ワークロードのセキュリティ
Data Infrastructure Insights

NetApp
December 19, 2024

目次

ワークロードのセキュリティ . . . 1
- ストレージワークロードのセキュリティについて . . . 1
- はじめに . . . 1
- アラート . . . 37
- フォレンジック . . . 44
- 自動応答ポリシー . . . 56
- 許可されたファイルタイプポリシー . . . 58
- ONTAP によるランサムウェア対策との統合 . . . 59
- ONTAPアクセス拒否との統合 . . . 62
- ユーザアクセスをブロックしています . . . 64
- ワークロードのセキュリティ：攻撃のシミュレーション . . . 69
- アラート、警告、およびエージェント / データソースコレクタの状態に関する電子メール通知の設定 . . . 73
- ワークロードセキュリティAPI . . . 74

ワークロードのセキュリティ

ストレージワークロードのセキュリティについて

データインフラに関するインサイトStorage Workload Security（旧称Cloud Secure）は、内部の脅威に関する実用的な情報に基づいてデータを保護します。ハイブリッドクラウド環境全体にわたるすべての企業データへのアクセスを一元的に可視化および制御できるため、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。

可視性

オンプレミスまたはクラウドに保存されている重要な企業データへのユーザアクセスを一元的に可視化し、制御できます。

データのアクセスと管理をタイムリーかつ正確に可視化できないツールや手動プロセスを置き換えます。ワークロードセキュリティは、クラウドストレージシステムとオンプレミスストレージシステムの両方で独自に動作し、悪意のあるユーザの行動をリアルタイムで警告します。

保護

高度な機械学習と異常検出機能により、悪意のあるユーザや悪意のあるユーザによる組織データの不正使用を防止します。

高度な機械学習とユーザの動作に関する異常検出によって、異常なデータアクセスをユーザに警告します。

コンプライアンス

オンプレミスまたはクラウドに保存されている重要な企業データへのユーザデータアクセスを監査することで、企業のコンプライアンスを確保します。

はじめに

ワークロードセキュリティの導入

Workload Securityを使用してユーザアクティビティを監視する前に、設定タスクを完了する必要があります。

ワークロードセキュリティシステムでは、エージェントを使用して、ストレージシステムからアクセスデータとディレクトリサービスサーバからのユーザ情報を収集します。

データの収集を開始する前に、次の項目を設定する必要があります。

タスク	関連情報

エージェントを設定します	"エージェントの要件" "エージェントを追加します" "* ビデオ * ：エージェントの配備"
ユーザディレクトリコネクタを設定します	"ユーザーディレクトリコネクターを追加します" "* ビデオ * ： Active Directory 接続"
データコレクタを設定する	[Workload Security]>[Collectors]をクリックし、設定するデータコレクタをクリックします。『**Data Collector Vendor Reference**』の項を参照してください。" ビデオ * ： **ONTAP SVM** 接続"
ユーザーアカウントを作成します	"ユーザアカウントを管理する"
トラブルシューティング	"* ビデオ * ：トラブルシューティング"

ワークロードセキュリティは、他のツールとも統合できます。たとえば、"このガイドを参照してください "Splunkとの統合などです。

ワークロードセキュリティエージェントの要件

データコレクタから情報を取得するには、必要があります"エージェントをインストールします"。Agent をインストールする前に、お使いの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の要件を満たしていることを確認してください。

コンポーネント	**Linux** 要件
オペレーティングシステム	* CentOS 8 Stream（64ビット）、CentOS 9 Stream、SELinux * openSUSE LEAP 15.3～15.5（64ビット）* Oracle Linux 8.6-8.8、9.1～9.4（64ビット）* Red Hat Enterprise Linux 8.6～9.4（64ビット）、9.1～9.4（64ビット）、SELinux * Rocky SP9.2-9.4専用のサーバを使用することを推奨します。
コマンド	インストールには「unzip」が必要です。また、インストール、スクリプトの実行、およびアンインストールには、「sudo su–」コマンドが必要です。
CPU	4個のCPUコア
メモリ	16GBのRAM
使用可能なディスクスペース	ディスク領域は次のように割り当てる必要があります。/opt/NetApp 36 GB (ファイルシステム作成後に35 GB以上の空き領域) 注:ファイルシステムを作成できるように、少し余分なディスク領域を割り当てることをお勧めします。ファイルシステムに35GB以上の空きスペースがあることを確認します。/optがNASストレージからマウントされたフォルダである場合は、ローカルユーザーがこのフォルダにアクセスできることを確認してください。ローカルユーザーがこのフォルダへのアクセス権を持っていない場合、AgentまたはData Collectorのインストールに失敗することがあります。詳細については、を参照してください。"トラブルシューティング"

コンポーネント	**Linux** 要件
ネットワーク	100 Mbps~1 Gbps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、および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は、Data Infrastructure Insights Acquisition Unitやエージェントと同じマシンにインストールできます。ただし、これらを別々のマシンにインストールすることを推奨します。これらが同じマシンにインストールされている場合は、次のようにディスク領域を割り当ててください。

使用可能なディスクスペース	Linux では 50 ～ 55 GB 、ディスクスペースは次のように割り当てます。 /opt/netapp 25-30 GB /var/log/netapp 25 GB

その他の推奨事項

- ONTAP システムとエージェントマシンの両方の時刻を、 *Network Time Protocol （ NTP; ネットワークタイムプロトコル） * または *Simple Network Time Protocol （ SNTP ） * を使用して同期することを強くお勧めします。

Cloud Network Access Rules の略

USベースの*ワークロード・セキュリティ環境の場合：

プロトコル	ポート	ソース	デスティネーション	製品説明
TCP	443	ワークロードセキュリティエージェント	< サイト名 > .cs01.cloudinsights.netapp.com < サイト名 > .c01.cloudinsights.netapp.com < サイト名 > .c02.cloudinsights.netapp.com	データインフラの分析情報へのアクセス
TCP	443	ワークロードセキュリティエージェント	gateway.c01.cloudinsights.netapp.com agentlogin.cs01.cloudinsights.netapp.com	認証サービスへのアクセス

欧州*ベースのワークロード・セキュリティー環境の場合：

プロトコル	ポート	ソース	デスティネーション	製品説明
TCP	443	ワークロードセキュリティエージェント	< サイト名 > .cs01-eu-1.cloudinsights.netapp.com < サイト名 > .c01-eu-1.cloudinsights.netapp.com < サイト名 > .c02-eu-1.cloudinsights.netapp.com	データインフラの分析情報へのアクセス
TCP	443	ワークロードセキュリティエージェント	gateway.c01.cloudinsights.netapp.com agentlogin.cs01-eu-1.cloudinsights.netapp.com	認証サービスへのアクセス

APACベースの*ワークロード・セキュリティ環境の場合：

プロトコル	ポート	ソース	デスティネーション	製品説明
TCP	443	ワークロードセキュリティエージェント	< サイト名 > .cs01-ap-1.cloudinsights.netapp.com < サイト名 > .c01-ap-1.cloudinsights.netapp.com < サイト名 > .c02-ap-1.cloudinsights.netapp.com	データインフラの分析情報へのアクセス
TCP	443	ワークロードセキュリティエージェント	gateway.c01.cloudinsights.netapp.com agentlogin.cs01-ap-1.cloudinsights.netapp.com	認証サービスへのアクセス

ネットワーク内ルール

プロトコル	ポート	ソース	デスティネーション	製品説明
TCP	389 （ LDAP ） 636 （ LDAPS / start-TLS ）	ワークロードセキュリティエージェント	LDAP サーバ URL	LDAP に接続します
TCP	443	ワークロードセキュリティエージェント	クラスタまたはSVMの管理IPアドレス（SVMコレクタの設定に応じて）	ONTAP との API 通信

