自律型ランサムウェア対策
ONTAP 9

NetApp
December 20, 2024

目次

自律型ランサムウェア対策

ONTAPの自律型ランサムウェア対策

ONTAP 9 .10.1以降では、自律型ランサムウェア対策（ARP）機能で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可能性がある異常なアクティビティをプロアクティブに検出し、警告します。攻撃が疑われると、ARP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、新しいスナップショットも作成します。

人工知能（ARP / AI）による自律型ランサムウェア対策

ARPは、ONTAP 9絶えず進化するランサムウェアの形態を99%の精度で検出するランサムウェア対策分析に機械学習モデルを採用することで、サイバーレジリエンスを向上させました。ARPの機械学習モデルは、シミュレーションされたランサムウェア攻撃の前後に、大規模なファイルデータセットで事前にトレーニングされています。このリソースを大量に消費するトレーニングはONTAPの外部で行われますが、このトレーニングからの学習はONTAP内部のモデルに使用されます。

FlexVolボリュームを備えたARP / AIのアクティブモードへの即時移行

ARP / AIとFlexVolボリュームには何もありません学習期間。ARP/AIは、インストールまたは9.16へのアップグレードの直後にアクティブモードで開始されます。クラスタをONTAP 9 .16.1にアップグレードすると、既存および新規のFlexVolボリュームでARP / AIがすでに有効になっている場合、それらのボリュームでARP / AIが自動的に有効になります。

"ARP/AIの有効化の詳細"

ARP/AIノシトウコウシン

最新のランサムウェアの脅威に対する最新の保護を維持するために、ARP / AIは、ONTAPの定期的なアップグレードおよびリリースサイクルの外で頻繁に自動更新を提供しています。あなたが持っているならば、"自動更新を有効にした"あなたはまた、セキュリティファイルの自動更新を選択した後、ARP/AIへの自動セキュリティ更新の受信を開始することができます。また、これらの更新を手動で行い、更新がいつ行われるかを制御することもできます。

System.16.1以降では、システムおよびファームウェアの更新に加えて、ONTAP 9 Managerを使用してARP/AIのセキュリティ更新を利用できます。

> 現在、ARP/AI機能はNASのみをサポートしています。自動更新機能では、System Managerへの導入に使用できる新しいセキュリティファイルが表示されますが、これらの更新プログラムはNASワークロードの保護にのみ適用されます。

"ARP / AIの更新に関する詳細はこちら"

ライセンスとイネーブルメント

ARPサポートはに含まれてい"ONTAP 1ライセンス"ます。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	ライセンス
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 .10.1からONTAP 9 .11.1以降にアップグレードする際に、システムでARPがすでに設定されている場合は、新しいAnti-ransomwareライセンスをインストールする必要はありません。新しいARP設定の場合は、新しいライセンスが必要です。
- ONTAP 9 ONTAP 9をAnti-ransomwareライセンスで有効にしていて、ARP.11.1以降からARP.10.1にリバートする場合は、警告メッセージが表示されるため、ARPの再設定が必要になることがあります。

"ARPのリバートについて説明します"です。

ONTAPランサムウェア対策戦略

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。

例えとして、車両の安全機能が挙げられます。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、前方衝突警告はすべて、より良い結果につながる追加の安全機能です。ランサムウェアからの保護についても同様の見方を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、SnapLock、Active IQデジタルアドバイザ（別名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が検出する内容

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（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。

ランサムウェアの検出や防御のシステムは、ランサムウェア攻撃からの安全性を完全に保証できません。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。

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

ラーニングモード

ARP.10.1~9.15.1で実行されているすべてのARP ONTAP 9と、ARP.16.1 ONTAP 9でFlexGroupボリュームに使用されているARP.16.1を有効にすると、ARP_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。ワークロード特性を評価するのに十分な時間を学習モードでARPを実行した後、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間隔が自動的に決定され、スイッチが自動化されます。これは30日前に発生する可能性があります。

コマンドは `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を表示します。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示される場合は、ONTAPが他のメトリックを収集しているため、このデータをアクティブモードに移行する際のベースとして使用しないでください。

アクティブモード

ONTAP 9 .10.1～9.15.1で実行されているARPの場合、最適な学習間隔が完了すると、ARPは_ACTIVE MODE_に切り替わります。ONTAP 9 .16.1以降のARP/AIでは、FlexVolボリュームでARPを使用する場合の学習期間はありません。FlexVolボリュームのARP / AIは、インストールまたは9.16.1へのアップグレード後すぐにアクティブモードで開始されます。FlexGroupボリュームでONTAP 9 .16.1とARPを使用している場合は、アクティブモードに移行する前に学習期間が必要です。

