テクニカル レポート

NetApp Cloud InsightsとSnapCenterによるFlexPodランサムウェア対策とリカバリ

NetApp
Roney John Daniel
2023年10月| TR-4961

提携協力：

概要

このテクニカルレポートでは、ランサムウェアの概要と拡散方法、および攻撃を監視、通知、修復するためにNetApp®とシスコシステムズがストレージ、コンピューティング、ネットワークの各レイヤで提供するソリューションの一部について説明します。本ドキュメントでは、NetAppのCloud Insights®とONTAP Autonomous Ransomware Protection®（ARP）のセキュリティ機能であるワークロードセキュリティのインストールと設定を中心に説明します。 これは、ランサムウェア攻撃や内部の脅威から保護するネイティブのONTAPセキュリティ機能です。また、VMとアプリケーションと整合性のあるバックアップとリカバリを実現するNetAppのSnapCenter®プラグインについても説明します。

目次

表一覧

図一覧

ランサムウェアの概要

ランサムウェアは、身代金が支払われない限り、被害者の個人データを公開したり、アクセスを永続的にブロックしたりするマルウェアです。

ランサムウェアは、刑務所のロックダウン、従業員のクレデンシャルと機密情報のオンライン漏えい、サイバー攻撃による国家的な緊急事態宣言など、2022年にも見出しを広げ続けています。対策を講じると、攻撃者はランサムウェアを生成して拡散する新しい方法を見つけ、ランサムウェアサービス（RaaS）を他のサイバー犯罪者に提供することもできます。

ランサムウェア攻撃を実行するには、攻撃者がデバイスまたはネットワークにアクセスする必要があります。攻撃者は、電子メール、ファイルのダウンロード、URLアクセスなどの通常の日常的な操作を通じて、誤って暗号化マルウェアプログラムをダウンロードさせます。マルウェアがコンピュータにインストールされると、設定された時間にアクティブ化され、すべてのローカルクライアントファイルと、企業ネットワーク上のNFS共有またはSMB/CIFS共有でアクセスできるすべてのファイルが暗号化されます。ファイルが暗号化されると、元のファイルが削除されるため、攻撃者が保持している復号キーでファイルを復号化しない限り、元のファイルにアクセスできません。

それはどのように広がっていますか?

ランサムウェアがあるコンピュータシステムから別のコンピュータシステムに拡散する方法はいくつかあります。最も一般的な方法には、電子メール、ファイルのダウンロード、ファイル共有、Web URLへのアクセスなどの通常の日常的な操作が含まれます。

攻撃者は、悪意のある添付ファイルやリンクを含むスパムメールを多数の人々に送信する可能性があり、添付ファイルやリンクを開いた人は知らず知らずにトラップに入る可能性があります。場合によっては、スピアフィッシングのテクニックが標的型攻撃に使用されることがあり、上司のふりをして従業員に電子メールを送信したり、同様にしています。攻撃者は、ソーシャルエンジニアリングを使用して、信頼できる友人や組織から送られてきたかのように、電子メールの添付ファイルを開くように人々を騙すこともできます。

攻撃者はまた、マルウェアを拡散する新しい方法を発見し、最新のものはUSBスティックを物理的に郵送するという形になっています。

ランサムウェアの種類

ランサムウェアには主に、スケアウェア、スクリーンロッカー、ランサムウェアの暗号化の3種類があります。

- **Scareware:** 通常、不正なセキュリティソフトウェアが含まれており、マルウェアが検出されたことをユーザーに怖がらせるポップアップメッセージが繰り返し生成され、それを取り除く唯一の方法はソフトウェアの代金を支払うことです。料金を支払わない場合は、ポップアップメッセージが繰り返し表示されますが、データは本質的に安全な場合があります。正規のサイバーセキュリティソフトウェアは、このような方法で顧客を勧誘するものではないことに注意してください。
- **スクリーンロッカーランサムウェア**:制限を解除するために支払いを要求しながら、ログインやファイルへのアクセスを制限するマルウェアの一種です。多くの場合、画面にはFBIやDOJなどの公式ロゴが表示され、コンピュータで違法行為が検出されたため、罰金を支払う必要があります。FBIまたは司法省は、この方法での支払いを要求するのではなく、むしろ違法またはテロ関連の活動のために、直接被疑者に接近することに注意してください。
- **ランサムウェアの暗号化：**ロックスクリーンランサムウェアと同じ意図ですが、その影響は非常に厄介です。この場合、データは暗号化され、攻撃者はデータを復号化して再配信するための支払いを要求します。身代金を支払っても、攻撃者がデータを復元したり、データを復号化するためのキーを提供したりする保証はありません。

どのような影響がありますか？

ランサムウェア攻撃は、直接的または間接的な影響を及ぼす可能性があります。影響は、データの性質、ダウンタイムの期間、組織がデータにアクセスできない期間によって異なります。ランサムウェア攻撃を受けると、次のような結果が発生する可能性があります。

- **貴重なデータの損失**

身代金を支払っても、データが完全に回復可能であるという保証はありません。これは、復号化プロセス中に復号化エラーやデータ損失の可能性があるためです。バックアップからシステムを再構築する場合は、最後のバックアップがいつ作成されたかによって、データの一部が失われる可能性が高くなります。

- **ビジネスの中断と収益の損失**

  時間はお金であり、ダウンタイムは機会の損失、サービスの停止、生産の不足などを通じて組織の収益に深刻な影響を与えます。

- **責任とコンプライアンスのコスト**

  機密データが侵害されたり公開されたりした場合、組織は訴訟コスト、罰金、ID監視を処理して、データが紛失または盗難にあったユーザーに補償する必要があります。データの使用と保護を管理する規制に準拠している組織は、コンプライアンス違反に対する急激な罰則や罰金を科す可能性もあります。

- **顧客の信頼とブランド名が損なわれた**

  ランサムウェア攻撃にどれだけ迅速に対応し、修復できるかにかかわらず、組織の評判や顧客の信頼を損なう可能性があります。

解決策とは

ランサムウェア攻撃からダウンタイムを最小限に抑えてリカバリできるのは良いことですが、攻撃を完全に防ぐことが理想的です。

この問題に単一の解決策はありません。新しいバリアントが進化しているため、検出機能とリカバリ機能を常に評価する必要があります。攻撃を防ぐために確認して修正する必要がある領域はいくつかありますが、攻撃を防止またはリカバリするための主要なコンポーネントは、データが格納されているデータセンターです。

日々の業務をセキュアに遂行できる環境を構築するうえで、ネットワーク、コンピューティング、ストレージのエンドポイントを保護するためのデータセンターの設計と機能が重要な役割を果たします。

本ドキュメントでは、NetApp Cloud Insights®のワークロードセキュリティ機能をFlexPod® ハイブリッドクラウドインフラと統合して、悪意のあるユーザのアクセスを迅速にブロックし、 ランサムウェア攻撃：

NetAppのランサムウェア対策ソリューション

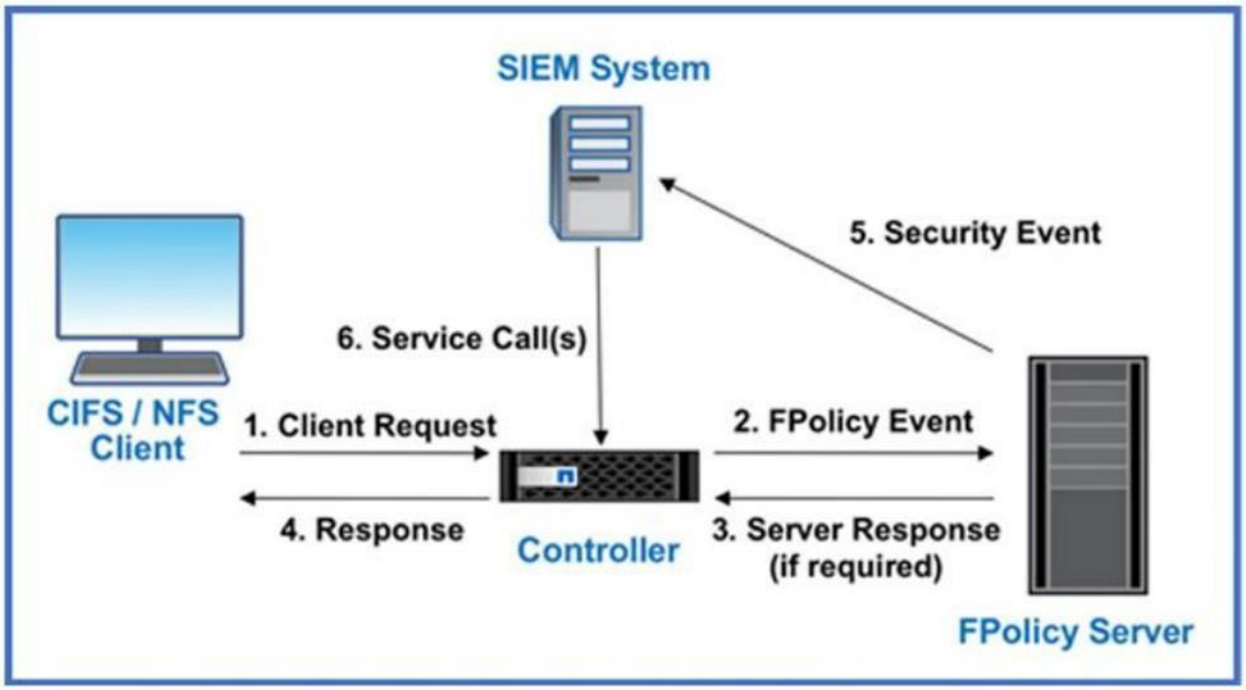
ランサムウェアの検出は、拡散を防ぎ、コストのかかるダウンタイムを回避できるように、できるだけ早く実行することが重要です。NetAppは、ONTAP® ソフトウェアとネイティブの検出/リカバリツールを使用した階層型防御アプローチを提供します。このセクションでは、NetAppがランサムウェア攻撃を検出、警告、リカバリするために提供するさまざまな機能やツールについて説明します。

- **NetApp® Active IQ®**（**AIQ**）NetApp ONTAPシステムをチェックし、FPolicyの有効化など、NetApp設定のベストプラクティスに準拠しているかどうかを確認します。
- **NetApp Active IQ Unified Manager®**（**AIQUM**）は、NetApp Snapshotコピーの異常な増加やストレージ効率の低下を示すアラートを生成します。これは、ランサムウェア攻撃の可能性を示している可能性があります。
- **ONTAP System Manager** を使用すると、Snapshotの変更率やStorage Efficiencyによる削減効果をリアルタイムで分析できます。
- **多要素認証（MFA）** を使用すると、管理SVMまたはデータSVMにログインする際にユーザに2つの認証方式の指定を要求することで、セキュリティを強化できます。ONTAPのバージョンに応じて、SSH公開鍵、ユーザ パスワード、Time-based One-Time Password（TOTP）を組み合わせて多要素認証を設定できます。ONTAP 9.13.1以降では、最初の認証方式としてSSH公開鍵とユーザパスワードを使用し、2番目の認証方式として時間ベースのワンタイムパスワード（TOTP）を使用できます。
- **Multi-Admin Verification（MAV；マルチ管理者検証）**を使用すると、ボリュームやSnapshotコピーの削除などの特定の処理を、指定した管理者の承認後にのみ実行できるようになります。これにより、侵害を受けた管理者、悪意のある管理者、または経験の浅い管理者が望ましくない変更やデータの削除を行えないようにすることができます。

- **Autonomous Ransomware Protection®（ARP）**NetApp ONTAP 9.10.1以降には、組み込みの機械学習（ML）を活用して、ボリュームワークロードのアクティビティとデータエントロピーを確認し、ランサムウェアを自動的に検出するランサムウェア対策機能が搭載されています。ONTAP 9.11.1では、この機能が強化された分析エンジンが強化され、データエントロピーとファイル拡張子を操作する新しいバリエーションのランサムウェアを検出します。この機能をワークロードセキュリティと統合して、Cloud Insightsダッシュボードでオンボックス保護のステータスを追跡できます。この機能は、Amazon FSxとCloud Volumes ONTAPでもサポートされています。ONTAP 9.12.1では、ARPスクリーニングプロファイルがNetApp SnapMirror®レプリケーションの一部として転送されるため、セカンダリストレージでランサムウェアから保護されます。ONTAP 9.13.1より前のバージョンでは、ARPをアクティブモードに切り替える前に、ラーニングモードで30日間実行することが推奨されていました。ONTAP 9.13.1以降では、ARPは自動的に最適な学習期間間隔を決定し、7日から30日後に自動的にアクティブモードに切り替わります。ONTAP 9.13.1では、ARP設定のマルチ管理検証がサポートされています。
- **NetAppのネイティブFPolicy** は、NFSまたはSMB / CIFSプロトコル経由のファイルアクセスの監視と管理に使用されるファイルアクセス通知フレームワークです。このゼロトラストエンジンは、「信頼せず、常に検証する」という概念に基づいて構築されています。FPolicyを使用すると、不要なファイルがNetAppストレージデバイスに保存されるのを防ぐことができます。この機能を利用すると、既知のランサムウェアファイル拡張子をブロックできます。ONTAP 9.12.1では、System ManagerまたはNetApp BlueXP™でワンクリックでFPolicyをアクティブ化できるようになりました。 この機能は、一般的なランサムウェア攻撃で使用される数千もの既知の一般的なランサムウェア拡張機能から保護します。
- ONTAPのFPolicy外部モードでは、ユーザ行動分析（UBA）が、ゼロデイランサムウェア攻撃を阻止するための鍵として、ユーザおよびエンティティ行動分析（UEBA）とも呼ばれます。UBAは、ユーザーおよびグループのデータアクセスパターンを追跡し、パターンの偏差を報告します。ユーザーが通常のパターン以外の操作を行った場合、UBAはファイルへのアクセスを拒否することもできます。UBAには外部モードのFPolicyサーバが必要です。

次に、セキュリティ情報イベント管理（SIEM）システムの例を示します（図1）。CIFS / SMBまたはNFSのすべてのクライアント要求がFPolicyサーバに送信され、このサーバによってアクセスが許可されるかどうかが決まります。

図1）FPolicy外部サーバ



この追加レベルの分析は、ユーザが操作しようとしているファイルデータに対するファイル権限を持っている場合でも実行されます。

注：ワークロードセキュリティ機能を備えたCloud Insightsは、NetApp独自の外部モードFPolicyサーバです。

- **NetApp Snapshot™ コピー** Snapshotは、ボリュームの読み取り専用イメージであり、ファイルシステムのある時点の状態をキャプチャします。 これらのコピーは、システムのパフォーマンスに影響を与えることなくデータを保護するのに役立ちます。同時に、大量のストレージスペースを占有することもありません。スケジュールされたSnapshotは、攻撃後にデータをリストアする必要がある場合に役立ちます。
- **NetApp SnapLock®**は、ランサムウェアに対するエンタープライズデータ保護とデータ耐障害性のための重要なコンポーネントです。変更不可の特別なボリュームを提供します。このボリュームには、特定の保持期間にわたってデータを保存し、消去や書き換えが不可能な状態にコミットできます。FlexGroupボリュームに格納されているユーザの本番環境データをSnapLockボリュームとして作成することもできるため、WORMで保護されたデータに対して、パフォーマンスの向上と大規模な拡張を実現できます。

ワークロードセキュリティの概要

NetApp Cloud Insightsは、クラウドベースの統合プラットフォームであるNetApp BlueXPのサービスの1つであり、ワークロードセキュリティ（旧称 **Cloud Secure**）はNetApp Cloud Insightsの機能です。オンプレミス環境とクラウド環境のすべての企業データアクセスを一元的に可視化して制御できるため、セキュリティとコンプライアンスの目標を確実に達成できます。内部ユーザ、外部ユーザ、ランサムウェア攻撃、不正ユーザによるアクセスの挙動を報告します。通常のデータアクセスパターンについてユーザとグループをプロファイリングし、リスクのある動作が検出された場合は、アラートが表示され、Snapshotコピーが自動的に作成されて迅速にリカバリできます。

内部者が信頼されていることを前提とした境界セキュリティツールとは異なり、ワークロードセキュリティはすべての人にゼロトラストを想定しています。監視対象の共有に対するすべてのアクティビティがリアルタイムで監視され、データを使用してすべてのユーザの作業コミュニティが自動的に識別されます。

さらに、すべてのドキュメントアクセスを監査できるため、規制要件へのコンプライアンスを確保できます。

ワークロードセキュリティの仕組み

ワークロードセキュリティはゼロトラストフレームワークに基づいているため、ノートラストのアプローチが必要です。すべてのデータアクセスアクティビティがリアルタイムで検査および分析され、悪意のある動作が検出されます。また、アラートが生成されてユーザまたは管理者に通知されます。

ワークロードセキュリティの主な機能は次の4つです。

- **ユーザアクティビティを監視し**ます。

  侵害を正確に識別するために、オンプレミス環境とハイブリッド クラウド環境の全域にわたって、ユーザの挙動を1つ1つ把握し、分析します。データの収集には、お客様の環境の仮想マシン（VM）にインストールされた軽量のステートレスデータコレクタエージェントを使用します。このデータには、Active DirectoryやLightweight Directory Access Protocol（LDAP）サーバのユーザデータ、NetApp ONTAP®やCloud Volumes ONTAP®（CVO）のユーザファイルアクティビティも含まれます。
- **異常を検出し、攻撃の可能性を特定**

  今日のランサムウェアやマルウェアは洗練されており、ランダムな拡張子やファイル名を使用しているため、シグネチャベース（ブロックリスト）ソリューションによる検出は効果がありません。ワークロードセキュリティでは、高度な機械学習アルゴリズムを使用して、異常なデータアクティビティを発見し、攻撃の可能性を検出します。臨機応変かつ正確に検知し、誤検出のノイズを減らすことができます。
- **自動応答ポリシー：**

  Workload Securityは、リスクの高い動作を検出すると、アラートを発してデータスナップショットを自動的に作成し、必要に応じて迅速にリカバリできるようにデータをバックアップします。
- **フォレンジックとユーザ監査レポート**

Workload Securityでは、グラフィカルインターフェイスを使用してアクティビティデータを細かく分析し、データ侵害の調査やユーザデータアクセス監査レポートの生成を行うことができます。ファイル データ アクティビティは、ユーザ、時間、アクティビティの種類、ファイル属性という複数の切り口で確認できます。

ワークロードセキュリティのコンポーネント

ワークロードセキュリティは、1つ以上のエージェントとデータコレクタを使用してユーザアクティビティを収集します。各エージェントは複数のデータコレクタをホストできますが、データコレクタの特定のセットを監視するために別 々 のエージェントをインストールすることもできます。エージェントは、収集したデータを分析のためにCloud Insightsに送信します。

本書の執筆時点で、ワークロードセキュリティでは次のユーザディレクトリコレクタとデータコレクタがサポートされています。

- Active Directory（AD）ユーザディレクトリコレクタ。
- LDAP Directory Server Collectorの略。
- ONTAP SVMデータコレクタ。
- Cloud Volumes ONTAPデータコレクタ
- Amazon FSx for NetApp ONTAP

詳細については、次のリンクを参照してください。
ワークロードセキュリティの概要

ワークロードセキュリティライセンス

ワークロードセキュリティはNetApp Cloud Insightsの機能として提供されています。Cloud Insightsはベーシックとプレミアムの2つのエディションで提供されています。Basicエディションは、有効なNetAppサポートアカウントをお持ちのすべてのNetAppのお客様が無料でご利用いただけます。Workload Securityはプレミアムエディションで提供されます。

Cloud Insightsに登録するには、以下のガイドラインに従ってください。

- BlueXPのアカウントに登録します（まだ登録していない場合）。これにより、パートナー様はNetAppのすべてのクラウドサービスにアクセスできるようになります。サインアップには、https://cloud.netapp.comまたはhttps://bluexp.netapp.comを使用します。
- Cloud Insightsの無償トライアルに登録して、利用可能な機能を確認できます。登録プロセスでは、Cloud Insights環境をホストするグローバルリージョンを選択できます。
- Cloud Insightsに登録して、プレミアムエディションを選択してください。

表1 に、Cloud Insightsサービスの主な機能を示します。

表1）Cloud Insightsのエディション

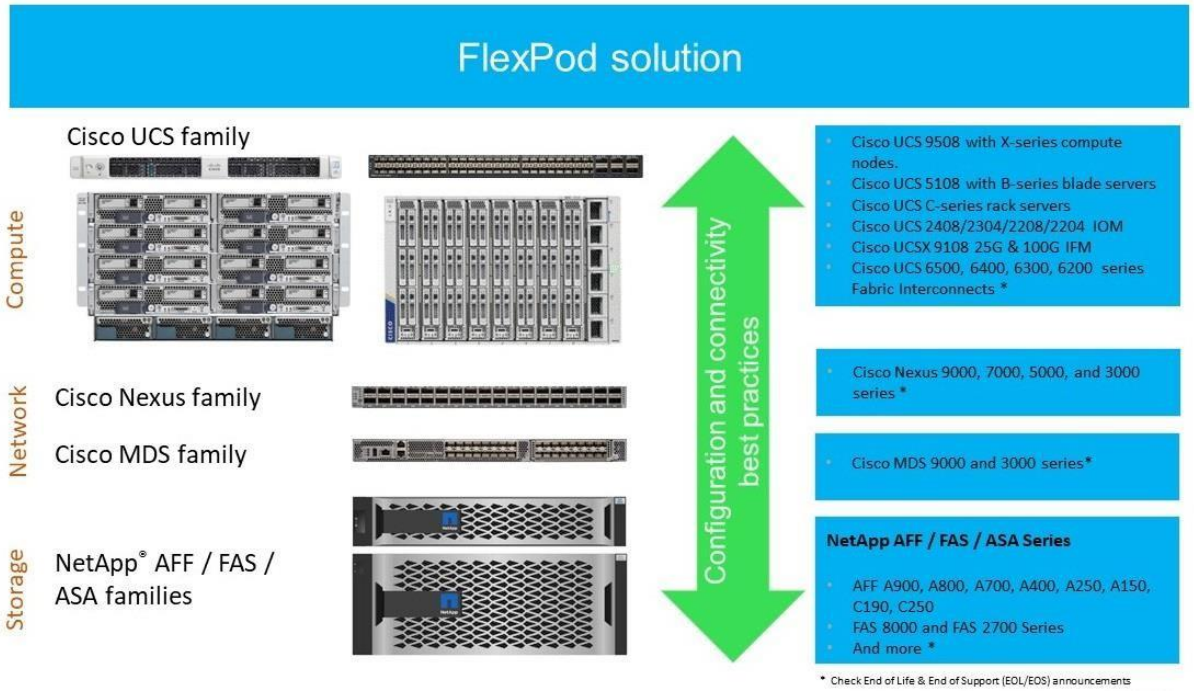
主な特長	Basicエディション	Premiumエディション
データ保持	7 日	13カ月
インフラとストレージの指標	NetAppのみ	マルチベンダー
カスタマイズ可能なダッシュボード	✓	✓
フォーラム、ドキュメント、トレーニングビデオ	✓	✓
ライブチャットとテクニカルサポート	-	✓
VM指標	-	✓
クラウド指標	-	✓
サービス指標	-	✓
監視とアラート	*	✓
API アクセス	✓	✓

主な特長	Basicエディション	Premiumエディション
シングルサインオン（SSO）	-	✓
ユーザ データ アクセスの監査	-	✓
AI / MLを使用した内部脅威の検出	-	✓
ビジネスインテリジェンスとレポート	-	✓

FlexPodの概要

FlexPodは、シスコシステムズとNetAppが提供するBoxアーキテクチャに組み込まれた、事前に設計、検証され、広く導入されているデータセンターです。FlexPodは12年以上前から存在しており、ハイブリッドクラウド環境をネイティブにサポートするデータセンター解決策へと進化しました。FlexPodは、耐障害性と柔軟性に優れたモジュラ型アーキテクチャを採用しているため、帯域幅とワークロードの要件に基づいて、コンピューティング、ネットワーク、ストレージの各コンポーネントを選択できます。図2に、さまざまなFlexPod設計の各レイヤでサポートされるコンポーネントを示します。

図2）FlexPod 解決策



FlexPodには、FlexPod DatacenterとFlexPod Expressの2種類があります。FlexPod Datacenterは、Cisco UCS B、C、Xシリーズサーバ、Cisco UCSファブリックインターコネクト、Cisco Nexus®およびMDSスイッチ、NetAppストレージを中心に構築された、拡張性に優れた仮想データセンターです。さまざまなエンタープライズワークロードだけでなく、パブリッククラウド、プライベートクラウド、ハイブリッドクラウド環境にも適しています。

FlexPod Expressは、Cisco Nexusスイッチ、Cisco UCS CシリーズサーバまたはCisco UCS Mini、およびNetAppストレージを使用したスケールダウンバージョンです。リモートオフィスやエッジのユースケースに適しています。

FlexPod XCSは、Cisco Intersightプラットフォームを使用してスタック全体の構成、監視、管理を行う、ハイブリッドクラウド環境向けの次世代FlexPodです。