プロトコル	ポート	ソース	デスティネーション	製品説明
TCP	35000 ~ 55000	SVM データ LIF の IP アドレス	ワークロードセキュリティエージェント	FPolicyイベントのONTAPからワークロードセキュリティエージェントへの通信。ONTAPがイベントをワークロードセキュリティエージェントに送信するには、これらのポートをワークロードセキュリティエージェントに対して開いておく必要があります。これには、ワークロードセキュリティエージェント自体のファイアウォールも含まれます（存在する場合）。これらのポートをすべて予約する必要はありませんが、予約するポートはこの範囲内である必要があります。最初に最大100個のポートを予約し、必要に応じて増やすことをお勧めします。
TCP	7	ワークロードセキュリティエージェント	SVM データ LIF の IP アドレス	エージェントからSVMのデータLIFへのエコー
SSH	22	ワークロードセキュリティエージェント	クラスタ管理	CIFS / SMBユーザブロックに必要です。

システムのサイジング

サイジングの詳細については、のドキュメントを参照して"イベントレートチェッカー"ください。

ワークロードセキュリティエージェントのインストール

ワークロードセキュリティ（旧Cloud Secure ）は、1つ以上のエージェントを使用してユーザアクティビティデータを収集します。エージェントはテナントのデバイスに接続し、ワークロードセキュリティSaaS層に送信されたデータを収集して分析します。エージェントVMを設定するには、を参照してください"エージェントの要件"。

開始する前に

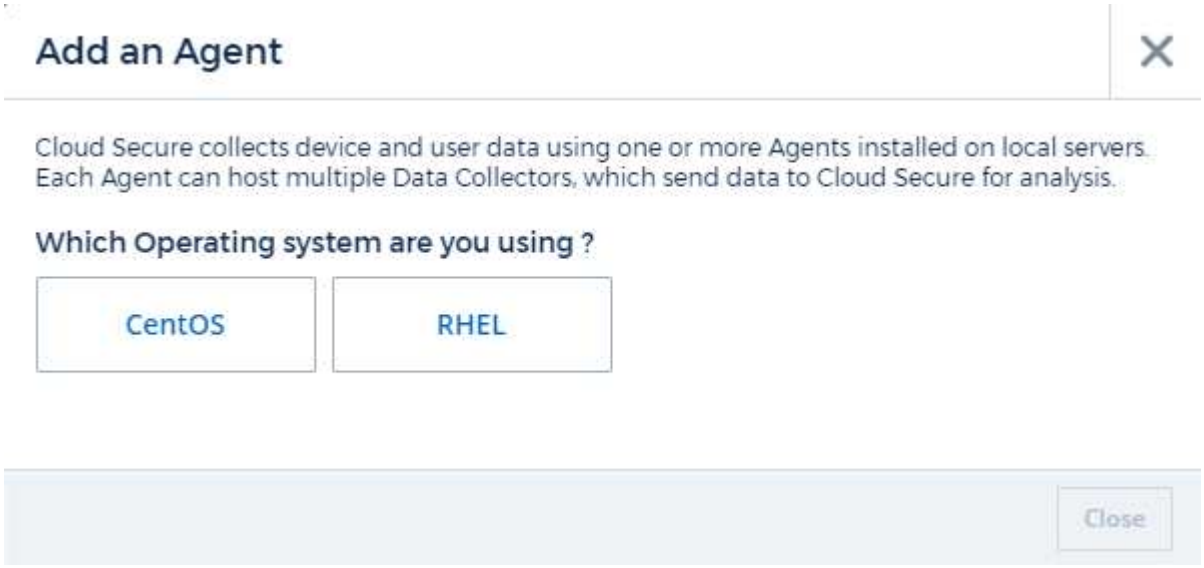
- インストール、スクリプトの実行、アンインストールには sudo 権限が必要です。

- エージェントのインストール中に、ローカルのuser_cssys_とローカルのgroup_cssys_がマシン上に作成されます。権限設定でローカルユーザの作成が許可されておらず、Active Directoryが必要な場合は、Active Directoryサーバにusername_csys_という名前のユーザを作成する必要があります。
- Data Infrastructure Insightsのセキュリティについては"ここをクリック"、こちらをご覧ください。

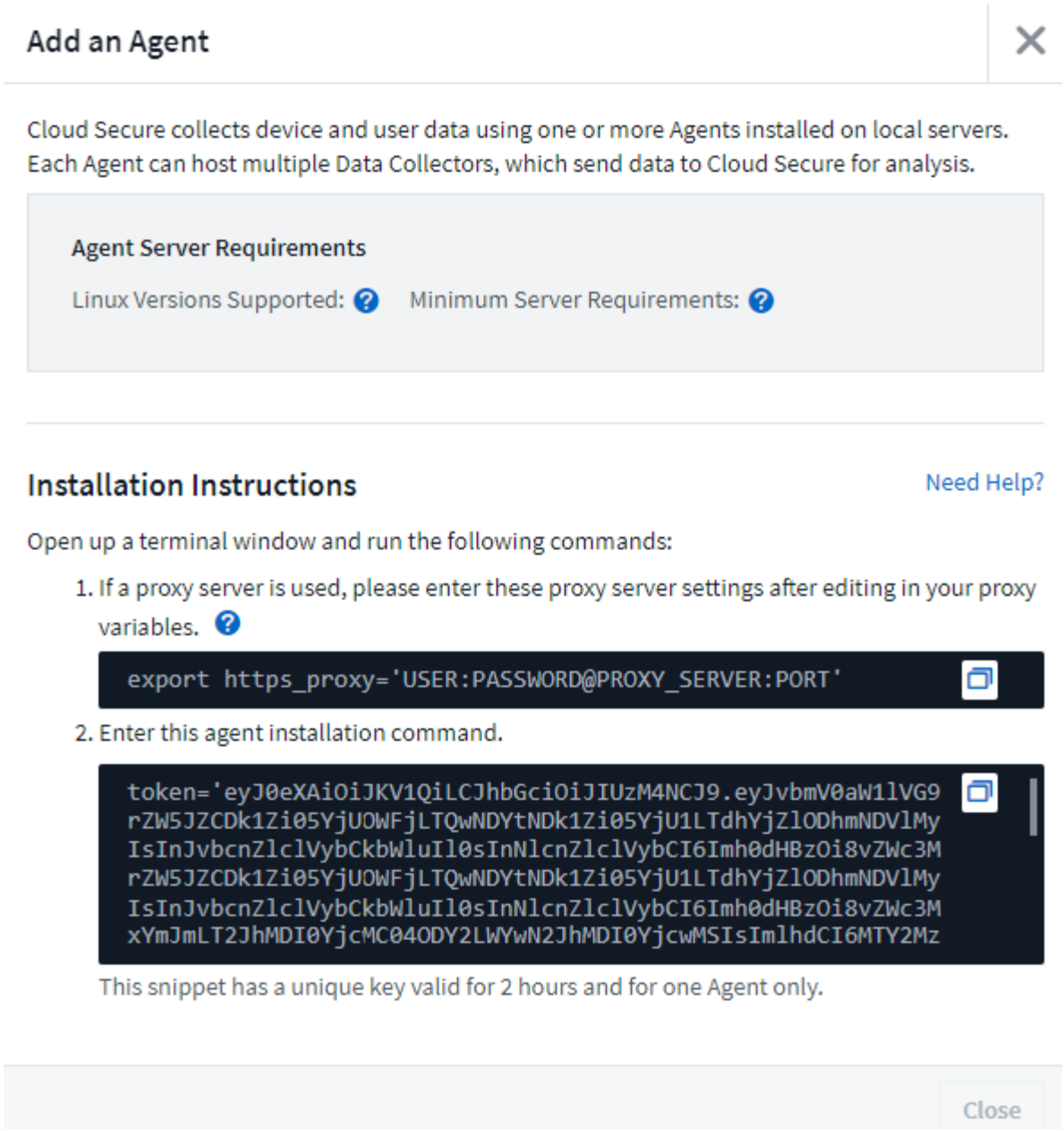
エージェントをインストールする手順

1. ワークロードセキュリティ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. [Collectors]>[Agents]>[+Agent]を選択します。

