自律的なランサムウェア防御
ONTAP 9

NetApp
August 31, 2024

目次

自律的なランサムウェア防御

Autonomous Ransomware Protection Overview

ONTAP 9.10.1以降のAutonomous RansProtection（ARP）機能では、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を示す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検出して警告します。

攻撃の疑いがある場合、ARPは、スケジュールされたSnapshotコピーからの既存の保護に加えて、新しいSnapshotコピーも作成します。

ライセンスとイネーブルメント

ARPにはライセンスが必要です。ARPは、 "ONTAP 1ライセンス"。ONTAP Oneライセンスがない場合は、使用しているONTAPのバージョンによって異なる他のライセンスを使用してARPを使用できます。

ONTAP リリース	使用許諾
ONTAP 9.11.1以降	anti_Ransomware
ONTAP 9.10.1	MT_EK_MGMT（マルチテナントキー管理）

- ONTAP 9.11.1以降にアップグレードしていて、ARPがすでにシステムに設定されている場合は、新しいアンチランサムウェアライセンスを購入する必要はありません。新しいARP設定の場合、新しいライセンスが必要です。
- ONTAP 9.11.1以降からONTAP 9.10.1にリバートする際に、ランサムウェア対策ライセンスでARPを有効にしていると、警告メッセージが表示され、ARPの再設定が必要になる場合があります。 "ARPのリバートについて説明します"。

System ManagerまたはONTAP CLIを使用して、ボリューム単位でARPを設定できます。

ONTAP ランサムウェア攻撃からの保護戦略

ランサムウェアの効果的な検出戦略には、複数の保護レイヤを含める必要があります。

例えは、車両の安全機能です。シートベルトなどの単一の機能に頼らず、事故時に完全に身を守ることができます。エアバッグ、アンチロックブレーキ、および前方衝突警告はすべて、より良い結果をもたらす追加の安全機能です。ランサムウェア攻撃からの保護は、同様の方法で確認する必要があります。

ONTAP には、ランサムウェアからの保護に役立つFPolicy、Snapshotコピー、SnapLock 、Active IQ デジタルアドバイザなどの機能が含まれていますが、以下では機械学習機能を備えたARP搭載機能に焦点を当てて説明します。

ONTAPのその他のランサムウェア対策機能の詳細については、を参照してください"ランサムウェアとNetAppの保護ポートフォリオ"。

ARPが検出するもの

ARPは、身代金が支払われるまで攻撃者がデータを保留するサービス拒否攻撃から保護するように設計されています。ARP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データまたはプレーンテキストとして識別する。
- 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（ONTAP 9.11.1以降）

ARPは、少数のファイルのみが暗号化された後、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、攻撃の疑いがあることを警告します。

ランサムウェア攻撃の安全性を完全に保証できるランサムウェア検出や防御システムはありません。攻撃が検出されない可能性はありますが、アンチウイルスソフトウェアが侵入を検出できなかった場合、ARPは重要な追加防御層として機能します。

学習モードとアクティブモード

ARPには2つのモードがあります。

- 学習（または「ドライラン」モード）
- アクティブ（または「有効」モード）

ARPをイネーブルにすると、_learning mode_で実行されます。学習モードでは、ONTAPシステムは、エントロピー、ファイル拡張子タイプ、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。ARPをラーニングモードで実行して、ワークロード特性を評価するのに十分な時間が経過したら、アクティブモードに切り替えてデータの保護を開始できます。ARPがアクティブモードに切り替わると、ONTAPはARP Snapshotコピーを作成して、脅威が検出された場合にデータを保護します。

ARPを学習モードのまま30日間放置することをお勧めします。ONTAP 9.13.1以降では、ARPによって最適な学習期間間隔が自動的に決定され、30日前にスイッチが自動化されます。

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。コマンド `security anti-ransomware volume workload-behavior show` ボリュームで検出されたファイル拡張子が表示されます。（このコマンドをラーニングモードの早い段階で実行し、ファイルタイプが正確に表現されている場合は、ONTAPが他のメトリックを収集しているため、そのデータをアクティブモードに移行するためのベースとして使用しないでください）。

ONTAP 9.11.1以降では、ARPの検出パラメータをカスタマイズできます。詳細については、を参照してください ARP攻撃検出パラメータを管理します。。

脅威の評価とARP Snapshotコピー

アクティブモードでは、ARPは学習した分析に対して測定された受信データに基づいて脅威の確率を評価します。ARPが脅威を検出すると、測定値が割り当てられます。

- 低：ボリュームの異常をいち早く検出したもの（たとえば、新しいファイル拡張子がボリュームに観察された場合）。
- 中程度:同じファイル拡張子を持つ複数のファイルが観察されます。
  - ONTAP 9.10.1では、中程度へのエスカレーションのしきい値は100個以上です。ONTAP 9.11.1以降では、ファイル数を変更できます。デフォルト値は20です。

脅威が低い状況では、ONTAPが異常を検出し、ボリュームのSnapshotコピーを作成して最適なリカバリポイントを作成します。ONTAPでは、ARP Snapshotコピーの名前の先頭に次の文字が付加されます。 `Anti-ransomware-backup` 簡単に識別できるようにするために `Anti_ransomware_backup.2022-12-20_1248`。

ONTAPがランサムウェアのプロファイルに異常が一致しているかどうかを判断する分析レポートを実行すると、脅威は「中程度」にエスカレーションされます。下位レベルの脅威はログに記録され、System Managerの[*イベント]セクションに表示されます。攻撃の可能性が中程度の場合、ONTAP によってEMS通知が生成され、脅威を評価するように求められます。ONTAPは低脅威に関するアラートを送信しませんが、ONTAP 9.14.1以降では、次のことが可能です。 アラート設定の変更。詳細については、を参照してください 異常な活動に対応する。。

脅威に関する情報は、レベルに関係なく、System Managerの[*イベント]セクションまたはを使用して表示できます `security anti-ransomware volume show` コマンドを実行します

ARP Snapshotコピーは最低2日間保持されます。ONTAP 9.11.1以降では、保持設定を変更できます。詳細については、を参照してください Snapshotコピーのオプションを変更します。

ランサムウェア攻撃のあとに ONTAP でデータをリカバリする方法

攻撃の疑いがある場合、システムはその時点でボリュームの Snapshot コピーを作成し、そのコピーをロックします。あとで攻撃が確認された場合は、ARP Snapshotコピーを使用してボリュームをリストアできます。

