ランサムウェア攻撃からデータを保護
ASA r2

NetApp
February 11, 2026

目次

ランサムウェア攻撃からデータを保護 . . . 1

ASA r2 ストレージ
システムに対するランサムウェア攻撃から保護するために、改ざん防止スナップショットを作成します。 . . . 1

SnapLock Complianceクロックの初期化 . . . 1

ASA r2 ストレージシステムで AI を活用した自律型ランサムウェア防御を有効化 . . . 1

クラスター内のすべてのストレージユニットでARP/AIを有効にする . . . 2

ストレージVM内のすべてのストレージユニットでARP/AIを有効にする . . . 2

ストレージVM内の特定のストレージユニットでARP/AIを有効にする . . . 3

ASA r2ストレージシステムでデフォルトの自律ランサムウェア保護を無効にする . . . 3

ASA r2 ストレージ システムの ARP/AI スナップショットの保持期間を変更する . . . 4

ASA r2 ストレージ システムの AI アラートによる自律的なランサムウェア防御に対応 . . . 5

ASA r2 ストレージシステムで AI を活用した自律ランサムウェア防御を一時停止または再開 . . . 6

ARP/AIを一時停止 . . . 6

ARP/AIを再開する . . . 6

ランサムウェア攻撃からデータを保護

ASA r2 ストレージ システムに対するランサムウェア攻撃から保護するために、改ざん防止スナップショットを作成します。

ランサムウェア攻撃に対する保護を強化するには、Snapshotをリモートクラスタにレプリケートし、デスティネーションSnapshotをロックして改ざんを防止します。ロックされたSnapshotは、誤ってまたは悪意を持って削除することはできません。ロックされたSnapshotを使用して、ランサムウェア攻撃によってストレージユニットが侵害された場合にデータをリカバリできます。

SnapLock Complianceクロックの初期化

改ざん防止Snapshotを作成する前に、ローカルクラスタとデスティネーションクラスタでSnapLock Complianceクロックを初期化する必要があります。

手順

1. [*Cluster] > [Overview] を選択します。
2. セクションで、[Initialize SnapLock Compliance Clock]*を選択します。
3. [初期化]*を選択します。
4. コンプライアンスクロックが初期化されていることを確認します。
   a. [*Cluster] > [Overview] を選択します。
   b. セクションでを選択し、 SnapLock Compliance Clock *を選択します。

次の手順

ローカルクラスタとデスティネーションクラスタでSnapLock Complianceクロックを初期化したら、を実行できます"ロックされたSnapshotを使用してレプリケーション関係を作成する"。

ASA r2 ストレージシステムで AI を活用した自律型ランサムウェア防御を有効化

ONTAP 9.17.1以降では、人工知能（ARP/AI）を搭載したAutonomous Ransomware Protectionを使用して、 ASA r2システムのデータを保護できます。ARP/AIは、潜在的なランサムウェアの脅威を迅速に検出し、データ保護のためのARPスナップショットを自動的に作成し、疑わしいアクティビティを警告するメッセージをSystem Managerに表示します。

ARPは、SAN環境において常に進化するランサムウェアを98%の精度で検出するランサムウェア対策分析用の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（回復力）を向上させます。ARPの機械学習モデルは、ランサムウェア攻撃のシミュレーション前後の大規模なファイルデータセットを用いて事前トレーニングされています。このリソース集約型のトレーニングはONTAPの外部で実行され、このトレーニングから得られる事前トレーニング済みモデルはONTAPに搭載されています。このモデルはアクセスも変更もできません。ARP/AIは有効化後すぐにアクティブになります。"学習期間"はありません。

ランサムウェアの検出・防止システムは、ランサムウェア攻撃からの完全な安全を保証することはできません。攻撃が検知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知できなかった場合、ARP/AIは重要な追加防御層として機能します。

タスクの内容

- ARP/AIサポートは、 "ONTAP Oneライセンス" 。
- ARP/AI はSnapMirror アクティブ同期、SnapMirror 同期、またはSnapLockによって保護されているストレージ ユニットではサポートされません。
- ONTAP 9.18.1以降では、ONTAP 9.18.1にアップグレードしてから12時間後、または新しいONTAP 9.18.1 ASA r2クラスタを初期化してから12時間後に、新しく作成されたすべてのストレージユニットでARP/AIがデフォルトで有効になります。
- ARP/AIを有効にしたら、 "セキュリティファイルの自動更新を有効にする"新しいセキュリティ更新プログラムを自動的に受信します。

クラスター内のすべてのストレージユニットで**ARP/AI**を有効にする

ONTAP 9.17.1を実行している場合は、クラスタ内に作成されたすべてのストレージユニットでARP/AIをデフォルトで有効にすることができます。

ONTAP 9.18.1以降では、すべての新規ストレージユニットでARP/AIがデフォルトで有効になっています。ONTAP 9.17.1で作成されたストレージユニットでARP/AIが有効になっていない場合は、手動で有効にすることができます。

