アラート

Cloud Insights

Tony Lavoie
August 26, 2021

目次

アラート

Cloud Secure アラートページには、最近の攻撃や警告のタイムラインが表示され、各問題の詳細を表示できます。

[アラートのリスト]

アラート

アラートリストには、選択した期間内に発生した攻撃および警告の総数、およびその期間内に発生した攻撃または警告のリストがグラフで表示されます。期間を変更するには、グラフの開始時間と終了時間のスライダを調整します。

アラートごとに次の情報が表示されます。

- 潜在的な攻撃 :*
- 予想される Attack_type （例：ランサムウェア）
- 潜在的な攻撃が検出された日時 _
- アラートの *Status* ：
  - 新規（新しいアラートのデフォルト）
  - 実行中です
  - 解決しました
  - 却下されました

    管理者は、アラートのステータスを変更し、調査に役立つメモを追加できます。

  [アラートステータスを変更します]

- アラートをトリガーした動作のユーザー（ *User* ）
- 攻撃の _ 証拠 _（多数のファイルが暗号化された場合など）
- アクションの実行 _（スナップショットが作成された場合など）
- 警告 :*
- 警告をトリガーした異常な動作 _
- 動作が検出された日付と時刻 _
- アラートの *Status* ：
  - 新規（新しいアラートのデフォルト）
  - 実行中です
  - 解決しました
  - 却下されました

    管理者は、アラートのステータスを変更し、調査に役立つメモを追加できます。

- アラートをトリガーした動作のユーザー（ *User* ）
- 概要 of the *Chang* （ファイルアクセスが異常に増加している場合など）
- 実行されたアクション _

フィルタオプション（ **Filter Options** ）

アラートは次の方法でフィルタできます。

- アラートの *Status*
- 特定のテキスト（ *Note*.
- _ 攻撃 / 警告 _ のタイプ
- 警告 / 警告をトリガーしたアクションのユーザー _

[Alert Details] ページ

アラートリストページのアラートリンクをクリックすると、そのアラートの詳細ページを開くことができます。アラートの詳細は、攻撃またはアラートのタイプによって異なる場合があります。たとえば、ランサムウェア攻撃の詳細ページには、次のような情報が表示される場合があります。

サマリセクション：

- 攻撃の種類（この例ではランサムウェア）とアラート ID （ Cloud Secure が割り当て）
- 攻撃が検出された日時
- 実行された処理（自動スナップショットの作成など）。Snapshot の時刻は概要セクションのすぐ下に表示されます）
- ステータス（新規、進行中など）

［ 攻撃結果 ］ セクション：

- 影響を受けるボリュームとファイルの数
- 検出の概要
- 攻撃中のファイルアクティビティを示すグラフ

[関連ユーザー **]** セクション：

このセクションでは、潜在的な攻撃に関与するユーザーの詳細を示します。ユーザーの上位アクティビティのグラフも含まれます。

ランサムウェア攻撃の可能性を示すアラートページ：[ランサムウェアアラートの例]

ランサムウェア攻撃の詳細ページ：[Ransomware Detail Page の例]

Snapshot 処理を実行します

Cloud Secure は、悪意のあるアクティビティが検出されたときにスナップショットを自動的に取得することでデータを保護し、データを安全にバックアップします。

を定義できます "自動応答ポリシー" ランサムウェア攻撃やその他の異常なユーザアクティビティが検出されるとスナップショットが作成されます。アラートページから手動で Snapshot を作成することもできます。

自動 Snapshot の作成：[アラート処置画面、 1000]

手動スナップショット：[アラート処置画面、 1000]

アラート通知

アラートの E メール通知は、アラートに対するすべての対処方法についてアラート受信者リストに送信されます。アラート受信者を設定するには、 [*Admin] > [Notifications] をクリックし、受信者ごとに電子メールアドレスを入力します。

保持ポリシー

アラートと警告は 13 カ月間保持されます。13 カ月を経過したアラートと警告は削除されます。Cloud Secure 環境を削除すると、その環境に関連付けられているすべてのデータも削除されます。

トラブルシューティング

問題	次の操作を実行します
Cloud Secure （ CS ）が作成したスナップショットの場合、 CS スナップショットのパージ / アーカイブ期間はありますか？	いいえCS スナップショットのパージ / アーカイブ期間は設定されていません。CS スナップショットのパージポリシーを定義する必要があります。を参照してください "ONTAP のドキュメント" ポリシーの設定方法については、を参照してください。
ONTAP では、 1 日に 1 時間ごとに Snapshot が作成される場合があります。Cloud Secure （ CS ）スナップショットは、そのスナップショットに影響を与えますか。CS スナップショットは時間単位のスナップショットを作成しますか？デフォルトの時間単位の Snapshot は停止しますか？	Cloud Secure Snapshot は 1 時間ごとの Snapshot には影響しません。CS スナップショットでは時間単位のスナップショット領域は使用されず、以前と同様に続行されます。デフォルトの時間単位 Snapshot は停止しません。
ONTAP で Snapshot 数が上限に達した場合、どうなるかを確認します。	最大 Snapshot 数に達すると、以降の Snapshot 作成が失敗し、 Snapshot がフルであることを示すエラーメッセージが Cloud Secure に表示されます。最も古い Snapshot を削除するには、 Snapshot ポリシーを定義する必要があります。定義しないと、 Snapshot は作成されません。ONTAP 9.3 以前では、ボリュームに格納できる Snapshot コピーは最大 255 個です。ONTAP 9.4 以降では、ボリュームに格納できる Snapshot コピーは最大 1023 個です。の詳細については、 ONTAP のマニュアルを参照してください "Snapshot 削除ポリシーを設定しています"。

問題	次の操作を実行します
Cloud Secure は Snapshot をまったく作成できません。	スナップショットの作成に使用されている役割に、https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html#a-note-about-permissions[proper 権限が割り当てられていることを確認します。Snapshot を作成するための適切なアクセス権を持つ sure _csrole_is create -vserver <vservername> -role csrole -cmddirname "volume snapshot" -access all が作成されていることを確認します
Cloud Secure から削除されたあとに再び追加された SVM では、 Snapshot で古いアラートが失敗します。SVM が再び追加されたあとに発生する新しいアラートについては、 Snapshot が作成されます。	これはまれなシナリオです。この問題が発生した場合は、 ONTAP にログインし、古いアラートに対して手動で Snapshot を作成してください。
_Alert Details_page では、 _Take Snapshot_Button の下に「 Last Attempt failed 」エラーが表示されます。エラーにカーソルを合わせると、「 invoke API command has timed out for the data collector with id 」というメッセージが表示されます。	これは、 SVM の LIF が ONTAP で _DISABLE_STATE になっている場合に、 SVM 管理 IP を介して Cloud Secure にデータコレクタが追加されたときに発生することがあります。ONTAP で特定の LIF を有効にし、 trigger_take Cloud Secure で手動でスナップショットを作成します。Snapshot 処理が成功します。