   [エージェントの追加] ページが表示されます。



3. エージェントサーバが最小システム要件を満たしていることを確認します。
4. エージェントサーバでサポートされているバージョンの Linux が実行されていることを確認するには、 _ サポートされているバージョン（ i ） _ をクリックします。
5. ネットワークでプロキシサーバを使用している場合は、プロキシセクションの指示に従ってプロキシサーバの詳細を設定してください。



6. [クリップボードにコピー] アイコンをクリックして、インストールコマンドをコピーします。
7. ターミナルウィンドウでインストールコマンドを実行します。
8. インストールが正常に完了すると、次のメッセージが表示されます。

完了後

1. を設定する必要があり"User Directory Collector の略"ます。
2. 1 つ以上のデータコレクタを設定する必要があります。

ネットワーク構成

ローカルシステム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。ポート範囲に関するセキュリティ上の問題がある場合は、 *35000 ： 35100* のように小さいポート範囲を使用できます。各 SVM は 2 つのポートを使用します。

手順

1. `sudo firewall-cmd --permanent --zone=public --add-port=35000-55000/tcp`
2. `sudo firewall-cmd --reload`

プラットフォームに応じて、次の手順を実行します。

- CentOS 7.x / RHEL 7.x * ：
  1. `sudo iptables-save | grep 35000`

出力例：

```
 -A IN_public_allow -p tcp -m tcp --dport 35000:55000 -m conntrack
-ctstate NEW,UNTRACKED -j ACCEPT
* CentOS 8.x / RHEL 8.x * ：
```

1. `sudo firewall-cmd --zone=public --list-ports | grep 35000`（CentOS 8の場合）

出力例：

```
35000-55000/tcp
```

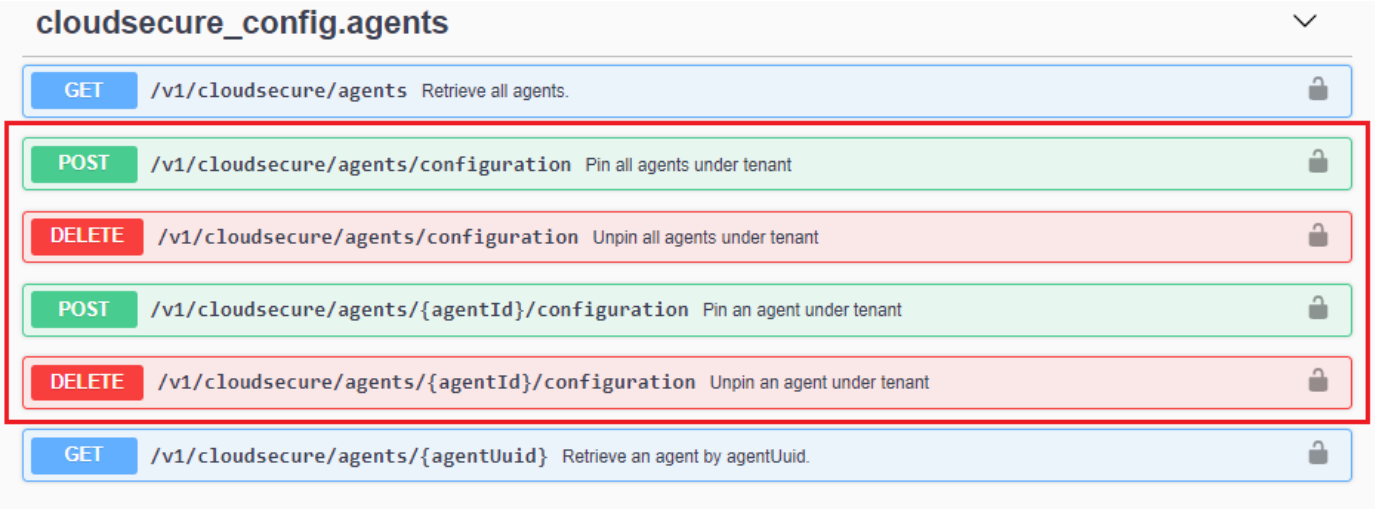
現在のバージョンでエージェントを「固定」する

デフォルトでは、Data Infrastructure Insights Workload Securityはエージェントを自動的に更新します。お客様によっては、自動更新を一時停止したい場合があります。これにより、次のいずれかが発生するまで、Agentは現在のバージョンのままになります。

- カスタマーはエージェントの自動更新を再開します。
- 30日が過ぎました。30日間は、エージェントが一時停止された日ではなく、最新のエージェント更新の日に開始されます。

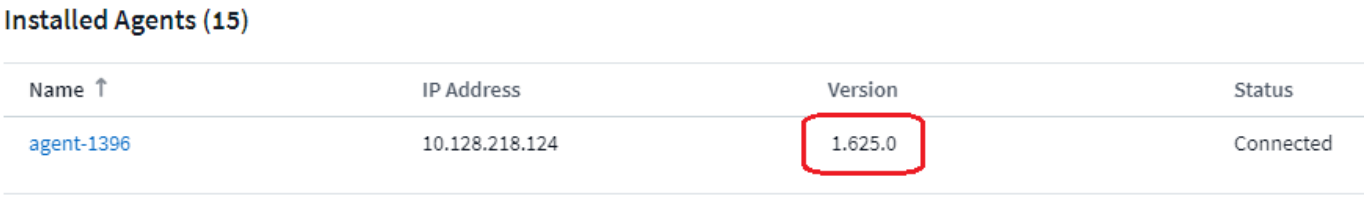
これらのいずれの場合も、エージェントは次回のワークロードセキュリティ更新時に更新されます。

エージェントの自動更新を一時停止または再開するには、_cloudsecure_config.agents_APIを使用します。



一時停止または再開のアクションが有効になるまで、最大5分かかることがあります。

現在のエージェントのバージョンは、*ワークロードセキュリティ>コレクタ*ページの*エージェント*タブで確認できます。



エージェントエラーのトラブルシューティング

既知の問題とその解決策を次の表に示します。

問題	解決策：
エージェントのインストール時に /opt/NetApp/cloudsecure/agent/logs/agent.log フォルダが作成されず、 install.log ファイルに関連情報が記録されません。	このエラーは、エージェントのブートストラップ中に発生します。ロガーが初期化される前に発生するため、エラーはログファイルに記録されません。エラーは標準出力にリダイレクトされ、 `journalctl -u cloudsecure-agent.service`コマンドを使用してサービスログに表示されます。このコマンドは、問題の詳細なトラブルシューティングに使用できます。est
「この Linux ディストリビューションはサポートされていません。インストールを終了しています。	このエラーは、サポートされていないシステムにAgentをインストールしようとしたときに表示されます。を参照して "エージェントの要件"
エージェントのインストールが次のエラーで失敗しました： "-bash: unzip: command not found"	unzip をインストールし、インストールコマンドを再度実行します。Yum がマシンにインストールされている場合は、「 yum install unzip 」を実行して解凍ソフトウェアをインストールしてください。その後、 Agent インストール UI からコマンドをコピーして CLI に貼り付け、再度インストールを実行します。

問題	解決策：

エージェントがインストールされ、実行されていました。しかし、エージェントは突然停止しました。	Agent マシンに SSH 接続します。でエージェントサービスのステータスを確認します `sudo systemctl status cloudsecure-agent.service`。1.ログに「Failed to start Workload Security daemon service」というメッセージが表示されているかどうかを確認します。2.csysユーザがAgentマシンに存在するかどうかを確認します。次のコマンドを root 権限で 1 つずつ実行し、 cssys ユーザとグループが存在するかどうかを確認します。
	`sudo id cssys`
	`sudo groups cssys`3.存在しない場合は、集中型モニタリングポリシーによって `cssys` ユーザが削除されている可能性があります。4.次のコマンドを実行して、csysユーザおよびグループを手動で作成します。
	`sudo useradd cssys`
	`sudo groupadd cssys`5.その後、次のコマンドを実行してエージェントサービスを再起動します。
	`sudo systemctl restart cloudsecure-agent.service`まだ実行されていない場合は、他のトラブルシューティングオプションを確認してください。

