は、 ONTAP管理者やNetAppサポートであってもデータを変更または削除することはできません。

従来の方法を使用したエアギャップ 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。サイバー ボールトによるエアギャップには、標準のデータ アクセス ネットワークの外部にある別のデータ レプリケーション ネットワークを使用して、スナップショット コピーを消去不可能な宛先に複製することが含まれます。

エアギャップ ネットワークの次のステップでは、必要のないときにサイバー ボールト上のすべてのデータ アクセスとレプリケーション プロトコルを無効にします。これにより、宛先サイトでのデータアクセスやデータの流出を防止できます。 SnapLock Complianceを使用すると、物理的な分離は必要ありません。 SnapLock Compliance は、保管されたポイントインタイムの読み取り専用スナップショット コピーを保護し、削除されずに変更不可能なデータの迅速な回復を実現します。

NetAppのサイバーボールトへのアプローチ

SnapLockを搭載したNetAppサイバー ボールトは、組織に最も重要なデータ資産を保護するための包括的かつ柔軟なソリューションを提供します。 NetApp は、 ONTAPの強化テクノロジーを活用することで、進化するサイバー脅威の影響を受けない、安全でエアギャップのある分離されたサイバー ボールトを作成できるようにします。 NetAppを使用すると、ストレージ インフラストラクチャの俊敏性と効率性を維持しながら、データの機密性、整合性、可用性を確保できます。

サイバー ボールト向けのNetAppリファレンス アーキテクチャの主な機能は次のとおりです。

- 安全で分離されたストレージ インフラストラクチャ (例: エアギャップ ストレージ システム)
- データのバックアップコピーは変更不可能かつ消去不可能です
- 厳格かつ個別のアクセス制御、複数の管理者による検証、多要素認証
- 迅速なデータ復元機能

サイバーボールトに関するよくある質問

サイバー ボールトは**NetApp**の製品ですか**?**

いいえ、「サイバー ボールト」は業界全体で使われている用語です。 NetApp は、顧客が独自のサイバー ボールトを簡単に構築し、数十のONTAPセキュリティ機能を活用してサイバー脅威からデータを保護できるようにするためのリファレンス アーキテクチャを作成しました。詳細は、"ONTAPドキュメントサイト" 。

NetAppのサイバー ボールトは、**LockVault** または**SnapVault**の別名ですか**?**

LockVault はData ONTAP 7 モードの機能でしたが、現在のバージョンのONTAPでは利用できません。

SnapVault は、現在 SnapMirror のボールト ポリシーで実現されている機能を表す従来の用語です。このポリシーにより、ソース ボリュームとは異なる数のスナップショット コピーを宛先で保持できるようになります。

Cyber Vault は、ボールト ポリシーとSnapLock Complianceを併用してSnapMirror を使用し、変更不可能で消去不可能なデータのコピーを作成しています。

サイバー ボールト、 **FAS** 、キャパシティ フラッシュ、パフォーマンス フラッシュに使用できる**NetApp**ハードウェアはどれですか**?**

このサイバー ボールティングのリファレンス アーキテクチャは、 ONTAPハードウェア ポートフォリオ全体に適用されます。お客様は、 AFF A シリーズ、 AFF C シリーズ、またはFASプラットフォームをボールトとして使用できます。フラッシュベースのプラットフォームは最も速いリカバリ時間を提供し、ディスクベースのプラットフォームは最もコスト効率の高いソリューションを提供します。回復するデータの量や、複数の回復が並行して行われているかどうかに応じて、ディスクベース システム (FAS) を使用すると、完了するまでに数日から数週間かかる場合があります。ビジネス要件を満たすサイバー ボールト ソリューションのサイズを適切に決定するには、 NetAppまたはパートナーの担当者にご相談ください。

Cloud Volumes ONTAP をサイバー ボールト ソースとして使用できますか**?**

はい。ただし、CVO をソースとして使用する場合は、 SnapLock Compliance がONTAPサイバー ボールトの要件であるため、データをオンプレミスのサイバー ボールトの宛先に複製する必要があります。ハイパースケーラー ベースの CVO インスタンスからのデータ複製では、送信料金が発生する可能性があります。

Cloud Volumes ONTAP をサイバーボールトの保存先として使用できますか**?**

Cyber Vault アーキテクチャは、ONTAP のSnapLock Compliance の消失不可性に依存しており、オンプレミス実装向けに設計されています。クラウドベースの Cyber Vault アーキテクチャは、将来の公開に向けて調査中です。

ONTAP Select をサイバー ボールト ソースとして使用できますか**?**

はい、 ONTAP Select はオンプレミスのハードウェア ベースのサイバー ボールト デスティネーションへのソースとして使用できます。

ONTAP Select をサイバー ボールトの保存先として使用できますか**?**

いいえ、 ONTAP Select はSnapLock Complianceを使用できないため、サイバー ボールトの保存先として使用しないでください。

NetAppのサイバー ボールトでは**SnapMirror**だけを使用していますか**?**

いいえ、 NetAppサイバー ボールト アーキテクチャは、多くのONTAP機能を活用して、安全で分離された、エアギャップ化された強化されたデータのコピーを作成します。どのような追加技術が使用できるかの詳細については、次の質問を参照してください。

サイバー ボールトに使用される他のテクノロジや構成はありますか**?**

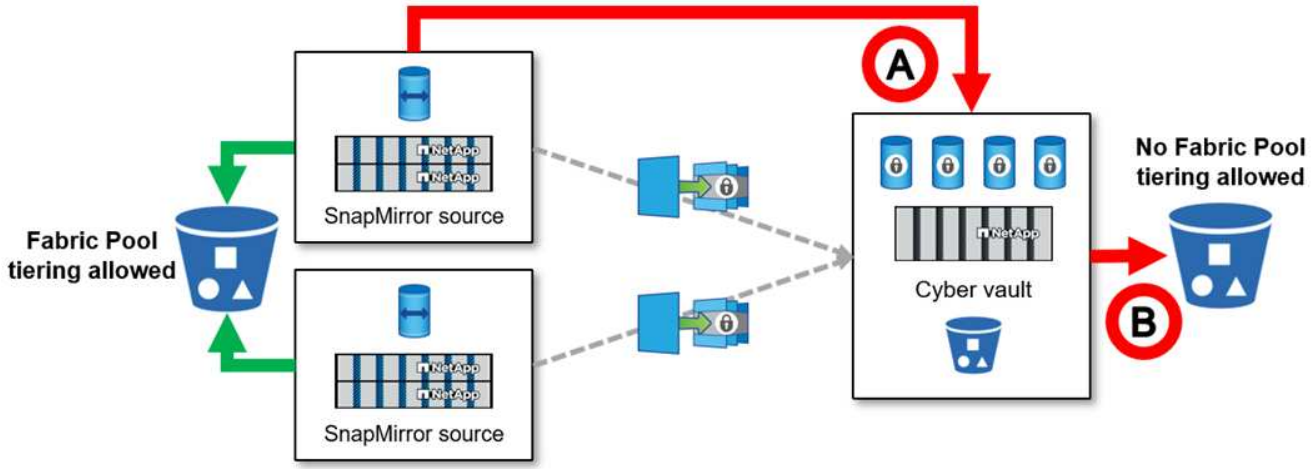
NetAppサイバー ボールトの基盤はSnapMirrorとSnapLock Complianceですが、改ざん防止スナップショット コピー、多要素認証 (MFA)、Multi Admin Verify、ロールベースのアクセス制御、リモートおよびローカルの監査ログなどの追加のONTAP機能を使用することで、データのセキュリティと安全性が向上します。

サイバー ボールトにとって、 **ONTAP**スナップショット コピーが他のものより優れている点は何ですか**?**

ONTAP Snapshot コピーはデフォルトでは変更不可であり、 SnapLock Complianceを使用して消去不可にすることができます。 NetAppサポートでもSnapLock Snapshot コピーを削除することはできません。より良い質問は、 NetAppサイバー ボールトが業界の他のサイバー ボールトよりも優れている点は何ですか、ということです。まず、 ONTAP は世界で最も安全なストレージであり、ハードウェア層とソフトウェア層の両方で機密データや極秘データを保存できる CSfC 認証を取得しています。詳細情報"CSfCはここにあります"。さらに、 ONTAP はストレージ層でエアギャップを設定でき、サイバー ボールト システムがレプリケーションを制御することで、サイバー ボールト ネットワーク内にエアギャップを作成できます。