ロックされた Snapshot コピーは、通常の方法で削除できません。ただし、後で攻撃をフォールスポジティブとしてマークする場合、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刻を把握していれば、ボリューム全体をSnapshotコピーの1つにリバートするだけでなく、さまざまなSnapshotコピー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。

ARPは、実績のあるONTAP データ保護とディザスタリカバリテクノロジを基盤として、ランサムウェア攻撃に対応しています。データのリカバリの詳細については、次のトピックを参照してください。

- "Snapshot コピーからのリカバリ（ System Manager ）"
- "Snapshot コピーからのファイルのリストア（ CLI ）"
- "スマートなランサムウェアリカバリ"

自動ランサムウェア対策による保護のユースケースと考慮事項

ONTAP 9.10.1以降では、自律型ランサムウェア対策（ARP）をNASワークロードで使用できます。ARPを導入する前に、推奨される使用方法とサポートされる設定、およびパフォーマンスへの影響について理解しておく必要があります。

サポートされる構成とサポートされない構成

ARPの使用を決定する際には、ボリュームのワークロードがARPに適していること、および必要なシステム構成を満たしていることを確認することが重要です。

最適なワークロード

ARPは次の用途に適しています。

- NFS ストレージ上のデータベース
- Windows または Linux のホームディレクトリ

  学習期間中に検出されなかった拡張子のファイルが作成される可能性があるため、このワークロードでは誤検出の可能性が高くなります。

- 画像とビデオ

  たとえば、医療記録やElectronic Design Automation（EDA）データなどです。

不適切なワークロード

ARPは次の用途には適していません。

- ファイルの作成や削除が頻繁に発生するワークロード（テスト/開発ワークロードなど、数秒で数十万個のファイルを処理）
- ARPの脅威検出機能は、ファイルの作成、名前変更、または削除アクティビティの異常な急増を認識できるかどうかに依存します。アプリケーション自体がファイルアクティビティのソースである場合、ランサムウェアのアクティビティと効果的に区別することはできません。
- アプリケーションまたはホストがデータを暗号化するワークロード。
  ARPは、着信データを暗号化されたものと暗号化されていないものと区別します。アプリケーション自体がデータを暗号化している場合は、機能の有効性が低下します。ただし、この機能は、ファイルアクティビティ（削除、上書き、作成、または新しいファイル拡張子を使用した作成または名前変更）およびファイルタイプに基づいて動作します。

サポートされている構成

ONTAP 9.10.1以降では、オンプレミスのONTAPシステムのNFSボリュームとSMBボリュームにARPを使用できます。

次のONTAPバージョンでは、その他の構成とボリュームタイプがサポートされます。

	ONTAP 9.15.1	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
非同期SnapMirrorで保護されているボリューム	✓	✓	✓	✓		
非同期SnapMirror（SVMディザスタリカバリ）で保護されるSVM	✓	✓	✓	✓		
SVM のデータ移動 (`vserver migrate`)	✓	✓	✓	✓		
FlexGroup ボリューム	✓	✓	✓			
管理者による検証が複数必要です	✓	✓	✓			

SnapMirrorと**ARP**の相互運用性

ONTAP 9.12.1以降では、非同期SnapMirrorデスティネーションボリュームでARPがサポートされます。ARPはSnapMirror Synchronousでサポートされていません**。

SnapMirrorソースボリュームがARP対応の場合、SnapMirrorデスティネーションボリュームには、ARP設定状態（ラーニング、有効化など）、ARPトレーニングデータ、およびARPで作成されたソースボリュームのSnapshotが自動的に取得されます。明示的な有効化は必要ありません。

デスティネーションボリュームは読み取り専用（RO）Snapshotコピーで構成されていますが、データに対してARP処理は実行されません。ただし、SnapMirrorデスティネーションボリュームが読み書き可能（rw）に変換されると、ARPはRW変換されたデスティネーションボリュームで自動的に有効になります。デスティネーションボリュームでは、ソースボリュームにすでに記録されている情報に加えて、ラーニング手順 を追加する必要はありません。

ONTAP 9.10.1および9.11.1では、ARP設定の状態、トレーニングデータ、およびSnapshotコピーが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転送されません。したがって、SnapMirrorデスティネーションボリュームがRWに変換されると、変換後にデスティネーションボリュームのARPがラーニングモードで明示的に有効になる必要があります。

ARPと仮想マシン

ARPは仮想マシン（VM）でサポートされます。ARP検出の動作は、VMの内部と外部の変更で異なります。ARPは、エントロピーの高いファイルがVM内にあるワークロードには推奨されません。

VM以外での変更

ARPは、新しい拡張子が暗号化されたボリュームに入った場合やファイル拡張子が変更された場合に、VMの外部にあるNFSボリュームでのファイル拡張子の変更を検出できます。検出可能なファイル拡張子の変更は次

のとおりです。

- .vmx
- .vmxf
- .vmdk
- -flat.vmdk
- .nvram
- .vMem
- .vmsd
- .vmsn
- .vswp
- .vmss
- .log
- -\#.log

VM内での変更

ランサムウェア攻撃がVMをターゲットにし、VMの外部で変更を行わずにVM内のファイルが変更された場合、ARPはVMのデフォルトエントロピーが低い場合（.txt、.docx、.mp4ファイルなど）に脅威を検出します。このシナリオではARPは保護スナップショットを作成しますが、VMの外部にあるファイル拡張子が改ざんされていないため、脅威アラートは生成されません。

デフォルトでは、ファイルが高エントロピー（.gzipやパスワードで保護されたファイルなど）の場合、ARPの検出機能は制限されます。この場合でもARPはプロアクティブなスナップショットを取得できますが、ファイル拡張子が外部で改ざんされていない場合、アラートはトリガーされません。

サポートされない構成です

ARPは、次のシステム設定ではサポートされていません。

- ONTAP S3 環境
- SAN 環境

ARPでは、次のボリューム構成はサポートされません。

- FlexGroupボリューム（ONTAP 9.10.1~9.12.1の場合）ONTAP 9.13.1以降では、FlexGroupボリュームがサポートされます）。
- FlexCacheボリューム（ARPは元のFlexVolボリュームではサポートされますが、キャッシュボリュームではサポートされません）
- ボリュームをオフラインにします
- SAN-only ボリューム
- SnapLock ボリューム
- SnapMirror Synchronous
- 非同期SnapMirror（ONTAP 9.10.1および9.11.1でのみサポートされません。非同期SnapMirrorは、ONTAP 9.12.1以降でサポートされます。詳細については、を参照してください [snapmirror]. ）