ARPがアクティブモードに切り替わると、ONTAPはARPスナップショットを作成して、脅威が検出された場合にデータを保護します。

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。

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。。

脅威評価とARPスナップショット

アクティブ モードのARPでは、学習した分析結果と測定された受信データの対比に基づいて、脅威の可能性が評価されます。ARPによって検出された脅威には、深刻度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検出された場合など）。このレベルの検出は、ARP/AIを搭載していないONTAP 9 .16.1より前のバージョンでのみ使用できます。
- **Moderate**: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、ファイル数は変更可能です。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、ボリュームのスナップショット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スナップショットの名前の先頭にを付けて、 `Anti-ransomware-backup`簡単に識別できるようにします（例：） `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では、低い脅威に関するアラートは送信されませんが、ONTAP 9 14.1以降では送信できま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 異常な活動への対応。

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

個 々 のARPスナップショットは2日間保持されます。複数のARPスナップショットがある場合、それらはデフォルトで5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 スナップショットのオプションを変更します。。

ランサムウェア攻撃後にONTAPでデータをリカバリする方法

攻撃が疑われると、その時点のボリュームSnapshotが作成され、そのコピーがロックされます。あとで攻撃が確認された場合は、ARPスナップショット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は、通常の方法では削除できません。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。

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からのリカバリ（System Manager）"
- "スナップショット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"

ARPのマルチ管理検証保護

ONTAP 9 13.1以降では、Autonomous Ransomware Protection（ARP;自律ランサムウェア対策）の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）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"。

自律型ランサムウェア対策のユースケースと考慮事項

ONTAP 9 10.1以降では、NASワークロードでAutonomous Ransomware Protection（ARP；自律型ランサムウェア対策）を使用できます。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EDA（Electronic Design Automation）データなどです。

適していないワークロード：

ARPは、次のワークロードには適していません。

- ファイルが頻繁に作成または削除されるワークロード（数秒間に数十万のファイルを削除するテスト / 開発ワークロードなど）
- 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。
- アプリケーションやホストがデータを暗号化するワークロードARPでは、受信データが暗号化されているかどうかを区別する機能を使用します。アプリケーション自体がデータを暗号化している場合、機能の有効性が低下します。ただしその場合も、ARP自体は、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や名前変更）とファイル タイプに基づいて引き続き機能します。

サポートされている構成

オンプレミスのONTAPシステムでは、ONTAP 9 10.1以降のNFSボリュームとSMB FlexVolボリュームでARPを使用できます。

その他の構成とボリューム タイプのサポート状況は、ONTAPのバージョン別に次の表に示します。

	ONTAP 9 .16.1	ONTAP 9 .15.1	ONTAP 9 .14.1	ONTAP 9 .13.1	ONTAP 9 12.1	ONTAP 9 .11.1	ONTAP 9 10.1
SnapMirror非同期で保護されているボリューム	✓	✓	✓	✓	✓		
SnapMirror非同期（SVMディザスタリカバリ）で保護されるSVM	✓	✓	✓	✓	✓		
SVMデータ移動（`vserver migrate`）	✓	✓	✓	✓	✓		
FlexGroupボリューム*	✓	✓	✓	✓			
マルチ管理者認証	✓	✓	✓	✓			
自動更新機能を備えたARP / AI	✓						

- ARP / AIはFlexGroupボリュームをサポートしていません。ARPが有効になっているFlexGroupボリュームは、ARP/AIの前に使用されていたのと同じARPモデルで動作し続けますONTAP 9。

SnapMirrorと**ARP**の相互運用性

ONTAP 9 .12.1以降では、SnapMirror非同期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同期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では、ARPの設定状態（ラーニング、有効など）、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、RWで変換されたデスティネーションボリュームでARPが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以外に、追加の学習手順は必要ありません。

ONTAP 9 .10.1および9.11.1ではSnapMirror、ARPの設定状態、トレーニングデータ、およびSnapshot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をRWに変換する場合、変換後にデスティネーションボリュームのARPをラーニングモードで明示的に有効にする必要があります。

ARPと仮想マシン

ARPは仮想マシン（VM）でサポートされています。ARPの検出動作は、VMの内部と外部の変更で異なります。ARPは、VM内でエントロピーの高いファイルが存在するワークロードには推奨されません。