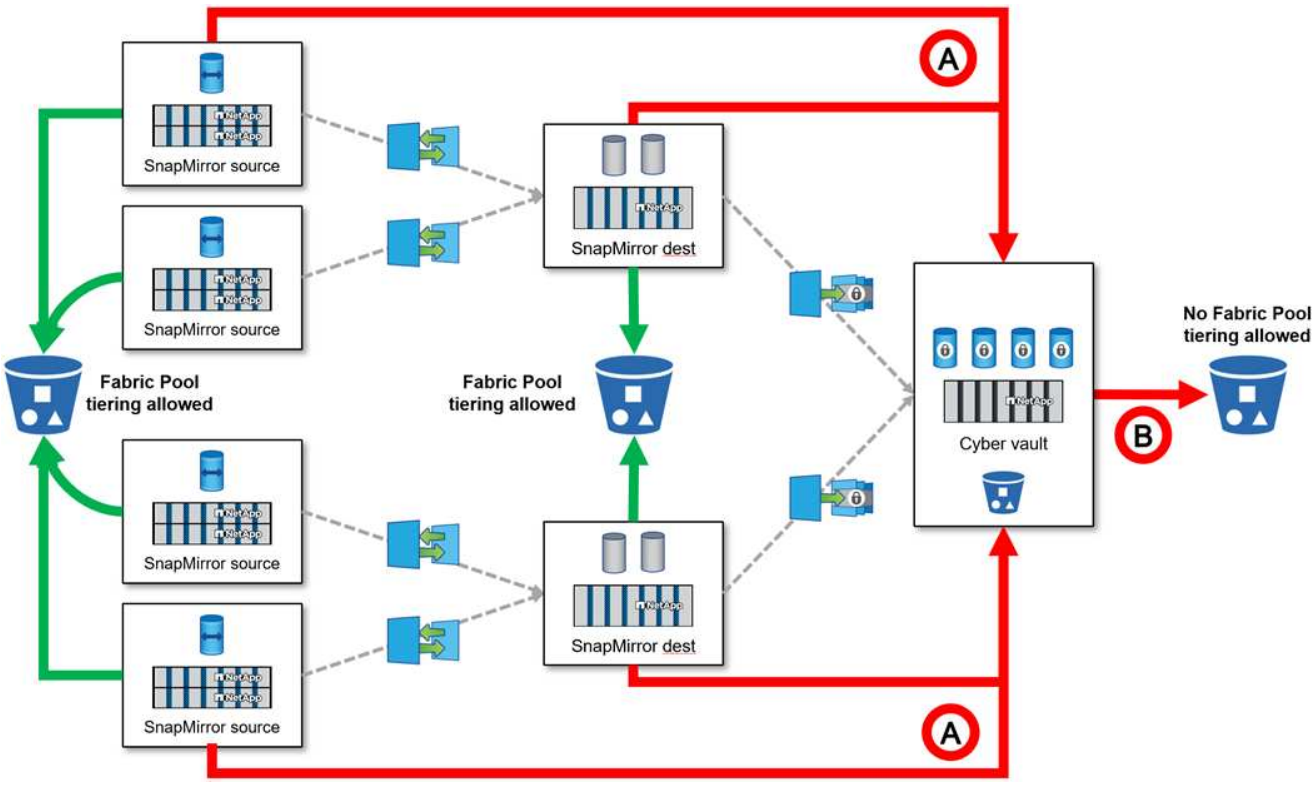
サイバー ボールト上のボリュームは**ONTAP**ファブリック プールを使用できますか**?**

いいえ、サイバー ボールト ボリューム (SnapLock Compliance SnapMirrorの宛先) は、ポリシーに関係なく、ファブリック プールを使用して階層化することはできません。



ファブリック プールをサイバー ボールトで使用できないシナリオは複数あります。

1. ファブリック プールのコールド層では、サイバー ボールト クラスターを使用することはできません。これは、S3 プロトコルを有効にすると、サイバー ボールト リファレンス アーキテクチャのセキュリティが無効になるためです。さらに、ファブリック プールに使用される S3 バケットは保護できません。
2. サイバー ボールトのSnapLock Complianceボリュームは、データがボリューム内でロックされているため、S3 バケットに階層化することはできません。



ONTAP S3 Worm はサイバー ボールトで使用できますか**?**

いいえ、S3 はリファレンス アーキテクチャのセキュリティの性質を無効にするデータ アクセス プロトコルです。

NetAppサイバー ボールトは、異なる**ONTAP**パーソナリティまたはプロファイルで実行されますか**?**

いいえ、これはリファレンスアーキテクチャです。お客様は"リファレンスアーキテクチャ"サイバー金庫を構築したり、"PowerShellスクリプトを作成して強化し検証する"サイバー金庫。

サイバー ボールトで **NFS**、**SMB**、**S3** などのデータ プロトコルをオンにできますか**?**

デフォルトでは、サイバー ボールトを安全にするためにデータ プロトコルを無効にする必要があります。ただし、データ プロトコルをサイバー ボールト上で有効にすると、回復のため、または必要なときにデータにアクセスできます。これは一時的に実行し、回復が完了したら無効にする必要があります。

既存の**SnapVault**環境をサイバー ボールトに変換できますか**?** それともすべてを再シードする必要がありますか**?**

○SnapMirrorの宛先（ボールトポリシー付き）であるシステムを取得し、データプロトコルを無効にし、"ONTAP強化ガイド"それを安全な場所に隔離し、参照アーキテクチャの他の手順に従って、宛先を再シードせずにサイバー ボールトにします。

*追加の質問はありますか?*ご質問は、ng-cyber-vault@netapp.com までメールでお送りください。ご質問には回答し、FAQ に追加させていただきます。

サイバー金庫のリソース

このサイバー ボールト情報に記載されている情報の詳細については、次の追加情報とセキュリティの概念を参照してください。

- "NetAppサイバー ボールト: 多層データ保護ソリューションの概要"
- "NetApp、業界初のAI駆動型オンボックスランサムウェア検出ソリューションでAAA評価を獲得"
- "地球上で最も安全なストレージでサイバーレジリエンスを向上"
- "ONTAPセキュリティ強化ガイド"
- "NetAppゼロトラスト"
- "NetAppサイバーレジリエンス"
- "NetAppデータ保護"
- "CLIによるクラスタとSVMのピアリングの概要"
- "SnapVaultアーカイブ"
- "設定、分析、cronスクリプト"

PowerShell を使用したONTAPサイバー ボールトの作成、強化、検証

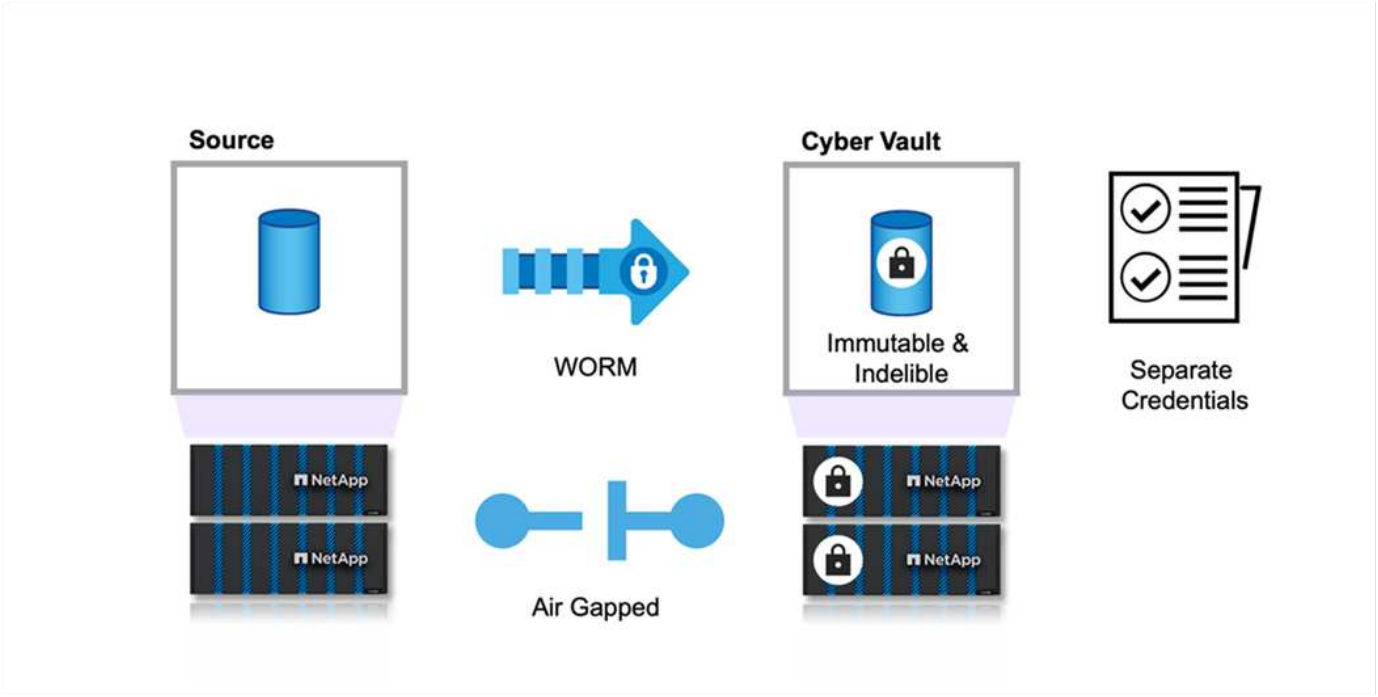
PowerShell を使用したONTAPサイバー ボールトの概要

今日のデジタル環境において、組織の重要なデータ資産を保護することは、単なるベストプラクティスではなく、ビジネス上の必須事項です。サイバー脅威はかつてない速さで進化しており、従来のデータ保護対策では機密情報を安全に保つことができなくなっています。ここでサイバー ボールトの出番となります。NetApp の最先端のONTAPベースのソリューションは、高度なエアギャップ技術と堅牢なデータ保護手段を組み合わせ、サイバー脅威に対する侵入不可能な障壁を構築します。サイバー ボールトは、最も重要なデータを安全な強化テクノロジーで分離することにより、攻撃対象領域を最小限に抑え、最も重要なデータが機密性を保ち、無傷のまま、必要なときにすぐに利用できるようにします。