FlexPodインフラはAnsibleプレイブックを使用して構成でき、エンドツーエンドのフローはCisco Validated Design（CVD）またはNetApp Verified Architectures（NVA）で文書化されています。

詳細については、FlexPod設計および導入ガイドを参照してください。

FlexPodソリューション

FlexPod設計ガイド- Cisco

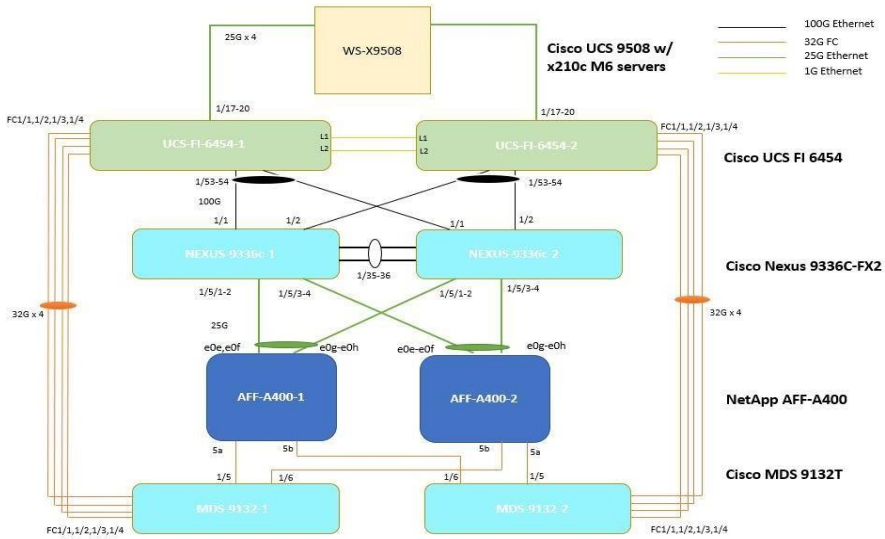
アーキテクチャの詳細

FlexPodデータセントートポロジは、Cloud Insightsでワークロードセキュリティ機能を検証するために使用します。ワークロードセキュリティエージェントマシンとして機能する管理ネットワークには、CentOS Linux VMが2台導入されています。これらのマシンは、Cloud Insightsソフトウェアサービス（SaaS）環境およびFlexPodスタックに導入されたデータコレクタにアクセスできます。1台のエージェントマシンで複数のデータコレクタを追跡できますが、このラボでは2台のマシンを導入します。1台はNetApp AFF-A400のSVMを追跡し、もう1台はActive Directoryサーバのユーザ属性を追跡します。エンドユーザアクティビティとランサムウェアシミュレーションのために、2台のUbuntu VMと1台のWindows 10 VMがFlexPodスタックに導入されます。

トポロジ

テスト対象のトポロジを次に示します（図3）。ワークロードセキュリティは特定のハードウェアやソフトウェアに依存しないため、FlexPodシステムはシームレスに動作する必要があります。

図3）FlexPodトポロジ図



ハードウェアおよびソフトウェアコンポーネント

テストで使用したハードウェアコンポーネントとソフトウェアコンポーネントを 表2に示します。

表2）ハードウェアとソフトウェア

タイプ	バージョン
SVMデータコレクタ	ONTAP 9.13.1を実行するNetApp AFF-A400
ユーザーディレクトリデータコレクタ	Active Directoryを実行するWindows Server 2016 Datacenterエディション
ワークロードセキュリティエージェント（2）	CentOS Stream 8とCloud Secure 1.531.0
エンドユーザアクセス用Linux VM（2）	Ubuntu 22.04.1 LTS

タイプ	バージョン
エンドユーザアクセス用のWindows VM	Windows 10 Enterprise
VMware vCenter Server	8.0
VMware vSphere向けNetApp ONTAPツール	9.12
VMware vSphere向けNetApp SnapCenterプラグイン	4.9

FlexPodが提供するランサムウェア対策

このセクションでは、FlexPod 解決策 で活用できる、シスコとNetAppが提供するランサムウェア対策機能について説明します。

ネットワーク

これらは、ランサムウェア対策をより広範な方法で実装するために使用できるシスコのセキュリティ機能とソリューションの一部です。

- **NetFlow**

  Cisco NX-OSは、拡張されたネットワーク異常およびセキュリティ検出を可能にする柔軟なNetFlow機能をサポートしています。Flexible NetFlowを使用すると、事前に定義された多数のフィールドからキーを選択して、特定のアプリケーションに最適なフローレコードを定義できます。FlexPodトポロジ内のNexusスイッチは、NetFlowレコードをCisco Secure Cloud Analyticsなどの外部コレクタに送信して、さらなる分析と悪意のあるアクティビティの検出を行うように設定できます。詳細については、次のリンクを参照してください。

  Nexus 9000シリーズスイッチでのNetFlowの設定

- **Cisco Identity Services Engine（ISE）**

  Cisco ISEは、市場をリードするセキュリティポリシー管理プラットフォームです。高度にセキュアなアクセス制御を統合および自動化して、ネットワークおよびネットワークリソースへのロールベースアクセスを実施します。Cisco ISEでは、TACACS+セキュリティプロトコルを使用してネットワークデバイスを管理し、ネットワークデバイスの設定を制御および監査できます。ISEを使用すると、誰がどのネットワークデバイスにアクセスし、関連するネットワーク設定を変更できるかをきめ細かく制御できます。ISEは物理アプライアンスまたは仮想アプライアンスとして使用でき、仮想アプライアンスは複数のホストOSにわたって使用できます。詳細については、次のリンクを参照してください。

  Cisco Identity Servicesエンジン

- **Cisco Secure IPS（NGIPS）**

  Cisco Firepower Next-Generation IPS（NGIPS）脅威アプライアンスは、物理および仮想フォームファクタで提供され、ネットワークの可視性、セキュリティインテリジェンス、自動化、高度な脅威保護を提供します。業界をリードする侵入防御機能と複数のテクニックを使用して、最も高度なネットワーク攻撃を検出し、それらから保護します。

  この製品ファミリの詳細については、次のリンクを参照してください。

  Cisco Secure IPS - Cisco

- **Cisco Secure Cloud Analytics**

  Cisco Secure Cloud Analytics（StealthWatch Cloud）は、プライベートクラウド、パブリッククラウド、ハイブリッドクラウド環境における内部および外部の脅威を特定するために使用できるソフトウェアサービス（SaaS）製品です。悪意のあるアクティビティをリアルタイムで特定するために必要な、実用的なセキュリティインテリジェンスと可視性を提供します。NetFlowレコードなどのネットワークフローとトラフィックテレメトリをリアルタイムまたはほぼリアルタイムで分析します。南北トラフィックとイースト/ウェストトラフィックを監視および分析し、疑わしいネットワークトラフィックが検出された場合は、自動または手動の応答機能を警告して提供できます。詳細については、次のリンクを参照してください。

  Cisco Secure Cloud Analytics

コンピューティング

- **Cisco Secure Endpoint**

  エンドポイント向けのCisco Secure Endpoint（旧称Advanced Malware Protection（AMP））は、マルチドメインコントロールポイント全体で高度なエンドポイント検出と応答を行うことで、クラウドで提供されるエンドポイント保護を提供します。脅威は、ソフトウェアウイルスや、ランサムウェア、ワーム、トロイの木馬、スパイウェア、アドウェア、 そしてファイルレスマルウェア。高度なマルウェア対策ソフトウェアは、コンピュータシステムからの脅威を効率的に防止、検出、削除するように設計されています。Cisco Secure Endpointは、Cisco Secure Xプラットフォームの製品として提供されています。詳細については、次のリンクを参照してください。

  Cisco Secure Endpoint

ストレージ

本ドキュメントで前述したNetAppのランサムウェア対策ソリューションは、セキュアなFlexPod環境の構築に活用できます。次のセクションでは、ワークロードセキュリティ機能について詳しく説明します。

FlexPodのCloud Insights

前述したように、Cloud InsightsはNetAppクラウドサービスであり、ワークロードセキュリティはCloud Insightsの機能です。プレミアムエディションでは、Cloud Insightsのすべての機能も利用できます。Cloud Insightsを使用すると、NetApp ONTAP、NetApp Cloud Volumes ONTAP、Amazon FSx for NetApp ONTAP、VMware vCenter、Cisco MDSスイッチ、Cisco Nexusスイッチ、ファイバチャネルサービスを実行するUCSファブリックインターコネクトなど、さまざまなデータコレクタからインベントリとパフォーマンスのデータを収集できます。カスタムダッシュボードを作成して、収集したデータを表示したり、レポートを生成したりできます。Cloud Insightsの監視機能とレポート機能については、本ドキュメントでは説明していません。ただし、 詳細については、TR-4868：『NetApp Cloud Insights for FlexPod』を参照してください。

FlexPodでのワークロードセキュリティの設定

ワークロードセキュリティエージェントマシンは、FlexPod環境内または外部にインストールできます。ただし、Cloud Insights SaaS環境およびFlexPod環境のデータコレクタへのIP接続が確立されている必要があります。ここでは、ワークロードセキュリティエージェントとデータコレクタを設定する手順を示します。

1. Linux VMにWorkload Security Agentをインストールしてデータを収集します。
2. アクティブディレクトリからユーザ属性を収集するようにユーザディレクトリコレクタを設定します（オプション）。
3. データコレクタを設定します。
4. 自動応答ポリシーを定義して、攻撃が発生した場合に自動的に対処します。
5. アラートのEメール通知を設定します。

VMにワークロードセキュリティエージェントをインストールしてデータを収集する

データコレクタからユーザアクティビティとファイルアクティビティを取得するには、エージェントをインストールする必要があります。ワークロードセキュリティエージェントは、Cloud Insights Acquisition Unitと同じマシンにインストールできます。ただし、これらは別のマシンにインストールすることを推奨します。ワークロードセキュリティエージェントを実行している単一のVMでは、最大50のデータコレクタを監視できます。

Agent Machineの要件

エージェントをインストールする前に、表3に示すように、環境がオペレーティングシステム、CPU、メモリ、およびディスクスペースを満たしていることを確認します。

表3）エージェントの要件

タイプ	コメント
オペレーティング システム	Linuxのライセンスバージョン （*Red Hat Enterprise Linux 7.x、8.x 64ビット、CentOS 7.x 64ビット、CentOS 8 Stream、またはUbuntu 20~22 64ビット*）。 **注：** SE（Security Enhanced）Linuxはサポートされていません。
CPU	4 CPU Cores
メモリ	16GB RAM
ディスクスペース	/opt/netapp 35GB（最小）
ネットワーク	100Mbps~1Gbpsのイーサネット接続、静的IPアドレス、すべてのデバイスへのIP接続、ワークロードセキュリティインスタンスへの必要なポート（80または443）。

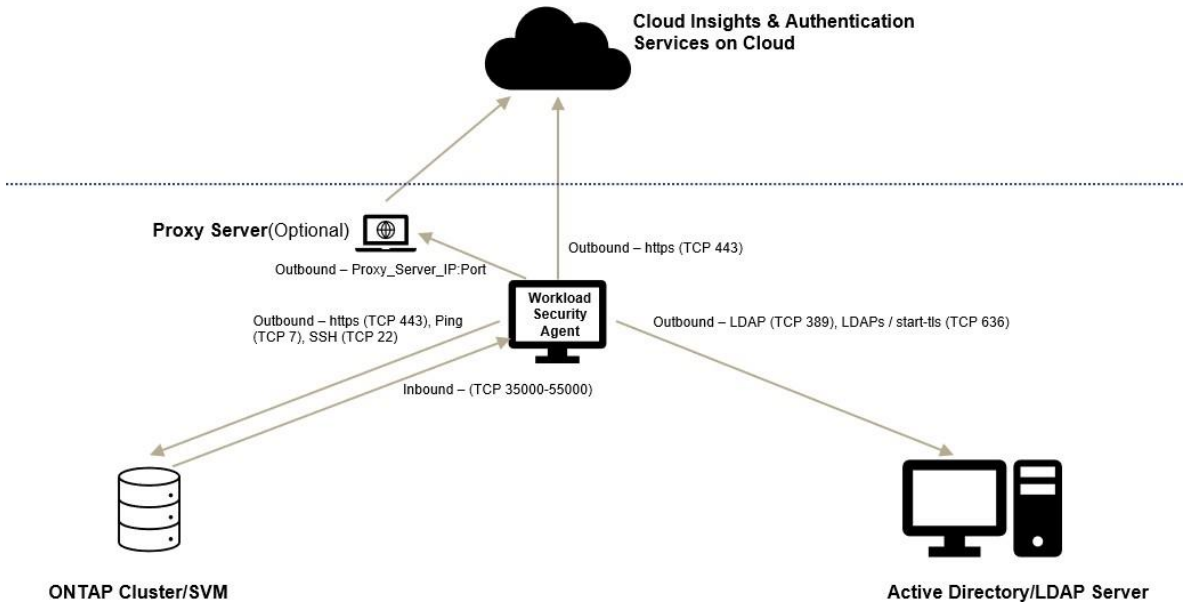
注： ワークロードセキュリティエージェントとCloud Insights Acquisition Unitが同じマシンにインストールされている場合は、50~55GB以上の空きディスクスペースが必要です（/opt/netappの場合は25~30GB、/var/log/netappの場合は25~30GB）。

注： ネットワークタイムプロトコル（NTP）または簡易ネットワークタイムプロトコル（SNTP）を使用して、ONTAPシステムとエージェントマシンの両方の時刻を同期することを強く推奨します。

インバウンドとアウトバウンドのアクセスルール

ワークロードセキュリティエージェントがCloud Insights SaaS環境およびデータコレクタに接続するには、エンドポイントとその間のネットワークファイアウォールで特定のポートを開く必要があります。エンドポイントとポートを下図に示します(図4)。

図4）クラウドとネットワーク内のルール



組織のセキュリティポリシーでTCP 35000-55000のように幅広いポートを開くことが許可されていない場合は、TCP 35000-35100などのより小さな範囲を設定できます。各SVMに2つのTCPポートが必要であることに注意してください。

次の表を参照して、必要なTCPポートを開くことができます。

クラウドネットワークアクセスルール

クラウドネットワークアクセスルールは、ワークロードセキュリティエージェントをクラウドでホストされるCloud Insights SaaS環境に接続することを目的としています。Cloud Insights環境が存在する地域に基づいてアクセス制御リスト(ACL)を開くには、次の表を参照してください(表 4、表5 、および 表6)。

表4）米国ベースのワークロードセキュリティ環境

プロトコル	ポート	デスティネーション	方向	説明
TCP	443	<site_name>.cs01.cloudinsights.netapp.com <site_name>.c01.cloudinsights.netapp.com <site_name>.c02.cloudinsights.netapp.com	アウトバウンド	Cloud Insightsへのアクセス
TCP	443	gateway.c01.cloudinsights.netapp.com agentlogin.cs01.cloudinsights.netapp.com	アウトバウンド	認証サービスへのアクセス

表5）ヨーロッパベースのワークロードセキュリティ環境

プロトコル	ポート	デスティネーション	方向	説明
TCP	443	<site_name>.cs01-eu-1.cloudinsights.netapp.com <site_name>.c01-eu-1.cloudinsights.netapp.com <site_name>.c02-eu-1.cloudinsights.netapp.com	アウトバウンド	Cloud Insightsへのアクセス
TCP	443	gateway.c01.cloudinsights.netapp.com agentlogin.cs01-eu-1.cloudinsights.netapp.com	アウトバウンド	認証サービスへのアクセス

表6）APACベースのワークロードセキュリティ環境

プロトコル	ポート	デスティネーション	方向	説明
TCP	443	<site_name>.cs01-ap-1.cloudinsights.netapp.com <site_name>.c01-ap-1.cloudinsights.netapp.com <site_name>.c02-ap-1.cloudinsights.netapp.com	アウトバウンド	Cloud Insightsへのアクセス
TCP	443	gateway.c01.cloudinsights.netapp.com agentlogin.cs01-ap-1.cloudinsights.netapp.com	アウトバウンド	認証サービスへのアクセス

インネットワークアクセスルール

ネットワーク内アクセスルールは、ワークロードセキュリティエージェントとデータコレクタ間の通信を目的としています。ネットワークおよびデータコレクタでACLを開く場合は、表7を参照してください。

表7）ネットワーク内のルール

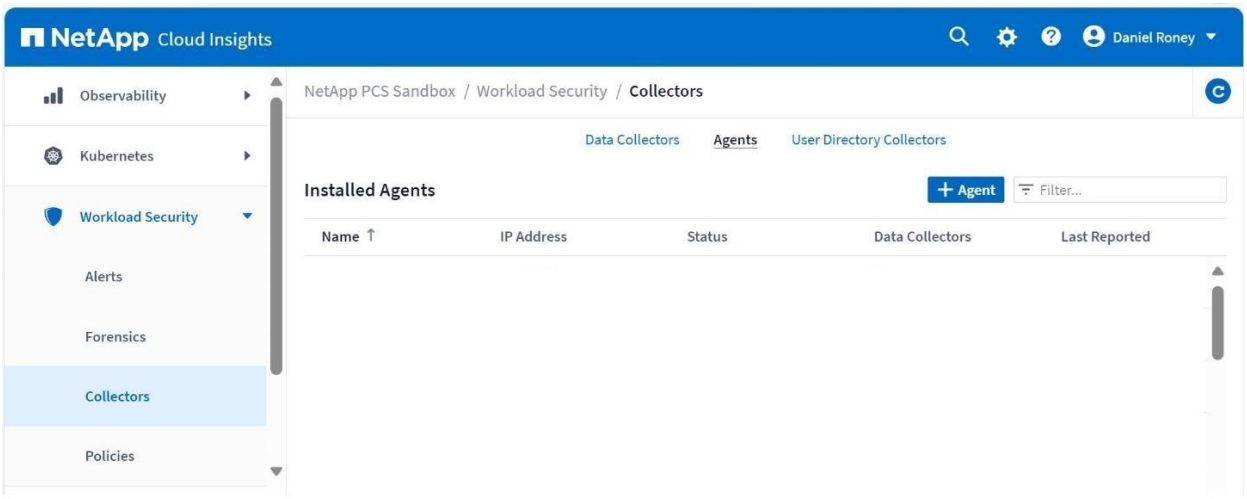
プロトコル	ポート	デスティネーション	方向	説明
TCP	389（LDAP） 636（LDAPS / START-TLS）	LDAP Server URL	アウトバウンド	LDAP に接続
TCP	443	クラスタまたはSVMの管理IPアドレス（SVMコレクタの設定によって異なる）	アウトバウンド	ONTAP との API 通信
TCP	35000-55000	SVM data LIF IP Addresses	インバウンド	FPolicyイベントのためのONTAPとの通信

プロトコル	ポート	デスティネーション	方向	説明
TCP	7	SVM data LIF IP Addresses	アウトバウンド	ワークロードセキュリティエージェントとONTAP間の単方向。エージェントがSVM LIFにpingを送信します。
SSH	22	クラスタ管理	アウトバウンド	CIFS / SMBユーザブロッキングの場合。

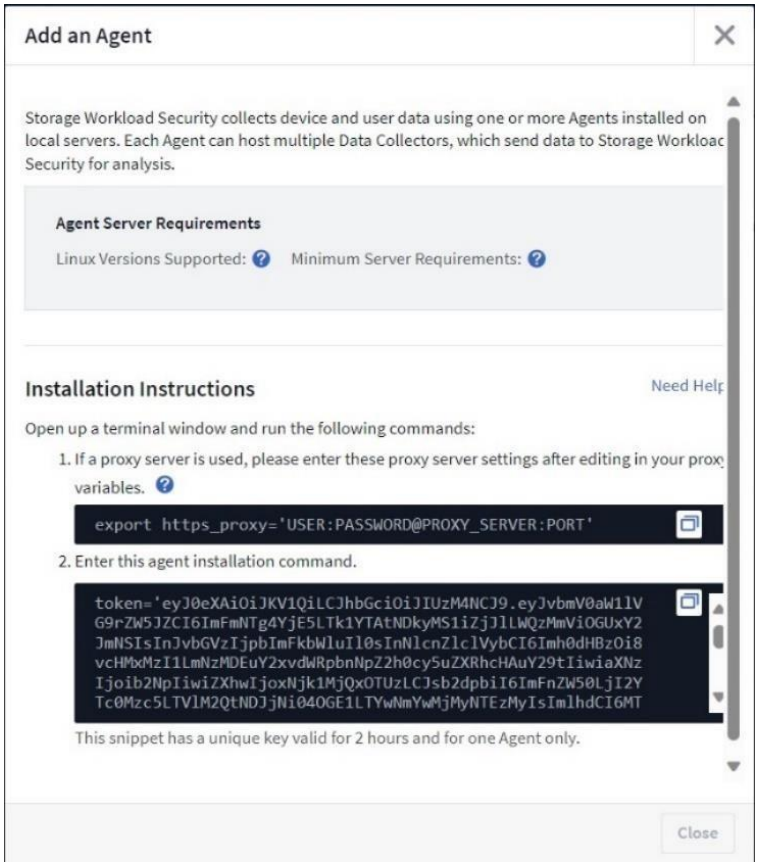
ワークロードセキュリティエージェントの設定手順

FlexPodのラボセットアップでは、CentOS 8ストリームベースのLinux VMに2つのワークロードセキュリティエージェントを設定します。1つはONTAP SVMデータコレクタを監視し、もう1つはActive Directoryユーザデータコレクタを監視します。エージェントをインストールするには、次の手順を実行します。

1. 管理者またはアカウント所有者としてCloud Insights環境にログインします。
2. 左側のペインで[Workload Security]メニューを展開し、 リストから[Collectors]を選択します。右側のペインの[エージェント]タブをクリックします。



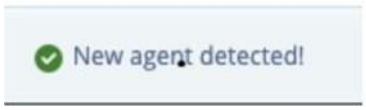
3. **[+ Agent]**をクリックします。次に示すように、**[エージェントの追加]**ページが表示されます。



4. **[?]**をクリックします。アイコンをクリックして、エージェントが最小システム要件を満たしていること、およびエージェントサーバがサポートされているバージョンのLinuxを実行していることを確認します。

ネットワークでプロキシサーバを使用している場合は、プロキシサーバの詳細を推奨事項に従って設定します。

5. ターミナルウィンドウを開き、上記の図のインストール手順に従って手順を実行します。
6. インストールが正常に完了すると、「新しいエージェントが検出されました！」というポップアップメッセージが表示されます。



次の例に示すように、エージェントサーバコンソールがサービスを開始します。

```
Starting CloudSecure Agent services.
                    Welcome to CloudSecure (R) 1.531.0
                    Agent

                     ___   ____
                    / __|  |  __|
                   | |     |_|__
                   | |__    __| |
                    \___|  |____|
  NetApp (R)

  Installation:       /opt/netapp/cloudsecure/agent
  Installation logs:  /var/log/netapp//cloudsecure/install
  Agent Logs:         /opt/netapp/cloudsecure/agent/logs

  To uninstall:
    sudo cloudsecure-agent-uninstall.sh --help
[admin@fp-cloud-secure-1 ~]$
```

7. 次の例に示すように、エージェントVMのワークロードセキュリティサービスのステータスを確認できます。

```
[admin@fp-cloud-secure-1 ~]$ sudo systemctl status cloudsecure-agent.service
[sudo] password for admin:
● cloudsecure-agent.service - Cloud Secure Agent Daemon Service
   Loaded: loaded (/usr/lib/systemd/system/cloudsecure-agent.service; enabled;
   Active: active (running) since Thu 2023-01-12 14:17:22 EST; 6 days ago
 Main PID: 1194 (java)
    Tasks: 77 (limit: 100910)
   Memory: 2.0G
   CGroup: /system.slice/cloudsecure-agent.service
           ├─ 1194 java -Dconfig.file=/opt/netapp/cloudsecure/agent/conf/applic
           └─96244 java -Dconfig.file=/opt/netapp/cloudsecure//data-collectors/

Jan 17 21:53:34 fp-cloud-secure-1 bash[1194]: Warning:
Jan 17 21:53:34 fp-cloud-secure-1 bash[1194]: The JKS keystore uses a proprieta
Jan 17 21:53:34 fp-cloud-secure-1 bash[1194]: Importing keystore /opt/netapp/cl
Jan 17 21:53:34 fp-cloud-secure-1 bash[1194]: [Storing /opt/netapp/cloudsecure/
Jan 17 21:53:34 fp-cloud-secure-1 bash[1194]: Certificate was added to keystore
Jan 17 21:53:34 fp-cloud-secure-1 bash[1194]: [Storing /opt/netapp/cloudsecure/
Jan 17 21:53:34 fp-cloud-secure-1 bash[1194]: Certificate was added to keystore
Jan 17 21:53:34 fp-cloud-secure-1 bash[1194]: [Storing /opt/netapp/cloudsecure/
Jan 17 21:53:36 fp-cloud-secure-1 bash[1194]: Warning: Nashorn engine is planne
Jan 17 21:53:36 fp-cloud-secure-1 bash[1194]: Warning: Nashorn engine is planne

[admin@fp-cloud-secure-1 ~]$
```