VMの外部での変更

ARPでは、暗号化されたボリュームに新しい拡張子のファイルが格納された場合や、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。変更を検出可能なファイル拡張子は、次のとおりです。

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

VMの内部での変更

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。ARPはこのシナリオで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。ARPはこの場合でもプロアクティブなスナップショットを作成できますが、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

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ボリュームもサポートされますが、ARP / AIより前に使用されていたARPモデルに限定されます）
- FlexCacheボリューム（元のFlexVol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）

- オフライン ボリューム
- SANのみのボリューム
- SnapLockボリューム
- SnapMirror同期
- SnapMirror非同期（ONTAP 9 .10.1および9.11.1でのみサポートされません。SnapMirror非同期は、ONTAP 9 12.1以降でサポートされています。詳細については、を参照して[snapmirror]ください）。
- 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	ノードあたりの最大ボリューム数（推奨値）	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：**[*]**
読み取り処理が多い場合や、データを圧縮できる場合があります。	150	最大IOPSの4%
書き込み中心でデータを圧縮できない	60	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、保護する、、 `security anti-ransomware volume pause`および `security anti-ransomware volume attack clear-suspect`ARPコマンドのMAVルールを作成する必要があり `security anti-ransomware volume disable`ます。MAVグループの各管理者は、MAV設定内の新しいルール要求を承認する必要があります"MAVルールを再度追加します"。

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、またはを使用してSVMレベルで `security anti-ransomware volume event-log modify`作成できます `security anti-ransomware vserver event-log modify`。

次のステップ

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

自律型ランサムウェア対策を有効にする

ONTAP 9 .10.1以降では、既存のボリュームで自律型ランサムウェア対策（ARP）を有効にするか、新しいボリュームを作成してARPを最初から有効にすることができます。

すべての新しいボリュームがAutonomous Ransomware Protection（ARP）でデフォルトで有効になるようにONTAPクラスタを設定する場合は、こちらを参照してください"関連するARP手順"。

タスクの内容

- * ONTAP 9 .10.1～9.15.1およびFlexGroupボリュームを使用するARP *これらのバージョンのONTAPでは、最初からARPを有効にする必要があります"ラーニングモード"（または「ドライラン」モード）。ラーニングモードで最初にARPをイネーブルにすると、システムはワークロードを分析して通常の動作を特定します。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。

- * FlexVolボリュームを使用しているONTAP 9 .16.1以降の場合* ARPを有効にすると、ARP/AI保護はすぐにアクティブモードで開始されます。学習期間は必要ありません。

> ⓘ 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。ARPを有効にしたボリュームでは、以前の通常のデータトラフィックの特性が新しいデータに基づいて想定されるため、既存のデータはスキャンおよび分析されません。

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。
- ONTAPのバージョンに対応したが正しいライセンス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が保護され、アクティブになっている必要があります"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 "EMSイベントを設定してEメール通知を送信する"。
- ONTAP 9 13.1以降では、Autonomous Ransomware Protection（ARP;自律ランサムウェア対策）の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）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"。

新規または既存のボリュームで**ARP**を有効にする

System ManagerまたはONTAP CLIを使用してARPを有効化できます。

System Manager

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. [ボリューム]概要の*タブで[ステータス]*を選択し、[無効]から[有効]に切り替えます。
   - ARPをONTAP 9 .15.1以前で使用している場合、またはFlexGroupボリュームでONTAP 9 .16.1を使用している場合は、* Anti-ransomware ボックスで Enabled in learning-mode *を選択します。

     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、スイッチが自動化されます。ラーニングモードからアクティブモードへの移行を手動で制御することができます"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"。

   - ONTAP 9 .16.1以降が搭載されたFlexVolボリュームでARPを使用している場合、ARP / AI機能はラーニング期間を必要とせず、デフォルトでアクティブモードが選択されます。
3. 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

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**を有効にする

1. 既存のボリュームを変更してランサムウェアからの保護を有効にします。
   - ONTAP 9 .15.1以前およびFlexGroupボリュームを使用するARPの場合は、ボリュームの状態を（ラーニングモード）に設定し `dry-run`ます。

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

   - ARP / AIボリュームとFlexVolボリュームがあるONTAP 9 .16.1以降の場合は、ボリュームの状態を（アクティブモード）に設定し `active`ます。

     ```
     security anti-ransomware volume active -volume <vol_name> -vserver
     <svm_name>
     ```