サイバー ボールトは、ファイアウォール、ネットワーク、ストレージなどの複数の保護層で構成された安全なストレージ施設です。これらのコンポーネントは、重要な業務運営に必要な重要な回復データを保護します。サイバー ボールトのコンポーネントは、ボールト ポリシーに基づいて重要な本番データと定期的に同期されますが、それ以外の場合はアクセスできません。この分離された切断されたセットアップにより、サイバー攻撃によって本番環境が侵害された場合でも、サイバー ボールトから信頼性の高い最終的な復旧を簡単に実行できるようになります。

NetApp、ネットワークを構成し、LIF を無効化し、ファイアウォール ルールを更新し、システムを外部ネットワークやインターネットから分離することで、サイバー ボールトのエアギャップを簡単に作成できます。この堅牢なアプローチにより、システムは外部ネットワークやインターネットから効果的に分離され、リモートからのサイバー攻撃や不正アクセスの試みに対する比類のない保護が提供され、システムはネットワークベースの脅威や侵入の影響を受けなくなります。

これをSnapLock Compliance保護と組み合わせると、 ONTAP管理者やNetAppサポートであってもデータを変更または削除できなくなります。 SnapLockは SEC および FINRA 規制に照らして定期的に監査されており、データの復元力が銀行業界の厳格な WORM およびデータ保持規制を満たしていることが保証されています。NetApp は、NSA CSfC によって極秘データの保存が認定された唯一のエンタープライズ ストレージです。



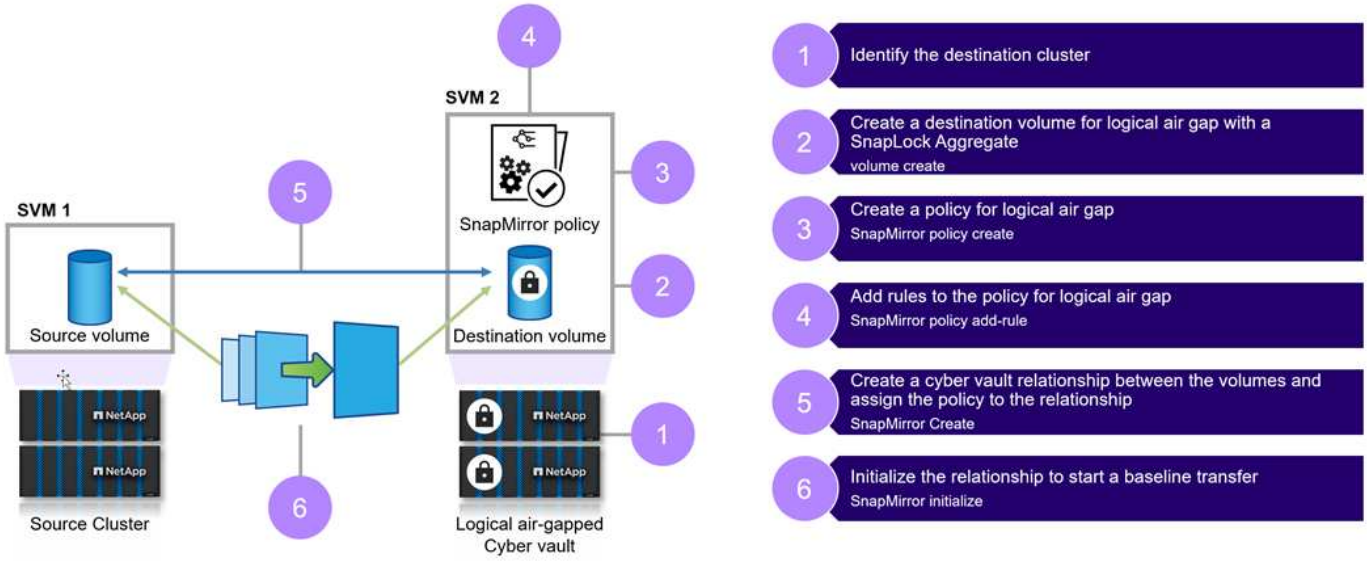
このドキュメントでは、増加するサイバー攻撃からさらに一層の保護を施し、迅速なリカバリを実現する不変のスナップショットを備えたオンプレミスのONTAPストレージ用の NetApp サイバー ボールトを別の指定されたONTAPストレージに自動的に構成する方法について説明します。このアーキテクチャの一部として、構成全体はONTAP のベスト プラクティスに従って適用されます。最後のセクションには、攻撃を受けた場合に回復を実行するための手順が記載されています。

FSx ONTAPを使用して AWS に指定されたサイバーボールトを作成する場合にも、同じソリューションを適用できます。

ONTAPサイバーボールトを作成するための大まかな手順

- ピアリング関係を作成する
  - ONTAPストレージを使用する本番サイトは、指定されたサイバーボールトONTAPストレージとピアリングされます。
- SnapLock Complianceボリュームを作成する
- SnapMirror関係とラベルを設定するルールを設定する
  - SnapMirror関係と適切なスケジュールが設定されている
- SnapMirror （ボールト）転送を開始する前に保持期間を設定する
  - コピーされたデータには保持ロックが適用され、これにより内部者やデータ障害によるデータ侵害がさらに防止されます。これを使用すると、保存期間が終了する前にデータを削除することはできません
  - 組織は要件に応じて数週間/数か月間このデータを保持できます。
- ラベルに基づいてSnapMirror関係を初期化する
  - 初期シードと増分永久転送はSnapMirrorスケジュールに基づいて実行されます
  - データはSnapLockコンプライアンスによって保護されており（変更不可かつ消去不可）、回復可能です。

- 厳格なデータ転送制御を実施する
  - サイバー ボールトは、生産現場のデータによって一定期間ロック解除され、ボールト内のデータと同期されます。転送が完了すると、接続は切断され、閉じられ、再びロックされます。
- 迅速な回復
  - 本番環境でプライマリが影響を受けた場合、サイバーボールトのデータは元の本番環境または別の選択された環境に安全に復元されます。



ソリューションコンポーネント

ソース クラスターと宛先クラスターで 9.15.1 を実行しているNetApp ONTAP 。

ONTAP One: NetApp ONTAP のオールインワン ライセンス。

ONTAP One ライセンスから使用される機能:

- SnapLock Compliance
- SnapMirror
- マルチ管理者認証
- ONTAPによって公開されるすべての強化機能
- サイバーボールト用の個別のRBAC認証情報

> すべてのONTAP統合物理アレイはサイバー ボールトに使用できますが、 AFF C シリーズの容量ベースのフラッシュ システムとFASハイブリッド フラッシュ システムは、この目的に最もコスト効率に優れた理想的なプラットフォームです。詳しくは"ONTAPサイバー ボールトのサイズ設定"サイズの目安としてご利用ください。

PowerShell を使用したONTAPサイバー ボールトの作成

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。 SnapLock Complianceを使用すると、物理的な分離は必要ありません。 SnapLock Compliance は、保管されたスナップショットのポイントインタイムの読み取り専用コピーを保護します。その結果、データにすぐにアクセスでき、削除や消去から保護され、変更や変更不可能から保護されます。

前提条件

このドキュメントの次のセクションの手順を開始する前に、次の前提条件が満たされていることを確認してください。

- ソース クラスタはONTAP 9 以降を実行している必要があります。
- ソース アグリゲートとデスティネーション アグリゲートはどちらも64ビットである必要があります。
- ソース クラスタとデスティネーション クラスタのピア関係が確立されている必要があります。
- ソース SVM と宛先 SVM はピアリングされている必要があります。
- クラスター ピアリング暗号化が有効になっていることを確認します。

ONTAPサイバー ボールトへのデータ転送を設定するには、いくつかの手順が必要です。プライマリ ボリュームで、適切なスケジュールを使用して、作成するコピーと作成するタイミングを指定するスナップショットポリシーを設定し、ラベルを割り当てて、 SnapVaultによって転送するコピーを指定します。セカンダリでは、転送する Snapshot コピーのラベルと、サイバー ボールトに保持するコピーの数を指定するSnapMirrorポリシーを作成する必要があります。これらのポリシーを設定した後、 SnapVault関係を作成し、転送スケジュールを確立します。

> このドキュメントでは、プライマリ ストレージと指定されたONTAPサイバー ボールトがすでにセットアップされ、構成されていることを前提としています。

> サイバー ボールト クラスターは、ソース データと同じデータ センターまたは異なるデータ センターに配置できます。

ONTAPサイバーボールトを作成する手順

1. コンプライアンス クロックを初期化するには、 ONTAP CLI または System Manager を使用します。
2. SnapLockコンプライアンスを有効にしたデータ保護ボリュームを作成します。
3. SnapMirror create コマンドを使用して、 SnapVaultデータ保護関係を作成します。
4. 宛先ボリュームのデフォルトのSnapLock Compliance保持期間を設定します。