8. プロンプトで次のコマンドを実行して、ワークロードセキュリティで使用されるポートを開きます。

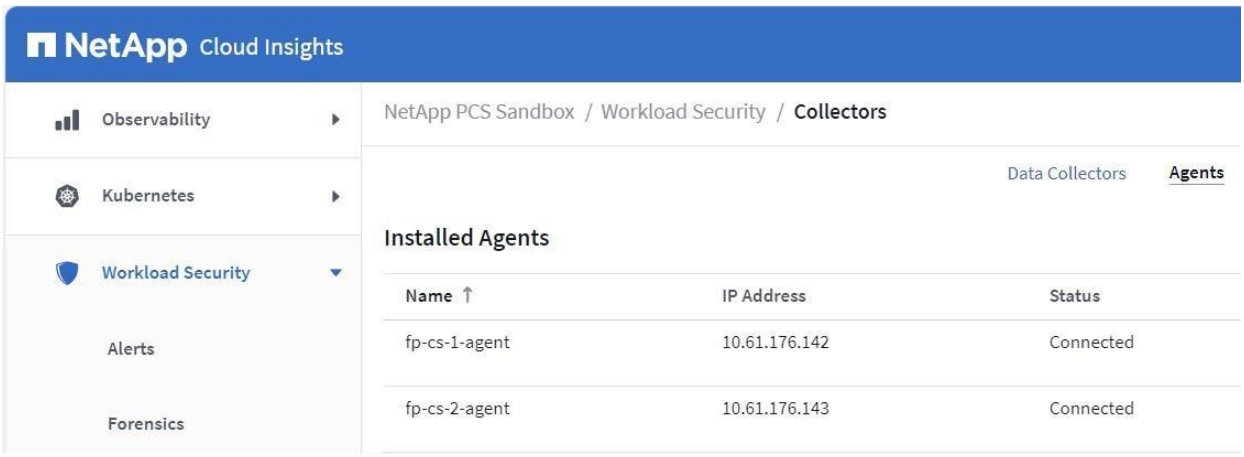
```
sudo firewall-cmd --permanent --zone=public --add-port=35000-55000/tcp

sudo firewall-cmd -reload
```

注： 各SVMは2つのポートを使用し、ワークロードセキュリティデータベースには複数のポートが必要であるため、セキュリティ上の懸念がある場合は、35000：35100以上の範囲を指定することを推奨します。

9. 問題次のコマンドを実行して、上記で設定した範囲に基づいて、開いているポートを確認します。

```
sudo firewall-cmd --zone=public --list-ports | grep 35000
```

10. 必要に応じて、手順2～6を繰り返して追加のエージェントをインストールします。
11. エージェントのステータスを確認するには、**[Workload Security]>[Collectors]**の順にクリックし、**[Agents]** タブを選択します。



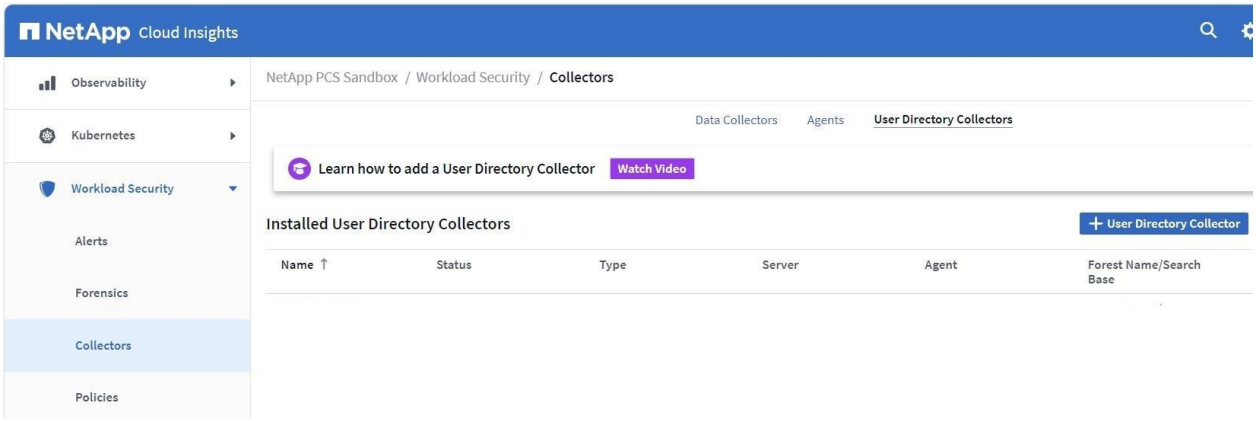
ユーザディレクトリコレクタの設定

この手順では、ユーザ環境にActive Directoryサーバがすでに存在し、ユーザディレクトリコネクタを設定するためのIPアドレスとフォレスト情報があることを前提としています。この手順の前に、ワークロードセキュリティエージェントを設定する必要があります。このタスクは、Cloud Insights管理者またはアカウント所有者が実行できます。

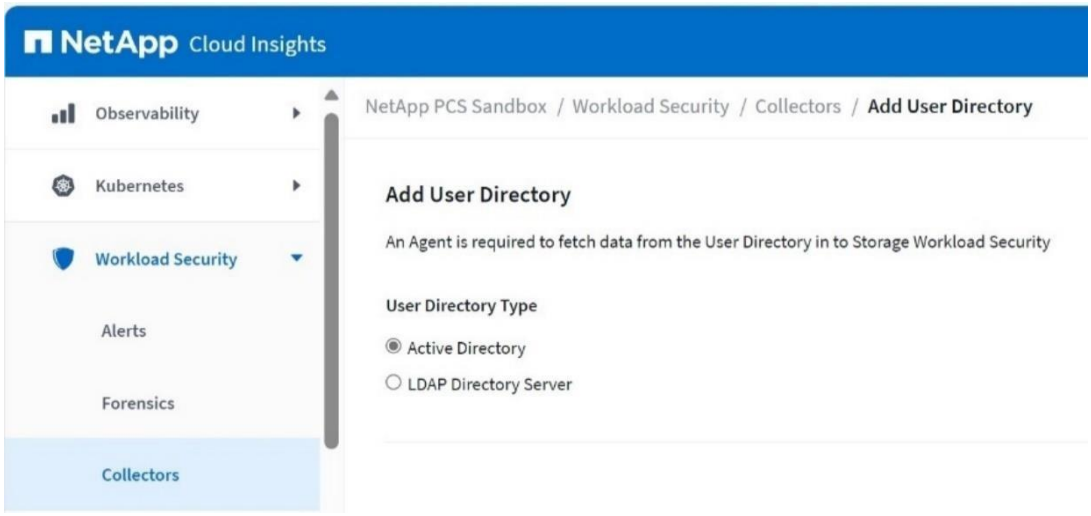
ユーザディレクトリコレクタの設定手順

手順に従って、ユーザディレクトリコレクタを設定します。

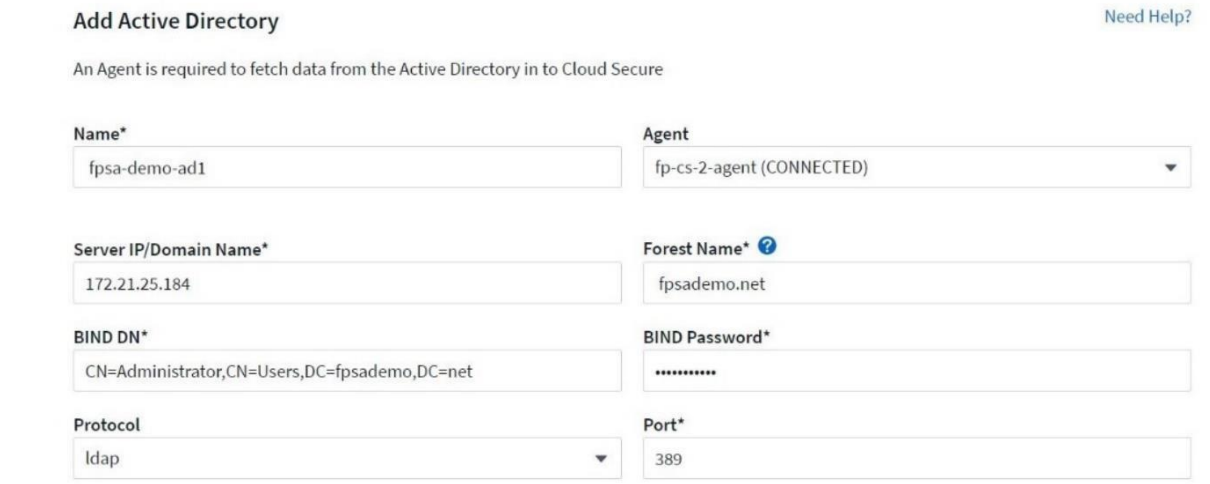
1. Cloud Insightsメニューで、**Workload Security > Collectors > User Directory Collectors> + User Directory Collector**をクリックします。



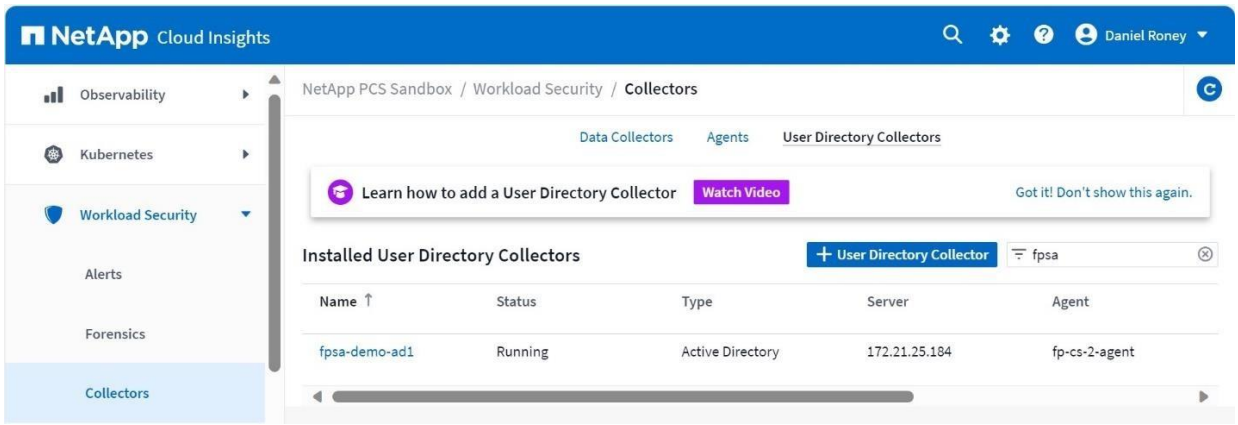
2. **[Add User Directory]** 画面が表示されます。**[Active Directory]**を選択し、**[Continue]**をクリックします。



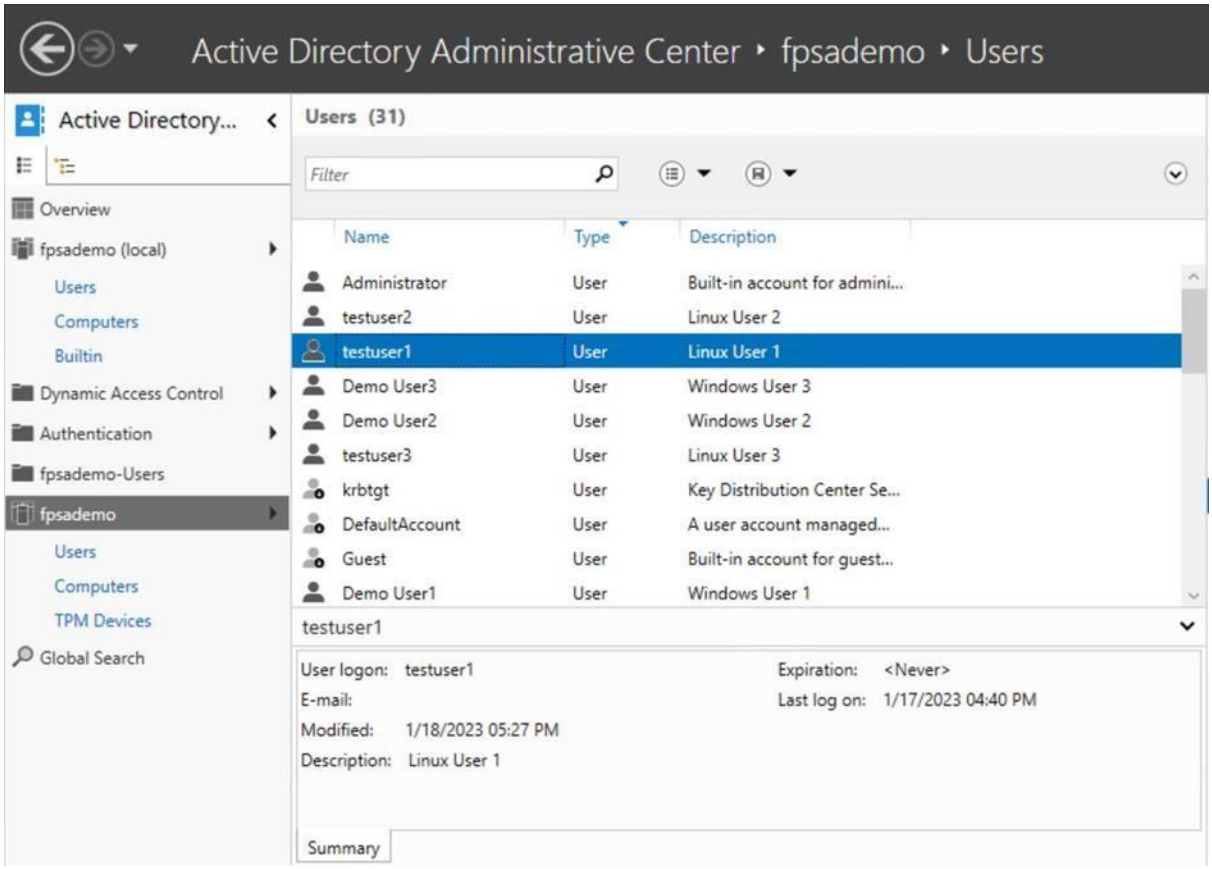
3. 以前にインストールしたエージェントを選択し、残りのフィールドに値を入力します。オプションの属性はデフォルト値のままにしておくことができます。**[Save]**をクリックして、ユーザディレクトリコレクタを追加します。



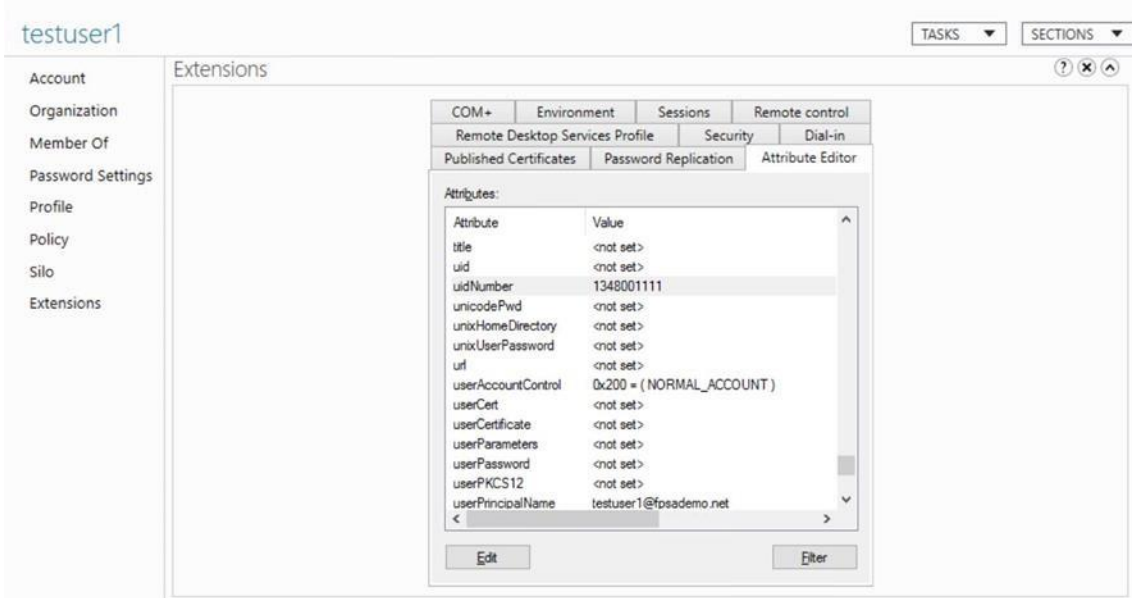
4. コレクタが **running** 状態であることを確認します。



デモ環境では、WindowsおよびLinuxユーザを認証するようにActive Directoryサーバを設定します。次の例は、Active Directoryで設定されているユーザを表示します。



エンコードされたユーザ名ではなくCloud Insightsにユーザ名を表示するには 、次のように各Linuxユーザのの**Active Directory**でuid属性を設定します。この例は、 **testuser1を示してい**ます。



注：LDAPサーバがある場合は、LDAPディレクトリコレクタとしてワークロードセキュリティに追加できます。手順は、Active Directoryの追加と同じです。詳細については、次のリンクを参照してください。

LDAP Directory Server Collectorの設定

ONTAPデータコレクタの設定

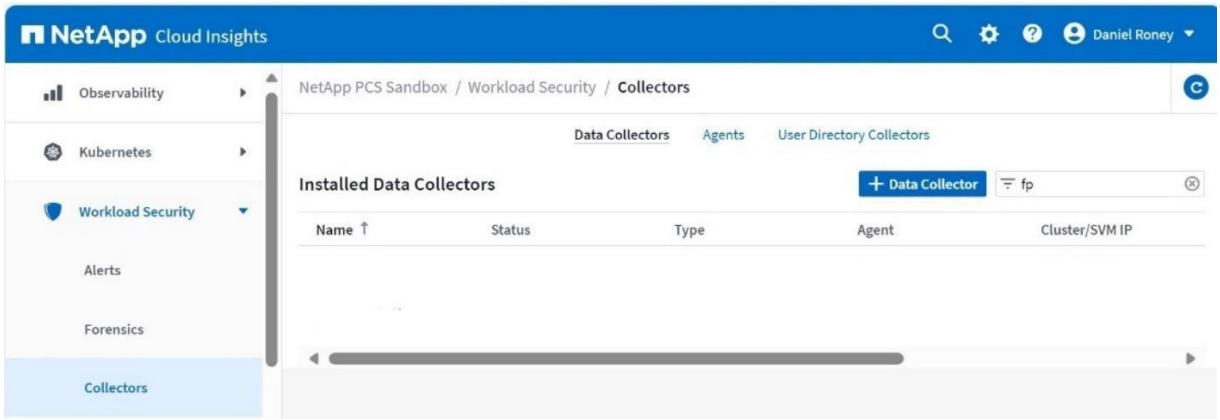
ワークロードセキュリティは現在、NetApp ONTAP SVM、NetApp Cloud Volumes ONTAP、Amazon FSx for NetApp ONTAPの3種類のONTAPデータコレクタをサポートしています。本ドキュメントでは、NetApp ONTAP SVMデータコレクタの評価を中心に説明します。

FlexPodトポロジでは、NFSプロトコルを使用する「CI_SVM」とCIFS / SMBを使用する「CI_CIFS_SVM」の2つのSVMがワークロードセキュリティデータコレクタとして設定されています。現在、NFSプロトコル4.0以前とSMBプロトコル3.1以前がサポートされています。

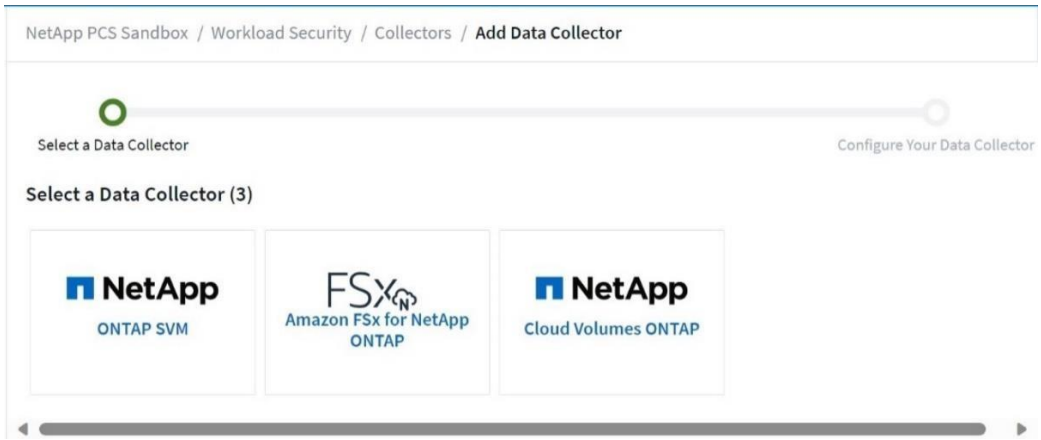
SVMデータコレクタの設定手順

手順に従って、2つのSVMデータコレクタを設定します。1つはCIFS / SMBプロトコル用に設定されたSVM、もう1つはNFSプロトコル用に設定されたSVMです。

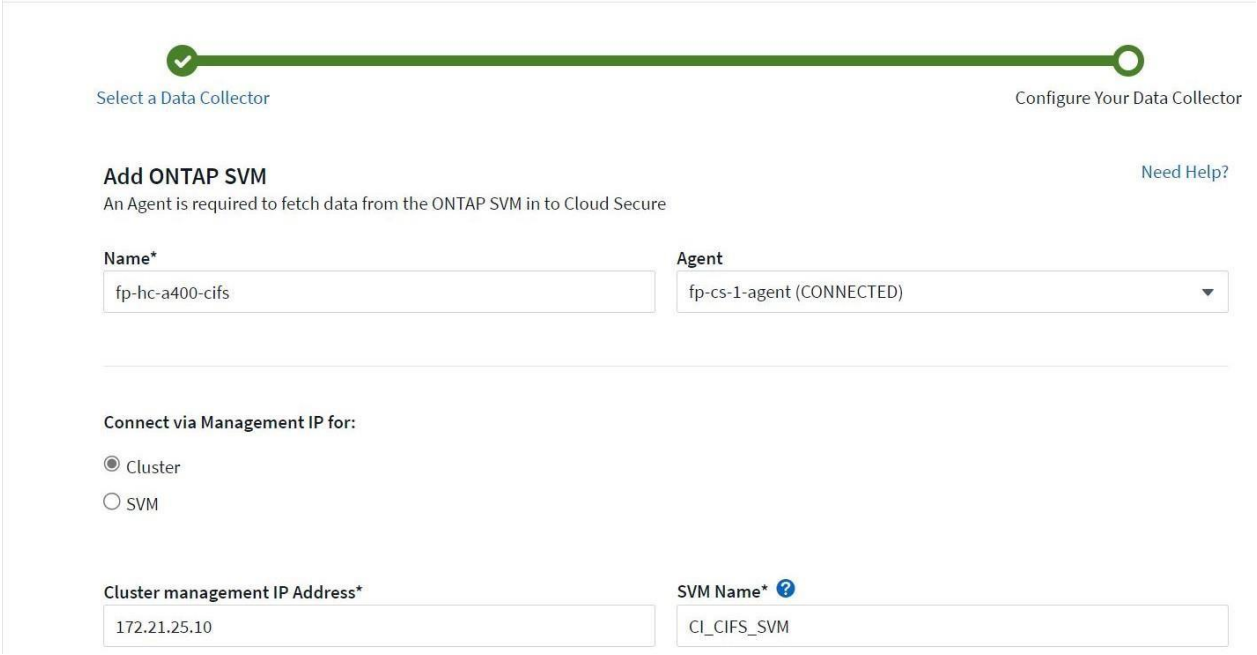
1. Cloud Insights環境に管理者またはアカウント所有者としてログインします。
2. **[Workload Security]>[Collectors]>[Data Collectors]>[+Data Collector]**をクリックします。