2. ONTAP 9 .13.1以降にアップグレードした場合、ARPのデフォルトステートがであると、 `dry-run`アクティブステート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
   ```

3. ボリュームのARPの状態を確認します。

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

新しいボリュームで**ARP**を有効にする

1. データをプロビジョニングする前に、ARPを有効にして新しいボリュームを作成します。
   - ONTAP 9 .15.1以前およびFlexGroupボリュームを使用するARPの場合は、状態を（ラーニングモード）に設定し `dry-run`ます。

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

   - ARP / AIボリュームとFlexVolボリュームがあるONTAP 9 .16.1以降の場合は、状態を（アクティブモード）に設定し `active`ます。

     ```
     volume create -volume <vol_name> -vserver <svm_name> -aggregate
     <aggr_name> -size <nn> -anti-ransomware-state active -junction-path
     </path_name>
     ```

2. ONTAP 9 .13.1以降にアップグレードした場合、ARPのデフォルトステートがであると、 `dry-run`アクティブステート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
   ```

3. ボリュームのARPの状態を確認します。

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

関連情報

- "学習期間後にアクティブモードに切り替える"

新しいボリュームで**Autonomous Ransomware Protection**をデフォルトで有効にする

ONTAP 9 .10.1以降では、Autonomous Ransomware Protection（ARP；自律型ランサムウェア対策）で新しいボリュームがデフォルトで有効になるようにStorage VM（SVM）を設定できます。この設定は、System ManagerまたはCLIを使用して変更できます。

デフォルトのARPを設定せずに新規または既存のボリュームを個別に設定する場合は、こちらを参照してください"関連するARP手順"。

タスクの内容

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。ARPは、NASボリューム用のARP機能を有効にしたあとにSVMに作成された新しいボリュームでのみデフォルトで有効になります。

既存のボリュームではARPは自動的に有効になりません。この手順で説明する設定の変更は、新しいボリュームにのみ影響します。方法をご確認ください"既存のボリュームのARPを有効にする"。

- * ONTAP 9 .10.1～9.15.1およびFlexGroupボリュームを使用するARP *デフォルトでは、ARPが有効になっている新しいボリュームは（「ドライラン」）モードに設定されてい"ラーニングモード"ます。このモードでは、システムは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。ラーニングモードは、手動（すべてのARPバージョン）または自動（ARP 9.13.1以降）でアクティブモードに移行できます。ARP 9.13.1以降では、ARP分析にアダプティブラーニングが追加され、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るようになりました。
- * FlexVolボリュームを使用しているONTAP 9 .16.1以降の場合* ARPを有効にすると、ARP/AI保護はすぐにアクティブモードで開始されます。学習期間は必要ありません。

開始する前に

- ONTAPのバージョンに対応したが正しいライセンス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、ランサムウェア対策に複数の認証されたユーザー管理者が必要になるように、Multi-Admin Verification（MAV）を有効にすることをお勧めします。"詳細"です。

手順

System ManagerまたはONTAP CLIを使用して、新しいボリュームに対してデフォルトでARPを有効にすることができます。

System Manager

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、を選択します 。
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 .16.1では、新しいFlexVolボリュームに対してアクティブモードが自動的に有効になるため、学習期間は必要ありません。

   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。ARPを有効にしたボリュームでは、以前の通常のデータトラフィックの特性が新しいデータに基づいて想定されるため、既存のデータはスキャンおよび分析されません。

4. ARP 9.13.1以降にアップグレードした場合は、必要に応じて*十分な学習後に自動的に学習からアクティブモードに切り替える*を選択します。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。

CLI

- 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。
  - ONTAP 9 .15.1以前およびFlexGroupボリュームの場合は、デフォルトの状態を（ラーニングモード）に設定し `dry-run`ます。

    ```
    vserver modify -vserver <svm_name> -anti-ransomware-default-volume-state
    dry-run
    ```

  - ARP / AIボリュームとFlexVolボリュームがあるONTAP 9 .16.1以降では、デフォルトの状態を（アクティブモード）に設定し `active`ます。

    ```
    vserver modify -vserver <svm_name> -anti-ransomware-default-volume-state
    active
    ```

- 新しいボリュームに対してデフォルトでARPを有効にして、新しいSVMを作成します。
  - ONTAP 9 .15.1以前およびFlexGroupボリュームの場合は、デフォルトの状態を（ラーニングモード）に設定し `dry-run`ます。

    ```
    vserver create -vserver <svm_name> -anti-ransomware-default-volume-state
    dry-run <other parameters as needed>
    ```

  - ARP / AIボリュームとFlexVolボリュームがあるONTAP 9 .16.1以降では、デフォルトの状態を（アクティブモード）に設定し `active`ます。