> デフォルトの保持期間は「最小に設定」です。バックアップ デスティネーションであるSnapLockボリュームには、デフォルトの保持期間が割り当てられます。この期間の値は、最初は最小 0 年、最大 100 年に設定されます (ONTAP 9.10.1 以降)。以前のONTAPリリースでは、値は 0 ～ 70 です。)各NetApp Snapshotコピーは、最初はこのデフォルトの保持期間でコミットされます。保存期間は必要に応じて後で延長できますが、短縮することはできません。詳細については、以下を参照してください。 "保持時間の設定の概要" 。

上記には手動の手順が含まれています。セキュリティ専門家は、大きなエラーの余地をもたらす手動管理を避

けるために、プロセスを自動化することを推奨しています。以下は、 SnapLockコンプライアンスの前提条件と構成、およびクロックの初期化を完全に自動化するコード スニペットです。

以下は、 ONTAPコンプライアンス クロックを初期化する PowerShell コードの例です。

```
function initializeSnapLockComplianceClock {
    try {
        $nodes = Get-NcNode

        $isInitialized = $false
        logMessage -message "Cheking if snaplock compliance clock is
initialized"
        foreach($node in $nodes) {
            $check = Get-NcSnaplockComplianceClock -Node $node.Node
            if ($check.SnaplockComplianceClockSpecified -eq "True") {
                $isInitialized = $true
            }
        }

        if ($isInitialized) {
            logMessage -message "SnapLock Compliance clock already
initialized" -type "SUCCESS"
        } else {
            logMessage -message "Initializing SnapLock compliance clock"
            foreach($node in $nodes) {
                Set-NcSnaplockComplianceClock -Node $node.Node
            }
            logMessage -message "Successfully initialized SnapLock
Compliance clock" -type "SUCCESS"
        }
    } catch {
        handleError -errorMessage $_.Exception.Message
    }
}
```

ONTAPサイバー ボールトを構成するための PowerShell コード例を次に示します。

```
function configureCyberVault {
    for($i = 0; $i -lt $DESTINATION_VOLUME_NAMES.Length; $i++) {
        try {
            # checking if the volume already exists and is of type
snaplock compliance
            logMessage -message "Checking if SnapLock Compliance volume
$($DESTINATION_VOLUME_NAMES[$i]) already exists in vServer
$DESTINATION_VSERVER"
```

```
            $volume = Get-NcVol -Vserver $DESTINATION_VSERVER -Volume
$DESTINATION_VOLUME_NAMES[$i] | Select-Object -Property Name, State,
TotalSize, Aggregate, Vserver, Snaplock | Where-Object { $_.Snaplock.Type
-eq "compliance" }
            if($volume) {
                $volume
                logMessage -message "SnapLock Compliance volume
$($DESTINATION_VOLUME_NAMES[$i]) already exists in vServer
$DESTINATION_VSERVER" -type "SUCCESS"
            } else {
                # Create SnapLock Compliance volume
                logMessage -message "Creating SnapLock Compliance volume:
$($DESTINATION_VOLUME_NAMES[$i])"
                New-NcVol -Name $DESTINATION_VOLUME_NAMES[$i] -Aggregate
$DESTINATION_AGGREGATE_NAMES[$i] -SnaplockType Compliance -Type DP -Size
$DESTINATION_VOLUME_SIZES[$i] -ErrorAction Stop | Select-Object -Property
Name, State, TotalSize, Aggregate, Vserver
                logMessage -message "Volume $($DESTINATION_VOLUME_NAMES[
$i]) created successfully" -type "SUCCESS"
            }

            # Set SnapLock volume attributes
            logMessage -message "Setting SnapLock volume attributes for
volume: $($DESTINATION_VOLUME_NAMES[$i])"
            Set-NcSnaplockVolAttr -Volume $DESTINATION_VOLUME_NAMES[$i]
-MinimumRetentionPeriod $SNAPLOCK_MIN_RETENTION -MaximumRetentionPeriod
$SNAPLOCK_MAX_RETENTION -ErrorAction Stop | Select-Object -Property Type,
MinimumRetentionPeriod, MaximumRetentionPeriod
            logMessage -message "SnapLock volume attributes set
successfully for volume: $($DESTINATION_VOLUME_NAMES[$i])" -type "SUCCESS"

            # checking snapmirror relationship
            logMessage -message "Checking if SnapMirror relationship
exists between source volume $($SOURCE_VOLUME_NAMES[$i]) and destination
SnapLock Compliance volume $($DESTINATION_VOLUME_NAMES[$i])"
            $snapmirror = Get-NcSnapmirror | Select-Object SourceCluster,
SourceLocation, DestinationCluster, DestinationLocation, Status,
MirrorState | Where-Object { $_.SourceCluster -eq
$SOURCE_ONTAP_CLUSTER_NAME -and $_.SourceLocation -eq "$($SOURCE_VSERVER)
:$($SOURCE_VOLUME_NAMES[$i])" -and $_.DestinationCluster -eq
$DESTINATION_ONTAP_CLUSTER_NAME -and $_.DestinationLocation -eq "
$($DESTINATION_VSERVER):$($DESTINATION_VOLUME_NAMES[$i])" -and ($_.Status
-eq "snapmirrored" -or $_.Status -eq "uninitialized") }
            if($snapmirror) {
                $snapmirror
                logMessage -message "SnapMirror relationship already
```

```
exists for volume: $($DESTINATION_VOLUME_NAMES[$i])" -type "SUCCESS"
            } else {
                # Create SnapMirror relationship
                logMessage -message "Creating SnapMirror relationship for
volume: $($DESTINATION_VOLUME_NAMES[$i])"
                New-NcSnapmirror -SourceCluster $SOURCE_ONTAP_CLUSTER_NAME
-SourceVserver $SOURCE_VSERVER -SourceVolume $SOURCE_VOLUME_NAMES[$i]
-DestinationCluster $DESTINATION_ONTAP_CLUSTER_NAME -DestinationVserver
$DESTINATION_VSERVER -DestinationVolume $DESTINATION_VOLUME_NAMES[$i]
-Policy $SNAPMIRROR_PROTECTION_POLICY -Schedule $SNAPMIRROR_SCHEDULE
-ErrorAction Stop | Select-Object -Property SourceCluster, SourceLocation,
DestinationCluster, DestinationLocation, Status, Policy, Schedule
                logMessage -message "SnapMirror relationship created
successfully for volume: $($DESTINATION_VOLUME_NAMES[$i])" -type "SUCCESS"
            }

        } catch {
            handleError -errorMessage $_.Exception.Message
        }
    }
}
```

1. 上記の手順が完了すると、 SnapLock ComplianceとSnapVaultを使用したエアギャップ サイバー ボールトの準備が整います。

スナップショット データをサイバー ボールトに転送する前に、 SnapVault関係を初期化する必要があります。ただし、その前に、金庫を保護するためにセキュリティ強化を実行する必要があります。

PowerShell を使用したONTAPサイバー ボールトの強化

ONTAPサイバー ボールトは、従来のソリューションと比較して、サイバー攻撃に対する優れた耐性を提供します。セキュリティを強化するためのアーキテクチャを設計する際には、攻撃対象領域を減らす対策を考慮することが重要です。これは、強化されたパスワード ポリシーの実装、RBAC の有効化、デフォルトのユーザー アカウントのロック、ファイアウォールの構成、Vault システムへの変更に対する承認フローの利用など、さまざまな方法で実現できます。さらに、特定の IP アドレスからのネットワーク アクセス プロトコルを制限すると、潜在的な脆弱性を制限するのに役立ちます。

ONTAP は、 ONTAPストレージを強化できる一連の制御を提供します。使用"ONTAPのガイダンスと構成設定"組織が情報システムの機密性、整合性、可用性に関して規定されたセキュリティ目標を達成できるように支援します。

強化のベストプラクティス

手動手順

1. 事前定義されたカスタム管理ロールを持つ指定ユーザーを作成します。

2. ネットワーク トラフィックを分離するために新しい IPspace を作成します。
3. 新しい IPspace に存在する新しい SVM を作成します。
4. ファイアウォール ルーティング ポリシーが適切に構成され、すべてのルールが定期的に監査され、必要に応じて更新されていることを確認します。

ONTAP CLIまたは自動化スクリプト経由

1. マルチ管理者認証（MFA）による管理の保護
2. クラスター間で転送中の標準データの暗号化を有効にします。
3. 強力な暗号化方式を使用して SSH を保護し、安全なパスワードを適用します。
4. グローバル FIPS を有効にします。
5. Telnet およびリモート シェル (RSH) を無効にする必要があります。
6. デフォルトの管理者アカウントをロックします。
7. データ LIF を無効にし、リモート アクセス ポイントを保護します。
8. 使用されていない、または不要なプロトコルとサービスを無効にして削除します。
9. ネットワーク トラフィックを暗号化します。
10. スーパーユーザーおよび管理者ロールを設定するときは、最小権限の原則を使用します。
11. 許可された IP オプションを使用して、特定の IP アドレスからの HTTPS および SSH を制限します。
12. 転送スケジュールに基づいてレプリケーションを一時停止および再開します。