- 制限されたボリューム
- Storage VMのルートボリューム
- 停止しているStorage VMのボリューム

ARPのパフォーマンスと周波数に関する考慮事項

ARPは、スループットとピークIOPSで測定した場合、システムパフォーマンスへの影響を最小限に抑えることができます。ARP機能の影響は、ボリュームのワークロードによって異なります。一般的なワークロードに推奨される構成の制限は次のとおりです。

ワークロードの特性	ノードあたりの推奨されるボリューム数の上限	ノード単位のボリューム制限を超えたときのパフォーマンスの低下：**[*]**
大量の読み取り処理や、データの圧縮が可能です。	一五 〇	最大IOPSの4%
大量の書き込みが発生し、データを圧縮することはできません。	60ドルだ	最大IOPSの10%

合格：[*]推奨制限を超過したボリュームの数に関係なく、システムパフォーマンスはこれらの割合を超えて低下することはありません。

ARP分析は優先順位付けされた順序で実行されるため、保護されたボリュームの数が増えるにつれて、各ボリュームでの分析の実行頻度は低下します。

ARPで保護されたボリュームを使用したマルチ管理者検証

ONTAP 9.13.1以降では、マルチ管理者検証（MAV）をイネーブルにしてARPによるセキュリティを強化できます。MAVを使用すると、少なくとも2人以上の認証された管理者が、保護されたボリュームでARPをオフにしたり、ARPを一時停止したり、疑わしい攻撃をfalse positiveとしてマークしたりする必要があります。方法をご確認ください "ARPで保護されたボリュームのMAVを有効にします"。

MAVグループの管理者を定義し、のMAVルールを作成する必要があります `security anti-ransomware volume disable`、 `security anti-ransomware volume pause`および `security anti-ransomware volume attack clear-suspect` 保護するARPコマンド。MAVグループの各管理者は、新しいルール要求とを承認する必要があります "MAVルールを再度追加します" MAV設定内。

ONTAP 9.14.1以降では、ARPスナップショットの作成および新しいファイル拡張子の監視に関するアラートが提供されます。これらのイベントのアラートは、デフォルトでは無効になっています。アラートはボリュームレベルまたはSVMレベルで設定できます。MAVルールは、次のコマンドを使用してSVMレベルで作成できます。 `security anti-ransomware vserver event-log modify` またはボリュームレベルで、`security anti-ransomware volume event-log modify`。

次のステップ

- "自動ランサムウェア対策を有効化"
- "ARPで保護されたボリュームのMAVを有効にする"

自動ランサムウェア対策を有効化

ONTAP 9.10.1以降のAutonomous Ransomware Protection（ARP）は、新規または既存

のボリュームで有効にできます。最初にARPをラーニングモードでイネーブルにします。このモードでは、システムがワークロードを分析して、通常の動作の特性を特定します。既存のボリュームでARPを有効にしたり、新しいボリュームを作成してARPを有効にしたりすることができます。

このタスクについて

ARPは、必ず最初にラーニング（またはドライラン）モードでイネーブルにする必要があります。アクティブモードで開始すると、過剰なfalse positiveレポートが発生する可能性があります。

ARPを学習モードで最低30日間実行することをお勧めします。ONTAP 9.13.1以降では、ARPによって最適な学習期間間隔が自動的に決定され、30日前にスイッチが自動化されます。詳細については、を参照してください "学習モードとアクティブモード"。

> 既存のボリュームでは、ラーニングモードとアクティブモードは新しく書き込まれたデータにのみ適用され、ボリューム内の既存のデータには適用されません。既存のデータはスキャンおよび分析されません。これは、以前の通常のデータトラフィックの特性が、ARPでボリュームを有効にした後の新しいデータに基づいていると見なされるためです。

作業を開始する前に

- NFSまたはSMB（またはその両方）に対してStorage VM（SVM）が有効になっている必要があります。
- 。 正しいライセンス ONTAP のバージョンに対応するがインストールされている必要があります。
- クライアントでNASワークロードを設定しておく必要があります。
- ARPを設定するボリュームは保護されており、アクティブなボリュームである必要があります "ジャンクションパス"。
- ボリュームの使用率が100%未満である必要があります。
- ARPアクティビティの通知を含む電子メール通知を送信するようにEMSシステムを設定することをお勧めします。詳細については、を参照してください "E メール通知を送信するように EMS イベントを設定します"。
- ONTAP 9.13.1以降では、Autonomous Ransomware Protection（ARP；自律ランサムウェア対策）設定に複数の認証済みユーザ管理者が必要になるように、Multi-admin Verification（MAV；マルチ管理者検証）を有効にすることを推奨します。詳細については、を参照してください "マルチ管理者検証を有効にします"。

ARPを有効にする

ARPは、System ManagerまたはONTAP CLIを使用して有効にできます。

System Manager の略

手順

1. [ストレージ]>[ボリューム]*を選択し、保護するボリュームを選択します。
2. [Volumes]の概要の*タブで、[Status]を選択し、[Anti-ransomware]*ボックスで[Disabled]から[Enabled in learning-mode]に切り替えます。
3. 学習期間が終了したら、ARPをアクティブモードに切り替えます。

   ONTAP 9.13.1以降では、ARPによって最適な学習期間間隔が自動的に決定され、スイッチが自動化されます。可能です "関連付けられているStorage VMでこの設定を無効にしてください" ラーニングモードをアクティブモードに切り替える場合は、手動で切り替えます。

   a. [ストレージ]>[ボリューム]*を選択し、アクティブモードにする準備ができたボリュームを選択します。
   b. [Volumes]概要の*タブで、**[Anti-ransomware]**ボックスで[Switch * to active mode]を選択します。
4. ボリュームのARP状態は、* Anti-ransomware *ボックスで確認できます。

   すべてのボリュームのARPステータスを表示するには、* Volumes ペインで Show/Hide を選択し、Anti-ransomware *ステータスがチェックされていることを確認します。

CLI の使用

CLIを使用してARPを有効にするプロセスは、既存のボリュームで有効にする場合と新しいボリュームで有効にする場合で異なります。

既存のボリュームで**ARP**を有効にします

1. 既存のボリュームを変更して、学習モードでランサムウェアからの保護を有効にします。

   ```
   security anti-ransomware volume dry-run -volume vol_name -vserver svm_name
   ```