使用可能なデータコレクタが表示されます。NetApp ONTAP SVMデータコレクタを選択します。

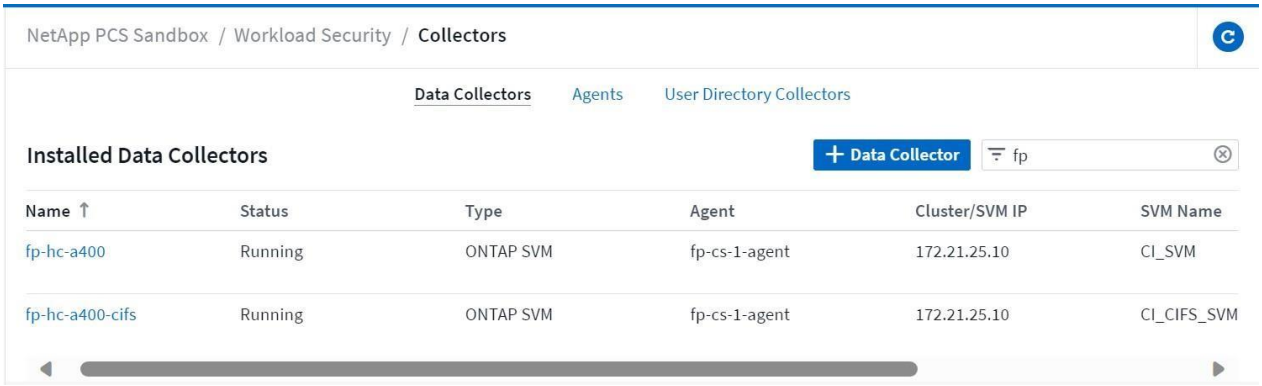


3. [SVM SVM]タイルにカーソルをNetApp合わせ、***[+Monitor]**をクリックします。ONTAP SVMの設定ページが表示されます。各フィールドに必要なデータを入力し、**[Save]**をクリックします。



メモ：クラスタ管理IPを使用してSVMを追加する場合は、SVMのデータLIFと管理LIFがエージェントVMからping可能であることを確認してください。LIFのゲートウェイ、ネットマスク、およびルートに問題がないかを確認してください。

4. 手順を繰り返して2つ目のSVM（ci_svm）を追加し、[NFS]プロトコルを選択します。
5. **[Workload Security]>[Collectors]>[Data Collectors]**をクリックして、データコレクタが **[Running]** 状態であることを確認します。



6. NetAppストレージにログインし、`<fpolicy show>` コマンドを問題します。このコマンドは、監視対象の各SVMのポリシーエンジンの名前とステータスを表示します。ステータスが「on」であることを確認します。

```
A400-G0312::>   fpolicy show
  (vserver fpolicy show)
                                        Sequence
Vserver       Policy Name               Number  Status   Engine
------------- ------------------------ --------  -------- ---------
CI_CIFS_SVM   cloudsecure_CI_CIFS_           1  on       cloudsecu
              SVM1_policy                                re_CI_
                                                         CIFS_
                                                         SVM1_
                                                         engine
CI_CIFS_SVM   cloudsecure_CI_CIFS_           2  on       cloudsecu
              SVM2_policy                                re_CI_
                                                         CIFS_
                                                         SVM2_
                                                         engine
CI_SVM        cloudsecure_CI_SVM3_           1  on       cloudsecu
              policy                                     re_CI_
                                                         SVM3_
                                                         engine
CI_SVM        cloudsecure_CI_SVM4_           2  on       cloudsecu
              policy                                     re_CI_
                                                         SVM4_
                                                         engine
4 entries were displayed.
```

7. 問題 <fpolicy show-engine> コマンドを使用して、各ノードのFPolicyサーバのステータスを確認します。

```
A400-G0312::> fpolicy show-engine
  (vserver fpolicy show-engine)
                                 FPolicy          Server         Server
Vserver Policy Name   Node       Server           Status         Type
------- ------------- ---------- ---------------- -------------- -----------
CI_CIFS_SVM                                       connected      primary
        cloudsecure_  A400-G0312- 10.61.176.142
        CI_CIFS_SVM1_ 01
        policy
CI_CIFS_SVM                                       connected      primary
        cloudsecure_  A400-G0312- 10.61.176.142
        CI_CIFS_SVM2_ 01
        policy
CI_SVM  cloudsecure_  A400-G0312- 10.61.176.142   connected      primary
        CI_SVM3_      01
        policy
CI_SVM  cloudsecure_  A400-G0312- 10.61.176.142   connected      primary
        CI_SVM4_      01
        policy
CI_CIFS_SVM                                       connected      primary
        cloudsecure_  A400-G0312- 10.61.176.142
        CI_CIFS_SVM1_ 02
        policy
CI_CIFS_SVM                                       connected      primary
        cloudsecure_  A400-G0312- 10.61.176.142
        CI_CIFS_SVM2_ 02
        policy
CI_SVM  cloudsecure_  A400-G0312- 10.61.176.142   connected      primary
        CI_SVM3_      02
        policy
CI_SVM  cloudsecure_  A400-G0312- 10.61.176.142   connected      primary
        CI_SVM4_      02
        policy
8 entries were displayed.
```

自動応答ポリシーを定義

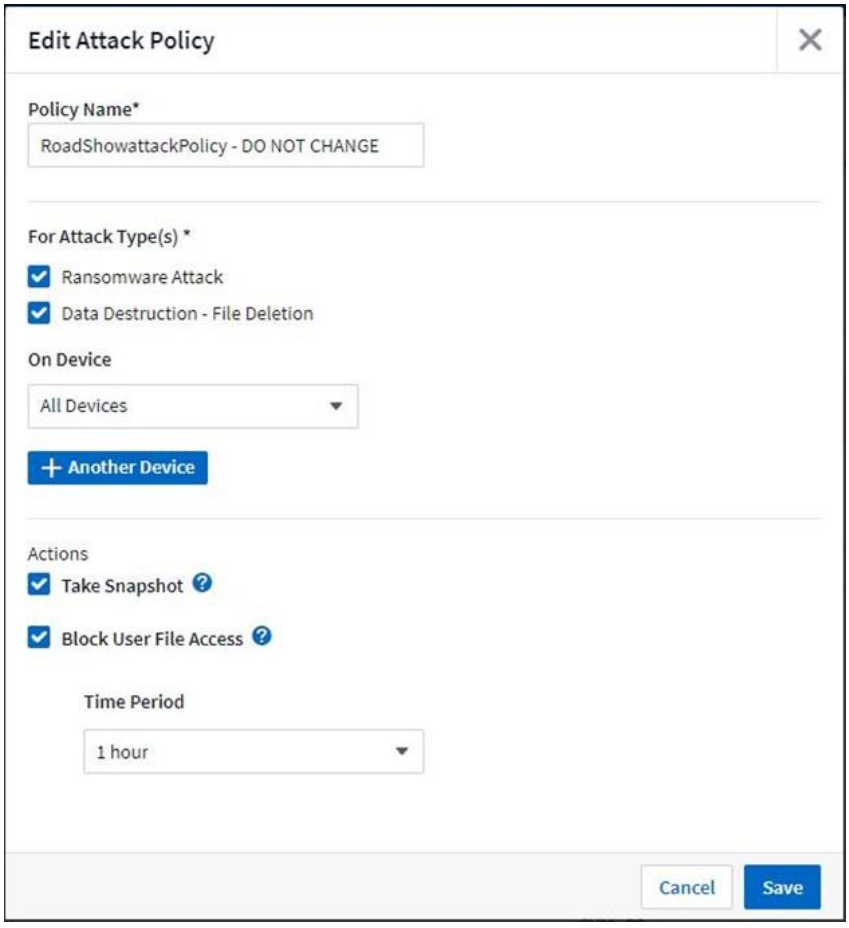
応答ポリシーは、攻撃またはユーザの異常な動作が発生した場合に特定のアクションをトリガーするために使用されます。攻撃または警告のポリシーを作成し、特定のデバイスまたはすべてのデバイスに適用できます。

自動応答ポリシーの設定手順

手順に従って、攻撃ポリシーと警告ポリシーを設定します。

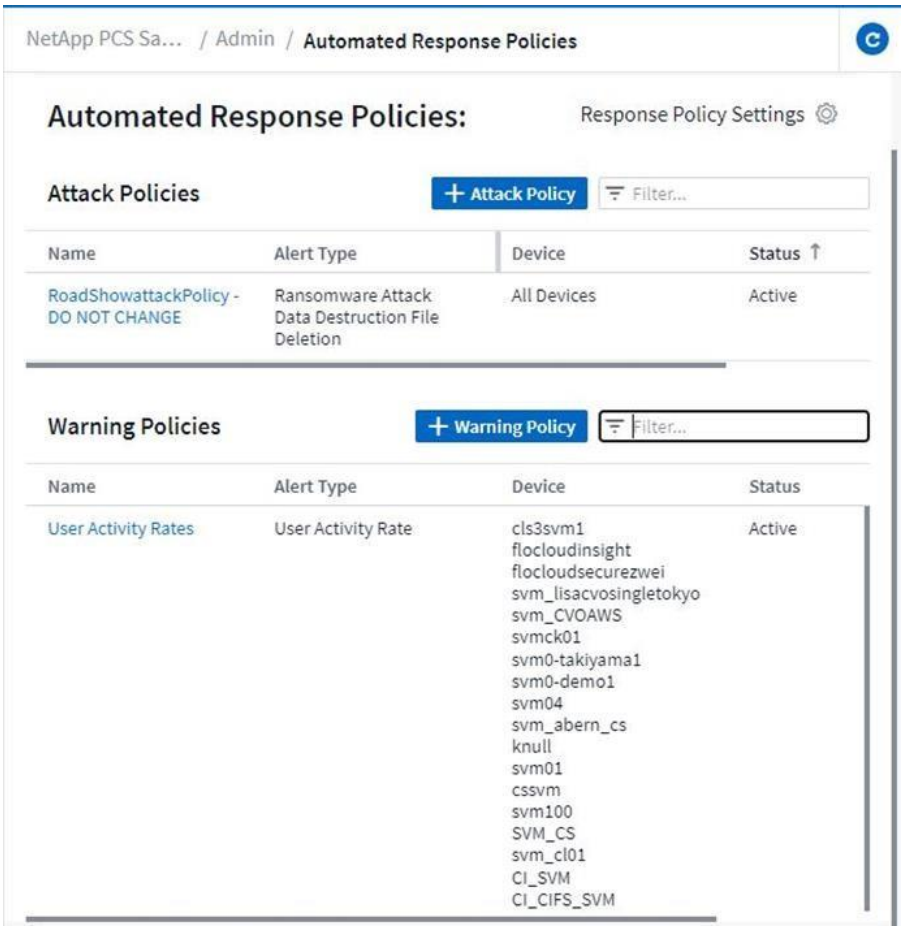
1. 攻撃ポリシーを作成するには、**[Workload Security]>[Policies]>[+Attack Policy]**に移動します。

   攻撃ポリシーの例を次に示します。関連する攻撃の種類とアクション、およびユーザがファイルアクセスを拒否される時間を選択できます。ポリシーは、特定のSVMまたは監視対象のすべてのSVMに適用できます。



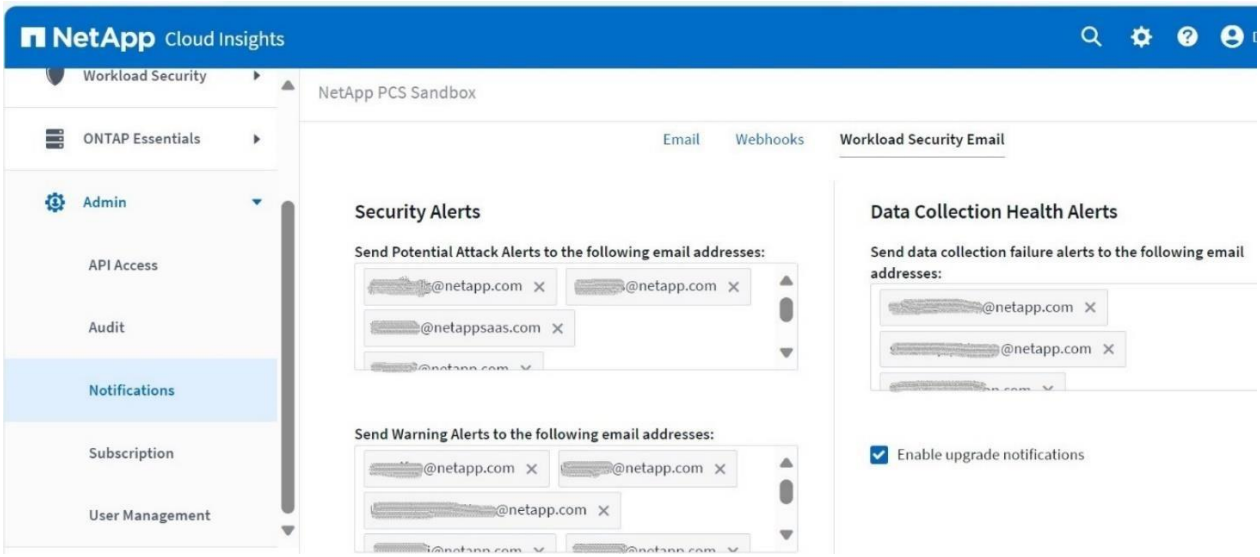
2. 警告ポリシーを作成するには、**[Workload Security]>[Policies]>[+Warning Policy]**を選択します。

   デモ環境での攻撃ポリシーと警告ポリシーを以下に示します。



Eメール通知の設定

電子メール通知は、潜在的な攻撃、警告、およびエージェント/データコレクタの健全性監視用に設定できます。ワークロードセキュリティのアラート受信者を設定するには、**[Admin]>[Notifications]>[Workload Security Email]** に移動し、各受信者の該当するセクションにEメールアドレスを入力します。



ONTAP Autonomous Ransomware Protection（ARP）の統合

ONTAP Autonomous Ransomware Protection（ARP）機能は、NAS（NFSおよびSMB）環境でワークロードを分析し、ランサムウェア攻撃の可能性があるファイル内の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。ワークロードセキュリティを使用して、ONTAPからARPイベントを受信し、次のアクションを実行できます。

- ボリューム暗号化イベントをユーザアクティビティに関連付けて、悪意のあるユーザを特定します。
- Snapshotの作成やユーザのファイルアクセスのブロックなど、自動応答ポリシーによって定義されたアクションを実装します。
- フォレンジック機能を提供：

✓ データ侵害の調査をお客様が実施できるようにします。

✓ 影響を受けたファイルを特定し、迅速なリカバリとデータ侵害の調査を支援します。

ARPはライセンスが必要な機能です。ARPライセンスの詳細については、次のリンクを参照してください。

https://docs.netapp.com/us-en/ontap/anti-ransomware/index.html

前提条件

1. 最新のONTAPリリースとパッチが推奨されます（現在はONTAP 9.13.1P2）。サポートされるONTAPリリースは9.10.1以上です。
2. ARPが有効なボリューム。
3. ワークロードセキュリティコレクタは、クラスタIP経由で追加する必要があります。
4. SVMを追加するときは、クラスタレベルのクレデンシャルを使用する必要があります。

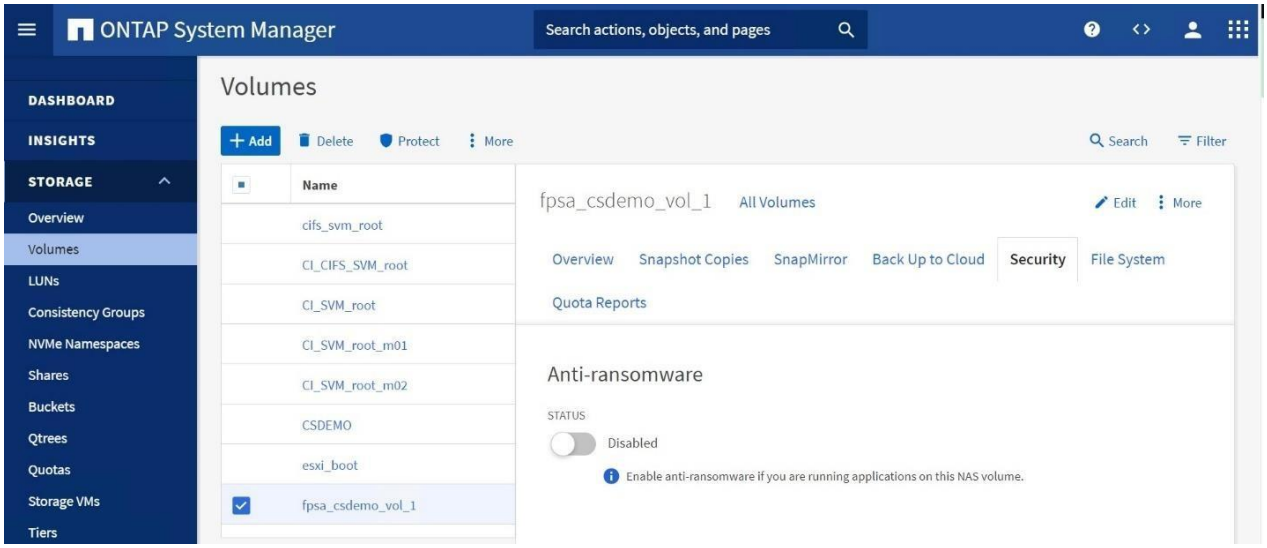
自律型ランサムウェア対策の有効化

ONTAPシステムマネージャまたはONTAP CLIを使用してARPを有効にする必要があります。Cloud Insights / ワークロードセキュリティでARPを有効にできません。有効にすると、アクティブモードに切り替わるまでラーニングモードで動作します。

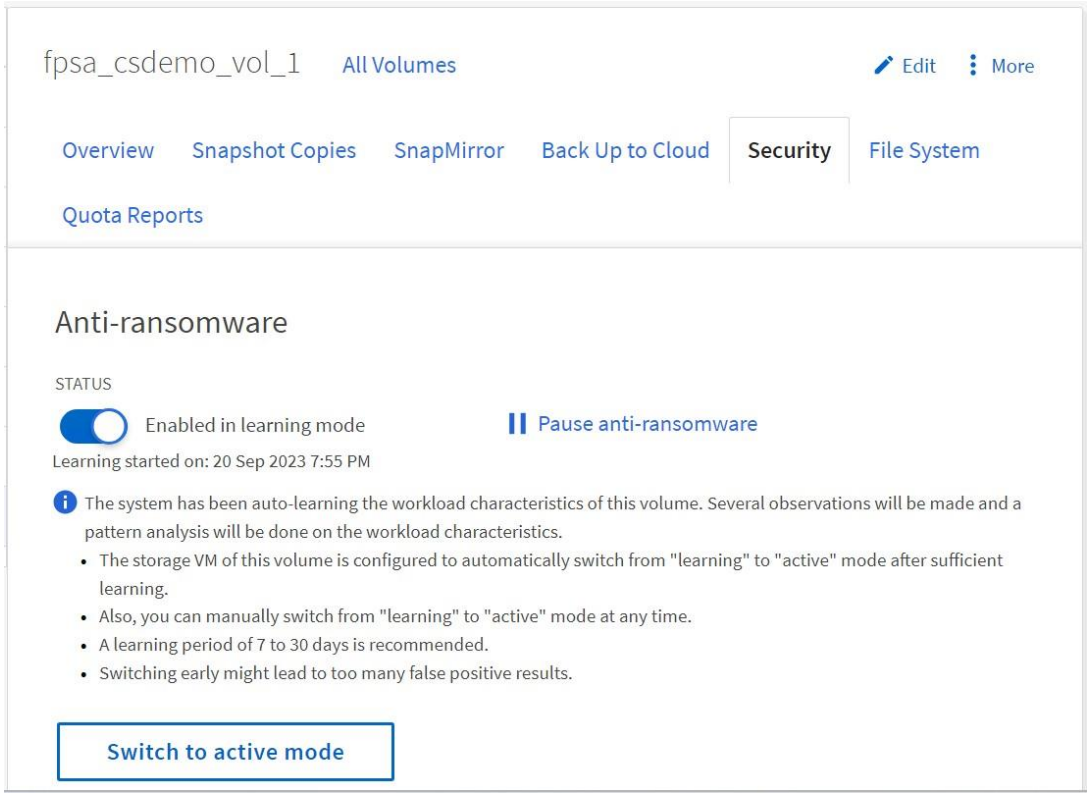
手順：

1. ONTAPシステムマネージャで、**[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[Security]タブで、**[Status]**を選択して、[Anti-ransomware]ボックスで[Disabled]から[Enabled]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。

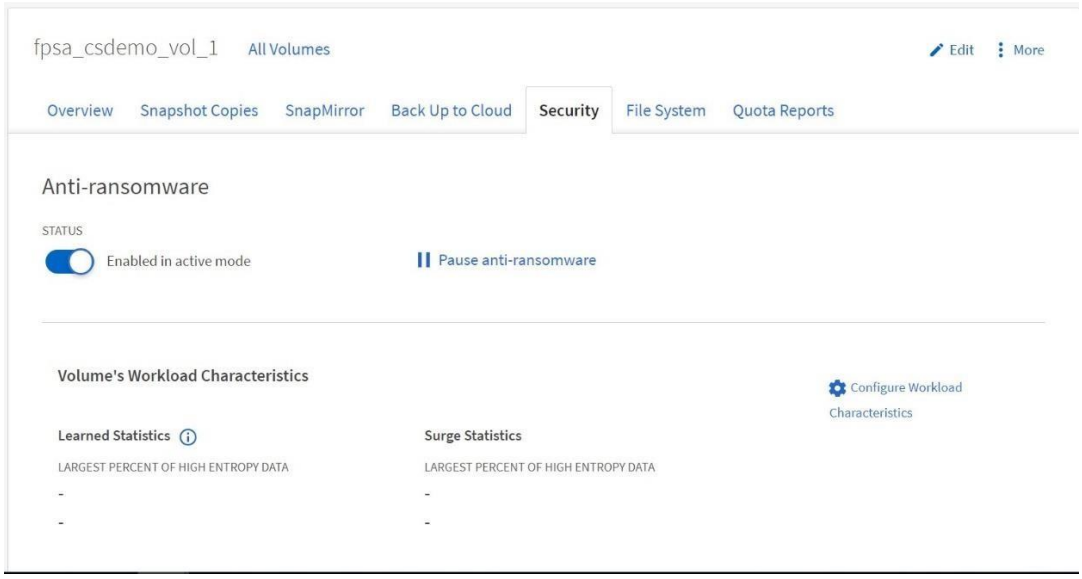
次のスクリーンショットは、ARPを有効にするためのONTAP System Managerユーザインターフェイスを示しています。



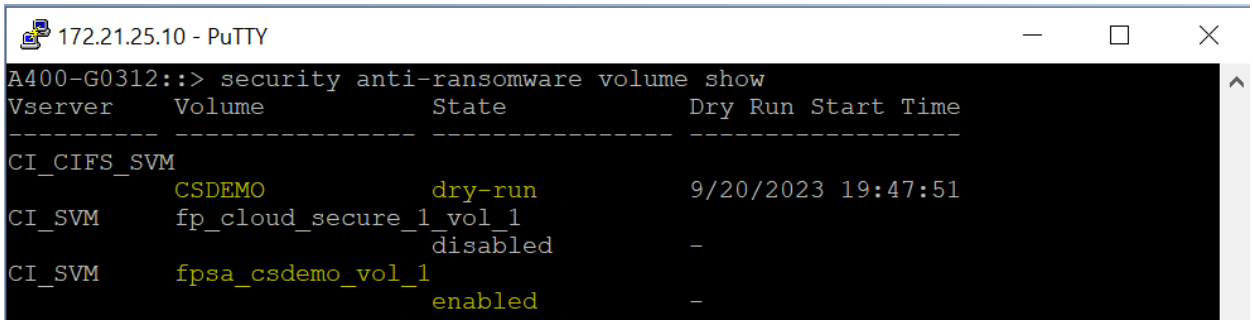
次のスクリーンショットは、ARPがイネーブルでラーニングモードで実行されている場合のARPのステータスを示しています。この画面から、無効化、一時停止、またはアクティブモードに切り替えることができます。