箇条書き 1 ～ 4 では、分離されたネットワークの指定、IP 空間の分離などの手動介入が必要であり、事前に実行する必要があります。強化の設定に関する詳細は、"ONTAPセキュリティ強化ガイド" 。残りは簡単に自動化でき、簡単に導入および監視できます。このオーケストレーションされたアプローチの目的は、ボールトコントローラーの将来性を確保するために強化手順を自動化するメカニズムを提供することです。サイバー金庫のエアギャップが開いている時間枠は可能な限り短くなります。 SnapVault は永久増分テクノロジーを活用し、最後の更新以降の変更のみをサイバー ボールトに移動することで、サイバー ボールトを開いたままにしておく時間を最小限に抑えます。ワークフローをさらに最適化するために、サイバー ボールトのオープンはレプリケーション スケジュールと調整され、接続ウィンドウが最小になるようにします。

ONTAPコントローラを強化するための PowerShell コード例を次に示します。

```
function removeSvmDataProtocols {
    try {

        # checking NFS service is disabled
        logMessage -message "Checking if NFS service is disabled on
vServer $DESTINATION_VSERVER"
        $nfsService = Get-NcNfsService
        if($nfsService) {
            # Remove NFS
            logMessage -message "Removing NFS protocol on vServer :
$DESTINATION_VSERVER"
            Remove-NcNfsService -VserverContext $DESTINATION_VSERVER
```

```
-Confirm:$false
            logMessage -message "NFS protocol removed on vServer :
$DESTINATION_VSERVER" -type "SUCCESS"
        } else {
            logMessage -message "NFS service is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

        # checking CIFS/SMB server is disabled
        logMessage -message "Checking if CIFS/SMB server is disabled on
vServer $DESTINATION_VSERVER"
        $cifsServer = Get-NcCifsServer
        if($cifsServer) {
            # Remove SMB/CIFS
            logMessage -message "Removing SMB/CIFS protocol on vServer :
$DESTINATION_VSERVER"
            $domainAdministratorUsername = Read-Host -Prompt "Enter Domain
administrator username"
            $domainAdministratorPassword = Read-Host -Prompt "Enter Domain
administrator password" -AsSecureString
            $plainPassword = [Runtime.InteropServices.Marshal
]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBSTR($
domainAdministratorPassword))
            Remove-NcCifsServer -VserverContext $DESTINATION_VSERVER
-AdminUsername $domainAdministratorUsername -AdminPassword $plainPassword
-Confirm:$false -ErrorAction Stop
            logMessage -message "SMB/CIFS protocol removed on vServer :
$DESTINATION_VSERVER" -type "SUCCESS"
        } else {
            logMessage -message "CIFS/SMB server is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

        # checking iSCSI service is disabled
        logMessage -message "Checking if iSCSI service is disabled on
vServer $DESTINATION_VSERVER"
        $iscsiService = Get-NcIscsiService
        if($iscsiService) {
            # Remove iSCSI
            logMessage -message "Removing iSCSI protocol on vServer :
$DESTINATION_VSERVER"
            Remove-NcIscsiService -VserverContext $DESTINATION_VSERVER
-Confirm:$false
            logMessage -message "iSCSI protocol removed on vServer :
$DESTINATION_VSERVER" -type "SUCCESS"
        } else {
```

```
            logMessage -message "iSCSI service is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

        # checking FCP service is disabled
        logMessage -message "Checking if FCP service is disabled on
vServer $DESTINATION_VSERVER"
        $fcpService = Get-NcFcpService
        if($fcpService) {
            # Remove FCP
            logMessage -message "Removing FC protocol on vServer :
$DESTINATION_VSERVER"
            Remove-NcFcpService -VserverContext $DESTINATION_VSERVER
-Confirm:$false
            logMessage -message "FC protocol removed on vServer :
$DESTINATION_VSERVER" -type "SUCCESS"
        } else {
            logMessage -message "FCP service is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

    } catch {
        handleError -errorMessage $_.Exception.Message
    }
}

function disableSvmDataLifs {
    try {
        logMessage -message "Finding all data lifs on vServer :
$DESTINATION_VSERVER"
        $dataLifs = Get-NcNetInterface -Vserver $DESTINATION_VSERVER |
Where-Object { $_.Role -contains "data_core" }
        $dataLifs | Select-Object -Property InterfaceName, OpStatus,
DataProtocols, Vserver, Address

        logMessage -message "Disabling all data lifs on vServer :
$DESTINATION_VSERVER"
        # Disable the filtered data LIFs
        foreach ($lif in $dataLifs) {
            $disableLif = Set-NcNetInterface -Vserver $DESTINATION_VSERVER
-Name $lif.InterfaceName -AdministrativeStatus down -ErrorAction Stop
            $disableLif | Select-Object -Property InterfaceName, OpStatus,
DataProtocols, Vserver, Address
        }
        logMessage -message "Disabled all data lifs on vServer :
$DESTINATION_VSERVER" -type "SUCCESS"
```

```
    } catch {
        handleError -errorMessage $_.Exception.Message
    }
}

function configureMultiAdminApproval {
    try {

        # check if multi admin verification is enabled
        logMessage -message "Checking if multi-admin verification is
enabled"
        $maaConfig = Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP
-Credential $DESTINATION_ONTAP_CREDS -Command "set -privilege advanced;
security multi-admin-verify show"
        if ($maaConfig.Value -match "Enabled" -and $maaConfig.Value -match
"true") {
            $maaConfig
            logMessage -message "Multi-admin verification is configured
and enabled" -type "SUCCESS"
        } else {
            logMessage -message "Setting Multi-admin verification rules"
            # Define the commands to be restricted
            $rules = @(
                "cluster peer delete",
                "vserver peer delete",
                "volume snapshot policy modify",
                "volume snapshot rename",
                "vserver audit modify",
                "vserver audit delete",
                "vserver audit disable"
            )
            foreach($rule in $rules) {
                Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP
-Credential $DESTINATION_ONTAP_CREDS -Command "security multi-admin-verify
rule create -operation `"$rule`""
            }

            logMessage -message "Creating multi admin verification group
for ONTAP Cluster $DESTINATION_ONTAP_CLUSTER_MGMT_IP, Group name :
$MULTI_ADMIN_APPROVAL_GROUP_NAME, Users : $MULTI_ADMIN_APPROVAL_USERS,
Email : $MULTI_ADMIN_APPROVAL_EMAIL"
            Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP
-Credential $DESTINATION_ONTAP_CREDS -Command "security multi-admin-verify
approval-group create -name $MULTI_ADMIN_APPROVAL_GROUP_NAME -approvers
$MULTI_ADMIN_APPROVAL_USERS -email `"$MULTI_ADMIN_APPROVAL_EMAIL`""
            logMessage -message "Created multi admin verification group
```

```
for ONTAP Cluster $DESTINATION_ONTAP_CLUSTER_MGMT_IP, Group name :
$MULTI_ADMIN_APPROVAL_GROUP_NAME, Users : $MULTI_ADMIN_APPROVAL_USERS,
Email : $MULTI_ADMIN_APPROVAL_EMAIL" -type "SUCCESS"

            logMessage -message "Enabling multi admin verification group
$MULTI_ADMIN_APPROVAL_GROUP_NAME"
            Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP
-Credential $DESTINATION_ONTAP_CREDS -Command "security multi-admin-verify
modify -approval-groups $MULTI_ADMIN_APPROVAL_GROUP_NAME -required
-approvers 1 -enabled true"
            logMessage -message "Enabled multi admin verification group
$MULTI_ADMIN_APPROVAL_GROUP_NAME" -type "SUCCESS"

            logMessage -message "Enabling multi admin verification for
ONTAP Cluster $DESTINATION_ONTAP_CLUSTER_MGMT_IP"
            Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP
-Credential $DESTINATION_ONTAP_CREDS -Command "security multi-admin-verify
modify -enabled true"
            logMessage -message "Successfully enabled multi admin
verification for ONTAP Cluster $DESTINATION_ONTAP_CLUSTER_MGMT_IP" -type
"SUCCESS"

            logMessage -message "Enabling multi admin verification for
ONTAP Cluster $DESTINATION_ONTAP_CLUSTER_MGMT_IP"
            Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP
-Credential $DESTINATION_ONTAP_CREDS -Command "security multi-admin-verify
modify -enabled true"
            logMessage -message "Successfully enabled multi admin
verification for ONTAP Cluster $DESTINATION_ONTAP_CLUSTER_MGMT_IP" -type
"SUCCESS"
        }

    } catch {
        handleError -errorMessage $_.Exception.Message
    }
}

function additionalSecurityHardening {
    try {
        $command = "set -privilege advanced -confirmations off;security
protocol modify -application telnet -enabled false;"
        logMessage -message "Disabling Telnet"
        Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP -Credential
$DESTINATION_ONTAP_CREDS -Command $command
        logMessage -message "Disabled Telnet" -type "SUCCESS"
```

```
        #$command = "set -privilege advanced -confirmations off;security
config modify -interface SSL -is-fips-enabled true;"
        #logMessage -message "Enabling Global FIPS"
        ##Invoke-SSHCommand -SessionId $sshSession.SessionId -Command
$command -ErrorAction Stop
        #logMessage -message "Enabled Global FIPS" -type "SUCCESS"

        $command = "set -privilege advanced -confirmations off;network
interface service-policy modify-service -vserver cluster2 -policy default-
management -service management-https -allowed-addresses $ALLOWED_IPS;"
        logMessage -message "Restricting IP addresses $ALLOWED_IPS for
Cluster management HTTPS"
        Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP -Credential
$DESTINATION_ONTAP_CREDS -Command $command
        logMessage -message "Successfully restricted IP addresses
$ALLOWED_IPS for Cluster management HTTPS" -type "SUCCESS"

        #logMessage -message "Checking if audit logs volume audit_logs
exists"
        #$volume = Get-NcVol -Vserver $DESTINATION_VSERVER -Name
audit_logs -ErrorAction Stop

        #if($volume) {
        #    logMessage -message "Volume audit_logs already exists!
Skipping creation"
        #} else {
        #    # Create audit logs volume
        #    logMessage -message "Creating audit logs volume : audit_logs"
        #    New-NcVol -Name audit_logs -Aggregate
$DESTINATION_AGGREGATE_NAME -Size 5g -ErrorAction Stop | Select-Object
-Property Name, State, TotalSize, Aggregate, Vserver
        #    logMessage -message "Volume audit_logs created successfully"
-type "SUCCESS"
        #}

        ## Mount audit logs volume to path /vol/audit_logs
        #logMessage -message "Creating junction path for volume audit_logs
at path /vol/audit_logs for vServer $DESTINATION_VSERVER"
        #Mount-NcVol -VserverContext $DESTINATION_VSERVER -Name audit_logs
-JunctionPath /audit_logs | Select-Object -Property Name, -JunctionPath
        #logMessage -message "Created junction path for volume audit_logs
at path /vol/audit_logs for vServer $DESTINATION_VSERVER" -type "SUCCESS"

        #logMessage -message "Enabling audit logging for vServer
$DESTINATION_VSERVER at path /vol/audit_logs"
        #$command = "set -privilege advanced -confirmations off;vserver
```

```
audit create -vserver $DESTINATION_VSERVER -destination /audit_logs
-format xml;"
        #Invoke-SSHCommand -SessionI  $sshSession.SessionId -Command
$command -ErrorAction Stop
        #logMessage -message "Successfully enabled audit logging for
vServer $DESTINATION_VSERVER at path /vol/audit_logs"

    } catch {
        handleError -errorMessage $_.Exception.Message
    }
}
```