   ONTAP 9.13.1以降を実行している場合は、アクティブ状態への変更が自動的に行われるように、アダプティブラーニングがイネーブルになります。この動作を自動的に有効にしない場合は、関連付けられているすべてのボリュームでSVMレベルの設定を変更します。

   ```
   vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to
   -enabled false
   ```

2. 学習期間が終了したら、保護ボリュームを変更してアクティブモードに切り替えます（まだ自動的に行われていない場合）。

   ```
   security anti-ransomware volume enable -volume vol_name -vserver svm_name
   ```

   volume modify コマンドを使用して、アクティブモードに切り替えることもできます。

   ```
   volume modify -volume vol_name -vserver svm_name -anti-ransomware-state
   active
   ```

3. ボリュームのARP状態を確認します。

   ```
   security anti-ransomware volume show
   ```

新しいボリュームで**ARP**を有効にします

1. データをプロビジョニングする前に、ランサムウェア対策を有効にした新しいボリュームを作成する。

   ```
   volume create -volume vol_name -vserver svm_name -aggregate aggr_name -size nn -anti-ransomware-state dry-run -junction-path /path_name
   ```

   ONTAP 9.13.1以降を実行している場合は、アクティブ状態への変更が自動的に行われるように、アダプティブラーニングがイネーブルになります。この動作を自動的に有効にしない場合は、関連付けられているすべてのボリュームでSVMレベルの設定を変更します。

   ```
   vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to -enabled false
   ```

2. 学習期間が終了したら、保護ボリュームを変更してアクティブモードに切り替えます（まだ自動的に行われていない場合）。

   ```
   security anti-ransomware volume enable -volume vol_name -vserver svm_name
   ```

   volume modify コマンドを使用して、アクティブモードに切り替えることもできます。

   ```
   volume modify -volume vol_name -vserver svm_name -anti-ransomware-state active
   ```

3. ボリュームのARP状態を確認します。

   ```
   security anti-ransomware volume show
   ```

新規ボリュームでの**Autonomous Ransomware Protection**のデフォルト設定の有効化

ONTAP 9.10.1以降のStorage VM（SVM）を設定して、学習モードのAutonomous Ransomware Protection（ARP）に対して新しいボリュームがデフォルトで有効になるようにすることができます。

このタスクについて

デフォルトでは、新しいボリュームは無効モードでARPを使用して作成されます。この設定は、System ManagerおよびCLIを使用して変更できます。デフォルトで有効になっているボリュームは、ラーニング（またはドライラン）モードでARPに設定されます。

ARPは、設定の変更後にSVMで作成されたボリュームでのみ有効になります。既存のボリュームではARPは有効になりません。方法をご確認ください "既存のボリュームでARPを有効にします"。

ONTAP 9.13.1以降、アダプティブラーニングがARP分析に追加され、ラーニングモードからアクティブモー

ドへの切り替えが自動的に行われます。詳細については、を参照してください "学習モードとアクティブモード"。

作業を開始する前に

- 。 正しいライセンス ONTAP のバージョンに対応するがインストールされている必要があります。
- ボリュームの使用率が100%未満である必要があります。
- ジャンクションパスがアクティブである必要があります。
- ONTAP 9.13.1以降では、マルチ管理者認証（MAV）を有効にして、ランサムウェア対策に2人以上の認証済みユーザ管理者が必要になるようにすることをお勧めします。 "詳細はこちら。"。

ARPをラーニングモードからアクティブモードに切り替えます。

ONTAP 9.13.1以降、アダプティブラーニングがARP分析に追加されました。学習モードからアクティブモードへの切り替えは自動的に行われます。ARPによるラーニングモードからアクティブモードへの自動切り替えは、次のオプションの設定に基づいて決定されます。

```
-anti-ransomware-auto-switch-minimum-incoming-data-percent
-anti-ransomware-auto-switch-duration-without-new-file-extension
-anti-ransomware-auto-switch-minimum-learning-period
-anti-ransomware-auto-switch-minimum-file-count
-anti-ransomware-auto-switch-minimum-file-extension
```

30日間の学習後、これらの条件の1つまたは複数が満たされていない場合でも、ボリュームは自動的にアクティブモードに切り替わります。つまり、自動切り替えが有効な場合、ボリュームは最大30日後にアクティブモードに切り替わります。最大値の30日は固定であり、変更できません。

デフォルト値を含むARP設定オプションの詳細については、を参照してください。 "ONTAP コマンドリファレンス"。

手順

デフォルトでは、System ManagerまたはONTAP CLIを使用してARPを有効にできます。

System Manager の略

1. [ストレージ]>[Storage VM]*を選択し、ARPで保護するボリュームを含むStorage VMを選択します。
2. *[設定]*タブに移動します。[Security（セキュリティ）]*で、[Anti-ransomware（ランサムウェア対策）]*タイルを探し、
3. NASボリュームのARPを有効にするには、このボックスをオンにします。Storage VM内の対応するすべてのNASボリュームでARPを有効にするには、追加のボックスをオンにします。

ONTAP 9.13.1にアップグレードした場合は、*十分な学習後に自動的に学習モードからアクティブモードに切り替える*設定が自動的に有効になります。これにより、ARPは最適な学習期間間隔を決定し、アクティブモードへの切り替えを自動化できます。手動でアクティブモードに移行する場合は、この設定をオフにします。

CLI の使用

1. 既存のSVMを変更して、新しいボリュームでデフォルトでARPを有効にします。
   `vserver modify -vserver svm_name -anti-ransomware-default-volume-state dry-run`

   CLIでは、新しいボリュームに対してARPがデフォルトで有効になっている新しいSVMを作成することもできます。
   `vserver create -vserver svm_name -anti-ransomware-default-volume-state dry-run [other parameters as needed]`

   ONTAP 9.13.1以降にアップグレードした場合は、アクティブ状態への変更が自動的に行われるように、アダプティブラーニングがイネーブルになります。この動作を自動的に有効にしない場合は、次のコマンドを使用します。

   ```
   vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to
   -enabled false
   ```

Autonomous Ransomware Protectionを一時停止して、ワークロードイベントを分析対象から除外します

通常とは異なるワークロードイベントが発生すると予想される場合は、一時的にRansomware Protection（ARP）分析を一時的に一時停止して再開できます。