次の画面は、ARPが「active」モードで実行されていることを示しています。



すべてのARPが有効なボリュームのステータスは、次のようにONTAP CLIを使用して確認できます。



GUIまたはCLIを使用したARPのイネーブル化と管理の詳細については、次のリンクを参照してください。

https://docs.netapp.com/us-en/ontap/anti-ransomware/enable-task.html

攻撃検出パラメータの微調整

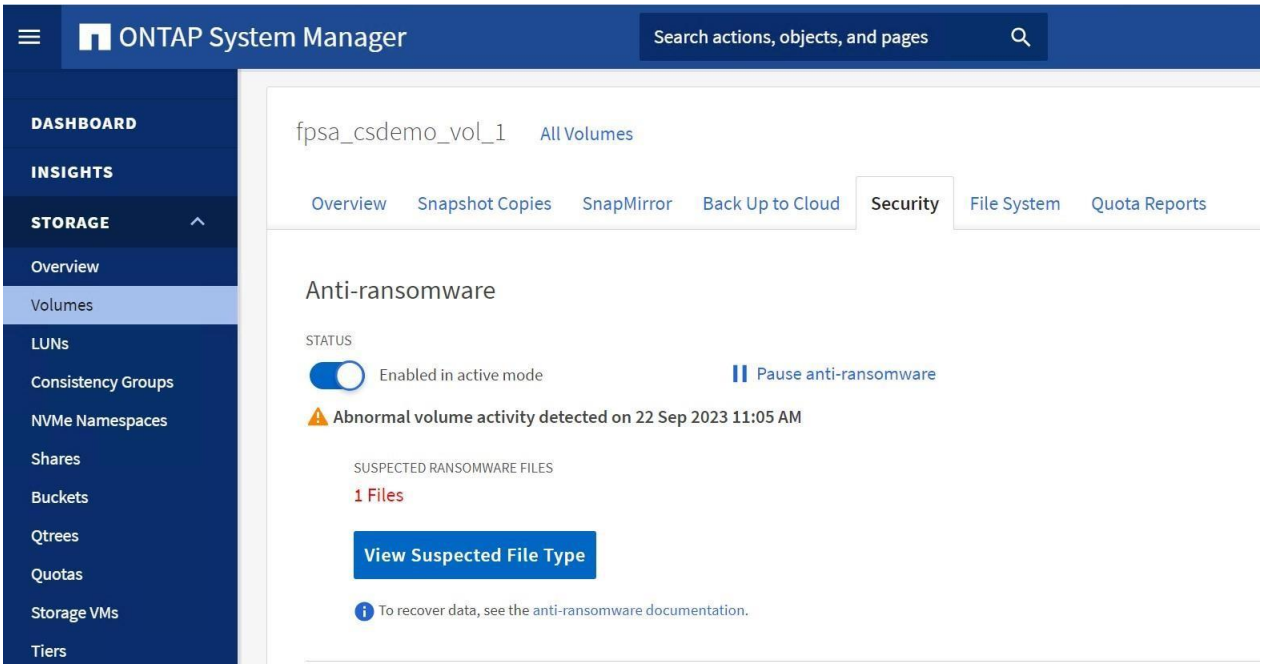
Autonomous Ransomware Protection（ARP）がラーニングモードで実行されている場合、ARPが有効な特定のボリュームのファイルエントロピー、ファイル拡張子、IOPSのベースライン値が開発されます。エントロピーとは、疑わしいファイル操作を決定するためにONTAPがファイル内のデータのランダム性を評価することである。ファイルIOPSは、作成、名前変更、削除されたファイルの数を記録したものです。これらのベースラインは、ARPがアクティブモードに切り替えられたときのランサムウェアの脅威を評価するために使用されます。

ONTAP 9.11.1以降では、特定のARPが有効なボリュームに対するランサムウェア検出のパラメータを変更できます。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。

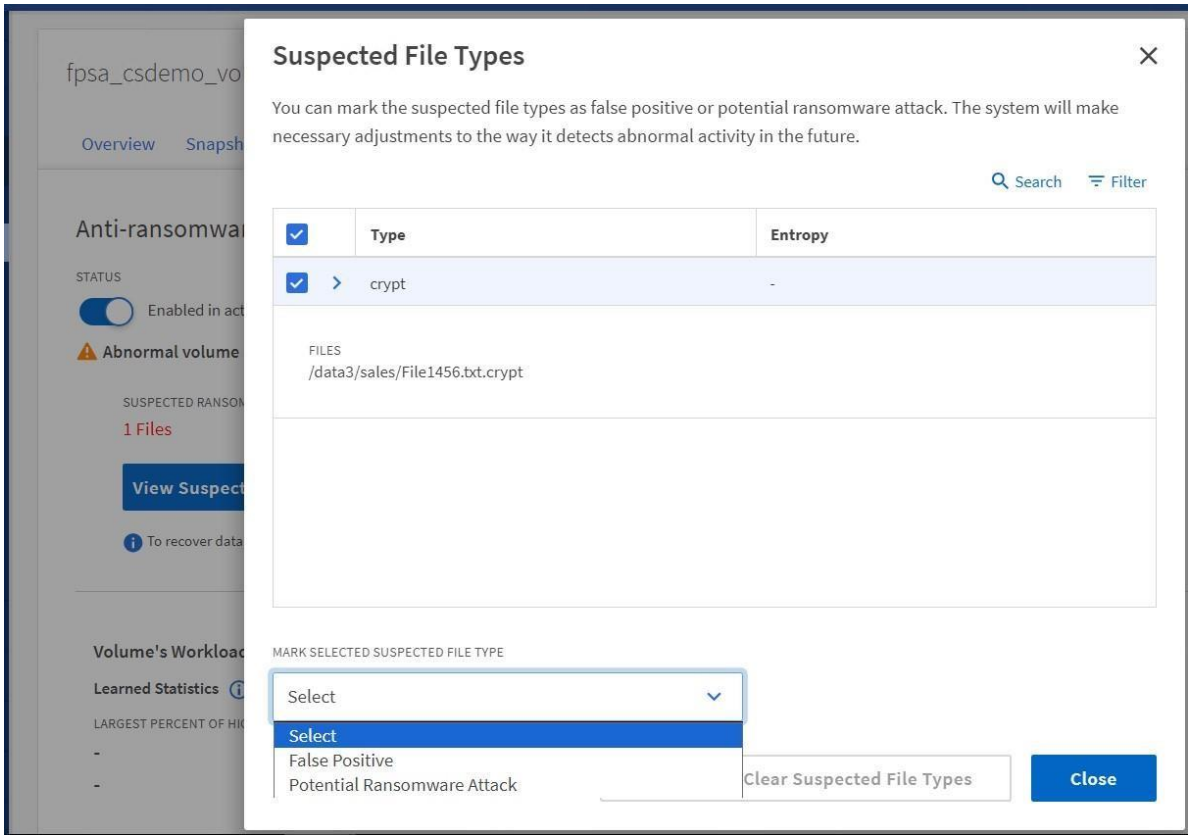
攻撃検出パラメータは、「***security anti-ransomware volume attack-detection-parameters modify***」コマンドを使用して変更できます。次のスクリーンショットは、テスト環境のARP対応ボリュームで有効になっているデフォルトのパラメータを示しています。これらのパラメータは、ボリュームのワークロード固有の要件に合わせて変更できます。

```
172.21.25.10 - PuTTY
A400-G0312::> security anti-ransomware volume attack-detection-parameters show -
vserver CI_SVM -volume fpsa_csdemo_vol_1
                                        Vserver Name : CI_SVM
                                         Volume Name : fpsa_csdemo_vol_1
          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
```

デフォルトでは、never-seen-beforeファイル拡張子の数は20に設定されています。ARPが有効なボリュームでNever-Seen-Beforeファイル拡張子が検出されると、ONTAPは**攻撃の可能性**を**低く**設定します。ボリュームSnapshotは、タグ **Anti-ransoms-backup**を使用してプロアクティブに作成されます。攻撃の可能性は、ファイル拡張子が十分でない場合、またはファイル拡張子と高いエントロピーがアタック検出パラメータで定義されているように、低いままです。攻撃の可能性が低い場合は、イベント管理システムにアラートは送信されませんが、次のようにSystem Managerに警告が表示されます。



管理者は、次の画面に示すように、疑わしいファイルタイプを確認し、System ManagerまたはCLIから誤検知またはランサムウェア攻撃の可能性があるとマークすることができます。false positiveとしてマークされると、新しく検出されたファイル拡張子は有効な拡張子と見なされ、このファイル拡張子に対する今後の攻撃は報告されません。作成されたSnapshotはただちに削除されます。



次のCLIコマンドを使用して、攻撃の可能性を確認したり、ファイル拡張子を確認したりすることもできます。

```
Cluster::> security anti-ransomware volume show -vserver <vserver name> -
volume <volume name>

Cluster::>  security anti-ransomware volume workload-behavior show -vserver <vserver
name> -volume <volume name>
```

疑わしいファイルタイプをfalse positiveとしてマークするには、次のコマンドを使用します。

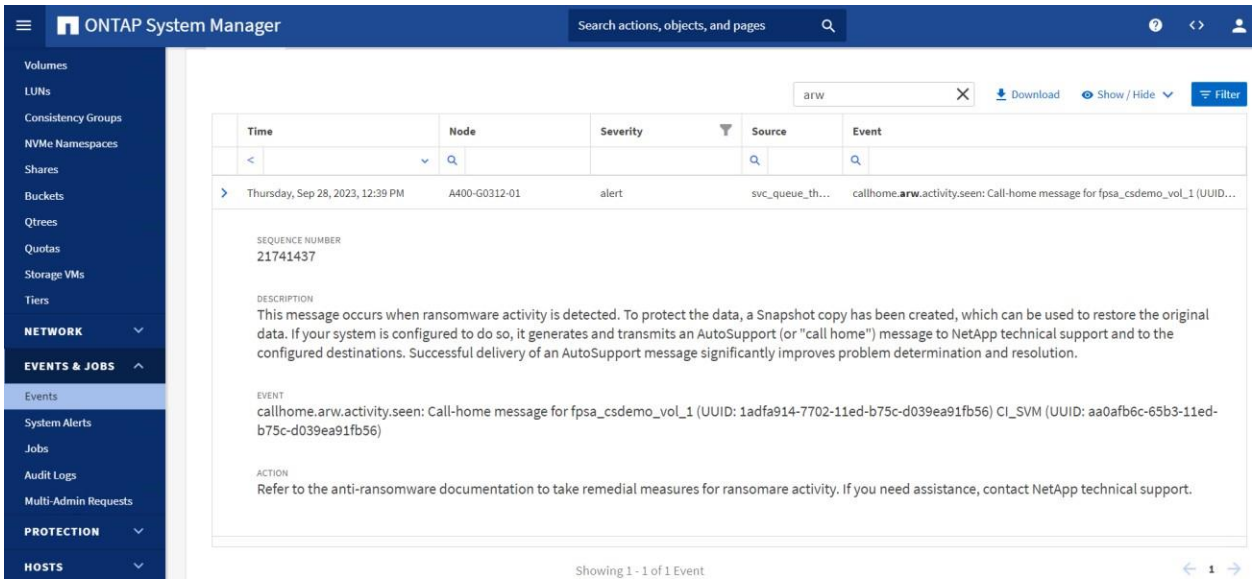
```
Cluster::> security anti-ransomware volume attack clear-suspect -vserver <vserver
name> -volume <volume name> -extensions <extension name> -false- positive
{true|false}
```

次のスクリーンショットは、テスト環境から取得した攻撃の可能性とファイル拡張子の情報を示しています。

```
172.21.25.10 - PuTTY
A400-G0312::>  security anti-ransomware volume show -vserver CI_SVM -volume fpsa_csdemo_vol_1

      Vserver Name: CI_SVM
       Volume Name: fpsa_csdemo_vol_1
             State: enabled
Dry Run Start Time: -
Attack Probability: low
   Attack Timeline: 9/22/2023 11:05:55
 Number of Attacks: 1

A400-G0312::> security anti-ransomware volume workload-behavior show -vserver CI_SVM -volume fpsa_csdemo_vol_1
                                     Vserver: CI_SVM
                                      Volume: fpsa_csdemo_vol_1
                        File Extensions Observed: swp, swx, txt~, log, log~,
                                                  sh, swpx, sh~, crypt
                Number of File Extensions Observed: 9

 Historical Statistics
                High Entropy Data Write Percentage: -
  High Entropy Data Write Peak Rate (KB/Minute): -
                File Create Peak Rate (per Minute): 150
                File Delete Peak Rate (per Minute): 150
                File Rename Peak Rate (per Minute): -

 Surge Observed
                                  Surge Timeline: -
                High Entropy Data Write Percentage: -
  High Entropy Data Write Peak Rate (KB/Minute): -
                File Create Peak Rate (per Minute): -
                File Delete Peak Rate (per Minute): -
                File Rename Peak Rate (per Minute): -
                    Newly Observed File Extensions: crypt
          Number of Newly Observed File Extensions: 1

A400-G0312::>
```

never-seen-beforeファイル拡張子の数が設定されたパラメータを超えると、攻撃の可能性がLowからModerateに変わります。この状況が発生するとEMS通知が生成され、ONTAP CLIおよびSystem Managerの[イベント]ページで確認できます。

```
172.21.25.10 - PuTTY
A400-G0312::> security anti-ransomware volume show -vserver CI_SVM -volume fpsa_csdemo_v
ol_1

      Vserver Name: CI_SVM
       Volume Name: fpsa_csdemo_vol_1
             State: enabled
Dry Run Start Time: -
Attack Probability: moderate
   Attack Timeline: 9/27/2023 13:21:15
 Number of Attacks: 1

A400-G0312::> event show -message-name *arw*
Time                Node             Severity      Event
------------------- ---------------- ------------- ---------------------------
9/28/2023 12:39:04  A400-G0312-01    ALERT         callhome.arw.activity.seen: Call-home
 message for fpsa_csdemo_vol_1 (UUID: 1adfa914-7702-11ed-b75c-d039ea91fb56) CI_SVM (UUID
: aa0afb6c-65b3-11ed-b75c-d039ea91fb56)

A400-G0312::>
```



考慮事項と制限事項

1. ARPは、アクティブモードに切り替える前に、ラーニング（またはドライラン）モードで機能する必要があります。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。Cloud Insightsのワークロードセキュリティ機能にはラーニングモードがなく、初日から完全に機能します。
2. ワークロードセキュリティでSVMが監視されていない場合でも、ONTAPによってARPイベントが生成されていれば、Cloud Insightsは引き続きイベントを受信します。ただし、アラートに関連するフォレンジック情報とユーザマッピングはキャプチャまたは表示されません。
3. NFS構成のVMDKでARPを使用する場合は、ARPの保護に制限があります。ARPとFPolicyを使用すると、NFS上のVMをVMDKレベルの暗号化から保護できます。VM内に高エントロピーファイルを含むワークロードがある場合、ARPは推奨されません。
4. 現時点では、ONTAP S3環境とSAN環境ではARPはサポートされていません。

詳細については、次のリンクを参照してください。

[自律型ランサムウェア対策のユースケースと考慮事項（netapp.com）]

注：

ランサムウェア攻撃からの保護を完全に保証できるランサムウェア検出 / 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、NetApp Autonomous Ransomware Protection（ARP）は重要な追加防御レイヤとして機能します。ARPは、少数のファイルが暗号化されて初めてほとんどのランサムウェア攻撃の拡散を検出できますが、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。

ユーザ事例

このセクションでは、いくつかのユースケースについて説明し、ワークロードセキュリティが問題の検出、アラート、データフォレンジックにどのように役立つかを確認します。

偶発的なファイル削除

問題点

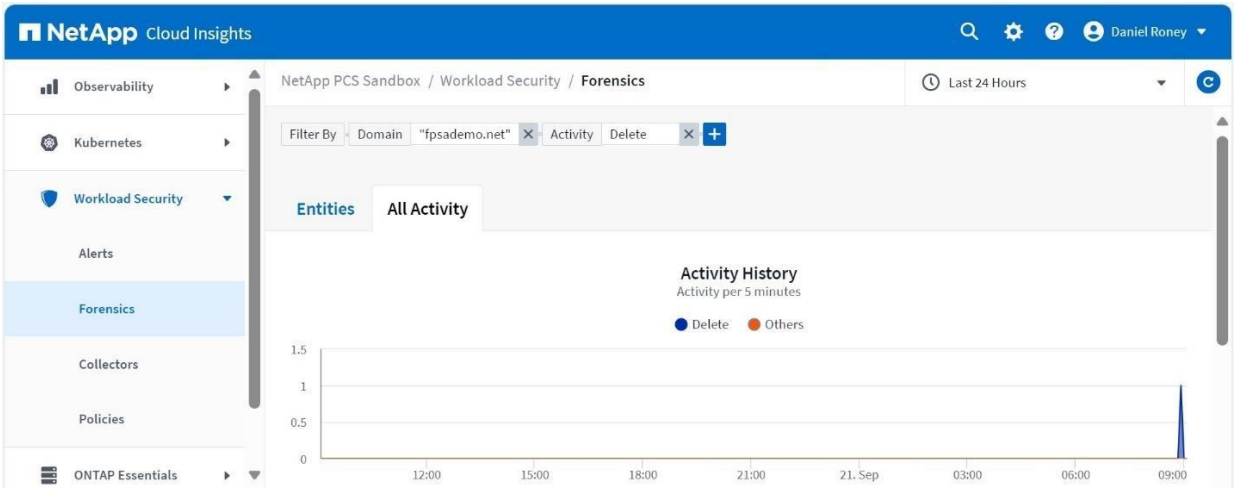
前日にアクセスした「sales-data-Jan2023.docx」がSMB共有にないとユーザから報告されました。

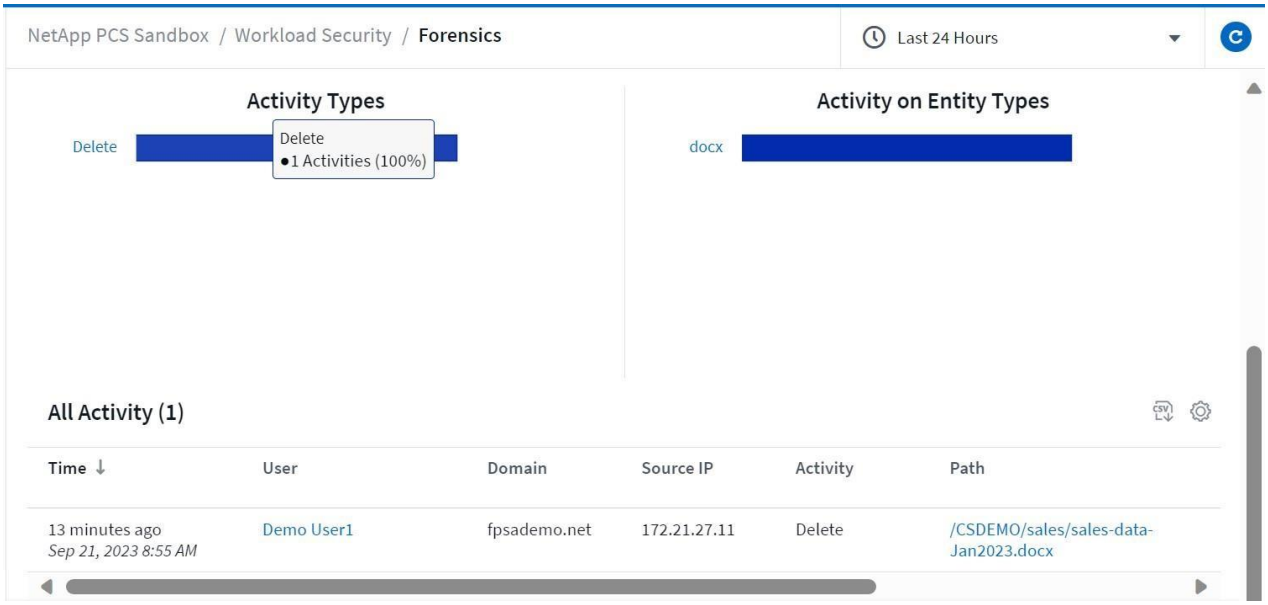
分析

[Workload Security forensics]ページを使用して、指定した期間内のすべてのファイル削除アクティビティを確認できます。結果は、ユーザー、時間、ドメイン、アクティビティ、パス、 デバイス（SVM）など。

この例では、過去24時間のすべての削除アクティビティがチェックされ、報告されたファイル削除を追跡します。

[Workload Security]>[Forensics]>[Activity Forensics]の順に選択し、すべての**アクティビティ**を「ドメイン」および「削除」アクティビティでフィルタリングします。





この例では、Workload Securityが削除アクティビティを登録し、ユーザ名、送信元IP、およびアクティビティの時刻を表示しています。これにより、追加の調査とファイルのリストアのためのベースラインが提供されます。

重要なポイント

ワークロードセキュリティのフォレンジック機能を使用すると、ファイル削除の詳細をすばやく特定できます。

機密ファイルが誤ってパブリックフォルダにコピーされました。

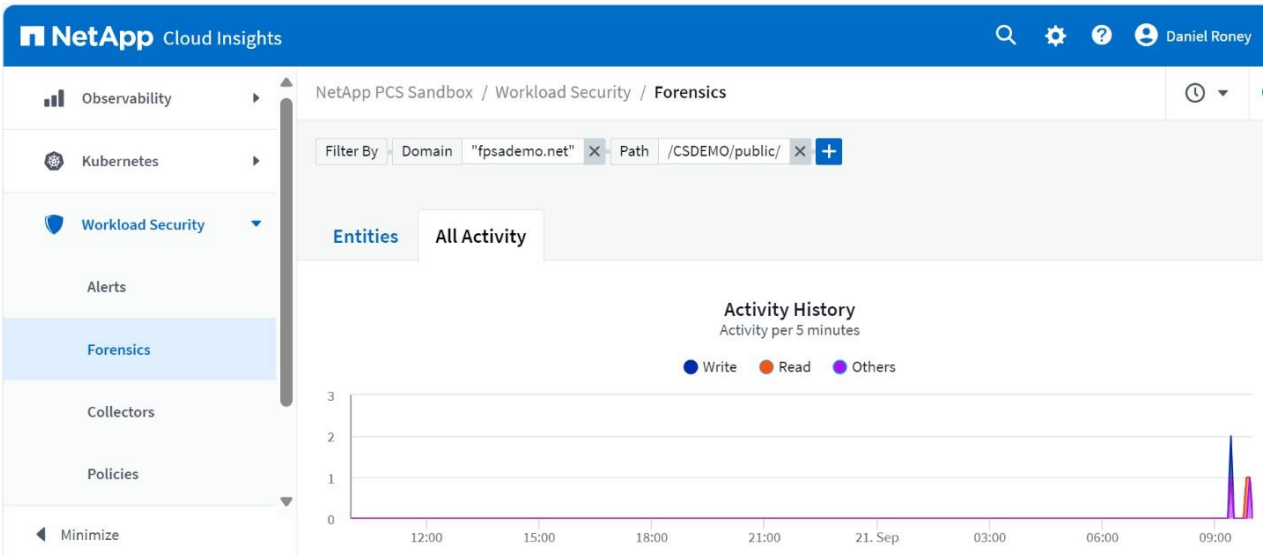
問題点

人事部の従業員が誤ってオファーレターをパブリックフォルダにコピーしました。従業員は30分でこの間違いに気づき、ファイルを削除しましたが、他の誰かがこのファイルをコピーまたは開いたかどうかはわかりませんでした。

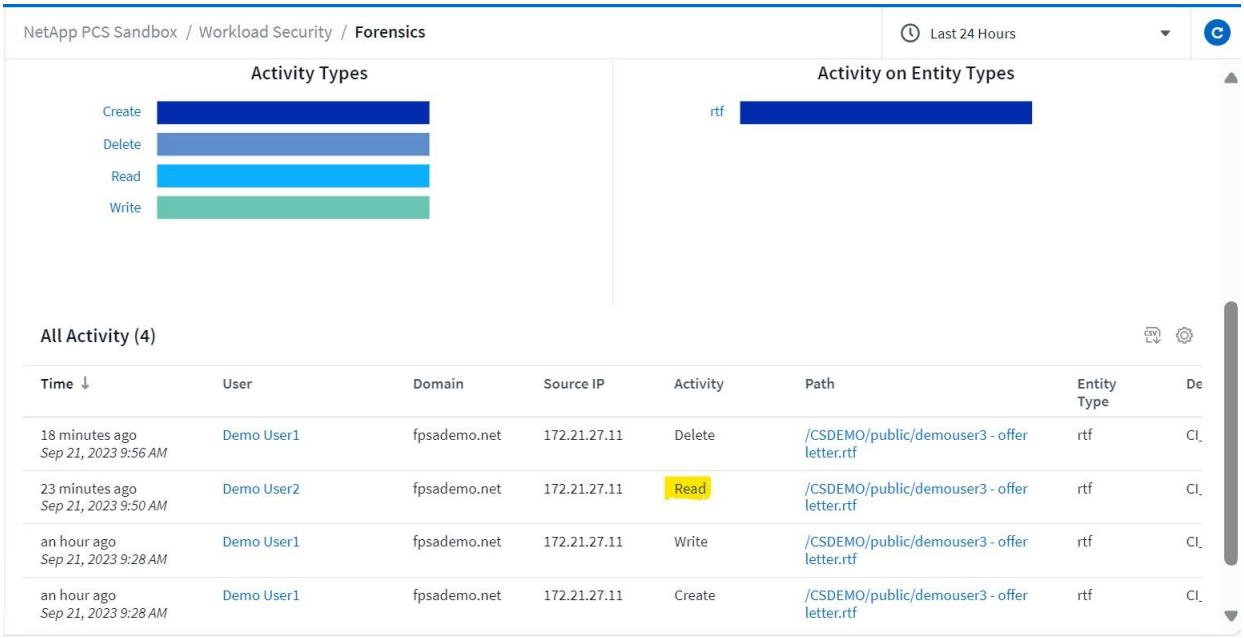
分析

ワークロードセキュリティのフォレンジックページを使用して、パブリックフォルダ内のすべてのファイルアクティビティをチェックし、ファイルを読んだ人がいないかどうかを確認します。

これを確認するには、**[Workload Security]>[Forensics]>[Activity Forensics]**に移動し、すべての**アクティビティ**をドメイン名とファイルパスでフィルタリングします。



この例では、ファイルに関連するすべてのアクティビティがタイムスタンプ、ユーザ名、およびアクティビティタイプとともに表示されます。**Demo User1** はファイルをパブリックディレクトリにコピーしたHR従業員で、**Demo User2**はファイルを読み取る従業員です。後で**デモユーザー1** がパブリックフォルダからファイルを削除しました。Workload Securityは、削除されたファイルのすべてのファイルアクティビティを追跡しました。これにより、元のユーザがパブリックディレクトリからファイルを削除する前に、別のユーザがそのファイルを開いたかどうかを確認できました。