エージェントには50個を超えるデータコレクタを追加できません。	エージェントに追加できるデータコレクタは 50 個までです。Active Directory 、 SVM 、その他のコレクタなど、すべてのコレクタタイプを組み合わせて使用できます。
Agent is in not_connected 状態であることが UI に表示されます。	エージェントを再起動する手順。1.Agent マシンに SSH 接続します。2.その後、次のコマンドを実行してエージェントサービスを再起動します。 `sudo systemctl restart cloudsecure-agent.service`でエージェントサービスのステータスを確認します `sudo systemctl status cloudsecure-agent.service`。4.エージェントは接続状態に移行する必要があります。
エージェント VM が Zscaler プロキシの背後にあり、エージェントのインストールに失敗しています。ZscalerプロキシのSSL検査により、ワークロードセキュリティ証明書はZscaler CAによって署名されたため、エージェントが通信を信頼していないと表示されます。	*.cloudinsights.netapp.com URL の Zscaler プロキシで SSL 検査をディセーブルにします。ZscalerがSSLを検査して証明書を置き換えた場合、Workload Securityは機能しません。

問題	解決策：
エージェントのインストール中に、解凍後にインストールがハングします。	「 chmod 755 -rf 」コマンドが失敗しています。このコマンドは、別のユーザに属する作業ディレクトリ内のファイルを含む root 以外の sudo ユーザがエージェントのインストールコマンドを実行している場合は失敗し、それらのファイルの権限を変更することはできません。失敗した chmod コマンドのため、残りのインストールは実行されません。1.「cloudsecure」という名前の新しいディレクトリを作成します。2.そのディレクトリに移動します。3.完全な「token=……/cloudsecure-agent-install.sh」インストールコマンドをコピーして貼り付け、Enterキーを押します。4.インストールを続行できます。
エージェントがまだ SaaS に接続できない場合は、ネットアップサポートでケースをオープンしてください。Data Infrastructure Insightsのシリアル番号を提供してケースをオープンし、記録したとおりにログをケースに添付します。	ケースにログを添付するには、次の手順を実行します。 1.root権限で以下のスクリプトを実行し、出力ファイル(cloudsecure-agent-symptions.zip)を共有しますNetApp /cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh。次のコマンドをroot権限で1つずつ実行し、出力を共有します。a. id csys b. groups csys ccat /etc/os-release
cloudsecure-agent-symptom-collector.shスクリプトが次のエラーで失敗します。[root@machine tmp]#/opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.shサービスログの収集アプリケーションログの収集エージェント設定の収集エージェントディレクトリ構造スナップショットの取得中のサービスステータススナップショット…… 。…… 。/opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh：line 52：zip：command not found error：/tmp/cloudsecure-agent-symptoms.zipを作成できませんでした	ZIPツールがインストールされていません。コマンド「yum install zip」を実行してzipツールをインストールします。次に、cloudsecure-agent-symptom-collector.shを再度実行します。
エージェントのインストールに失敗し、useradd ：Cannot create directory/home/cssysというメッセージが表示されます	このエラーは、権限がないためにユーザのログインディレクトリを/homeの下に作成できない場合に発生することがあります。回避策 では、次のコマンドを使用してcssysユーザを作成し、そのログインディレクトリを手動で追加します。_sudo useradd user_name -m -d home_DIR_m：ユーザのホームディレクトリがない場合は作成します。-d：新しいユーザは'ユーザのログイン・ディレクトリの値としてhome_DIRを使用して作成されますたとえば、_sudo useradd cssys-m-d/cssys_はuser_cssys_を追加し、rootの下にそのログインディレクトリを作成します。

問題	解決策：
エージェントはインストール後に実行されていません。*systemctl status cloudsecure-agent.service* NetApp cloudsecure-agent.service:には次の情報が表示されます。[root@demo ~]# systemctl status cloudsecure-agent.service agent.service /cloudsecure/agent/bin/cloudsecure-agent n/a–Workload Security Agent Daemon Service Loaded: Loaded (/usr/lib/systemd/system/cloudsecure-agent.service; enabled; vendor preset : disabled) cloudsecure-agent.service8月03日21：12：26 demo systemd [1]：cloudsecure-agent.serviceが失敗しました。	これは'_cssys_userにインストール権限がないために失敗することがあります/opt/netappがNFSマウントで、_cssys_userがこのフォルダにアクセスできない場合、インストールは失敗します。_cssys_は、マウントされた共有にアクセスする権限がない可能性があるワークロードセキュリティインストーラによって作成されたローカルユーザです。これを確認するには、_cssys_userを使用して/opt/netapp/cloudsecure/agent/bin/cloudsecure-agentにアクセスします。「Permission denied」が返された場合、インストール許可は表示されません。マウントされたフォルダではなく、マシンのローカルディレクトリにインストールします。
エージェントは最初にプロキシサーバを介して接続され、エージェントのインストール時にプロキシが設定されました。これでプロキシサーバが変更されました。エージェントのプロキシ設定はどのように変更できますか。	agent.propertiesを編集して、プロキシの詳細を追加できます。次の手順を実行します。1.プロパティファイルが格納されているフォルダ（cd /opt/netapp/cloudsecure/conf 2）に変更します。任意のテキストエディタを使用して、_agent.properties_ファイルを開いて編集します。3.次の行を追加または変更しま す。agent_proxy_host=scspa1950329001.vm.com NetApp agent_proxy_port=80 agent_proxy_user=pxuser agent_proxy_password=pass1234 4.ファイルを保存します。5.エージェントを再起動します。sudo systemctl restart cloudsecure-agent.service

ワークロードセキュリティエージェントの削除

ワークロードセキュリティエージェントを削除する場合は、そのエージェントに関連付けられているすべてのデータコレクタを先に削除する必要があります。

エージェントの削除

エージェントを削除すると、そのエージェントに関連付けられているすべてのデータコレクタが削除されます。別のエージェントでデータコレクタを設定する場合は、 Agent を削除する前に、 Data Collector 設定のバックアップを作成する必要があります。

開始する前に

1. ワークロードセキュリティポータルから、エージェントに関連付けられているすべてのデータコレクタが削除されていることを確認します。

   注：関連するすべてのコレクタが停止状態にある場合は、この手順を無視してください。

エージェントを削除する手順：

1. エージェント VM に SSH 接続し、次のコマンドを実行します。プロンプトが表示されたら、「 y 」と入力して続行します。

```
sudo /opt/netapp/cloudsecure/agent/install/cloudsecure-agent-
uninstall.sh
Uninstall CloudSecure Agent? [y|N]:
```

2. [Workload Security]>[Collectors]>[Agents]*をクリックします。

   設定されたエージェントのリストが表示されます。

3. 削除するエージェントのオプションメニューをクリックします。
4. [削除（ Delete ）] をクリックします。

   [エージェントの削除 *] ページが表示されます。

5. 削除を確認するには、 * Delete * をクリックします。

Active Directory （ AD ）ユーザディレクトリコレクタの設定

ワークロードセキュリティは、Active Directoryサーバからユーザ属性を収集するように設定できます。

開始する前に

- このタスクを実行するには、Data Infrastructure Insightsの管理者またはアカウント所有者である必要があります。
- Active Directory サーバをホストしているサーバの IP アドレスを確認しておく必要があります。
- ユーザディレクトリコネクタを設定する前に、エージェントを設定する必要があります。

ユーザーディレクトリコレクタの設定手順

1. [Workload Security]メニューで、**[Collectors]>[User Directory Collector]>[+ User Directory Collector]*** をクリックし、[Active Directory]*を選択します。

   [Add User Directory] 画面が表示されます。

次の表に必要なデータを入力して、 User Directory Collector を設定します。

名前	製品説明
名前	ユーザディレクトリの一意の名前。例： *GlobalADCollector*
エージェント	リストから設定済みエージェントを選択します
サーバの IP / ドメイン名	Active Directory をホストしているサーバの IP アドレスまたは完全修飾ドメイン名（ FQDN ）