PowerShell を使用したONTAPサイバー ボールトの検証

強力なサイバー ボールトは、攻撃者が昇格された権限で環境にアクセスするための資格情報を持っている場合でも、高度な攻撃に耐えられる必要があります。

ルールが設定されると、ボールト側のスナップショットを削除しようとする試み (何らかの方法で攻撃者が侵入できたと仮定) は失敗します。必要な制限を設けてシステムを保護することで、すべての強化設定に同じことが適用されます。

スケジュールに基づいて構成を検証するための PowerShell コード例。

```
function analyze {

    for($i = 0; $i -lt $DESTINATION_VOLUME_NAMES.Length; $i++) {
        try {
            # checking if volume is of type SnapLock Compliance
            logMessage -message "Checking if SnapLock Compliance volume
$($DESTINATION_VOLUME_NAMES[$i]) exists in vServer $DESTINATION_VSERVER"
            $volume = Get-NcVol -Vserver $DESTINATION_VSERVER -Volume
$DESTINATION_VOLUME_NAMES[$i] | Select-Object -Property Name, State,
TotalSize, Aggregate, Vserver, Snaplock | Where-Object { $_.Snaplock.Type
-eq "compliance" }
            if($volume) {
                $volume
                logMessage -message "SnapLock Compliance volume
$($DESTINATION_VOLUME_NAMES[$i]) exists in vServer $DESTINATION_VSERVER"
-type "SUCCESS"
            } else {
                handleError -errorMessage "SnapLock Compliance volume
$($DESTINATION_VOLUME_NAMES[$i]) does not exist in vServer
$DESTINATION_VSERVER. Recommendation: Run the script with SCRIPT_MODE
`"configure`" to create and configure the cyber vault SnapLock Compliance
volume"
            }
```

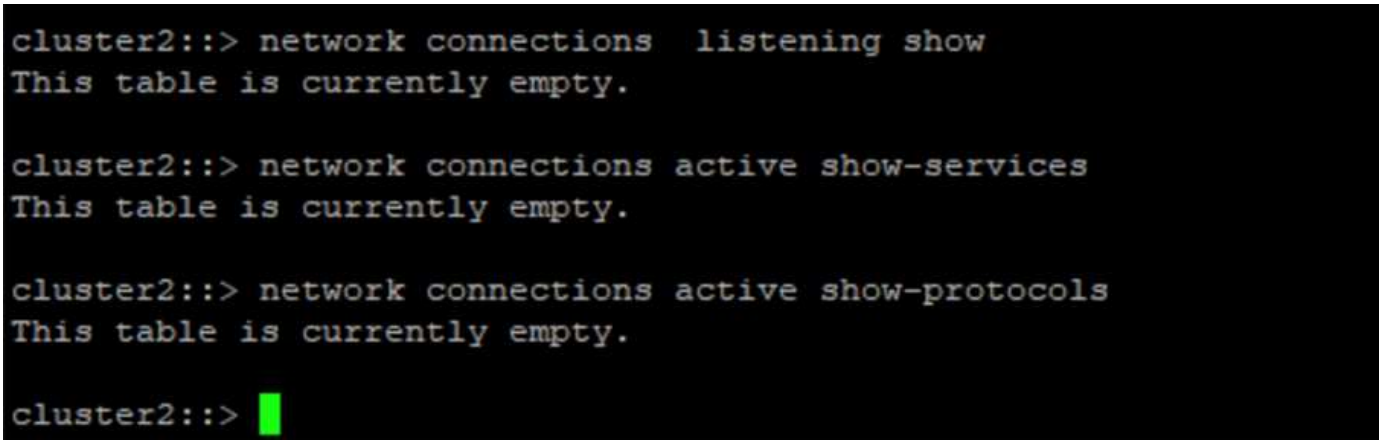
```
            # checking SnapMirror relationship
            logMessage -message "Checking if SnapMirror relationship
exists between source volume $($SOURCE_VOLUME_NAMES[$i]) and destination
SnapLock Compliance volume $($DESTINATION_VOLUME_NAMES[$i])"
            $snapmirror = Get-NcSnapmirror | Select-Object SourceCluster,
SourceLocation, DestinationCluster, DestinationLocation, Status,
MirrorState | Where-Object { $_.SourceCluster -eq
$SOURCE_ONTAP_CLUSTER_NAME -and $_.SourceLocation -eq "$($SOURCE_VSERVER)
:$($SOURCE_VOLUME_NAMES[$i])" -and $_.DestinationCluster -eq
$DESTINATION_ONTAP_CLUSTER_NAME -and $_.DestinationLocation -eq "
$($DESTINATION_VSERVER):$($DESTINATION_VOLUME_NAMES[$i])" -and $_.Status
-eq "snapmirrored" }
            if($snapmirror) {
                $snapmirror
                logMessage -message "SnapMirror relationship successfully
configured and in healthy state" -type "SUCCESS"
            } else {
                handleError -errorMessage "SnapMirror relationship does
not exist between the source volume $($SOURCE_VOLUME_NAMES[$i]) and
destination SnapLock Compliance volume $($DESTINATION_VOLUME_NAMES[$i])
(or) SnapMirror status uninitialized/unhealthy. Recommendation: Run the
script with SCRIPT_MODE `"configure`" to create and configure the cyber
vault SnapLock Compliance volume and configure the SnapMirror
relationship"
            }
        }
        catch {
            handleError -errorMessage $_.Exception.Message
        }
    }

    try {

        # checking NFS service is disabled
        logMessage -message "Checking if NFS service is disabled on
vServer $DESTINATION_VSERVER"
        $nfsService = Get-NcNfsService
        if($nfsService) {
            handleError -errorMessage "NFS service running on vServer
$DESTINATION_VSERVER. Recommendation: Run the script with SCRIPT_MODE
`"configure`" to disable NFS on vServer $DESTINATION_VSERVER"
        } else {
            logMessage -message "NFS service is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }
```

```
        # checking CIFS/SMB server is disabled
        logMessage -message "Checking if CIFS/SMB server is disabled on
vServer $DESTINATION_VSERVER"
        $cifsServer = Get-NcCifsServer
        if($cifsServer) {
            handleError -errorMessage "CIFS/SMB server running on vServer
$DESTINATION_VSERVER. Recommendation: Run the script with SCRIPT_MODE
`"configure`" to disable CIFS/SMB on vServer $DESTINATION_VSERVER"
        } else {
            logMessage -message "CIFS/SMB server is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

        # checking iSCSI service is disabled
        logMessage -message "Checking if iSCSI service is disabled on
vServer $DESTINATION_VSERVER"
        $iscsiService = Get-NcIscsiService
        if($iscsiService) {
            handleError -errorMessage "iSCSI service running on vServer
$DESTINATION_VSERVER. Recommendation: Run the script with SCRIPT_MODE
`"configure`" to disable iSCSI on vServer $DESTINATION_VSERVER"
        } else {
            logMessage -message "iSCSI service is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

        # checking FCP service is disabled
        logMessage -message "Checking if FCP service is disabled on
vServer $DESTINATION_VSERVER"
        $fcpService = Get-NcFcpService
        if($fcpService) {
            handleError -errorMessage "FCP service running on vServer
$DESTINATION_VSERVER. Recommendation: Run the script with SCRIPT_MODE
`"configure`" to disable FCP on vServer $DESTINATION_VSERVER"
        } else {
            logMessage -message "FCP service is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

        # checking if all data lifs are disabled on vServer
        logMessage -message "Finding all data lifs on vServer :
$DESTINATION_VSERVER"
        $dataLifs = Get-NcNetInterface -Vserver $DESTINATION_VSERVER |
Where-Object { $_.Role -contains "data_core" }
        $dataLifs | Select-Object -Property InterfaceName, OpStatus,
```