重要なポイント

ワークロードセキュリティは、監視対象のSMB / CIFS共有またはNFS共有内にあるファイルに対するすべてのアクティビティを追跡できます。この機能は、機密データファイルに関連するアクティビティをトレースする場合に非常に便利です。

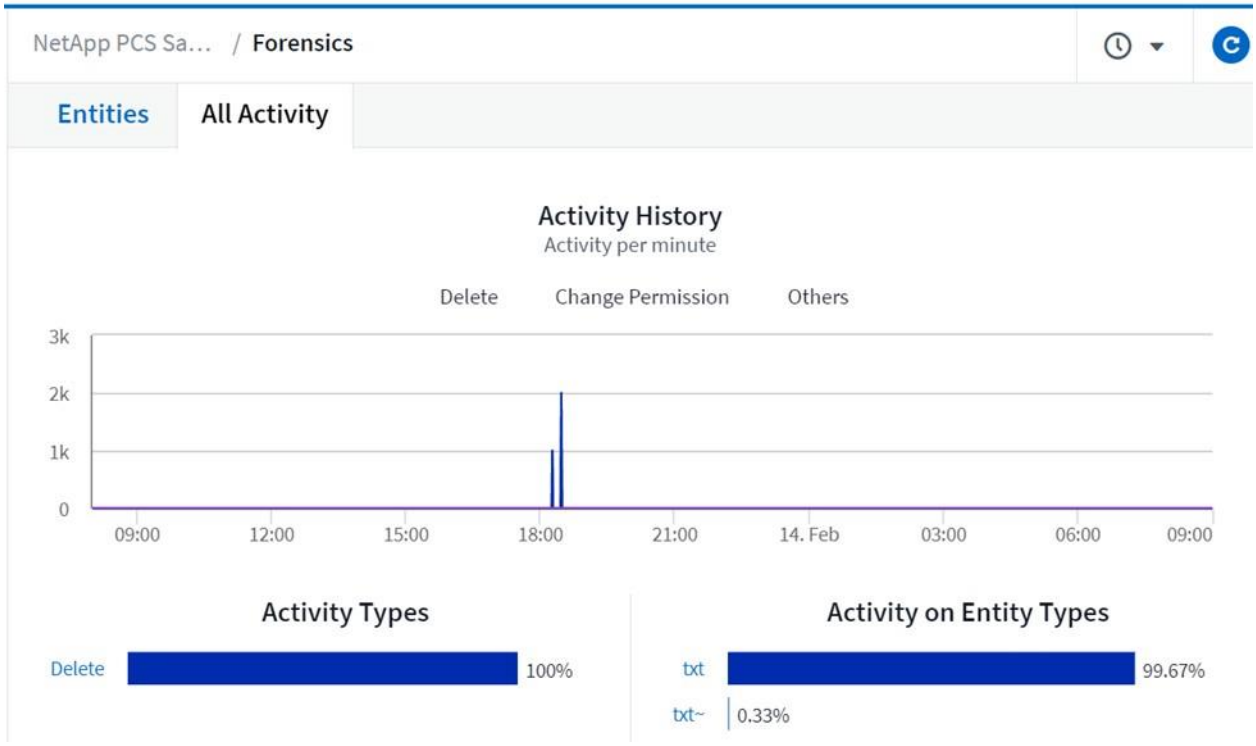
ファイルの一括削除

問題点

前日に使用可能だったいくつかのテキストファイルがNFS共有にないとユーザから報告されました。

分析

Cloud Insightsはこの事件の鑑識を行うために立ち上げられました。過去24時間のファイルアクティビティは、アクティビティ「delete」とエンティティタイプ「txt」に基づいてフィルタリングされ、削除アクティビティの詳細が表示されます。



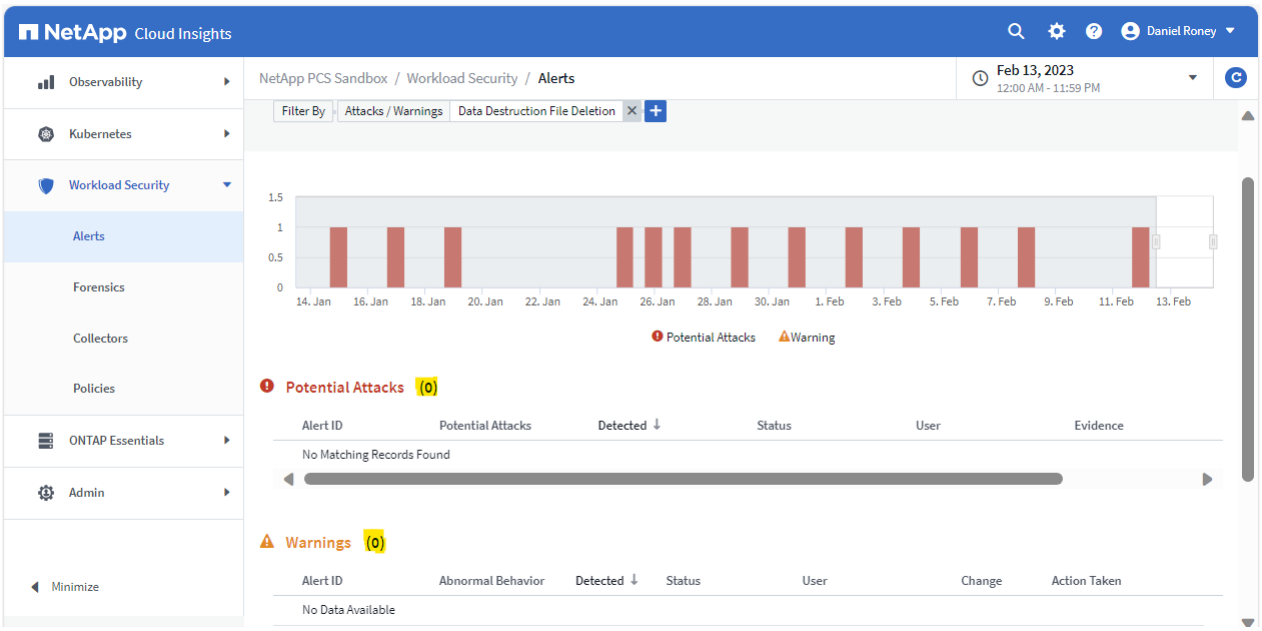
この例では、その間に2つの一括ファイル削除アクティビティがあり、これには3000を超えるテキストファイルが含まれています。

All Activity (3,015)

Time ↓	User	Domain	Source IP	Activity	Path	Entity Type	Device
2 days ago *Feb 13, 2023 6:28 PM*	testuser2		172.21.27.13	Delete	/fpsa_csdemo_vol_1/data2/hr/File2000.txt	txt	CI_SVM
2 days ago *Feb 13, 2023 6:28 PM*	testuser2		172.21.27.13	Delete	/fpsa_csdemo_vol_1/data2/hr/File1998.txt	txt	CI_SVM
2 days ago *Feb 13, 2023 6:28 PM*	testuser2		172.21.27.13	Delete	/fpsa_csdemo_vol_1/data2/hr/File1997.txt	txt	CI_SVM
2 days ago *Feb 13, 2023 6:28 PM*	testuser2		172.21.27.13	Delete	/fpsa_csdemo_vol_1/data2/hr/File1996.txt	txt	CI_SVM
2 days ago *Feb 13, 2023 6:28 PM*	testuser2		172.21.27.13	Delete	/fpsa_csdemo_vol_1/data2/hr/File1995.txt	txt	CI_SVM
2 days ago *Feb 13, 2023 6:28 PM*	testuser2		172.21.27.13	Delete	/fpsa_csdemo_vol_1/data2/hr/File1994.txt	txt	CI_SVM

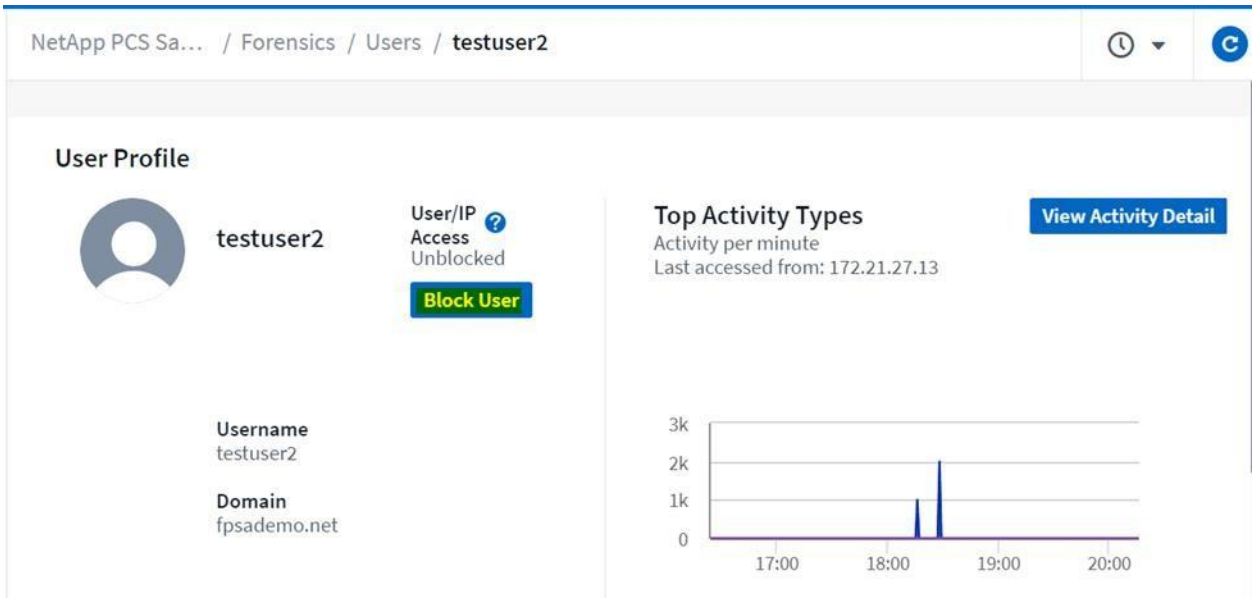
2 days ago *Feb 13, 2023 6:16 PM*	testuser2	172.21.27.13	Delete	/fpsa_csdemo_vol_1/data/File1524.txt	txt	CI_SVM
2 days ago *Feb 13, 2023 6:16 PM*	testuser2	172.21.27.13	Delete	/fpsa_csdemo_vol_1/data/File1522.txt	txt	CI_SVM
2 days ago *Feb 13, 2023 6:16 PM*	testuser2	172.21.27.13	Delete	/fpsa_csdemo_vol_1/data/File1523.txt	txt	CI_SVM

このアクティビティではデータ破棄アラートは生成されませんでした。これは **[Alerts]** ページで確認できます。**[Alerts]**をクリックし、[Attack/Warnings]でフィルタリングして、**[Data Destruction File Deletion]**を選択します。



Cloud Insights管理者は、調査の進行中にこのユーザが共有にアクセスすることをブロックできます。これを行うには、**ユーザー名をクリックし**ます。これにより、指定された期間ユーザーをブロックするオプションがあるユーザープロファイルにリダイレクトされます。調査によってユーザーの悪意が証明された場合、管理者はユーザーを永続的にブロックできます。

次の例は、「**testuser2**」のユーザプロファイルを示しています。管理者は **[Block User]** ボタンをクリックしてユーザをブロックできることに注意してください。



重要なポイント

Cloud Insights管理者は、ワークロードセキュリティを使用して、2つのフォルダにある3000を超えるファイルに影響した一括ファイル削除アクティビティの詳細を指定できます。Cloud Insights管理者は、調査の進行中に特定の期間、ユーザーをブロックすることもできます。

攻撃ポリシーで「データ破壊とファイル削除」が設定されていても、なぜ一括削除のアラートが生成されなかったのか疑問に思うかもしれません。ファイル削除は一般的なアクティビティであり、データ破壊アラートは異常な大量ファイル削除アクティビティに対してのみ生成されます。ワークロードセキュリティでは、まず、個々のユーザとユーザグループのユーザ行動を学習する必要があります。次に、ベースラインを確立し、動作の変化を探します。このユーザに対して確立されたベースラインは、意図しないことを証明するのに十分ではなかったため、アラートは生成されませんでした。ランサムウェアの検出については、Cloud Insightsはトレーニングを必要とせず、初日から有効になります。

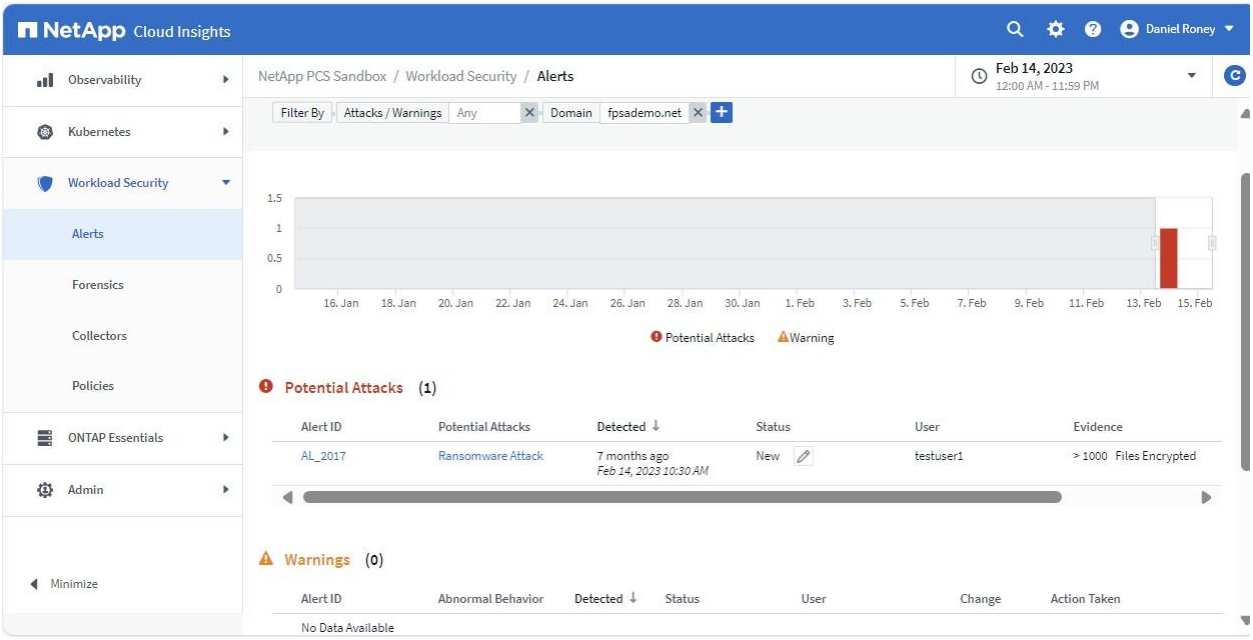
一括ファイル暗号化によるランサムウェア攻撃のシミュレーション

問題点

Cloud Insights管理者が、ランサムウェア攻撃の可能性があるというEメールアラートを受信しました。

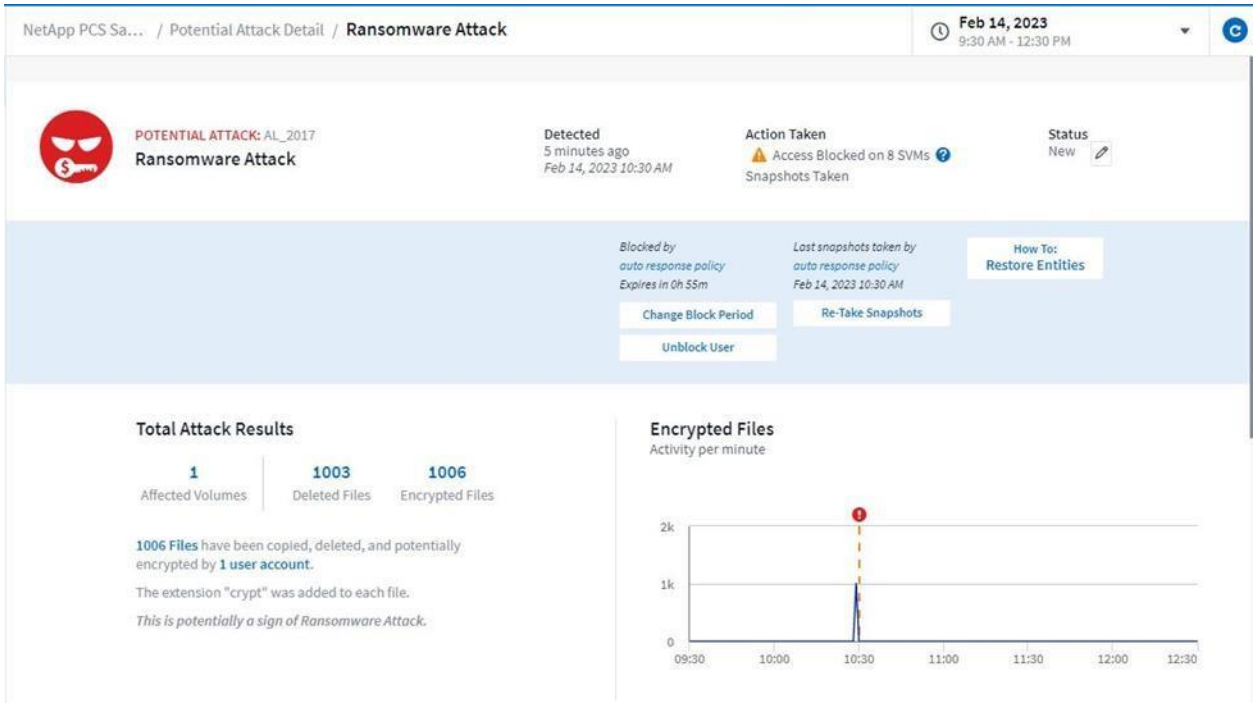
分析

Cloud Insightsが起動してアラートを確認します。1000を超えるファイルがtestuser1によって暗号化されていることが報告されています。



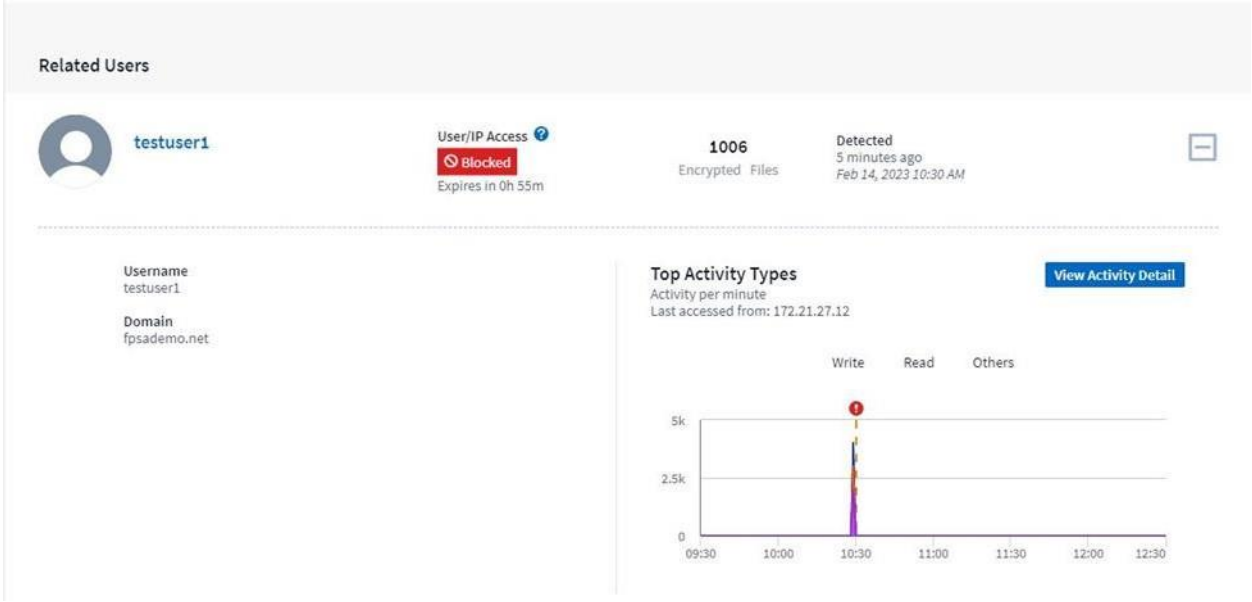
.

アラートIDをクリックすると、攻撃の詳細と実行されたアクションが表示されます。



ご覧のように、自動応答ポリシーがトリガーされ、ユーザがブロックされます。Snapshotコピーも作成されます。この画面には、ブロック期間を変更したり、正当なアクティビティであることが判明した場合にユーザーのロックを解除したりするための追加オプションもあります。

下にスクロールすると、最終アクセスのユーザの追加情報とIPアドレス、履歴、影響を受けるボリューム、Snapshotの情報が表示されます。



Linuxホストにtestuser1としてログインし、NFS共有へのアクセスを試みます。この例では、testuser1に対するアクセスが拒否されています。

重要なポイント

ワークロードセキュリティは、ユーザデータのアクセスパターンの変化に基づいてランサムウェア攻撃を効果的に検出し、報告します。このユースケースでは、ユーザが監視対象のNFS共有内の多数のテキストファイルを暗号化します。ワークロードセキュリティは、すぐにランサムウェア攻撃の可能性があると判断し、ユーザをブロックしました。Cloud Insights管理者がアクティビティを分析し、正当なアクティビティであることが判明した場合はユーザのブロックを解除するためのアラートが生成されました。データのリストアが必要になった場合に備えて、ボリュームのSnapshotコピーも作成されました。

ランサムウェア攻撃後のデータのリカバリ

ランサムウェア攻撃からリカバリし、インシデント前の状態にデータをリストアするには、攻撃者が保持している復号化キーへのアクセスが必要になる場合があります。これは多くの場合、攻撃者に身代金を支払う必要がありますが、攻撃者が以前に約束したようにキーをリリースしたり、データを復号化したりする保証はありません。さらに、身代金を支払うことで、攻撃者は攻撃を継続することができます。

ランサムウェアからのリカバリプランが設定されていれば、組織はタイムリーに通常の運用を再開できます。ランサムウェアからのリカバリ計画には、通常、組織が攻撃に備える方法、進行中の攻撃に対処する方法、攻撃からリカバリするために何をすべきかが含まれます。ランサムウェア攻撃を受けた場合、最初に感じるのは、データを瞬時にリカバリすることかもしれません。これは確かに可能ですが、ランサムウェアが戻ってこないようにするための他の手順を実行しないと、再感染や長時間の停止につながる可能性があります。環境を適切かつ包括的に修正するには、主に3つの手順があります。最初のステップはアウトブレイクを封じ込めることです。これには、感染したクライアントをネットワークから切断して特定し、隔離することが含まれます。切断されたら、次のステップは感染したシステムをクリーンアップし、可能であればパッチを適用することです。パッチを適用すると、システムがネットワークに再接続されたときに再感染するのを防ぐことができます。最後のステップは、データのリカバリとリストアです。組織は、データ損失を削減するために、ビジネスクリティカルなすべてのデータを合理的な頻度でバックアップする必要があります。データのバックアップはビジネスの運用をリストアするために重要であり、攻撃の直前に作成されたバックアップにアクセスすると、ランサムウェア攻撃後のデータ損失を大幅に削減できます。

このセクションでは、ONTAPのボリュームSnapshotリストア機能と、ランサムウェア攻撃からのリカバリに非常に役立つNetAppのSnapCenter®プラグインについて説明します。SnapCenterプラグインを使用すると、VMと整合性のあるバックアップとアプリケーションと整合性のあるバックアップをスケジュールに基づいて作成し、必要に応じてリストア処理を実行できます。

ONTAPボリュームSnapshotリストア

前述したランサムウェア攻撃シミュレーションのユースケースでは、Cloud Insightのワークロードセキュリティ機能の自動応答ポリシーによって、攻撃が検出されるとすぐにボリュームスナップショットがトリガーされていました。このスナップショットには暗号化されたファイルがほとんど含まれていない場合もありますが、最小限の暗号化されたファイルを使用して、攻撃に近い時点にボリュームをリストアすると便利です。コアONTAPをお持ちのお客様は、Autonomous Ransomware Protection（ARP；自律型ランサムウェア対策）を通じて、ランサムウェアの検出、アラート、スナップショット機能も利用できます。Cloud Insightsとは異なり、ARPはフォレンジック機能をネイティブに提供していませんが、Cloud Insightsと統合すると、フォレンジック機能のレイヤが追加され、ユーザマッピングと分析データの保持期間が最大13カ月になります。

次のスクリーンショットでは、影響を受けるデバイス、ボリューム、およびWorkload Security自動応答ポリシーによって取得されたスナップショットが表示されています。ワークロードのセキュリティによって作成されるSnapshotは「**cloudsecure_attack_auto_**」タグで始まります。