フォレスト名	ディレクトリ構造のフォレストレベル。フォレスト名には、 SVM で所有しているドメイン名と同様に、 *x.y.z _⇒* 、 *Direct domain name* の両方の形式が使用できます。*[* 例： *hq.companyname.com] _DC= x* 、 *DC=y* 、 *DC=z⇒* 相対識別名（例： DC=HQ 、 DC=companyname 、 DC=com ）。あるいは、次のように指定できます。 *OU=engineering* 、 *DC=HQ* 、 *DC=companyname* 、 *DC=com*[特定の OU でフィルタリング] _CN=username 、 OU=engineering 、 DC=companyname 、 DC=netapp 、 DC=com [指定のユーザだけを OU から取得] <engineering>]_CN=Acrobat ユーザ、 CN=Users 、 DC=users 、 DC=user 、 DC=s以降 、 <company=c 、 <company>s 、 <company=c 、 <company>s 、 <company>s 、 <companyname=c 、 <company>s 、 <username> で、 <users,<users,<users,<username>s 、 <users,<username>s 、 <username,<users,<user> 、 <username,<users,<
バインド DN	ディレクトリの検索が許可されています。例:_username@companyname.com_または_username@domainname.com_また、ドメイン読み取り専用権限が必要です。ユーザは、セキュリティグループ_Read-Only Domain Controllers_のメンバーである必要があります。
バインドパスワード	ディレクトリサーバのパスワード（バインド DN で使用されるユーザ名のパスワード）
プロトコル	LDAP 、 ldaps 、 ldap-start-TLS
ポート	ポートを選択します

Active Directory でデフォルトの属性名が変更されている場合は ' 次の Directory Server 必須属性を入力しますほとんどの場合、これらの属性名は Active Directory で _not_modified となります。この場合、デフォルトの属性名をそのまま使用できます。

属性	ディレクトリサーバの属性名
表示名	名前
SID	objectSID を指定します
ユーザー名	sAMAccountName

次の属性を追加するには、オプション属性を含めるをクリックします。

属性	ディレクトリサーバの属性名
Eメールアドレス	メール
電話番号	電話番号
ロール	タイトル
国	共同

都道府県	状態
部門	部門
写真	サムネイル写真
ManagerDN	マネージャー
グループ	メンバーOf

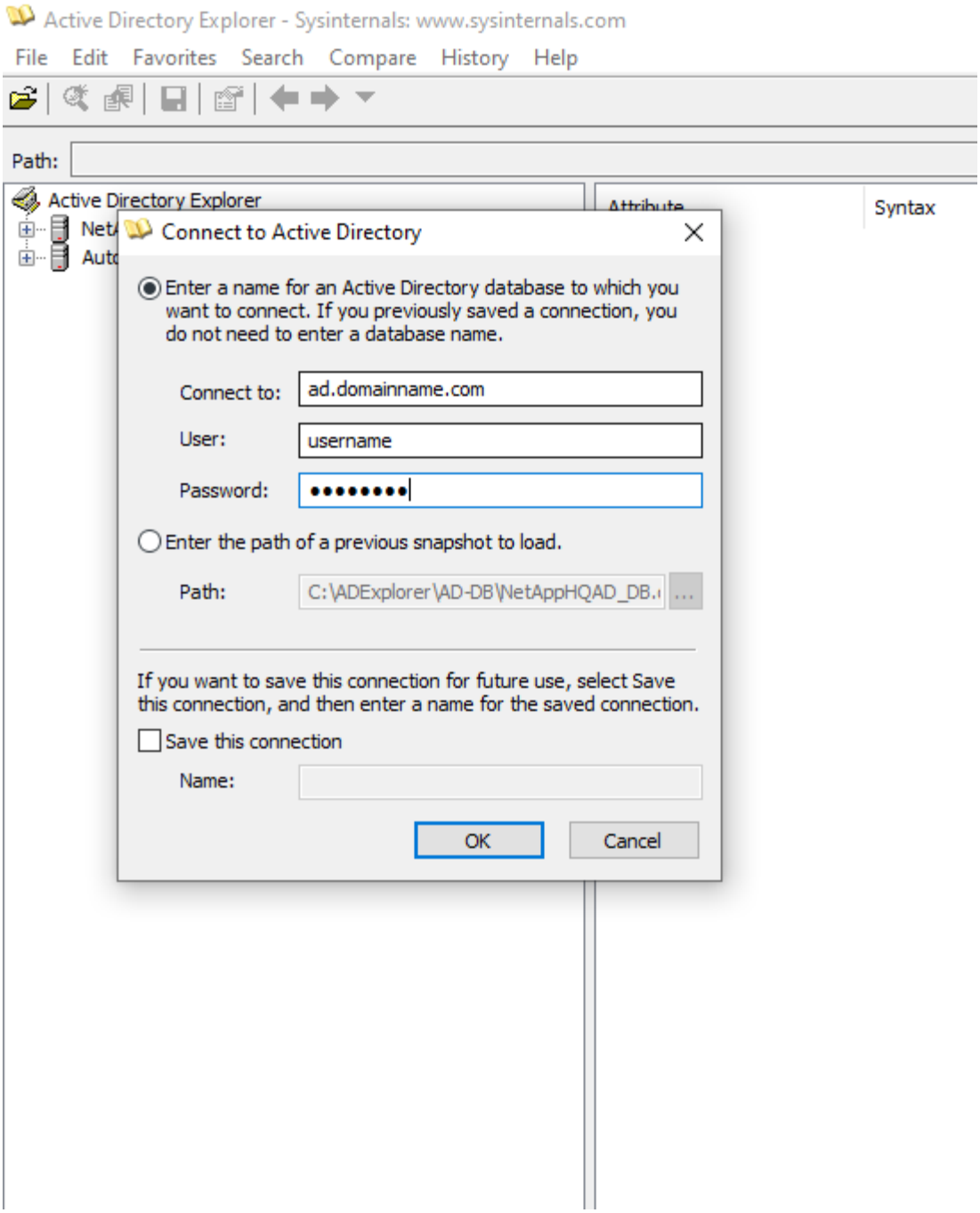
ユーザディレクトリコレクタ設定のテスト

LDAP ユーザ権限および属性定義は、次の手順で検証できます。

- 次のコマンドを使用して、ワークロードセキュリティのLDAPユーザ権限を検証します。

```
ldapsearch -o ldif-wrap=no -LLL -x -b "dc=netapp,dc=com" -h 10.235.40.29 -p
389 -D Administrator@netapp.com -W
```

- AD エクスプローラを使用して、 AD データベースの移動、オブジェクトのプロパティと属性の表示、権限の表示、オブジェクトのスキーマの表示、高度な検索の実行を行い、保存して再実行することができます。
  - ADサーバに接続できるすべてのWindowsマシンにインストールします"AD エクスプローラ"。
  - ADディレクトリサーバのユーザ名/パスワードを使用してADサーバに接続します。



ユーザディレクトリコレクタ設定エラーのトラブルシューティング

次の表に、コレクタの設定時に発生する可能性のある既知の問題と解決策を示します。

問題	解決策：
ユーザディレクトリコネクタを追加すると、「エラー」状態になります。「 Invalid credentials provided for LDAP server 」 (LDAP サーバーの資格情報が無効です) というエラーが表示されます	入力したユーザ名またはパスワードが正しくありません。を編集し、正しいユーザ名とパスワードを入力します。