手順

1. System Managerで、* Cluster > Settings *の順に選択します。
2. *ランサムウェア対策*の横にあるを選択してから、*既存のすべてのストレージユニットで有効にする*を選択します。
3. *有効*を選択します。

ストレージ**VM**内のすべてのストレージユニットで**ARP/AI**を有効にする

ONTAP 9.17.1 を使用している場合、ストレージ仮想マシン（VM）内に作成されたすべてのストレージユニットで ARP/AI をデフォルトで有効化できます。つまり、ストレージVM内に新規に作成されたストレージユニットでは、ARP/AI が自動的に有効化されます。また、ストレージVM内の既存のストレージユニットに ARP/AI を適用することもできます。

ONTAP 9.18.1以降では、すべての新規ストレージユニットでARP/AIがデフォルトで有効になっています。ONTAP 9.17.1で作成されたストレージユニットでARP/AIが有効になっていない場合は、手動で有効にすることができます。

手順

1. System Manager で、クラスター **>** ストレージ **VM** を選択します。
2. ARP/AI を有効にするストレージ VM を選択します。
3. セキュリティ*セクションの*ランサムウェア対策*の横にある；次に、「*ランサムウェア対策設定の編集」を選択します。
4. *ランサムウェア対策を有効にする*を選択します。

これにより、選択したストレージ VM 上に作成される今後のすべてのストレージ ユニットで ARP/AI がデフォルトで有効になります。

5. 選択したストレージ VM 上の既存のストレージ ユニットに ARP を適用するには、[この変更をこのストレージ **VM** 上のすべての適用可能な既存のストレージ ユニットに適用する] を選択します。
6. [保存（ Save ）] を選択します。

結果

ストレージ VM 上に作成するすべての新しいストレージ ユニットは、デフォルトでランサムウェア攻撃から保護されており、疑わしいアクティビティは System Manager で報告されます。

ストレージ**VM**内の特定のストレージユニットで**ARP/AI**を有効にする

ONTAP 9.17.1 を実行していて、ストレージ VM 内のすべてのストレージユニットで ARP/AI を有効にしたくない場合は、有効にする特定のユニットを選択できます。

ONTAP 9.18.1以降では、すべての新規ストレージユニットでARP/AIがデフォルトで有効になっています。ONTAP 9.17.1で作成されたストレージユニットでARP/AIが有効になっていない場合は、手動で有効にすることができます。

手順

1. System Managerで、*[ストレージ]*を選択します。
2. ARP/AI を有効にするストレージ ユニットを選択します。
3. 選択⋮ ; 次に、「ランサムウェア対策を有効にする」を選択します。
4. *有効*を選択します。

結果

選択したストレージ ユニットはランサムウェア攻撃から保護されており、疑わしいアクティビティは System Manager に報告されます。

ASA r2ストレージシステムでデフォルトの自律ランサムウェア保護を無効にする

新しい ONTAP 9.18.1 ASA r2 クラスタを初期化するか、クラスタを ONTAP 9.18.1 にアップグレードすると、12 時間の猶予期間が経過した後、すべての新規ストレージユニットで ARP/AI がデフォルトで自動的に有効化されます。猶予期間中に ARP/AI を無効化しない場合、猶予期間終了時に新規ストレージユニットに対してクラスタ全体で ARP/AI が有効化されます。

ONTAP 9.17.1で作成されたストレージユニットは、ARP/AI用に"手動で有効化"する必要があります。

手順

最初の12時間の猶予期間中または猶予期間後に、デフォルトの有効化を無効にすることができます。

System Manager

1. [* Cluster]>[Settings]（設定）*を選択します。
2. ARPを無効にする：
   - 12時間の猶予期間中に無効にするには：
     i. *Anti-ransomware*で、*Don’t enable*を選択してから*Disable*を選択します。
   - 12時間の猶予期間後に無効にするには：
     i. *ランサムウェア対策*の下で、 を選択してから、*新しいストレージユニットに対して有効にする*の選択を解除します。
     ii. *保存*を選択します

CLI

1. デフォルトの有効化ステータスを確認します：

```
security anti-ransomware auto-enable show
```

2. 既存および新規ボリュームのデフォルトの有効化を無効にします：

```
security anti-ransomware auto-enable modify -default-existing-volume
-state false -default-new-volume-state false
```

ASA r2 ストレージ システムの ARP/AI スナップショットの保持期間を変更する

人工知能（ARP/AI）による自律ランサムウェア保護は、 ASA r2システムのストレージユニット1台以上で異常なアクティビティを検出すると、ストレージユニットのデータを保護するためにARPスナップショットを自動的に作成します。ストレージ容量とデータに対するビジネス要件に応じて、デフォルトのARPスナップショットの保持期間を増減できます。例えば、ビジネスクリティカルなアプリケーションの保持期間を延長して、必要に応じてデータ復旧のための保持期間を長くしたり、それほど重要でないアプリケーションの保持期間を短縮してストレージ容量を節約したりすることができます。