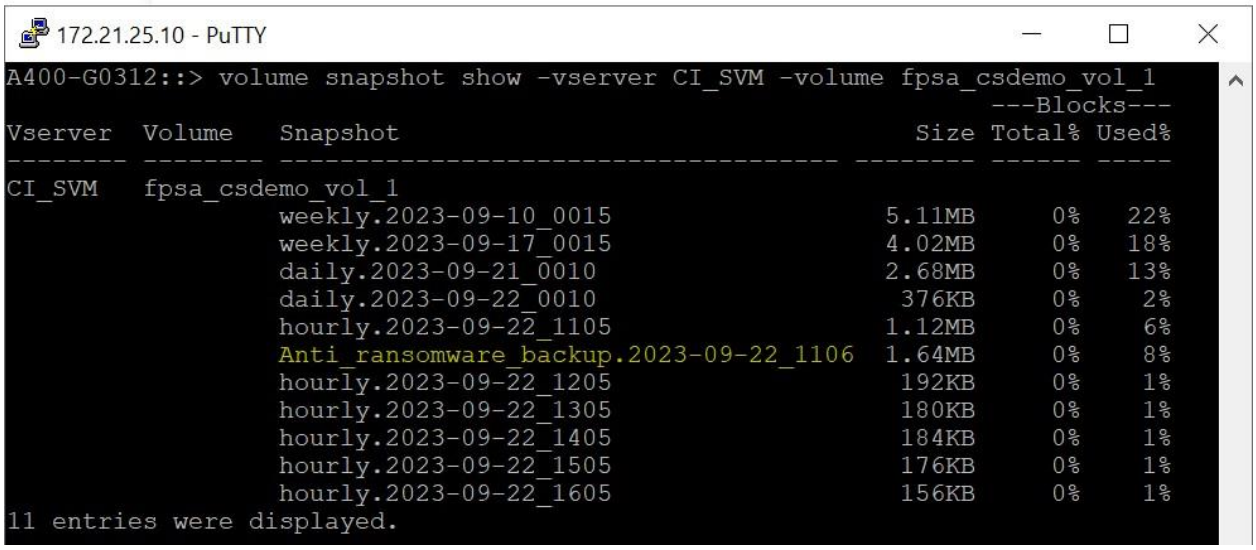
次のコマンドを使用して、Snapshotにボリュームをリストアできます。

```
Cluster::> volume snapshot restore -vserver <vserver name> -volume <volume name> -
snapshot <snapshot name>
```

```
A400-G0312::> volume snapshot restore -vserver CI_SVM -volume fpsa_csdemo_vol_1 -
snapshot cloudsecure_attack_auto_1676388648746
```

注：

Autonomous Ransomware Protectionによって生成されるSnapshotは、「Anti_ransoms_backup」で始まります。たとえば、次のスクリーンショットは、ARPが有効なボリュームでnever-seen-beforeファイル拡張子が検出されたときに、ARP機能によってトリガーされたSnapshotを示しています。



ボリュームSnapshotリストアを使用したデータのリカバリの詳細については、次のリンクを参照してください。

https://docs.netapp.com/us-en/ontap/anti-ransomware/recover-data-task.html

SnapCenter Plug-in for VMware vSphere（SCV）

SnapCenter Plug-in for VMware vSphere（SCV）（旧NetAppデータブローカー）は、Linuxベースのスタンドアロン仮想アプライアンスであり、仮想化されたデータベースおよびファイルシステムに対するSnapCenterのデータ保護処理をサポートします。VM、データストア、VMDKに対して、スペース効率に優れた、クラッシュ整合性のあるVM整合性バックアップおよびリストア処理を高速で実行できます。SnapCenter Plug-in for VMware vSphereは、MS-SQL、Exchange、Oracle、SAP-HANAなどのSnapCenterアプリケーションベースのプラグインと連携して、VMware環境でアプリケーションと整合性のあるバックアップおよびリストア処理を実行できます。

注：

- VMと整合性のあるSnapshotコピーにはVMware Toolsが必要です。VMware Toolsがインストールおよび実行されていない場合、ファイルシステムは休止されず、クラッシュ整合性Snapshotが作成されます。VM整合性およびクラッシュ整合性を備えたデータ保護を実現するために、SnapCenter Serverをインストールする必要はありません。
- アプリケーション整合性（VMDK経由のアプリケーションまたはRawデバイスマッピング（RDM）経由のアプリケーション）のデータ保護処理を行うには、SnapCenterサーバをインストールする必要があります。SnapCenterは、SnapCenter VMwareプラグインをネイティブに活用して、VMDK、rawデバイス マッピング（RDM）、およびNFSデータストア上のすべてのデータ保護処理を実行します。

vCenterのSnapCenter Plug-in for VMwareを使用すると、次の操作を実行できます。

- 仮想マシンのポリシー、リソースグループ、およびバックアップスケジュールを作成します。
- 仮想マシン、VMDK、データストアをバックアップします。
- 仮想マシン、VMDK、およびファイルとフォルダのリストア（WindowsゲストOSの場合）
- VMDKを接続および接続解除します。
- 仮想マシンおよびデータストアに対するデータ保護処理を監視し、レポートを作成します。
- RBACセキュリティと一元化されたロール委譲をサポートします。
- WindowsゲストOSのゲストファイルまたはフォルダ（単一または複数）をサポートします。
- Single File SnapRestoreを使用して、プライマリおよびセカンダリのSnapshotコピーから効率的なストレージベースをリストアできます。
- 保護されている仮想マシンと保護されていない仮想マシン、およびバックアップ、リストア、マウントジョブのステータスを可視化するダッシュボードとレポートを生成します。
- セカンダリSnapshotコピーから仮想ディスクを接続または接続解除します。
- 仮想ディスクを代替仮想マシンに接続します。

vCenterでVMware vSphere Client GUIを使用して、VMware仮想マシン（従来のVMとvVol VM）、VMDK、およびデータストアのすべてのバックアップ処理とリストア処理を実行できます。vVol VM（vVolデータストア内のVM）の場合は、クラッシュ整合性バックアップのみがサポートされます。また、VMやVMDKをリストアしたり、ゲストOS上に存在するファイルとフォルダをリストアしたりすることもできます。

SnapCenter Plug-in for VMware vSphereの導入

SCV導入手順は、新規および既存のSnapCenterユーザによって異なります。

これまでSnapCenterを使用したことがなく、SnapCenterバックアップがない場合は、次のワークフローを使用して作業を開始してください。

https://docs.netapp.com/us-en/sc-plugin-vmware-vSphere/scpivs44_deployment_workflow_for_new_users.html

SnapCenterバックアップをすでに所有しているSnapCenterユーザの場合は、次のワークフローを使用して作業を開始してください。

https://docs.netapp.com/us-en/sc-plugin-vmware-vSphere/scpivs44_deployment_workflow_for_existing_users.html

手順

1. Open Virtual Appliance（OVA）およびEntrustのルート証明書と中間証明書をインストールします。

VMware vCenter 7.0.3以降のバージョンでは、Entrust証明書によって署名されたOVAは信頼されなくなりました。OVAと証明書のフォルダが格納された.tarファイルをダウンロードし、以下の手順に従って証明書をインストールする必要があります。

https://docs.netapp.com/us-en/sc-plugin-vmware-vSphere/scpivs44_download_the_ova_open_virtual_appliance.html

2. SnapCenter Plug-in for VMware vSphereを導入する

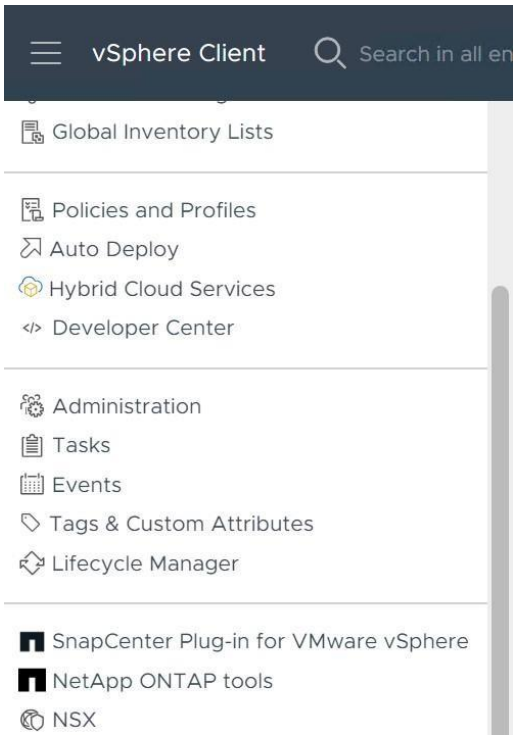
SnapCenterの機能を使用して、仮想マシン上のVM、データストア、アプリケーションと整合性のあるデータベースを保護するには、SnapCenter Plug-in for VMware vSphereを導入する必要があります。SCV 4.9は検証済み環境に導入されています。詳細については、次の手順を参照してください。

https://docs.netapp.com/us-en/sc-plugin-vmware-vsphere/scpivs44_deploy_snapcenter_plug-in_for_vmware_vsphere.html

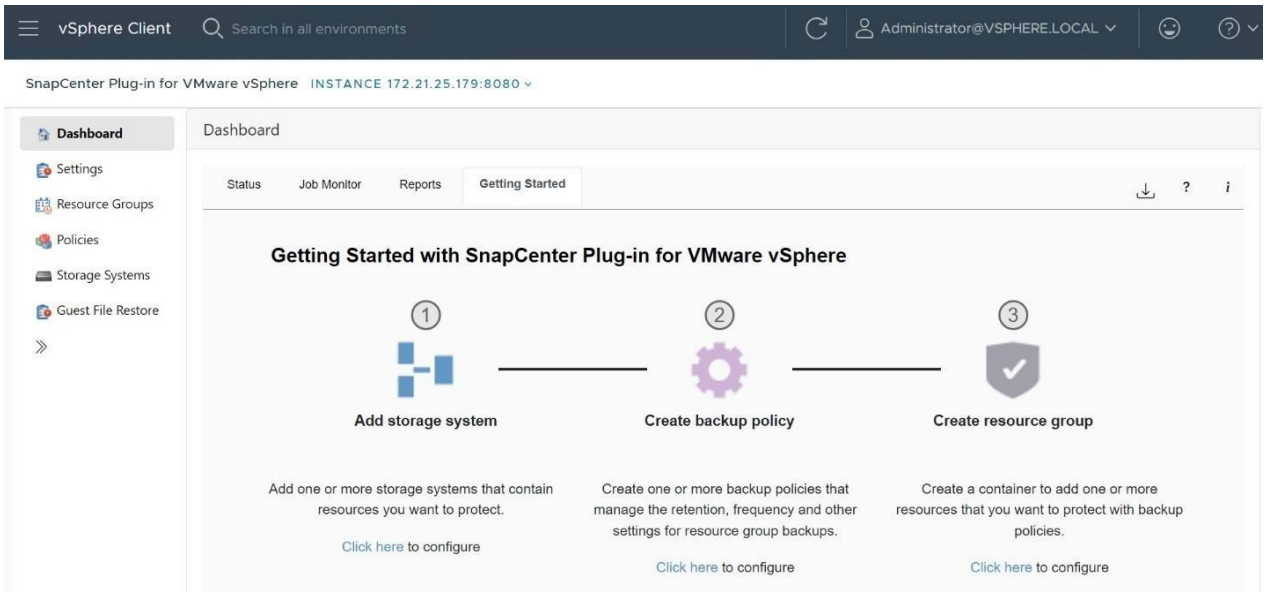
VMとデータストアのバックアップ

バックアップを作成する前に、SnapCenter Plug-in for VMware vSphereを使用してバックアップポリシーを設定し、ストレージを接続し、リソースグループを作成する必要があります。

VMware vSphere Client GUIを開き、**[Menu]** ボタンをクリックして、 プルダウンリストから**SnapCenter Plug-in for VMware vSphere**を選択します。



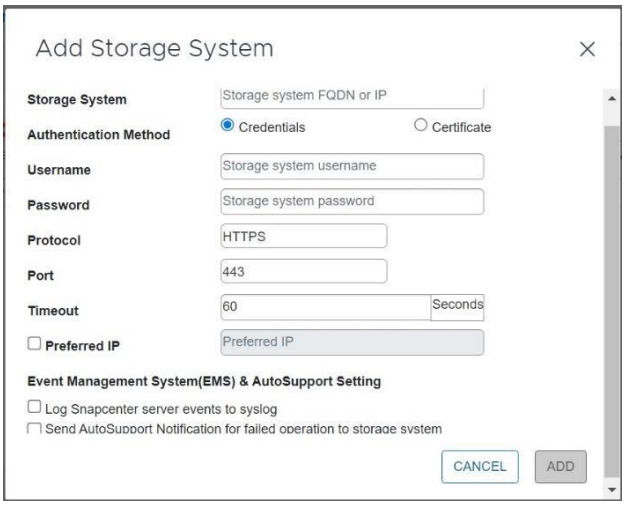
SCVプラグインが開いたら、左側のペインで[Dashboard]をクリックし、 右側のペインで[Getting Started]タブを選択します。このタブには、VMとデータストアをバックアップするためのSCVプラグインの設定手順が表示されます。各ステップの下にあるハイパーリンクをクリックすると、それぞれのステップのウィザードが開きます。または、左側のペインでストレージシステム、ポリシー、またはリソースグループを右クリックして新しい項目を作成し、設定ウィザードを開くこともできます。



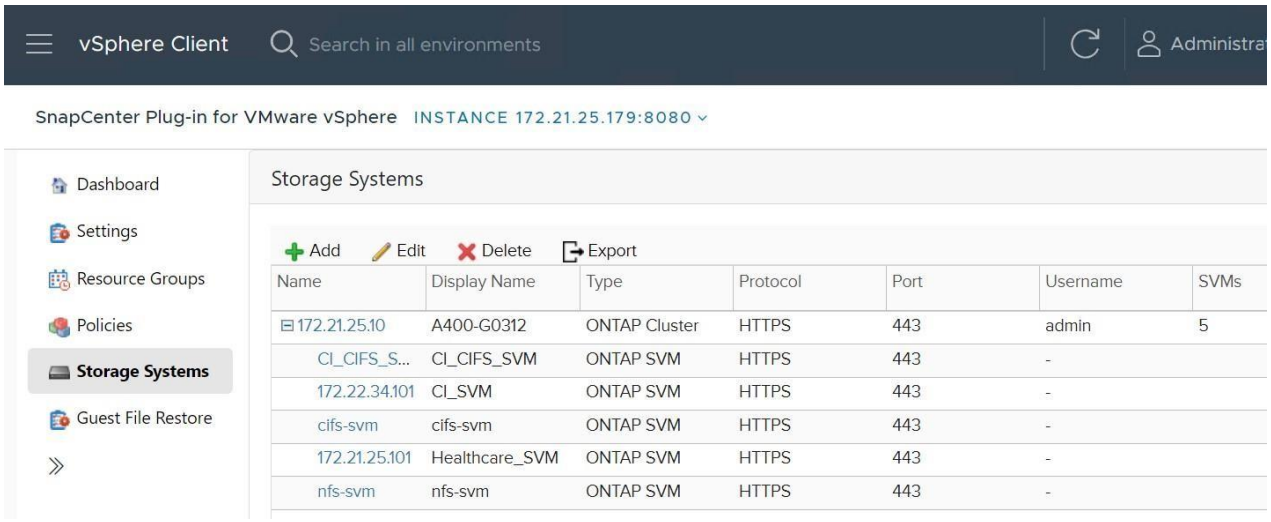
1. ストレージクラスタとStorage VMを追加

SCVプラグインの左側ナビゲータペインで、**[Storage Systems]**をクリックし、**[Add]** ボタンを選択します。

[ストレージシステムの追加]ダイアログボックスで、SVMまたはクラスタの基本情報を入力し、[追加]を選択します。



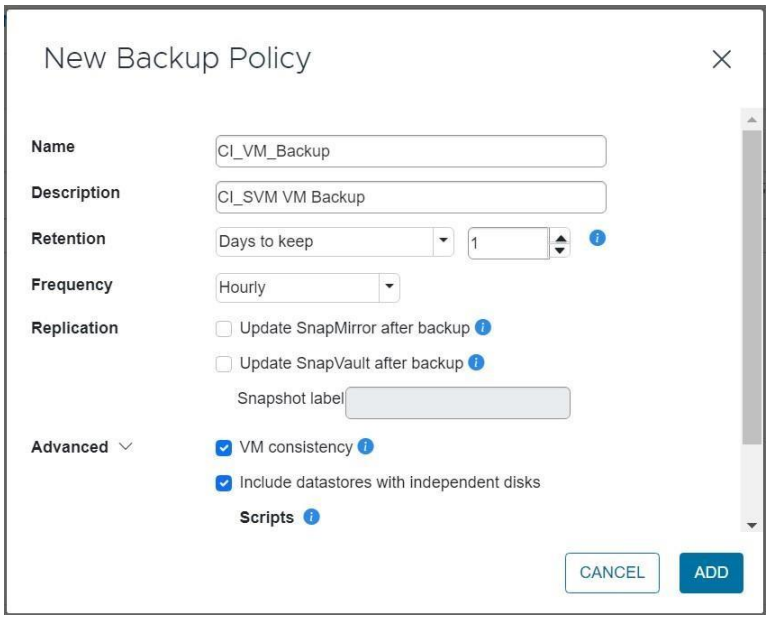
次のスクリーンショットは、追加されたストレージクラスタとSVMを示しています。



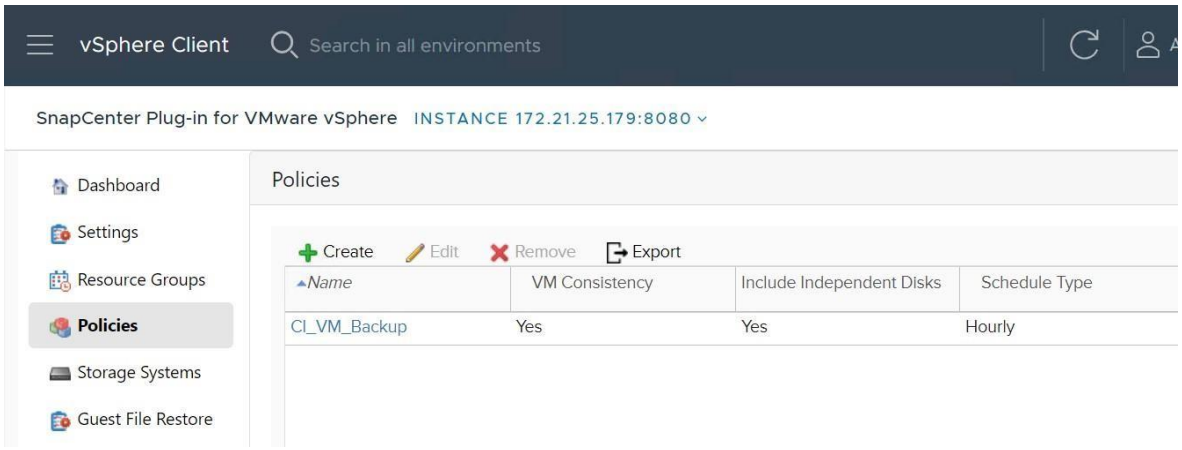
2. バックアップ ポリシーの作成

SCVプラグインの左側のナビゲーションペインで、**[Policies]**をクリックし、**[Create]** ボタンをクリックします。

[New Backup Policy]ページで、ポリシーの設定情報を入力し、[Add]をクリックします 。



この例では、毎時バックアップポリシーを作成し、このポリシーを使用して作成されたバックアップを1日間保持します。

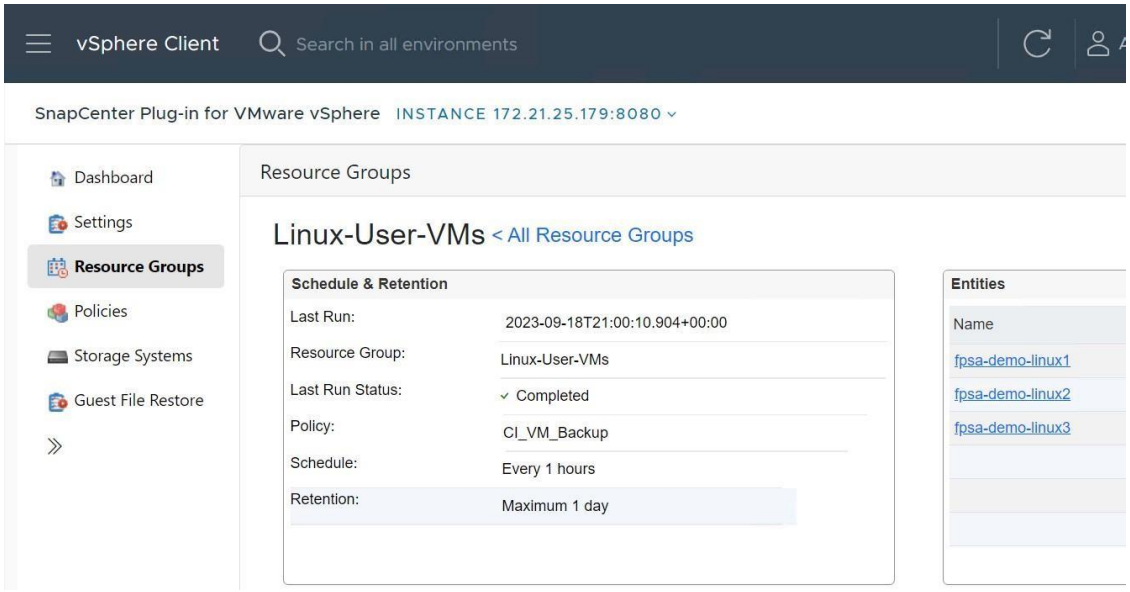


3. リソース グループの作成

SCVプラグインの左側ナビゲータペインで、**[Resource Groups]**をクリックし、**[Create]**を選択します。

[Create Resource Group]ウィザードの各ページで必要な情報を入力し、リソース グループに含めるVMとデータストアを選択し、適用するバックアップ ポリシーを選択し、バックアップ スケジュールを指定します。

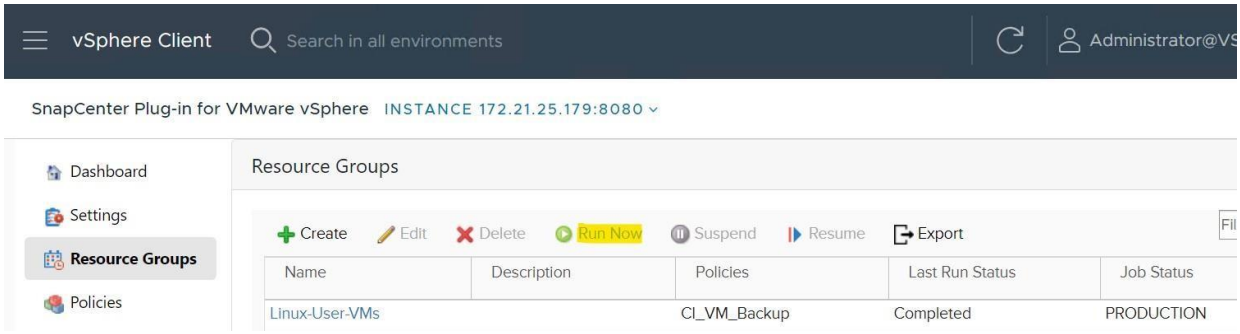
この例では、3台のLinux VMをバックアップするためのリソースグループを作成しています。



4. バックアップの実行

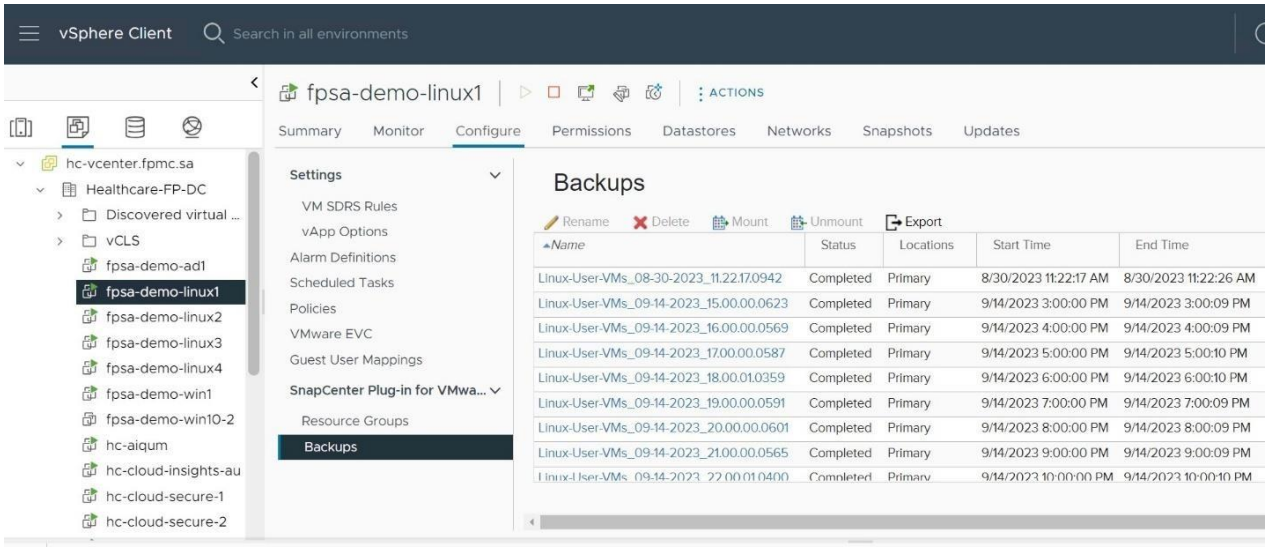
バックアップは、リソース グループに設定されたバックアップ ポリシーに従って実行されます。