問題	解決策：
ユーザディレクトリコネクタを追加すると、「エラー」状態になります。「 DN=DC=HQ,DC=domainname,DC=com に対応するオブジェクトをフォレスト名として提供できませんでした」というエラーが表示されます。	指定したフォレスト名が正しくありません。正しいフォレスト名を編集して入力します。
ドメインユーザーのオプションの属性は、[ワークロードセキュリティユーザープロファイル]ページに表示されません。	これは、 CloudSecure で追加されたオプション属性の名前と Active Directory の実際の属性名が一致しないことが原因である可能性があります。正しいオプションの属性名を編集して入力します。
データコレクタでエラーが発生し、「 LDAP ユーザを取得できませんでした。失敗の理由：サーバに接続できません。接続が null です "	_Restart_Button をクリックして、コレクタを再起動します。
ユーザディレクトリコネクタを追加すると、「エラー」状態になります。	必須フィールドに有効な値（ Server 、 forest-name 、 bind-dn 、 bind-Password ）が指定されていることを確認してください。bind-DN 入力が常に「 Administrator@<domain_forest_name> 」またはドメイン管理者権限を持つユーザーアカウントとして提供されていることを確認してください。
ユーザディレクトリコネクタを追加すると、「再試行中」の状態になります。「 Unable to define state of the collector 、 reason TCP command [Connect (localhost:35012, None, List() 、 some (,seconds),true)] failed because of java.net.ConnectionException:Connection refused 」というエラーが表示されます。	AD サーバに対して指定された IP または FQDN が正しくありません。を編集し、正しい IP アドレスまたは FQDN を指定します。
ユーザディレクトリコネクタを追加すると、「エラー」状態になります。「 LDAP 接続の確立に失敗しました」というエラーが表示されます。	AD サーバに対して指定された IP または FQDN が正しくありません。を編集し、正しい IP アドレスまたは FQDN を指定します。
ユーザディレクトリコネクタを追加すると、「エラー」状態になります。「設定をロードできませんでした。理由：データソースの設定でエラーが発生しました。具体的な理由： /connector/conf/application.conf ： 70 ： ldap.ldap-port には number ではなく string 型があります。	指定したポートの値が正しくありません。AD サーバのデフォルトのポート値または正しいポート番号を使用してみてください。
必須属性から始めて、機能しました。オプションの属性を追加した後、オプションの属性データは AD から取得されません。	これは、 CloudSecure で追加されたオプションの属性と Active Directory の実際の属性名が一致しないことが原因である可能性があります。正しい必須またはオプションの属性名を編集して入力します。
コレクタの再起動後、 AD 同期はいつ行われますか。	コレクタが再起動するとすぐに AD 同期が実行されます。約 15 分で約 30 万人のユーザデータが取得され、 12 時間ごとに自動的に更新されます。
ユーザデータは AD から CloudSecure に同期されます。データを削除するタイミング	更新がない場合、ユーザデータは 13 カ月間保持されます。テナントが削除されると、データは削除されます。

問題	解決策：
ユーザーディレクトリコネクタが「エラー」状態になります。" コネクタでエラーが発生しました。サービス名： usersLDAP 。失敗の理由： LDAP ユーザを取得できませんでした。失敗の理由： 80090308 ： LdapErr: DSID-0C090453 、 comment: AcceptSecurityContext error 、 data 52e 、 v3839	指定したフォレスト名が正しくありません。正しいフォレスト名を指定する方法については、上記を参照してください。
電話番号がユーザプロファイルページに入力されていません。	これは、多くの場合、 Active Directory の属性マッピングの問題が原因です。1.Active Directoryからユーザーの情報を取得する特定のActive Directoryコレクタを編集します。2.オプションの属性の下には、Active Directory属性「telephonenumber」にマッピングされたフィールド名「電話番号」があります。4.ここで、前述のようにActive Directoryエクスプローラツールを使用してActive Directoryを参照し、正しい属性名を確認してください。3.Active Directory に「telephonenumber」という名前の属性があり、実際にユーザの電話番号が含まれていることを確認します。5.Active Directoryで「phonenumber」に変更されているとします。6.次に、CloudSecure User Directoryコレクタを編集します。オプションの属性セクションで、「 telephonenumber 」を「 phonenumber 」に置き換えます。7.Active Directory コレクタを保存すると、コレクタが再起動してユーザの電話番号を取得し、ユーザプロファイルページに同じ番号が表示されます。
Active Directory（AD）サーバで暗号化証明書（SSL）が有効になっている場合、Workload Security User Directory CollectorはADサーバに接続できません。	ユーザーディレクトリコレクタを設定する前に、 AD サーバーの暗号化を無効にします。ユーザの詳細情報が取得されてから 13 カ月間表示されます。ユーザーの詳細を取得した後に AD サーバーが切断された場合、新しく追加された AD 内のユーザーは取得されません。再度取得するには、ユーザディレクトリコレクタをADに接続する必要があります。
Active DirectoryのデータはCloudInsightsのセキュリティに存在します。CloudInsightsからすべてのユーザ情報を削除する必要がある。	CloudInsights SecurityからActive Directoryユーザー情報のみを削除することはできません。ユーザを削除するには、テナント全体を削除する必要があります。

LDAP Directory Server Collector の設定

ワークロードセキュリティを設定して、LDAPディレクトリサーバからユーザ属性を収集します。

開始する前に

- このタスクを実行するには、Data Infrastructure Insightsの管理者またはアカウント所有者である必要があります。
- LDAP ディレクトリサーバをホストしているサーバの IP アドレスを確認しておく必要があります。
- LDAP ディレクトリコネクタを設定する前に、エージェントを設定する必要があります。

ユーザーディレクトリコレクタの設定手順

1. [Workload Security]メニューで、**[Collectors]>[User Directory Collector]>[+ User Directory Collector]*** をクリックし、[LDAP Directory Server]*を選択します。

   [Add User Directory] 画面が表示されます。

次の表に必要なデータを入力して、 User Directory Collector を設定します。

名前	製品説明
名前	ユーザディレクトリの一意の名前。たとえば、「 *GlobalLDAPCollector* 」と入力します
エージェント	リストから設定済みエージェントを選択します
サーバの IP / ドメイン名	LDAP ディレクトリサーバをホストするサーバの IP アドレスまたは完全修飾ドメイン名（ FQDN ）
ベース検索	LDAP サーバ検索ベースの検索ベースでは、 SVM でドメイン名を直接指定する場合と、 *x.y.z _ = >* の両方の形式を使用できます。*[* 例： *hq.companyname.com] _DC= x* 、 *DC=y* 、 *DC=z⇒* 相対識別名（例： DC=HQ 、 DC=companyname 、 DC=com ）。あるいは、次のように指定できます。 *OU=engineering* 、 *DC=HQ* 、 *DC=companyname* 、 *DC=com*[特定の OU でフィルタリング] _CN=username 、 OU=engineering 、 DC=companyname 、 DC=netapp 、 DC=com [OU から <username> を使用する特定のユーザだけを取得] <engineering>]_CN=Acrobat ユーザ、 CN=Users 、 DC=users 、 DC=user 、 DC=s,DC=s以降 、 <company=c 、 <company=< 企業名 >
バインド DN	ディレクトリの検索が許可されています。例：uid=ldapuser、cn=users、cn=accounts、dc=domain、dc=companyname、dc=com uid=john、cn=users、cn=accounts、dc=dorp、dc=company、dc=com（ユーザjohn@dorp.company.comの場合）dorp.company.com
アカウント	ユーザ
―ジョン	―アンナ
バインドパスワード	ディレクトリサーバのパスワード（バインド DN で使用されるユーザ名のパスワード）
プロトコル	LDAP 、 ldaps 、 ldap-start-TLS
ポート	ポートを選択します

LDAP ディレクトリサーバでデフォルトの属性名が変更されている場合は ' 次の Directory Server 必須属性を入力しますこれらの属性名のほとんどは、 LDAP ディレクトリサーバで _not_modified となります。この場合、デフォルトの属性名をそのまま使用できます。

属性	ディレクトリサーバの属性名
表示名	名前

UNIX ID	uidNumber
ユーザー名	UID

次の属性を追加するには、オプション属性を含めるをクリックします。

属性	ディレクトリサーバの属性名
Eメールアドレス	メール
電話番号	電話番号
ロール	タイトル
国	共同
都道府県	状態
部門	部門番号
写真	写真
ManagerDN	マネージャー
グループ	メンバーOf