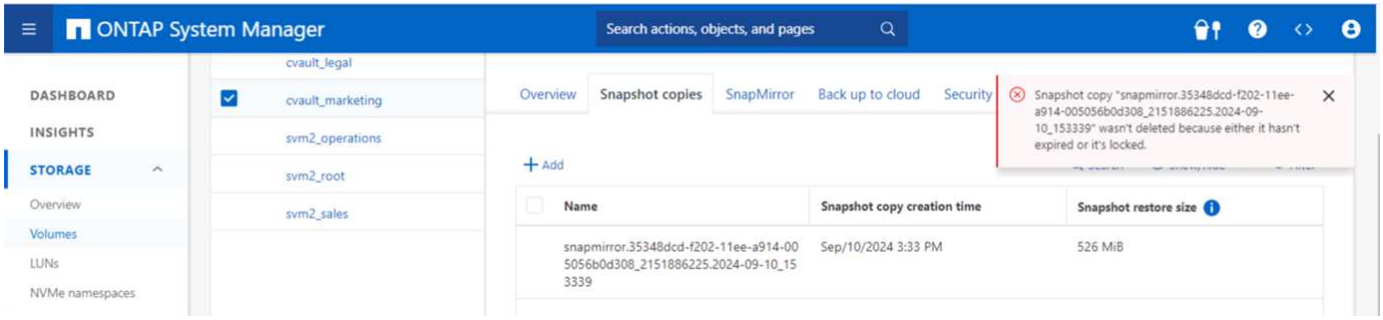
```
DataProtocols, Vserver, Address

        logMessage -message "Checking if all data lifs are disabled for
vServer : $DESTINATION_VSERVER"
        # Disable the filtered data LIFs
        foreach ($lif in $dataLifs) {
            $checkLif = Get-NcNetInterface -Vserver $DESTINATION_VSERVER
-Name $lif.InterfaceName | Where-Object { $_.OpStatus -eq "down" }
            if($checkLif) {
                logMessage -message "Data lif $($lif.InterfaceName)
disabled for vServer $DESTINATION_VSERVER" -type "SUCCESS"
            } else {
                handleError -errorMessage "Data lif $($lif.InterfaceName)
is enabled. Recommendation: Run the script with SCRIPT_MODE `"configure`"
to disable Data lifs for vServer $DESTINATION_VSERVER"
            }
        }
        logMessage -message "All data lifs are disabled for vServer :
$DESTINATION_VSERVER" -type "SUCCESS"

        # check if multi-admin verification is enabled
        logMessage -message "Checking if multi-admin verification is
enabled"
        $maaConfig = Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP
-Credential $DESTINATION_ONTAP_CREDS -Command "set -privilege advanced;
security multi-admin-verify show"
        if ($maaConfig.Value -match "Enabled" -and $maaConfig.Value -match
"true") {
            $maaConfig
            logMessage -message "Multi-admin verification is configured
and enabled" -type "SUCCESS"
        } else {
            handleError -errorMessage "Multi-admin verification is not
configured or not enabled. Recommendation: Run the script with SCRIPT_MODE
`"configure`" to enable and configure Multi-admin verification"
        }

        # check if telnet is disabled
        logMessage -message "Checking if telnet is disabled"
        $telnetConfig = Invoke-NcSsh -Name
$DESTINATION_ONTAP_CLUSTER_MGMT_IP -Credential $DESTINATION_ONTAP_CREDS
-Command "set -privilege advanced; security protocol show -application
telnet"
        if ($telnetConfig.Value -match "enabled" -and $telnetConfig.Value
-match "false") {
            logMessage -message "Telnet is disabled" -type "SUCCESS"
```

```
        } else {
            handleError -errorMessage "Telnet is enabled. Recommendation:
Run the script with SCRIPT_MODE `"configure`" to disable telnet"
        }

        # check if network https is restricted to allowed IP addresses
        logMessage -message "Checking if HTTPS is restricted to allowed IP
addresses $ALLOWED_IPS"
        $networkServicePolicy = Invoke-NcSsh -Name
$DESTINATION_ONTAP_CLUSTER_MGMT_IP -Credential $DESTINATION_ONTAP_CREDS
-Command "set -privilege advanced; network interface service-policy show"
        if ($networkServicePolicy.Value -match "management-https:
$($ALLOWED_IPS)") {
            logMessage -message "HTTPS is restricted to allowed IP
addresses $ALLOWED_IPS" -type "SUCCESS"
        } else {
            handleError -errorMessage "HTTPS is not restricted to allowed
IP addresses $ALLOWED_IPS. Recommendation: Run the script with SCRIPT_MODE
`"configure`" to restrict allowed IP addresses for HTTPS management"
        }
    }
    catch {
        handleError -errorMessage $_.Exception.Message
    }
}
```

このスクリーンショットは、Vault コントローラーに接続がないことを示しています。



このスクリーンショットは、スナップショットを改ざんすることができないことを示しています。



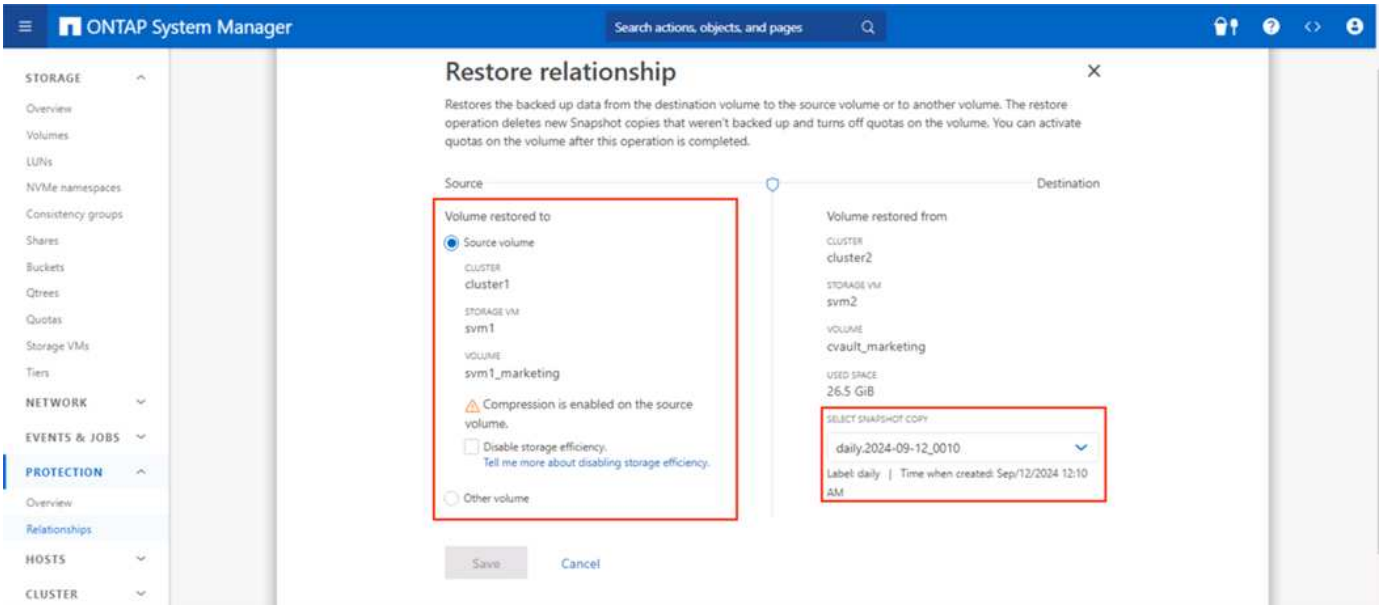
エアギャップ機能を検証および確認するには、次の手順に従います。

- ネットワーク分離機能と、データが転送されていないときに接続を停止する機能をテストします。
- 許可された IP アドレス以外のエンティティから管理インターフェイスにアクセスできないことを確認します。
- 追加の承認レイヤーを提供するために、複数の管理者による検証が実施されていることを確認します。
- CLIおよびREST API経由でのアクセス機能を検証する
- ソースから、ボールトへの転送操作をトリガーし、ボールトされたコピーが変更されないことを確認します。
- ボールトに転送された不変のスナップショットのコピーを削除してみます。
- システム クロックを改ざんして保持期間を変更しようとします。

ONTAPサイバーボールトデータリカバリ

運用データセンターでデータが破壊された場合でも、サイバー ボールトからのデータは選択した環境に安全に復元できます。物理的にエアギャップされたソリューションとは異なり、エアギャップされたONTAPサイバー ボールトは、 SnapLock ComplianceやSnapMirrorなどのネイティブのONTAP機能を使用して構築されます。その結果、回復プロセスは高速かつ簡単に実行できるようになります。