ONTAP 9.13.1以降では、マルチ管理者検証（MAV）をイネーブルにして、複数の認証済みユーザ管理者がARPを一時停止する必要があります。 "詳細はこちら。"。

このタスクについて

ARPの一時停止中は、イベントはログに記録されず、新しい書き込みに対するアクションも記録されません。ただし、分析処理はバックグラウンドで以前のログに対して続行されます。

ARP無効機能を使用して分析を一時停止しないでください。これにより、ボリュームのARPが無効になり、学習されたワークロードの動作に関する既存の情報はすべて失われます。これには学習期間の再開が必要です。

手順

ARPは、System ManagerまたはONTAP CLIを使用して一時停止できます。

System Manager の略

1. [ストレージ]>[ボリューム]*を選択し、ARPを一時停止するボリュームを選択します。
2. [Volumes]の概要の[* **Security**]タブで、[Anti-ransomware]ボックスの*[Pause anti-ransomware]*を選択します。

> ONTAP 9.13.1以降では、MAVを使用してARP設定を保護している場合、一時停止操作によって、1人以上の追加管理者の承認を得るように求められます。 "すべての管理者から承認を受ける必要があります" MAV承認グループに関連付けられているか、操作が失敗します。

CLI の使用

1. ボリュームのARPを一時停止します。

   ```
   security anti-ransomware volume pause -vserver svm_name -volume vol_name
   ```

2. 処理を再開するには、を使用します `resume` コマンドを実行します

   ```
   security anti-ransomware volume resume -vserver svm_name -volume vol_name
   ```

3. *ARP設定を保護するためにMAV（ONTAP 9.13.1以降で使用可能）を使用している場合は、一時停止操作によって、1人以上の追加管理者の承認を得るように求められます。MAV承認グループに関連付けられているすべての管理者から承認を受ける必要があります。そうしないと、操作は失敗します。

   MAVを使用していて、予定されている一時停止操作で追加の承認が必要な場合は、各MAVグループ承認者が次の処理を行います。

   a. 要求を表示します。

      ```
      security multi-admin-verify request show
      ```

   b. リクエストを承認します。

      ```
      security multi-admin-verify request approve -index[number returned from show request]
      ```

      最後のグループ承認者に対する応答は、ボリュームが変更され、ARPの状態が一時停止されたことを示します。

      MAVを使用していて、MAVグループ承認者である場合は、一時停止操作要求を拒否できます。

   ```
   security multi-admin-verify request veto -index[number returned from show request]
   ```

自律型ランサムウェア対策攻撃検出パラメータの管理

ONTAP 9.11.1以降では、特定の自律型ランサムウェア対策が有効なボリュームでランサムウェア検出のパラメータを変更し、通常のファイルアクティビティとして既知の急増を報告できます。検出パラメータを調整すると、特定のボリュームワークロードに基づいてレポートの精度が向上します。

攻撃検出の仕組み

Autonomous Ransomware Protection（ARP；自律型ランサムウェア対策）がラーニングモードの場合、ボリューム動作のベースライン値が設定されます。これらはエントロピー、ファイル拡張子、およびONTAP 9.11.1以降のIOPSです。これらのベースラインは、ランサムウェアの脅威を評価するために使用されます。これらの条件の詳細については、を参照してください。 ARPが検出するもの。

ONTAP 9.10.1では、次の両方の条件が検出されると、ARPは警告を発行します。

- 以前にボリュームで認識されなかったファイル拡張子を持つファイルが20個を超える
- 高エントロピーデータ

ONTAP 9.11.1以降では、_only_one条件が満たされた場合にARPから脅威警告が発行されます。たとえば、ボリュームで以前に観察されたことがないファイル拡張子を持つ20を超えるファイルが24時間以内に観察された場合、ARPはこれをthreat_expendered_of observed entropyに分類します。（24時間と20ファイルの値はデフォルトであり、変更可能です）。

ONTAP 9.14.1以降では、ARPが新しいファイル拡張子を監視したとき、およびARPがスナップショットを作成したときにアラートを設定できます。詳細については、を参照してください [modify-alerts]

特定のボリュームやワークロードでは、異なる検出パラメータが必要です。たとえば、ARP対応ボリュームで多数の種類のファイル拡張子がホストされている場合、以前に見たことのないファイル拡張子のしきい値をデフォルトの20よりも大きい値に変更したり、以前に見たことのないファイル拡張子に基づいて警告を無効にしたりすることができます。ONTAP 9.11.1以降では、特定のワークロードに適した攻撃検出パラメータを変更できます。

攻撃検出パラメータの変更

ARP対応ボリュームの想定される動作によっては、攻撃検出パラメータを変更することができます。

手順

1. 既存の攻撃検出パラメータを表示します。

```
security anti-ransomware volume attack-detection-parameters show -vserver
svm_name -volume volume_name
```

```
security anti-ransomware volume attack-detection-parameters show
-vserver vs1 -volume vol1
                                                Vserver Name : vs1
                                                 Volume Name : vol1
            Is Detection Based on High Entropy Data Rate? : true
  Is Detection Based on Never Seen before File Extension? : true
                  Is Detection Based on File Create Rate? : true
                  Is Detection Based on File Rename Rate? : true
                  Is Detection Based on File Delete Rate? : true
           Is Detection Relaxing Popular File Extensions? : true
                High Entropy Data Surge Notify Percentage : 100
                 File Create Rate Surge Notify Percentage : 100
                 File Rename Rate Surge Notify Percentage : 100
                 File Delete Rate Surge Notify Percentage : 100
 Never Seen before File Extensions Count Notify Threshold : 20
       Never Seen before File Extensions Duration in Hour : 24
```

2. 表示されているフィールドはすべて、ブール値または整数値で変更できます。フィールドを変更するには、 `security anti-ransomware volume attack-detection-parameters modify` コマンドを実行します

   パラメータの完全なリストについては、を参照してください。 "ONTAP コマンドリファレンス"。

既知のサージを報告

ARPは、アクティブモードでも検出パラメータのベースライン値の変更を継続します。1回限りのサージ、または新しい日常の特徴であるサージのいずれかのボリュームアクティビティのサージを知っている場合は、それを安全として報告する必要があります。これらの急増を安全として手動で報告することは、ARPの脅威評価の精度を向上させるのに役立ちます。

1回限りの急増を報告する

1. 既知の状況で1回限りのサージが発生していて、ARPで将来の状況でも同様のサージを報告する場合は、ワークロードの動作からサージをクリアします。

   ```
   security anti-ransomware volume workload-behavior clear-surge -vserver
   svm_name -volume volume_name
   ```