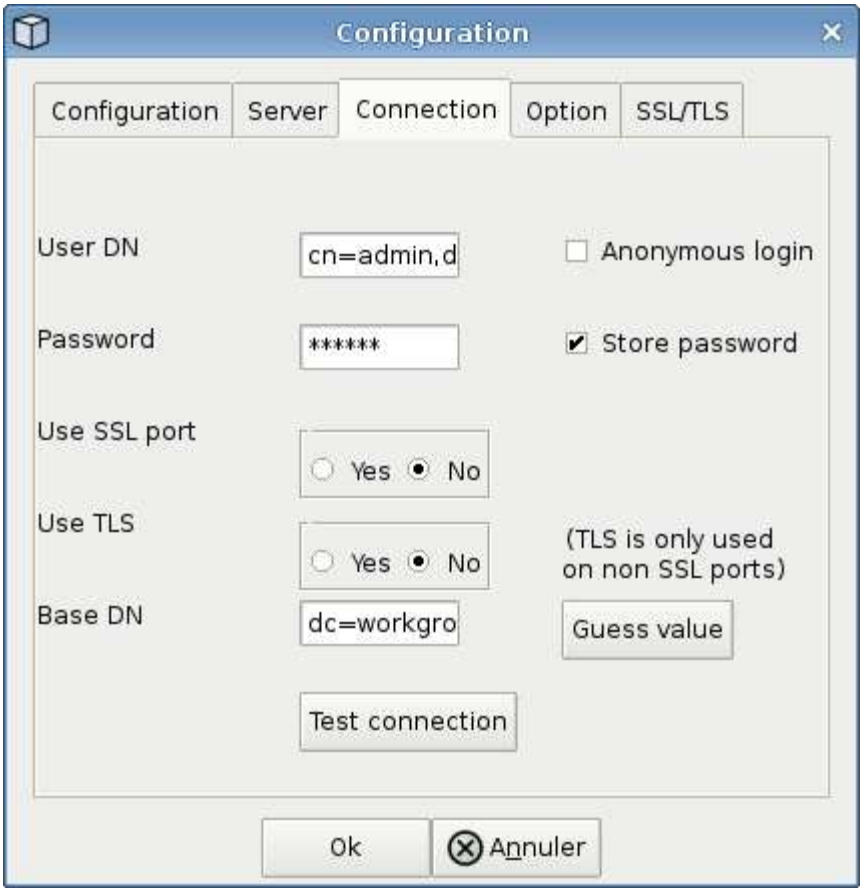
ユーザディレクトリコレクタ設定のテスト

LDAP ユーザ権限および属性定義は、次の手順で検証できます。

- 次のコマンドを使用して、ワークロードセキュリティのLDAPユーザ権限を検証します。

```
 ldapsearch -D "uid=john
,cn=users,cn=accounts,dc=dorp,dc=company,dc=com" -W -x -LLL -o ldif-
wrap=no -b "cn=accounts,dc=dorp,dc=company,dc=com" -H
ldap://vmwipaapp08.dorp.company.com
* LDAP エクスプローラを使用して、 LDAP
データベースの移動、オブジェクトのプロパティと属性の表示、権限の表示、オブジェクトのスキーマの表示、高度な検索の実行を行い、保存して再実行することができます。
```

  - LDAP(http://jxplorer.org/サーバーに接続できる任意のWindowsマシンに、LDAPエクスプローラ(http://ldaptool.sourceforge.net/またはJava LDAPエクスプローラをインストールします。
  - LDAPディレクトリサーバのユーザ名/パスワードを使用してLDAPサーバに接続します。



LDAP ディレクトリコレクタ設定エラーのトラブルシューティング

次の表に、コレクタの設定時に発生する可能性のある既知の問題と解決策を示します。

問題	解決策：
LDAP Directory Connector を追加すると、「 Error 」状態になります。「 Invalid credentials provided for LDAP server 」 (LDAP サーバーの資格情報が無効です) というエラーが表示されます	指定したバインド DN またはバインドパスワードまたは検索ベースが正しくありません。を編集し、正しい情報を入力します。
LDAP Directory Connector を追加すると、「 Error 」状態になります。「 DN=DC=HQ,DC=domainname,DC=com に対応するオブジェクトをフォレスト名として提供できませんでした」というエラーが表示されます。	入力された検索ベースが正しくありません正しいフォレスト名を編集して入力します。
ドメインユーザーのオプションの属性は、[ワークロードセキュリティユーザープロファイル]ページに表示されません。	これは、 CloudSecure で追加されたオプション属性の名前と Active Directory の実際の属性名が一致しないことが原因である可能性があります。フィールドでは大文字と小文字が区別されます正しいオプションの属性名を編集して入力します。
データコレクタでエラーが発生し、「 LDAP ユーザを取得できませんでした。失敗の理由：サーバに接続できません。接続が null です "	_Restart_Button をクリックして、コレクタを再起動します。

問題	解決策：
LDAP Directory Connector を追加すると、「 Error 」状態になります。	必須フィールドに有効な値（ Server 、 forest-name 、 bind-dn 、 bind-Password ）が指定されていることを確認してください。bind-DN 入力が常に uid=ldapuser,cn=Users,cn=account,dc=domain,dc=companyname,dc=com として提供されていることを確認します。
LDAP Directory Connector を追加すると、「再試行中」の状態になります。「 Failed to Determine the health of the collector したがって retrying again 」というエラーが表示されます。	正しいサーバIPと検索ベースが提供されていることを確認します///
LDAP ディレクトリの追加中に、「 Failed to Determine the collector within 2 retries 、 try restarting the collector again (Error Code: AGENT008) 」というエラーが表示されます。	正しいサーバ IP と検索ベースが提供されていることを確認します
LDAP Directory Connector を追加すると、「再試行中」の状態になります。「 Unable to define state of the collector 、 reason TCP command [Connect (localhost:35012, None, List() 、 some (,seconds),true)] failed because of java.net.ConnectionException:Connection refused 」というエラーが表示されます。	AD サーバに対して指定された IP または FQDN が正しくありません。を編集し、正しい IP アドレスまたは FQDN を指定します。////
LDAP Directory Connector を追加すると、「 Error 」状態になります。「 LDAP 接続の確立に失敗しました」というエラーが表示されます。	LDAP サーバに対して指定された IP または FQDN が正しくありません。を編集し、正しい IP アドレスまたは FQDN を指定します。または、指定されたポートの値が正しくありません。LDAP サーバのデフォルトのポート値または正しいポート番号を使用してみてください。
LDAP Directory Connector を追加すると、「 Error 」状態になります。「設定をロードできませんでした。理由：データソースの設定でエラーが発生しました。具体的な理由： /connector/conf/application.conf ： 70 ： ldap.ldap-port には number ではなく string 型があります。	指定したポートの値が正しくありません。AD サーバのデフォルトのポート値または正しいポート番号を使用してみてください。
必須属性から始めて、機能しました。オプションの属性を追加した後、オプションの属性データは AD から取得されません。	これは、 CloudSecure で追加されたオプションの属性と Active Directory の実際の属性名が一致しないことが原因である可能性があります。正しい必須またはオプションの属性名を編集して入力します。
コレクタの再起動後、 LDAP 同期はいつ行われますか。	コレクタが再起動するとすぐに LDAP 同期が実行されます。約 15 分で約 30 万人のユーザデータが取得され、 12 時間ごとに自動的に更新されます。
ユーザデータは LDAP から CloudSecure に同期されます。データを削除するタイミング	更新がない場合、ユーザデータは 13 カ月間保持されます。テナントが削除されると、データは削除されます。