    ```
    vserver modify -vserver <svm_name> -anti-ransomware-default-volume-state
    active
    ```

- ONTAP 9 .13.1以降にアップグレードした場合、デフォルトの状態がであると、 `dry-run`アダプティブラーニングがイネーブルになり、アクティブ状態への変更が自動的に行われます。この動作を自動

的に有効にしない場合は、既存のSVMを変更します。

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

関連情報

- "学習期間後にアクティブモードに切り替える"

自動更新でARP / AIを有効にする

ARPは、ONTAP 9 .16.1以降、人工知能（ARP/AI）を使用した自律型ランサムウェア対策を採用し、脅威の検出と対応を強化しています。クラスタをONTAP 9 .16.1にアップグレードすると、FlexVolボリュームでARP / AIがすでに有効になっている場合、それらのボリュームでARP / AIが自動的に有効になります。ARPを有効にしていない場合、またはクラスタの自動更新を有効にしていない場合は、この手順に記載されているいずれかのシナリオに従う必要があります。

ONTAP 9にアップグレードする前に、"既存のARP検出をすべて終了します。"を参照してください。

開始する前に

- ARP / AIを使用するには、FlexVolボリュームが必要です。FlexGroupボリュームがある場合、ARP/AIの前に使用されていたARPモデルは、ONTAP 9にアップグレードしても引き続き動作します。16.1

ONTAP 9 .16.1にアップグレードすると、FlexVolボリュームを含む既存のARPインスタンスに対して、ARPがアクティブモードで自動的に有効になります。ARP / AIは広範な機械学習モデルでトレーニングされるため、学習期間は不要になりました。アップグレード前に完了していないラーニング期間は自動的に終了し、ボリュームはアクティブモードに移行されます。

手順

1. 使用している構成に固有のシナリオに従います。
   - * ONTAP 9を実行している新しいクラスタの場合"ARPの有効化"。16.1 *：。ARPはデフォルトではイネーブルになっていません。ARPを有効にすると、保護対象として選択したボリュームでARP / AI機能がアクティブモードで自動的に有効になります。
   - **ARP**が有効になっている**ONTAP 9 .16.1**に最近アップグレードされた既存のクラスタの場合:アクションは必要ありません。ARP/AIは、保護対象として選択したFlexVolボリュームの新しいARPによる脅威保護方法に自動的になります。
   - **ARP**が有効になっていない**ONTAP 9 .16.1**に最近アップグレードされた既存のクラスタ:"ARPの有効化"ARPをイネーブルにすると、ARP/AIは自動的に新しいARPによる脅威保護方法になります。
2. ARP/AIを有効にしたら、ARP/AI保護アップデートを配信してインストールするかどうかを決定します"自動または手動"。

関連情報

- "ARP / AIの更新"

AI（ARP / AI）で自律型ランサムウェア対策を更新

最新のランサムウェアの脅威に対する保護を最新の状態に保つために、ARP / AIでは、通常のONTAPリリースサイクル外に発生する自動更新を提供しています。

ONTAP 9 .16.1以降では、システムおよびファームウェアの更新に加えて、ARP / AIのセキュリティ更新プログラムもSystem Managerソフトウェアのダウンロードから入手できます。ONTAPクラスタがすでに登録されている場合は"システムとファームウェアの自動更新"、ARP/AIセキュリティ更新プログラムが利用可能になると自動的に通知されます。また、ONTAPがセキュリティ更新プログラムを自動的にインストールするように変更することもできます環境設定の更新。

必要に応じて、ARP / AIを手動で更新するNetAppサポートサイトから更新プログラムをダウンロードし、System Managerを使用してインストールできます。

> ⓘ 現在、ARP/AI機能はNASのみをサポートしています。自動更新機能では、System Managerへの導入に使用できる新しいセキュリティファイルが表示されますが、これらの更新プログラムはNASワークロードの保護にのみ適用されます。

タスクの内容

ONTAP 9 .16.1以降では、System Managerを使用してのみARP/AIを更新できます。

ARP/AIのアップデート設定を選択してください

System Managerでは、セキュリティファイルの自動更新を有効にするページの設定がに設定されます（自動`Show notifications`ファームウェアおよびシステム更新にすでに登録されている場合）。ONTAPで最新のアップデートを自動的に適用する場合は、アップデート設定をに変更できます `Automatically update`。ダークサイトを使用している場合や、更新を手動で実行する場合は、通知を表示するか、セキュリティ更新を自動的に却下するかを選択できます。