ランサムウェア攻撃が発生し、サイバー ボールトから回復する必要がある場合、サイバー ボールトに保存されているスナップショット コピーを使用して暗号化されたデータを復元するため、回復プロセスはシンプルで簡単です。



リカバリのためにデータを迅速に検証、分離、分析する必要がある場合に、データをオンラインに戻すより高速な方法を提供することが要件となっている場合。これは、スナップロック タイプ オプションを非スナップロック タイプに設定してFlexCloneを使用することで簡単に実現できます。

ONTAP 9.13.1 以降では、snaplock-type オプションを「non-snaplock」に設定してFlexCloneを作成することにより、 SnapLockボールト関係の宛先SnapLockボリューム上のロックされたSnapshot コピーを即座に復元できます。ボリュームクローン作成操作を実行するときは、スナップショットコピーを「親スナップショット」として指定します。 SnapLockタイプのFlexCloneボリュームの作成に関する詳細情報"ここをクリックしてください。"

サイバー ボールトからの回復手順を練習することで、サイバー ボールトに接続してデータを取得するための適切な手順が確立されます。サイバー攻撃発生時の復旧には、手順の計画とテストが不可欠です。

その他の考慮事項

ONTAPベースのサイバー ボールトを設計および導入する際には、追加の考慮事項があります。

容量サイジングの考慮事項

ONTAPサイバー ボールトの宛先ボリュームに必要なディスク領域の量はさまざまな要因によって異なりますが、最も重要なのはソース ボリュームのデータの変更率です。宛先ボリュームのバックアップ スケジュールとスナップショット スケジュールは両方とも宛先ボリュームのディスク使用量に影響し、ソース ボリュームの変更率は一定にならない可能性があります。エンドユーザーやアプリケーションの動作の将来的な変化に対応するために必要な容量に加えて、追加のストレージ容量のバッファーを用意しておくことをお勧めします。

ONTAPで 1 か月間の保持関係のサイズを決定するには、プライマリ データセットのサイズ、データ変更率（日次変更率）、重複排除と圧縮による節約（該当する場合）など、いくつかの要素に基づいてストレージ要件を計算する必要があります。

手順は次のとおりです。

最初のステップは、サイバー ボールトで保護しているソース ボリュームのサイズを確認することです。これは、サイバー ボールトの宛先に最初に複製されるデータの基本量です。次に、データセットの毎日の変化率を推定します。これは毎日変更されるデータの割合です。データがどれだけ動的であるかをよく理解することが重要です。

例えば：

- プライマリデータセットのサイズ = 5TB
- 日次変化率 = 5% (0.05)
- 重複排除と圧縮効率 = 50% (0.50)

それでは計算を見てみましょう。

- 毎日のデータ変化率を計算します。

```
Changed data per day = 5000 * 5% = 250GB
```

- 30 日間の変更されたデータの合計を計算します。

```
Total changed data in 30 days = 250 GB * 30 = 7.5TB
```

- 必要な合計ストレージを計算します。

```
TOTAL = 5TB + 7.5TB = 12.5TB
```

- 重複排除と圧縮による節約を適用します。

```
EFFECTIVE = 12.5TB * 50% = 6.25TB
```

ストレージニーズの概要

- 効率性がなければ、サイバー ボールト データの 30 日分を保存するには **12.5 TB** が必要になります。
- 効率が 50% の場合: 重複排除と圧縮後に **6.25 TB** のストレージが必要になります。

スナップショット コピーではメタデータによる追加のオーバーヘッドが発生する可能性がありますが、通常はそれほど大きくありません。

1 日に複数のバックアップが作成される場合は、1 日に作成される Snapshot コピーの数に応じて計算を調整します。

時間の経過に伴うデータの増加を考慮して、サイズが将来にも対応できることを確認します。

プライマリ/ソースへのパフォーマンスの影響

データ転送はプル操作であるため、プライマリ ストレージのパフォーマンスへの影響は、ワークロード、データ量、およびバックアップの頻度によって異なります。ただし、データ転送はデータ保護とバックアップ タスクをサイバー ボールト ストレージ システムにオフロードするように設計されているため、プライマリ システムへの全体的なパフォーマンスへの影響は通常は中程度で管理可能です。初期の関係のセットアップと最初の完全バックアップ中に、大量のデータがプライマリ システムからサイバー ボールト システム (

SnapLock Complianceボリューム) に転送されます。これにより、プライマリ システムのネットワーク トラフィックと I/O 負荷が増加する可能性があります。最初の完全バックアップが完了すると、 ONTAP は最後のバックアップ以降に変更されたブロックを追跡して転送するだけで済みます。これにより、初期レプリケーションと比較して I/O 負荷が大幅に軽減されます。増分更新は効率的であり、プライマリ ストレージのパフォーマンスへの影響は最小限に抑えられます。ボールト プロセスはバックグラウンドで実行されるため、プライマリ システムの運用ワークロードに干渉する可能性が軽減されます。

- 追加の負荷を処理するために十分なリソース (CPU、メモリ、IOPS) がストレージ システムにあることを確認すると、パフォーマンスへの影響が軽減されます。

設定、分析、**cron**スクリプト

NetAppは、"ダウンロード可能な単一のスクリプト"サイバー ボールト関係を構成、検証、およびスケジュールするために使用されます。

このスクリプトが行うこと

- クラスタ ピアリング
- SVMピアリング
- DPボリュームの作成
- SnapMirror関係と初期化
- サイバーボールトに使用されるONTAPシステムを強化する
- 転送スケジュールに基づいて関係を休止および再開する
- セキュリティ設定を定期的に検証し、異常を示すレポートを生成する

このスクリプトの使い方

"スクリプトをダウンロードする"スクリプトを使用するには、以下の手順に従ってください。

- Windows PowerShell を管理者として起動します。
- スクリプトが含まれているディレクトリに移動します。
- スクリプトを実行するには `.\`必要なパラメータを含む構文

> すべての情報が入力されていることを確認してください。最初の実行時 (構成モード) には、本番環境と新しいサイバー ボールト システムの両方の資格情報が求められます。その後、SVM ピアリング (存在しない場合)、ボリューム、およびシステム間のSnapMirrorが作成され、初期化されます。

> Cron モードを使用すると、データ転送の停止と再開をスケジュールできます。

動作モード

自動化スクリプトは3つの実行モードを提供します - `configure`、 `analyze`そして `cron`。

```
if($SCRIPT_MODE -eq "configure") {
        configure
    } elseif ($SCRIPT_MODE -eq "analyze") {
        analyze
    } elseif ($SCRIPT_MODE -eq "cron") {
        runCron
    }
```

- 構成 - 検証チェックを実行し、システムをエアギャップとして構成します。
- 分析 - 異常や疑わしいアクティビティに関する情報を監視グループに送信し、構成が変更されないようにする自動監視およびレポート機能。
- Cron - 切断されたインフラストラクチャを有効にするために、cron モードは LIF の無効化を自動化し、転送関係を静止します。

システムのパフォーマンスとデータの量に応じて、選択したボリューム内のデータの転送に時間がかかります。

```
./script.ps1 -SOURCE_ONTAP_CLUSTER_MGMT_IP "172.21.166.157"
-SOURCE_ONTAP_CLUSTER_NAME "NTAP915_Src" -SOURCE_VSERVER "svm_NFS"
-SOURCE_VOLUME_NAME "Src_RP_Vol01" -DESTINATION_ONTAP_CLUSTER_MGMT_IP
"172.21.166.159" -DESTINATION_ONTAP_CLUSTER_NAME "NTAP915_Destn"
-DESTINATION_VSERVER "svm_nim_nfs" -DESTINATION_AGGREGATE_NAME
"NTAP915_Destn_01_VM_DISK_1" -DESTINATION_VOLUME_NAME "Dst_RP_Vol01_Vault"
-DESTINATION_VOLUME_SIZE "5g" -SNAPLOCK_MIN_RETENTION "15minutes"
-SNAPLOCK_MAX_RETENTION "30minutes" -SNAPMIRROR_PROTECTION_POLICY
"XDPDefault" -SNAPMIRROR_SCHEDULE "5min" -DESTINATION_CLUSTER_USERNAME
"admin" -DESTINATION_CLUSTER_PASSWORD "PASSWORD123"
```

ONTAPサイバーボルト PowerShell ソリューションの結論

NetApp は、 ONTAPが提供する強力な強化手法によるエアギャップを活用することで、進化するサイバー脅威に耐性のある、安全で分離されたストレージ環境の構築を可能にします。これらすべては、既存のストレージ インフラストラクチャの俊敏性と効率性を維持しながら実現されます。この安全なアクセスにより、企業は既存の人材、プロセス、テクノロジー フレームワークへの変更を最小限に抑えながら、厳格な安全性と稼働時間の目標を達成できるようになります。

ONTAPサイバー ボールトはONTAPのネイティブ機能を使用して、データの変更不可能で消去不可能なコピーを作成することで、追加の保護を実現する簡単な方法です。 NetApp のONTAPベースのサイバー ボールトを全体的なセキュリティ体制に追加すると、次のことが可能になります。

- 運用ネットワークとバックアップ ネットワークから分離され切断された環境を作成し、ユーザー アクセスを制限します。

著作権に関する情報

商標に関する情報