ベースラインサージの修正

1. 報告されたサージを通常のアプリケーション動作と見なす必要がある場合は、サージを報告してベースラインサージ値を変更します。

   ```
   security anti-ransomware volume workload-behavior update-baseline-from-surge
   -vserver svm_name -volume volume_name
   ```

ARPアラートの設定

ONTAP 9.14.1以降では、ARPで2つのARPイベントのアラートを指定できます。

- ボリューム上の新しいファイル拡張子の観察
- ARPスナップショットの作成

これら2つのイベントのアラートは、個 々 のボリュームまたはSVM全体に対して設定できます。SVMでアラートを有効にした場合、アラートの設定は有効にしたあとに作成されたボリュームにのみ継承されます。デフォルトでは、アラートはどのボリュームでも有効になっていません。

イベントアラートは、マルチ管理者検証で制御できます。詳細については、を参照してください ARPで保護されたボリュームを使用したマルチ管理者検証。

System Manager の略

ボリュームのアラートの設定

1. ボリュームに移動します。設定を変更するボリュームを個別に選択します。
2. セキュリティタブを選択し、イベントセキュリティ設定を選択します。
3. 新しいファイル拡張子が検出されましたおよびランサムウェアスナップショットが作成されましたのアラートを受信するには、**Severity**見出しの下のドロップダウンメニューを選択します。イベントを生成しないから通知に設定を変更します。
4. 保存を選択します。

SVMのアラートを設定する

1. [Storage VM]**に移動し、設定を有効にするSVMを選択します。
2. [**Security*]**見出しの下で、**[** Anti-ransomware*]カードを探します。[Edit Ransomware Event Severity]を選択します ⋮ 。
3. 新しいファイル拡張子が検出されましたおよびランサムウェアスナップショットが作成されましたのアラートを受信するには、**Severity**見出しの下のドロップダウンメニューを選択します。イベントを生成しないから通知に設定を変更します。
4. 保存を選択します。

CLI の使用

ボリュームのアラートの設定

- 新しいファイル拡張子にアラートを設定するには、次の手順を実行します。

  ```
  security anti-ransomware volume event-log modify -vserver svm_name -is
  -enabled-on-new-file-extension-seen true
  ```

- ARPスナップショットの作成に関するアラートを設定するには、次の手順を実行します。

  ```
  security anti-ransomware volume event-log modify -vserver svm_name -is
  -enabled-on-snapshot-copy-creation true
  ```

- を使用して設定を確認します。 `anti-ransomware volume event-log show` コマンドを実行します

SVMのアラートを設定する

- 新しいファイル拡張子にアラートを設定するには、次の手順を実行します。

  ```
  security anti-ransomware vserver event-log modify -vserver svm_name -is
  -enabled-on-new-file-extension-seen true
  ```

- ARPスナップショットの作成に関するアラートを設定するには、次の手順を実行します。

  ```
  security anti-ransomware vserver event-log modify -vserver svm_name -is
  -enabled-on-snapshot-copy-creation true
  ```

- を使用して設定を確認します。 `security anti-ransomware vserver event-log show` コマンドを実行します

詳細情報

- "Autonomous Ransomware Protection AttacksとAutonomous Ransomware Protectionのスナップショットについて理解する"

異常な活動に対応する。

Autonomous Ransomware Protection（ARP）は、保護されたボリュームで異常なアクティビティを検出すると、警告を発行します。通知を評価して、アクティビティが許容可能か（false positive）、または攻撃が悪意のあるものと思われるかどうかを判断する必要があります。

このタスクについて

ARPは、高データエントロピー、データ暗号化による異常なボリュームアクティビティ、および異常なファイル拡張子の組み合わせを検出すると、疑わしいファイルのリストを表示します。

警告が表示されたら、次の2つの方法のいずれかでファイルアクティビティを指定して応答します。

- 偽陽性

  特定されたファイルタイプはワークロードに想定されているため、無視してかまいません。

- ランサムウェア攻撃の可能性

  特定されたファイルタイプは、ワークロード内で予期せぬものであり、攻撃の可能性として扱う必要があります。

どちらの場合も、通知を更新してクリアすると、通常のモニタリングが再開されます。ARPは、選択したファイルアクティビティを使用して、脅威評価プロファイルに評価を記録します。

攻撃の疑いがある場合は、通知をクリアする前に、攻撃であるかどうかを確認し、攻撃である場合はそれに対応し、保護されたデータを復元する必要があります。 "ランサムウェア攻撃から回復する方法の詳細をご覧ください"。

ボリューム全体をリストアする場合、クリアする通知はありません。

作業を開始する前に

ARPはアクティブモードで実行されている必要があります。

手順

異常なタスクには、System ManagerまたはONTAP CLIを使用して対応できます。

System Manager の略

1. 「異常なアクティビティ」の通知を受け取ったら、リンクをクリックします。または、**[ボリューム]*** 概要の[セキュリティ]*タブに移動します。

   警告は*メニューの[概要]*ペインに表示されます。

2. 「 Detected Abnormal volume activity （異常ボリュームアクティビティの検出）」というメッセージが表示されたら、疑わしいファイルを確認します。

   タブで、[疑わしいファイルの種類の表示]*を選択します。

3. [疑わしいファイルの種類 *] ダイアログボックスで、各ファイルの種類を調べて、「 False Positive 」または「 Potential Ransomware Attack 」としてマークします。

選択した値	対処方法
誤検出	[Update]*および[Clear Suspect File Types]*を選択して、決定を記録し、通常のARPモニタリングを再開します。 ONTAP 9.13.1以降では、MAVを使用してARP設定を保護している場合、clear-suspect操作によって、1人以上の追加管理者の承認を得るように求められます。 "すべての管理者から承認を受ける必要があります" MAV承認グループに関連付けられているか、操作が失敗します。
潜在的なランサムウェア攻撃	攻撃に対応し、保護されたデータを復元します。次に、* Update および Clear Suspect File Types *を選択して、決定を記録し、通常のARPモニタリングを再開します。 ボリューム全体をリストアした場合、クリアされる疑わしいファイルタイプは存在しません。

CLI の使用

1. ランサムウェア攻撃の疑いがある場合は、攻撃の時間と重大度を確認します。

   ```
   security anti-ransomware volume show -vserver svm_name -volume vol_name
   ```