開始する前に

自動セキュリティ更新の場合は、を参照してください "AutoSupportとAutoSupport OnDemandを有効にし、転送プロトコルをHTTPSに設定する必要があります。"。

手順

1. System Managerで、*[クラスタ]>[設定]>[ソフトウェアの更新]*をクリックします。
2. [ソフトウェアの更新]*セクションで、を選択します →。
3. [ソフトウェアの更新]ページで、[その他のすべての更新]タブを選択します。
4. [その他のすべての更新]タブを選択し、*[詳細]*をクリックします。
5. [自動更新設定の編集]*を選択します。
6. [自動更新の設定]ページで、*[セキュリティファイル]*を選択します。
7. セキュリティファイル（ARP/AIアップデート）に対して実行するアクションを指定します。

   自動的に更新するか、通知を表示するか、または更新を自動的に却下するかを選択できます。

   > ⓘ セキュリティ更新が自動的に更新されるようにするには、AutoSupportおよびAutoSupport OnDemandを有効にし、転送プロトコルをHTTPSに設定する必要があります。

8. 利用条件に同意し、*[保存]*を選択します。

最新のセキュリティパッケージを使用して**ARP/AI**を手動で更新する

Active IQ Unified Managerに登録しているかどうかに応じて、適切な手順を実行します。

意図しないARPダウングレードを避けるために、現在のバージョンよりも新しいARPアップデートのみをインストールしてください。

デジタルアドバイザ搭載の**ONTAP 9 .16.1**以降

手順

1. System Managerで、*[ダッシュボード]*に移動します。

   クラスタに対して推奨されるセキュリティ更新プログラムがある場合は、* Health *セクションにメッセージが表示されます。

2. アラートメッセージをクリックします。
3. 推奨される更新プログラムのリストのセキュリティ更新プログラムの横にある*[アクション]*を選択します。
4. アップデートをすぐにインストールする場合は*をクリックし、後でインストールする場合は[スケジュール]*をクリックします。

   更新がすでにスケジュールされている場合は、*編集*または*キャンセル*することができます。

ONTAP 9 .16.1以降（デジタルアドバイザなし）

手順

1. に移動"NetAppサポートサイト"してログインします。
2. クラスタのARP / AIの更新に使用するセキュリティパッケージを選択します。
3. ネットワーク上のHTTPサーバまたはFTPサーバ、またはARP / AIを使用してクラスタからアクセスできるローカルフォルダにファイルをコピーします。
4. System Managerで、*[クラスタ]>[設定]>[ソフトウェアの更新]*をクリックします。
5. で、[その他のすべての更新]*タブを選択します。
6. [手動アップデート]ペインで、*[セキュリティファイルの追加]*をクリックし、次のいずれかの環境設定を使用してファイルを追加します。
   - サーバからダウンロード:セキュリティファイルパッケージのURLを入力します。
   - ローカルクライアントからアップロード：ダウンロードしたTGZファイルに移動します。

     ファイル名がで始まり、がファイル拡張子である `.tgz` ことを確認します `ontap_security_file_arpai_`。

7. [追加]*をクリックして更新を適用します。

ARP / AIの更新を確認

却下された、またはインストールに失敗した自動更新の履歴を表示するには、次の手順を実行します。

1. System Managerで、*[クラスタ]>[設定]>[ソフトウェアの更新]*をクリックします。
2. [ソフトウェアの更新]*セクションで、を選択します →。
3. [ソフトウェアの更新]ページで、**[**その他のすべての更新**]***タブを選択し、[詳細]*をクリックします。
4. [すべての自動更新を表示]*を選択します。

関連情報

- "ARP / AIを有効にする"
- "ソフトウェアアップデートのEメール配信登録"

学習期間後にARPアクティブモードに切り替える

Autonomous Ransomware Protection（ARP）9.15.1以前またはARPがFlexGroupボリュームで実行されている場合は、ARP対応ボリュームをラーニングモードからアクティブモードに手動または自動で切り替えます。ARPが推奨される最低30日間のラーニングモードの実行を完了したら、手動でアクティブモードに切り替えることができます。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。

ONTAP 9 .16.1以降が搭載されたFlexVolボリュームでARPを使用している場合、ARP / AI機能はラーニング期間を必要とせず、デフォルトでアクティブモードが選択されます。

> 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。ARPを有効にしたボリュームでは、以前の通常のデータトラフィックの特性が新しいデータに基づいて想定されるため、既存のデータはスキャンおよび分析されません。