ARP スナップショットのデフォルトの保持期間は、異常なアクティビティに応じて実行するアクションによって異なります。

このアクションを実行すると...	**ARP** スナップショットは、デフォルトで次の期間保持されます...
誤検知としてマーク	12 時間
潜在的なランサムウェア攻撃としてマーク	7日間

このアクションを実行すると...	**ARP** スナップショットは、デフォルトで次の期間保持されます...
すぐに行動を起こさないでください	10日間

デフォルトの保持期間は、 ONTAPコマンドラインインターフェイス（CLI）を使用して変更できます。"ONTAP自動スナップショットのオプションを変更する"デフォルトの保存期間を変更する手順については、こちらをご覧ください。

ASA r2 ストレージ システムの AI アラートによる自律的なランサムウェア防御に対応

人工知能（ARP/AI）を活用した自律ランサムウェア保護機能が、 ASA r2システムのストレージユニット1台以上で異常なアクティビティを検知した場合、System Managerダッシュボードに警告が表示されます。警告を確認し、アクティビティを確認し、必要に応じてデータへの潜在的な脅威を阻止するための措置を講じてください。

ARP/AI警告メッセージが表示された場合は、対処する前に、適切なアプリケーション整合性チェッカーを使用して、ストレージユニット上のデータの整合性を確認してください。ストレージユニットのデータ整合性を確認することで、アクティビティが許容できるものなのか、それともランサムウェア攻撃の可能性があるものなのかを判断するのに役立ちます。

異常な活動が...	操作
許容できる	アクティビティを誤検知としてマークします。
潜在的なランサムウェア攻撃	アクティビティを潜在的なランサムウェア攻撃としてマークします。
不確定	すぐに行動を起こさないでください。ストレージユニットを最大7日間監視してください。ストレージユニットが正常に動作し続ける場合は、そのアクティビティを誤検知としてマークしてください。ストレージユニットが異常なアクティビティを示し続ける場合は、そのアクティビティをランサムウェア攻撃の可能性としてマークしてください。

手順

1. System Manager で、 * Dashboard * を選択します。

   ARP が 1 つ以上のストレージ ユニットで異常なアクティビティを検出した場合、[警告] の下にメッセージが表示されます。

2. 警告メッセージを選択します。
3. イベントの概要*で、異常なアクティビティが発生しているストレージ ユニットの数を示す *警告 メッセージを選択します。
4. 異常なアクティビティが発生しているストレージ ユニット の下で、ストレージ ユニットを選択します。
5. *セキュリティ*を選択します。

ストレージ ユニットで異常なアクティビティが発生した場合は、[ランサムウェア対策] の下にメッセージが表示されます。

6. *アクションを選択*を選択します。
7. *誤検知としてマーク*を選択するか、*潜在的なランサムウェア攻撃としてマーク*を選択します。

次の手順

ストレージユニットのアクティビティに急増が見られる場合（一時的な急増、または新たな常態を特徴づける急増のいずれか）は、それらを安全として報告する必要があります。これらの急増を手動で安全として報告することで、ARPの脅威評価の精度向上に役立ちます。"既知のARP/AIサージを報告する"方法をご確認ください。

ASA r2 ストレージシステムで AI を活用した自律ランサムウェア防御を一時停止または再開

ONTAP 9.17.1以降では、人工知能（ARP/AI）を活用した自律型ランサムウェア保護機能を使用して、 ASA r2システムのデータを保護できます。異常なワークロードイベントを計画している場合は、ランサムウェア攻撃の誤検知を防ぐため、ARP/AI分析を一時的に停止することができます。ワークロードイベントが完了したら、ARP/AI分析を再開できます。

ARP/AIを一時停止

異常なワークロード イベントを開始する前に、ランサムウェア攻撃の誤検出を防ぐために、ARP/AI 分析を一時的に停止する必要がある場合があります。

手順

1. System Managerで、*[ストレージ]*を選択します。
2. ARP/AI を一時停止するストレージ ユニットを選択します。
3. *ランサムウェア対策を一時停止*を選択します。

結果

選択したストレージ ユニットの ARP/AI 分析は一時停止され、ARP/AI を再開するまで System Manager で疑わしいアクティビティは報告されません。

ARP/AIを再開する

異常なワークロード中に ARP/AI を一時停止した場合は、ワークロードが完了したら、ランサムウェア攻撃からデータを保護するために ARP/AI を再開する必要があります。

手順

1. System Managerで、*[ストレージ]*を選択します。
2. ARP/AI を再開するストレージ ユニットを選択します。
3. *ランサムウェア対策を再開*を選択します。

結果

潜在的なランサムウェア攻撃の分析が再開され、疑わしいアクティビティが System Manager に報告されます。