   出力例：

   ```
   Vserver Name: vs0
   Volume Name: vol1
   State: enabled
   Attack Probability: moderate
   Attack Timeline: 9/14/2021 01:03:23
   Number of Attacks: 1
   ```

   EMS メッセージを確認することもできます。

   ```
   event log show -message-name callhome.arw.activity.seen
   ```

2. 攻撃レポートを生成し、出力先をメモします。

   ```
   security anti-ransomware volume attack generate-report -volume vol_name
   -dest-path file_location/
   ```

   出力例：

   ```
   Report "report_file_vs0_vol1_14-09-2021_01-21-08" available at path
   "vs0:vol1/"
   ```

3. 管理クライアントシステムのレポートを表示します。例：

   ```
   [root@rhel8 mnt]# cat report_file_vs0_vol1_14-09-2021_01-21-08

   19  "9/14/2021 01:03:23"   test_dir_1/test_file_1.jpg.lckd
   20  "9/14/2021 01:03:46"   test_dir_2/test_file_2.jpg.lckd
   21  "9/14/2021 01:03:46"   test_dir_3/test_file_3.png.lckd`
   ```

4. ファイル拡張子の評価に基づいて、次のいずれかの操作を実行します。

   - 誤検出

     次のコマンドを入力して決定を記録し、許可された拡張子のリストに新しい拡張子を追加して、通常のランサムウェア対策の監視を再開します。
     `anti-ransomware volume attack clear-suspect -vserver svm_name -volume vol_name [extension identifiers] -false-positive true`

     拡張機能を識別するには、次のいずれかのパラメータを使用します。
     `[-seq-no integer]` 疑わしいリスト内のファイルのシーケンス番号。
     `[-extension text, … ]` ファイル拡張子
     `[-start-time date_time -end-time date_time]` 消去されるファイル範囲の開始時刻と終了時刻。形式は「MM/DD/YYYY HH:MM:SS」です。

   - ランサムウェア攻撃の可能性

     攻撃に応答し "ARPによって作成されたバックアップスナップショットからデータをリカバリします"。データがリカバリされたら、次のコマンドを入力して決定事項を記録し、通常のARPモニタリングを再開します。

     ```
     anti-ransomware volume attack clear-suspect -vserver svm_name -volume
     vol_name [extension identifiers] -false-positive false
     ```

     拡張機能を識別するには、次のいずれかのパラメータを使用します。
     `[-seq-no integer]` 疑わしいリスト内のファイルのシーケンス番号
     `[-extension text, … ]` ファイル拡張子
     `[-start-time date_time -end-time date_time]` 消去されるファイル範囲の開始時刻と終了時刻。形式は「MM/DD/YYYY HH:MM:SS」です。

ボリューム全体をリストアした場合、クリアされる疑わしいファイルタイプは存在しません。ARPによって作成されたバックアップスナップショットが削除され、攻撃レポートがクリアされます。

5. MAVと予想されるを使用している場合 `clear-suspect` 操作には追加の承認が必要です。各MAVグループ承認者は次のことを行う必要があります。

   a. 要求を表示します。

      ```
      security multi-admin-verify request show
      ```

   b. 通常のランサムウェア対策監視の再開要求を承認します。

      ```
      security multi-admin-verify request approve -index[number returned from show request]
      ```

   最後のグループ承認者に対する応答は、ボリュームが変更され、誤検出が記録されたことを示します。

6. MAVを使用していて、MAVグループ承認者である場合は、疑わしいリクエストを却下することもできます。

   ```
   security multi-admin-verify request veto -index[number returned from show request]
   ```

詳細情報

- "KB：自律型ランサムウェア対策攻撃と自律型ランサムウェア対策スナップショットについて"。

ランサムウェア攻撃のあとにデータをリストア

Autonomous Ransomware Protection（ARP；自律型ランサムウェア対策）で、`Anti_ransomware_backup` ランサムウェアの潜在的な脅威を検出した場合。これらのARP Snapshotコピーまたはボリュームの別のSnapshotコピーのいずれかを使用して、データをリストアできます。

このタスクについて

ボリュームに SnapMirror 関係が設定されている場合は、 Snapshot コピーからリストアしたあと、すぐにボリュームのすべてのミラーコピーを手動でレプリケートします。レプリケートしないと、ミラーコピーを使用できなくなり、削除および再作成が必要になることがあります。

以外のSnapshotからリストアするには `Anti_ransomware_backup` スナップショットシステム攻撃が特定された後、最初にARPスナップショットを解放する必要があります。

システム攻撃が報告されていない場合は、最初に `Anti_ransomware_backup` その後、Snapshotコピーを使用して、選択したSnapshotコピーからボリュームをリストアします。

手順

データは、System ManagerまたはONTAP CLIを使用してリストアできます。

System Manager の略

システム攻撃後の復元

1. ARPスナップショットから復元するには、手順2に進みます。以前のSnapshotコピーからリストアするには、まずARP Snapshotのロックを解除する必要があります。
   a. Storage > Volumes （ストレージ）を選択します。
   b. を選択し、[疑わしいファイルタイプの表示]*を選択します。
   c. ファイルを「False Positive」としてマークします。
   d. [更新]*および[疑わしいファイルの種類をクリア]*を選択します。
2. ボリューム内のSnapshotコピーを表示します。

   [ストレージ]>[ボリューム]を選択し、ボリュームと Snapshotコピー*を選択します。
3. リストアするSnapshotコピーの横にあるを選択し、*[リストア]*を選択します ⋮ 。

システム攻撃が特定されなかった場合のリストア

1. ボリューム内のSnapshotコピーを表示します。

   [ストレージ]>[ボリューム]を選択し、ボリュームと Snapshotコピー*を選択します。
2. それらを選択します ⋮ スナップショットを選択します `Anti_ransomware_backup` 。
3. [* Restore] を選択します。
4. メニューに戻り、使用する**Snapshot**コピーを選択します。**[** Restore] を選択します。

CLI の使用

システム攻撃後の復元

1. ARP Snapshotコピーからリストアするには、手順2に進みます。以前のSnapshotコピーからデータをリストアするには、ARP Snapshotのロックを解除する必要があります。

   を使用している場合にのみ、以前のSnapshotコピーからリストアする前にAnti-Ransomware SnapLockを解放する必要があります `volume snap restore` 以下のコマンドを実行します。 FlexClone、Single File Snap Restore、またはその他の方法を使用してデータをリストアする場合は、この作業は必要ありません。