学習期間後に手動でアクティブモードに切り替える

FlexGroupボリュームを含むONTAP 9 .10.1~9.15.1およびARPの場合、System ManagerまたはONTAP CLIを使用して、ARPラーニングモードからアクティブモードに手動で移行することができます。

System Manager

手順

1. [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。
2. [Volumes]概要の*タブで、**[Anti-ransomware]**ボックスで[Switch to active mode]*を選択します。
3. ボリュームのARP状態は、* Anti-ransomware *ボックスで確認できます。

CLI

手順

1. 学習期間が終了したら、保護されている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（自動的に切り替えられていない場合）。

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

   modify volume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
   ```

2. ボリュームのARPの状態を確認します。

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

学習モードからアクティブモードへの自動切り替え

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。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"。

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

異常なワークロードイベントが発生する可能性がある場合は、Autonomous Ransomware Protection（ARP）分析をいつでも一時的に中断して再開できます。

ONTAP 9 .13.1以降では、複数の認証済みユーザ管理者がARPを一時停止するように、Multi-admin Verification（MAV;マルチ管理者検証）をイネーブルにできます。

"MAVの詳細については、こちらをご覧ください"です。

タスクの内容

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、以前のログについてはバックグラウンドで分析処理が続行されます。

> 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、学習したワークロードの動作に関する既存の情報がすべて失われます。これには、学習期間の再起動が必要になります。

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

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

1. ボリュームで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、次のコマンドを使用し `resume`ます。

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

3. ONTAP 9設定を保護するためにMAV（ARP .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、操作が失敗します。

   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. 要求を承認します。

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

      最後のグループの承認者には、ボリュームが変更され、ARPが一時停止状態になった旨の応答が返されます。

      MAVを使用していて、MAVグループの承認者である場合、一時停止処理の要求を却下できます。

   ```
   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、Autonomous Ransomware Protectionが有効になっている特定の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が検出する内容。

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。

> 誤検出アラートの数を減らすには、**[ストレージ]>[ボリューム]>[セキュリティ]>[ワークロード特性の設定]***に移動し、[新しいファイルタイプの監視]*を無効にします。この設定は、ONTAP 9ではデフォルトで無効になっています。14.1 P7、9.15.1 P1、および9.16.1 RC以降では無効になっています。

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、攻撃検出パラメータを変更して、特定のワークロードに適したパラメータにすることができます。

攻撃検出パラメータの変更

ARPが有効になっているボリュームで想定される動作に応じて、攻撃検出パラメータの変更が必要になることがあります。

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. 表示されているすべてのフィールドは、ブール値か整数値で変更できます。フィールドを変更するには、コマンドを使用し `security anti-ransomware volume attack-detection-parameters modify`ます。

   この手順で説明されているコマンドの詳細については、を"ONTAPコマンド リファレンス"参照してください。

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。ボリュームアクティビティのサージ（1回限りのサージ、またはニューノーマルの特徴であるサージ）を知っている場合は、それらを安全であると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測
- 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、個々のボリュームか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、アラートを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

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

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
```

- コマンドを使用して設定を確認し `anti-ransomware volume event-log show`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
```

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

関連情報

- "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"です。

異常な活動への対応

Autonomous Ransomware Protection（ARP）は、保護されたボリューム内の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。

タスクの内容

ARPは、高いデータエントロピー、データ暗号化を伴う異常なボリュームアクティビティ、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

  指定されたファイルタイプはワークロードで想定されているものであり、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で想定されていないため、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"です。

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。

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

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てください。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」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. [Suspected File Types]ダイアログボックスで、各ファイルタイプを確認し、「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。
ランサムウェア攻撃の可能性	攻撃に対応し、保護されたデータをリストアします。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、疑わしいファイルタイプをクリアする必要はありません。

CLI

1. ランサムウェア攻撃の疑いがあるという通知を受け取ったら、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で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。

   - False positive

     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`

     次のいずれかのパラメータを使用して、拡張子を識別します。疑わしいリスト内のファイルのシーケンス番号
     `[-extension text, … ]`。
     `[-seq-no integer]`クリアするファイル範囲のファイル拡張子の
     `[-start-time date_time -end-time date_time]`開始時間と終了時間。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
     ```

     次のいずれかのパラメータを使用して、拡張子を識別します。
     `[-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]`消去するファイルの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、疑わしいファイルタイプをクリアする必要はありません。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を使用していて、想定される操作に追加の承認が必要な場合 `clear-suspect`、各MAVグループ承認者は次の作業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"です。