リソースグループを選択したあとに[Run Now]をクリックして、[Resource Groups]ページでオンデマンドバックアップを実行することもできます。



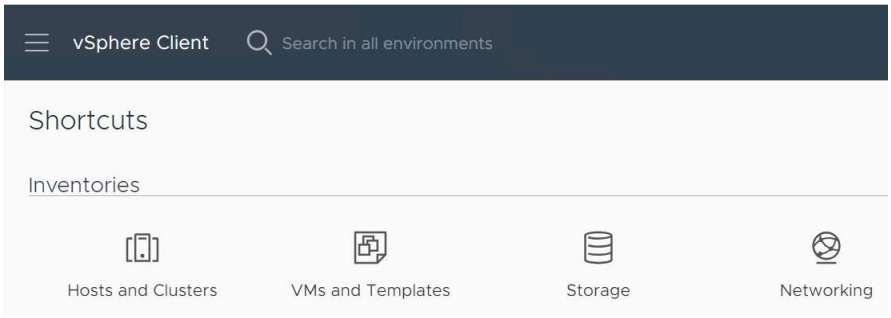
5. VMのバックアップの表示

VMのバックアップを表示するには、インベントリリストで**[Hosts and Clusters]**を開き、VMを選択して **[Configure]** タブを選択し、**SnapCenter Plug-in for VMware vSphere]**セクションで**[Backups]**をクリックします。右側のペインに、使用可能なすべてのバックアップが表示されます。

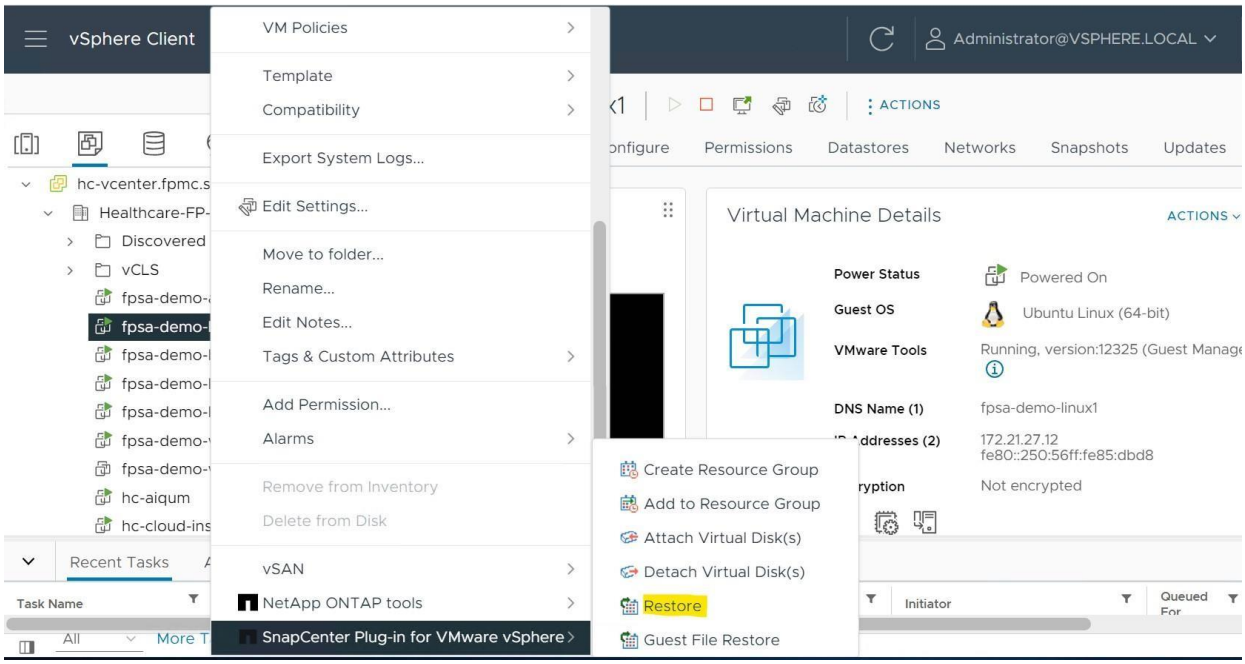


バックアップからのVMのリストア

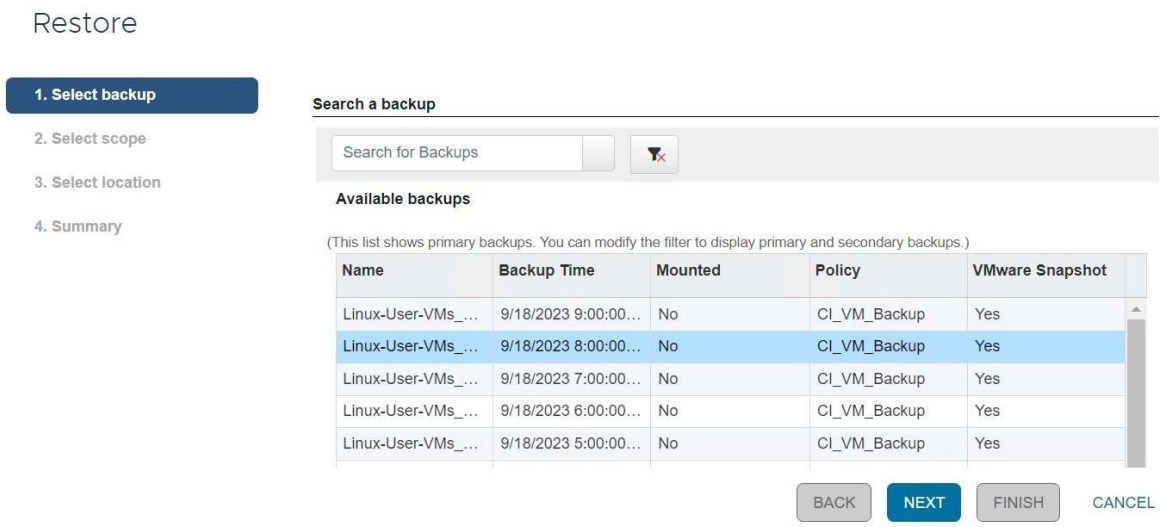
VMware vSphere ClientのGUIで、左上にある[メニュー]ボタンをクリックしてショートカットを選択し、インベントリリストから[仮想マシンおよびテンプレート]を選択します。



左側のナビゲーションペインで、VMを右クリックし、ドロップダウンリストから**NetApp SnapCenter Plug-in for VMware vSphere**を選択し、2番目のドロップダウンリストから**[Restore]**を選択してウィザードを開始します。



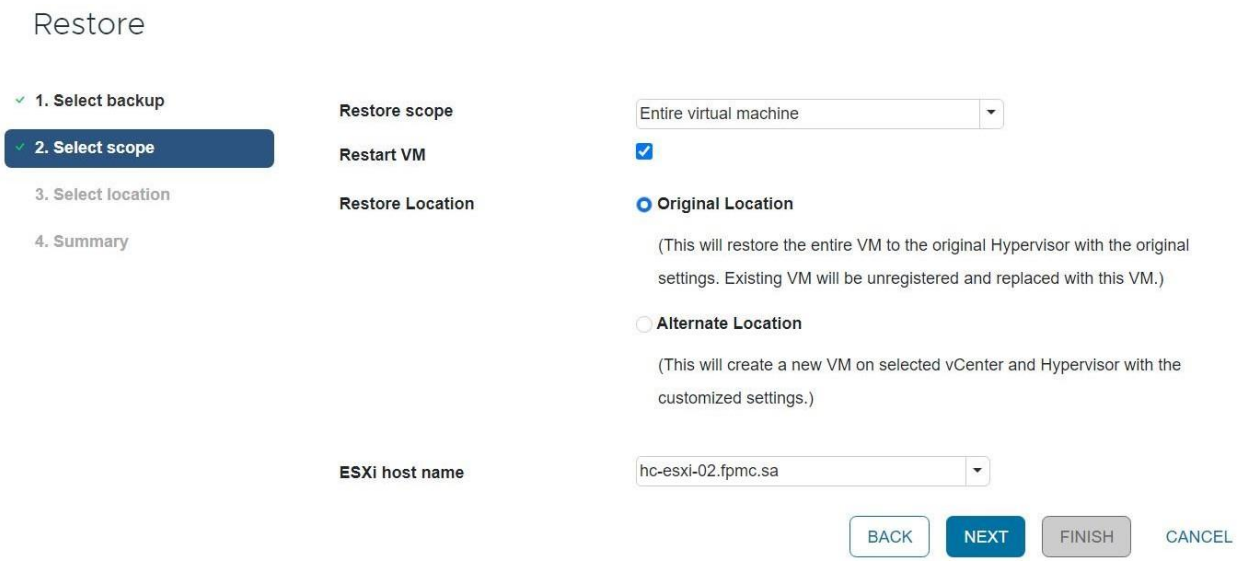
[Restore]ウィザードの **[Select Backup]**ページで、リストア元のバックアップSnapshotコピーを選択し、[Next]をクリックします。



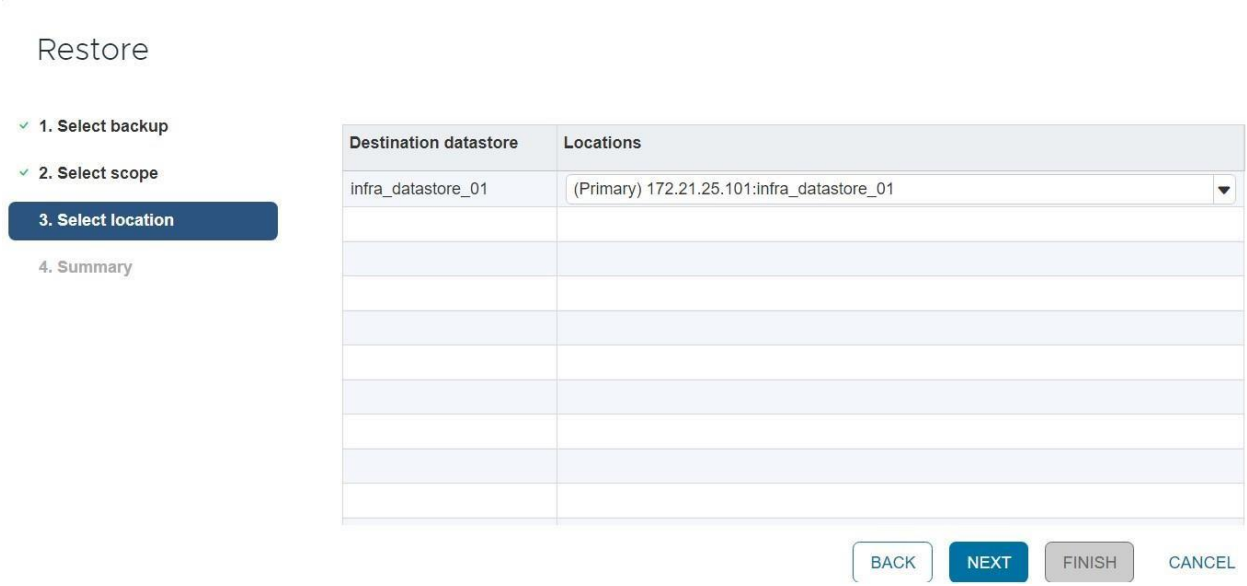
[Select Scope]ページで、[Restore scope]フィールドで[Entire virtual machine]を選択し、リストア先を選択してから、バックアップのマウント先の情報を入力します。チェックボックスをクリックしてVMを再起動することもできます。

[Alternate Location]をリストア先として選択した場合は、選択したvCenterとハイパーバイザーにカスタマイズした設定で新しいVMが作成されます。

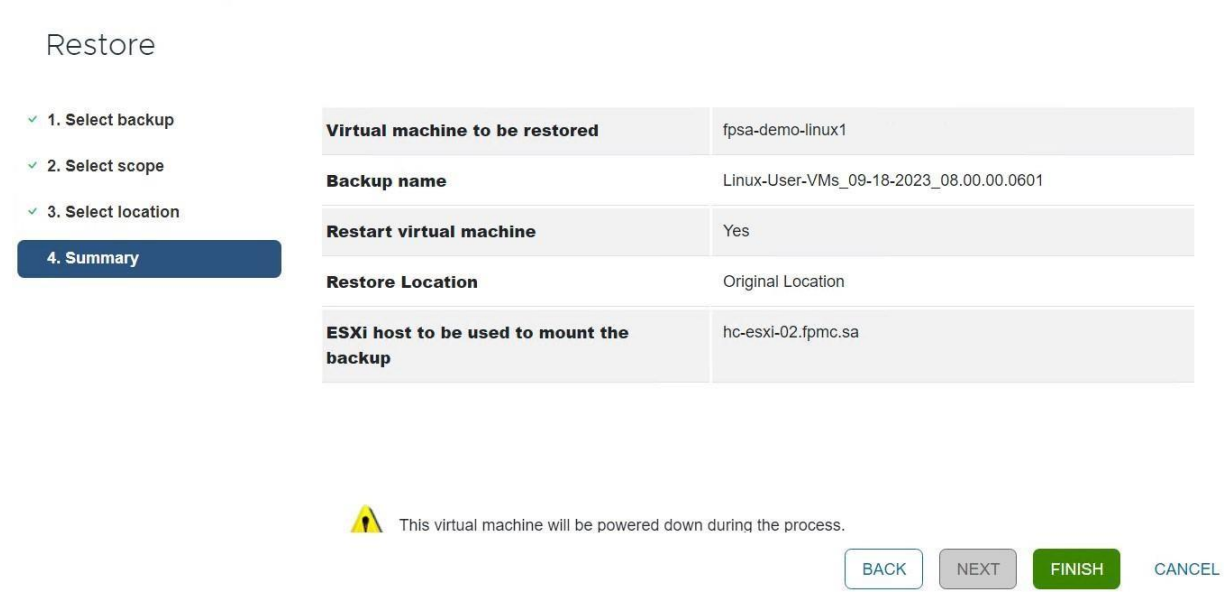
この例では、リストア先として**[Original Location]**が選択されています。



[Select Location]ページで、リストアするデータストアの場所を選択し、[Next]をクリックします。



[Summary]ページを確認し、[Finish]をクリックします。



注： 画面下部の**[Recent Tasks]**をクリックすると、処理の進捗状況を監視できます。更新された情報を表示するには、画面を更新します。

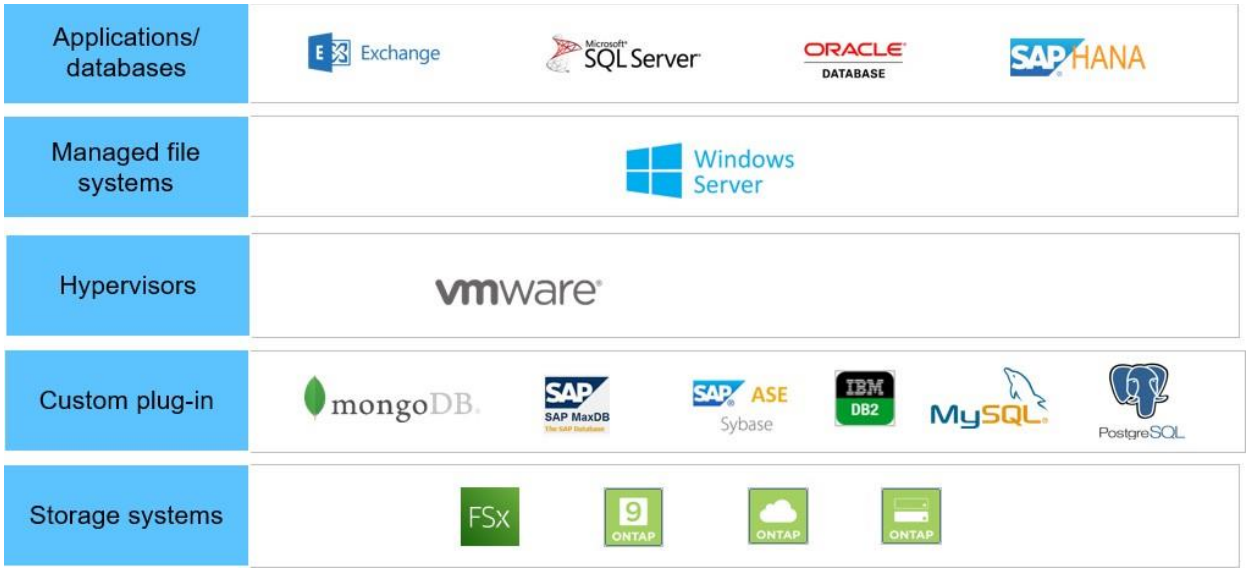
アプリケーションと整合性のあるバックアップとリカバリを実現するSnapCenterプラグイン

SnapCenterは、NetAppが提供するソフトウェアパッケージで、アプリケーションとデータベースと整合性のあるバックアップ、検証、クローニング、リカバリに重点を置いています。SnapCenterは、SnapCenterサーバとSnapCenterプラグインで構成されています。

SnapCenterサーバは、さまざまなアプリケーション、データベース、ファイルシステム、ハイパーバイザー用のプラグインをサポートする共通のインターフェイスを備えた一元化されたサーバです。SnapCenterを使用すると、プラグインをリモートホストに一元的に導入し、バックアップ、検証、クローニング、リストアの処理をスケジュール設定して監視できます。

SnapCenterプラグインを次の図に示します（図5）。

図5）SnapCenterプラグイン



- Plug-in for Microsoft Windows -このプラグインは、Windowsファイルシステムのバックアップ、リカバリ、およびクローニングを処理します。また、Windowsでのディスクのプロビジョニング、ディスクのサイズ変更、SMB共有の作成、iSCSI接続、igroup接続にも使用されます。これは、Microsoft SQL ServerおよびMicrosoft Exchange Serverプラグインのバックグラウンドコンポーネントとしても使用されます。
- Plug-in for Microsoft SQL Server -このプラグインは、Microsoft SQL Serverデータベースのバックアップ、リカバリ、およびクローニングを処理します。
- Plug-in for Microsoft Exchange Server - Microsoft Exchange Serverデータベースのバックアップとリカバリを処理します。
- Plug-in for SAP HANA Database - SAP HANAデータベースのバックアップ、リカバリ、クローニングを処理します。
- Plug-in for Oracle Database - Oracleデータベースのバックアップ、リカバリ、クローニングを処理します。
- Plug-in for UNIX -このプラグインは、Oracle Database Plug-inのバックグラウンドコンポーネントとして使用されます。本書の執筆時点では、このプラグインを使用してLinuxファイルシステムをバックアップすることはできませんが、この機能は24年前半に予定されています。

さらに、SnapCenterには次の機能があります。

- カスタムプラグインを作成する機能。独自のプラグインを作成してSnapCenterで使用できます。これらのコミュニティでサポートされているプラグインの詳細については、NetAppオートメーションストアを参照してください。

SnapCenterでは、一元化されたRole-Based Access Control（RBAC；ロールベースアクセス制御）も使用でき、すべてのプラグインを対象としたレポートと一元化されたダッシュボードも提供されます。

SnapCenterの詳細については、次のリンクを参照してください。

NetApp Support Site -すべての製品- SnapCenter（Guide Me）

Microsoft SQL Serverデータベースの保護

SnapCenter Plug-in for Microsoft SQL Serverは、Snapshotデータの管理と保護を目的とした、複数のアプリケーション/データベースを一元管理するSnapCenterフレームワークの一部です。SnapManager®for Microsoft SQL Server製品と同等の機能を備えていますが、パフォーマンスと拡張性を向上させるためにSnapCenterプラグインが完全に書き換えられました。SnapCenterは、2012年から2022年までMicrosoft SQL Serverバージョンをサポートしています。SnapCenter Plug-in for Microsoft SQL Serverのライセンスは SnapCenter Standardライセンスに含まれているため、追加ライセンスは必要ありません。

SnapCenter SQLプラグインの設定およびSQLデータベースのバックアップとリストアについては、次のCVDを参照してください。

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_sql2022_xseries.html

まとめ

攻撃者がランサムウェアを生成して拡散する新しい方法を見つけると、ランサムウェアの検出と削除のための新しい手法を開発し、採用する必要があります。Cloud Insightsのワークロードセキュリティ機能は、NetAppセキュリティの優れたツールです。ユーザのデータアクセスパターンの変化に基づいてランサムウェア攻撃の可能性を検出し、ユーザアクセスをブロックして被害を最小限に抑えることができます。収集されたファイルとユーザアクティビティデータは、最大13カ月間、フォレンジックアクティビティとユーザ監査レポートに使用できます。コアONTAPを使用しているお客様は、Autonomous Ransomware Protection（ARP；自律型ランサムウェア対策）によるきめ細かな検出機能を利用できます。さらに、Cloud Insightsと統合して、アラートやフォレンジックのアクティビティを行うこともできます。いずれかの検出方法で生成されるSnapshotコピーは、攻撃に近いポイントにデータをリストアする場合に役立ち、攻撃による被害を最小限に抑えることができます。

ランサムウェアからのリカバリには、データのバックアップとリストアの処理が重要な役割を果たします。したがって、それらは事業計画にとって戦略的に重要です。これらのアクティビティの実装は、攻撃が発生した場合にレポート機能とリカバリ機能に妥協がないように、ランサムウェアリカバリ計画に含める必要があります。最も重要なことは、ランサムウェアの検出、削除、リストアを支援できる適切なテクノロジパートナーを選択することです。FlexPod with Cloud Insightsは、ランサムウェア攻撃や内部の脅威の可能性を監視して検出するために必要な機能を備えています。また、NetApp SnapCenter製品は、VMとアプリケーションと整合性のあるバックアップを作成し、必要に応じてデータをリストアします。

確認応答

このドキュメントの作成にご協力いただいた以下の方々に感謝申し上げます。

- マーク・コナハン、Cloud Insights PM
- Amit Schwartz、ワークロードセキュリティPM
- Sandeep Putrevu氏Insightエンジニアリング
- FlexPod TMEチーム（シスコおよびNetApp）

詳細情報の入手方法

- NetApp Cloud Insightsのドキュメント
  https://docs.netapp.com/us-en/cloudinsights/index.html
- SnapCenterソフトウェアのドキュメント
  https://docs.netapp.com/us-en/snapcenter/index.html
- 自律型ランサムウェア対策（ARP）
  https://docs.netapp.com/us-en/ontap/anti-ransomware/
- TR-4802：『FlexPod、the解決策to Ransomware』
  https://docs.netapp.com/us-en/flexpod/security/security-ransomware_what_is_ransomware.html#how-does-ransoms-work
- TR-4868：『NetApp Cloud Insights for FlexPod』
  https://docs.netapp.com/us-en/flexpod/hybrid-cloud/cloud-insights_netapp_cloud_insights_for_flexpod.html
- TR-4572：『The NetApp 解決策for ransomware』
  https://www.netapp.com/media/7334-tr4572.pdf

バージョン履歴

バージョン	日付	ドキュメントの改訂履歴
バージョン1.0	2023年3月	初版
バージョン2.0	2023年9月	▪ ランサムウェアからのリカバリ計画の一環として、VMと整合性のあるバックアップとリストアを行うためのSnapCenter Plug-in for VMware vSphereを追加。 ▪ 名前の変更を反映するため、Cloud Secureをワークロードセキュリティに置き換えました。 ▪ 現行のワークロードセキュリティグラフィカルユーザインターフェイスに基づいてテキストとスクリーンショットを更新。

本ドキュメントに記載されている製品や機能のバージョンがお客様の環境でサポートされるかどうかについては、NetApp サポート サイトで Interoperability Matrix Tool (IMT)を参照してください。NetApp IMT には、NetApp がサポートする構成を構築するために使用できる製品コンポーネントやバージョンが定義されています。サポートの可否は、お客様の実際のインストール環境が公表されている仕様に従っているかどうかによって異なります。

機械翻訳に関する免責事項

原文は英語で作成されました。英語と日本語訳の間に不一致がある場合には、英語の内容が優先されます。公式な情報については、本資料の英語版を参照してください。翻訳によって生じた矛盾や不一致は、法令の順守や施行に対していかなる拘束力も法的な効力も持ちません。

著作権に関する情報

商標に関する情報