   攻撃を「誤検知」および「疑いのないもの」としてマークします。
   `anti-ransomware volume attack clear-suspect -vserver` *`svm_name`* `-volume` *`vol_name`* `[`*`extension identifiers`*`] -false-positive true`
   拡張機能を識別するには、次のいずれかのパラメータを使用します。
   `[-seq-no` *`integer`*`]` 疑わしいリスト内のファイルのシーケンス番号。
   `[-extension` *`text`*`, … ]` ファイル拡張子
   `[-start-time` *`date_time`* `-end-time` *`date_time`*`]` 消去されるファイル範囲の開始時刻と終了時刻。形式は「MM/DD/YYYY HH:MM:SS」です。
2. ボリューム内の Snapshot コピーの一覧を表示します。

```
volume snapshot show -vserver <SVM> -volume <volume>
```

次の例は、のSnapshotコピーを示しています `vol1`：

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

3. Snapshot コピーからボリュームの内容をリストアします。

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot
<snapshot>
```

次の例は、の内容をリストアします `vol1`：

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

システム攻撃が特定されなかった場合のリストア

1. ボリューム内の Snapshot コピーの一覧を表示します。

```
volume snapshot show -vserver <SVM> -volume <volume>
```

次の例は、のSnapshotコピーを示しています `vol1`：

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                  State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Snapshot コピーからボリュームの内容をリストアします。

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot
<snapshot>
```

次の例は、の内容をリストアします `vol1`：

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

3. 必要なSnapshotコピーを使用してボリュームをリストアする場合は、手順1と2を繰り返します。

詳細情報

- "KB：ONTAPでのランサムウェア対策とリカバリ"

自動Snapshotコピーのオプションを変更します

ONTAP 9.11.1以降では、ランサムウェア攻撃の疑いがある場合に自動的に生成されるAutonomous Ransomware Protection（ARP）Snapshotコピーの保持設定をCLIで制御できます。

作業を開始する前に

変更できるのはノードSVM上のARP Snapshotオプションだけです。

手順

1. 現在のARP Snapshotコピー設定をすべて表示するには、次のように入力します。
   `vserver options -vserver` *`svm_name`* `arw*`

。 `vserver options` コマンドは非表示のコマンドです。マニュアルページを表示するには、と入力します `man vserver options` ONTAP CLIで実行します。

2. 選択した現在のARP Snapshotコピー設定を表示するには、次のように入力します。
`vserver options -vserver svm_name -option-name arw_setting_name`
3. ARP Snapshotコピーの設定を変更するには、次のように入力します。
`vserver options -vserver svm_name -option-name arw_setting_name -option-value arw_setting_value`

次の設定を変更できます。

ARW設定	説明
`arw.snap.max.count`	指定した時間に1つのボリューム内に存在可能なARP Snapshotコピーの最大数を指定します。古いコピーは、ARP Snapshotコピーの総数がこの指定した制限内に収まるように削除されます。 。 `-option-value` パラメータには、3～8の整数を指定できます。デフォルト値は6です。
`arw.snap.create.interval.hours`	ARP Snapshotコピーの間隔（hours_between）を指定します。データエントロピーベースの攻撃が疑われ、最後に作成されたARP Snapshotコピーが指定した間隔よりも古い場合、新しいARP Snapshotコピーが作成されます。 。 `-option-value` パラメータには、1～48の整数を指定できます。デフォルト値は4です。
`arw.snap.normal.retain.interval.hours`	ARP Snapshotコピーを保持する期間（時間）を指定します。ARP Snapshotコピーが保持しきい値に達すると、他のARP Snapshotコピーが削除される前に作成されます。保持しきい値よりも古いARP Snapshotコピーは1つしか存在できません。 。 `-option-value` パラメータには、4~96の整数を指定できます。デフォルト値は48です。
`arw.snap.max.retain.interval.days`	ARP Snapshotコピーを保持できる最大期間（日数）を指定します。ボリュームで攻撃が報告されていない場合、指定した期間よりも古いARP Snapshotコピーは削除されます。 中程度の脅威が検出された場合、ARP Snapshotコピーの最大保持間隔は無視されます。脅威に対応して作成されたARP Snapshotコピーは、脅威に対応するまで保持されます。脅威を誤検出としてマークすると、ボリューム上のARP Snapshotコピーが削除されます。 。 `-option-value` パラメータには、1～365の整数を指定できます。デフォルト値は5です。

ARW設定	説明
arw.snap.create.interval.hours.post.max.count	ボリュームにすでに最大数のARP Snapshotコピーが含まれている場合の、ARP Snapshotコピーの間隔（interval_in hours_between）を指定します。最大数に達すると、ARP Snapshotコピーが削除されて、新しいコピー用のスペースが確保されます。このオプションを使用すると、新しいARP Snapshotコピーの作成速度を下げて、古いコピーを保持することができます。ボリュームにすでに最大数のARP Snapshotコピーが含まれている場合は、次のARP Snapshotコピー作成ではなく、このオプションで指定した間隔が使用されます。 arw.snap.create.interval.hours。 。 -option-value パラメータには、4~48の整数を指定できます。デフォルト値は8です。
arw.surge.snap.interval.days	IOサージに応答して作成されるARP Snapshotコピーの間隔（日数）を指定します。ONTAPは、IOトラフィックが急増し、最後に作成されたARP Snapshotコピーがこの指定された間隔よりも古い場合に、ARP Snapshotサージコピーを作成します。このオプションは、ARPサージSnapshotコピーの保持期間（日数_）も指定します。 。 -option-value パラメータには、1～365の整数を指定できます。デフォルト値は5です。
arw.snap.new.extns.interval.hours	このオプションは、新しいファイル拡張子が検出されたときに作成されるARP Snapshotコピーの間隔（interval_in hours_between）を指定します。次の場合に新しいARP Snapshotコピーが作成されます。 新しいファイル拡張子が監視されます。新しいファイル拡張子を監視したときに作成された以前のSnapshotは、この指定された間隔よりも古いものです。新しいファイル拡張子を頻繁に作成するワークロードでは、この間隔を使用してARP Snapshotコピーの頻度を制御できます。このオプションは、arw.snap.create.interval.hours`では、データエントロピーベースのARP Snapshotコピーの間隔を指定します。 。 `-option-value パラメータには、24～8760の整数を指定できます。デフォルト値は48です。

著作権に関する情報

商標に関する情報