ランサムウェア攻撃後にデータをリストア

Autonomous Ransomware Protection（ARP）は、ランサムウェアの潜在的な脅威を検出したときにという名前のSnapshotを作成します `Anti_ransomware_backup`。これらのARPスナップショットまたはボリュームの別のスナップショットのいずれかを使用してデータをリストアできます。

タスクの内容

ボリュームにSnapMirror関係がある場合は、Snapshot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。ミラーコピーを使用しないと、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可能性があります。

システム攻撃が特定された後、スナップショット以外のスナップショットからリストアするには `Anti_ransomware_backup`、まず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Snapshotからリストアしてから、選択したSnapshotからボリュームを以降にリストアする必要があります `Anti_ransomware_backup`。

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

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。以前のスナップショットから復元するには、まずARPスナップショット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、[疑わしいファイルの種類を表示]*を選択します。
   c. ファイルを「ランサムウェア攻撃の可能性」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**を選択します。**[** Restore] を選択します。

CLI

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。以前のスナップショットからデータを復元するには、ARPスナップショットのロックを解除する必要があります。

   以下のようにコマンドを使用している場合にのみ、以前のスナップショットから復元する前にAnti-Ransomware SnapLockを解放する必要があり `volume snap restore`ます。FlexClone、単一ファイルSnapRestore、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。

   攻撃をランサムウェア攻撃の可能性としてマークし(`-false-positive false`、疑いのあるファイルをクリアし(`clear-suspect`ます):
   `anti-ransomware volume attack clear-suspect -vserver *svm_name* -volume *vol_name* [*extension identifiers*] -false-positive false`次のいずれかのパラメータを使用して、拡張子を特定します。
   `[-seq-no *integer*]`容疑者リスト内のファイルのシーケンス番号。
   `[-extension *text*, … ]`クリアするファイル範囲のファイル拡張子の
   `[-start-time *date_time* -end-time *date_time*]`開始時間と終了時間。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 `vol1`ます。

```
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 `vol1`ます。

```
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 `vol1`ます。

```
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 `vol1`ます。

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

3. 手順1と2を繰り返して、必要なSnapshotを使用してボリュームをリストアします。

関連情報

- "KB：ONTAPでのランサムウェア対策とリカバリ"

自動スナップショットのオプションを変更します。

ONTAP 9 .11.1以降では、CLIを使用して、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の保持設定を制御できます。

開始する前に

変更できるのはノードSVM上のARP Snapshotオプションのみです。

手順

1. 現在のARPスナップショット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> -option-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、ONTAP CLIでと入力します `man vserver options。

2. 選択した現在のARPスナップショット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スナップショット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の設定	説明
`arw.snap.max.count`	一度にボリューム内に存在できるARP Snapshotの最大数を指定します。古いコピーは削除され、ARPスナップショットの総数がこの指定された制限内に収まるようになります。 `-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スナップショット間のinterval_in 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スナップショットが指定された間隔よりも古い場合、新しいARPスナップショットが作成されます。 `-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スナップショットを保持する期間（時間単位）を指定します。ARPスナップショットが保持しきい値に達すると、他のARPスナップショット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スナップショットは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スナップショット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、この期間よりも古いARPスナップショットは削除されます。 中程度の脅威が検出された場合、ARPスナップショット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スナップショットは、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、ONTAPはそのボリュームのARPスナップショットを削除します。 `-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の設定	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が含まれている場合の、ARP Snapshotの間隔（interval_in hours_between）を指定します。最大数に達すると、新しいコピー用のスペースを確保するためにARPスナップショットが削除されます。このオプションを使用すると、古いコピーを保持するために、新しいARPスナップショットの作成速度を下げることができます。ボリュームにすでに最大数のARP Snapshotが含まれている場合は、ではなく、このオプションで指定した間隔が次回のARP Snapshot作成に使用され`arw.snap.create.interval.hours`ます。 `-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スナップショット間のinterval_in days_between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スナップショットがこの指定された間隔よりも古い場合に、ARPスナップショットサージコピーを作成します。このオプションは、ARPサージスナップショットの保持期間（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の間隔（interval_in hours_between）を指定します。新しいファイル拡張子が監視されると、新しいARPスナップショットが作成されます。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スナップショットは、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、この間隔はARPスナップショットの頻度を制御するのに役立ちます。このオプションはとは独立して存在し`arw.snap.create.interval.hours`、データエントロピーベースのARPスナップショット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