問題	解決策：
LDAP Directory Connector により、「 Error 」状態になります。" コネクタでエラーが発生しました。サービス名： usersLDAP 。失敗の理由： LDAP ユーザを取得できませんでした。失敗の理由： 80090308 ： LdapErr: DSID-0C090453 、 comment: AcceptSecurityContext error 、 data 52e 、 v3839	指定したフォレスト名が正しくありません。正しいフォレスト名を指定する方法については、上記を参照してください。
電話番号がユーザプロファイルページに入力されていません。	これは、多くの場合、 Active Directory の属性マッピングの問題が原因です。1.Active Directoryからユーザーの情報を取得する特定のActive Directoryコレクタを編集します。2.オプションの属性の下には、Active Directory属性「telephonenumber」にマッピングされたフィールド名「電話番号」があります。4.ここで、前述のようにActive Directoryエクスプローラツールを使用してLDAPディレクトリサーバを参照し、正しい属性名を確認してください。3.LDAPディレクトリに「telephonenumber」という名前の属性があり、実際にはユーザの電話番号が含まれていることを確認します。5.LDAPディレクトリで'phonenumber'に変更されているとします。6.次に、CloudSecure User Directoryコレクタを編集します。オプションの属性セクションで、「 telephonenumber 」を「 phonenumber 」に置き換えます。7.Active Directoryコレクタを保存すると、コレクタが再起動してユーザの電話番号を取得し、ユーザプロファイルページに同じ番号が表示されます。
Active Directory（AD）サーバで暗号化証明書（SSL）が有効になっている場合、Workload Security User Directory CollectorはADサーバに接続できません。	ユーザーディレクトリコレクタを設定する前に、 AD サーバーの暗号化を無効にします。ユーザの詳細情報が取得されてから 13 カ月間表示されます。ユーザーの詳細を取得した後に AD サーバーが切断された場合、新しく追加された AD 内のユーザーは取得されません。再度取得するには、ユーザディレクトリコレクタが AD に接続されている必要があります。

ONTAP SVM Data Collector の設定

ワークロードセキュリティでは、データコレクタを使用して、デバイスからファイルとユーザのアクセスデータを収集します。

開始する前に

- このデータコレクタは、次の機能でサポートされています。
  - Data ONTAP 9.2 以降のバージョン最高のパフォーマンスを得るには、9.13.1よりも新しいバージョンのData ONTAPを使用してください。
  - SMBプロトコルバージョン3.1以前。
  - ONTAP 9.151以降を搭載したNFS 4.1以前のバージョン。
  - FlexGroup は ONTAP 9.4 以降のバージョンでサポートされます
  - ONTAP Select がサポートされています

- サポートされるのはデータタイプの SVM のみです。Infinite Volume を備えた SVM はサポートされません。
- SVM には複数のサブタイプがあります。このうち、サポートされるのは_DEFAULT_、*SYNC_SOURE*、および_SYNC_destination_のみです。
- データコレクタを設定する前のAgent"を設定する必要があります"。
- ユーザディレクトリコネクタが正しく設定されていることを確認します。正しく設定されていないと、イベントはエンコードされたユーザ名で表示され、 Active Directory に保存されているユーザの実際の名前ではなく、 [Activity Forensics] ページに表示されます。
- •ONTAP永続ストアは9.14.1以降でサポートされています。
- 最適なパフォーマンスを得るには、FPolicyサーバをストレージシステムと同じサブネットに設定する必要があります。
- 次のどちらかの方法で SVM を追加する必要があります。
  - クラスタ IP 、 SVM 名、およびクラスタ管理のユーザ名とパスワードを使用する。これは推奨される方法です。
    - SVM 名は ONTAP に表示されるとおりに指定する必要があり、大文字と小文字が区別されます。
  - SVM SVM 管理 IP 、ユーザ名、およびパスワードを使用する
  - 完全な管理者クラスタ/ SVM管理ユーザ名とパスワードを使用できない場合、または使用したくない場合は、以下のセクションで説明するように、Privilegesの小さいカスタムユーザを作成できます。「権限に関する注意事項」このカスタムユーザは、 SVM アクセスまたはクラスタアクセス用に作成できます。
    - o 以下の「権限に関するメモ」セクションに記載されているように、少なくとも csrole の権限を持つ役割を持つ AD ユーザを使用することもできます。も参照してください"ONTAPのドキュメント"。
- 次のコマンドを実行して、 SVM に正しいアプリケーションが設定されていることを確認します。

```
clustershell::> security login show -vserver <vservername> -user-or
-group-name <username>
```

出力例

```
Vserver: svmname
                                                                  Second
User/Group                  Authentication                 Acct   Authentication
Name           Application  Method        Role Name        Locked Method
-------------- -----------  ------------- ---------------- ------ --------------
vsadmin        http         password      vsadmin          no     none
vsadmin        ontapi       password      vsadmin          no     none
vsadmin        ssh          password      vsadmin          no     none
3 entries were displayed.
:
```

- SVMにCIFSサーバが設定されていることを確認します。clustershell：：：> `vserver cifs show`

  Vserver 名、 CIFS サーバ名、およびその他のフィールドが返されます。

- SVM の vsadmin ユーザのパスワードを設定します。カスタムユーザまたはクラスタ管理者ユーザを使用

する場合は、この手順はスキップします。clustershell：：：> `security login password -username vsadmin -vserver svmname`

- SVM の vsadmin ユーザの外部アクセスのロックを解除します。カスタムユーザまたはクラスタ管理者ユーザを使用する場合は、この手順はスキップします。clustershell：：：> `security login unlock -username vsadmin -vserver svmname`
- データ LIF のファイアウォールポリシーが「 GMT 」（「 data 」ではない）に設定されていることを確認します。専用の管理LIFを使用してSVMを追加する場合は、この手順をスキップします。clustershell：：：> `network interface modify -lif <SVM_data_LIF_name> -firewall-policy mgmt`
- ファイアウォールが有効になっている場合は、 Data ONTAP データコレクタを使用してポートの TCP トラフィックを許可する例外を定義する必要があります。

  設定については、を参照してください"エージェントの要件"。この環境オンプレミスエージェントおよびクラウドにインストールされたエージェント。

- Cloud ONTAP SVM を監視するために AWS EC2 インスタンスにエージェントがインストールされている場合は、そのエージェントとストレージが同じ VPC 内に存在する必要があります。これらの VPC が個別の VPC 内にある場合は、 VPC 間に有効なルートが必要です。

ユーザアクセスブロックの前提条件

次の点に注意して"ユーザアクセスブロック"ください。

この機能を使用するには、クラスタレベルのクレデンシャルが必要です。

クラスタ管理者のクレデンシャルを使用している場合、新しい権限は不要です。

ユーザに付与された権限でカスタムユーザ（_csuser_など）を使用している場合は、次の手順に従ってワークロードセキュリティにユーザをブロックする権限を付与します。

クラスタクレデンシャルを持つ csuser の場合、 ONTAP コマンドラインから次の手順を実行します。

```
security login role create -role csrole -cmddirname "vserver export-policy
rule" -access all
security login role create -role csrole -cmddirname set -access all
security login role create -role csrole -cmddirname "vserver cifs session"
-access all
security login role create -role csrole -cmddirname "vserver services
access-check authentication translate" -access all
security login role create -role csrole -cmddirname "vserver name-mapping"
-access all
```

アクセス権に関する注意事項

クラスタ管理**IP**を使用して追加する場合の権限：

クラスタ管理管理者ユーザがワークロードセキュリティを使用してONTAP SVMデータコレクタにアクセスできない場合は、次のコマンドに示すロールを持つ「csuser」という新しいユーザを作成できます。Cluster Management IPを使用するようにWorkload Securityデータコレクタを設定する場合は、「csuser」のユーザ名

とパスワードを使用します。

新しいユーザを作成するには、クラスタ管理者のユーザ名とパスワードを使用して ONTAP にログインし、ONTAP サーバで次のコマンドを実行します。

```
security login role create -role csrole -cmddirname DEFAULT -access
readonly
```

```
security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "volume snapshot"
-access all -query "-snapshot cloudsecure_*"
security login role create -role csrole -cmddirname "event catalog"
-access all
security login role create -role csrole -cmddirname "event filter" -access
all
security login role create -role csrole -cmddirname "event notification
destination" -access all
security login role create -role csrole -cmddirname "event notification"
-access all
security login role create -role csrole -cmddirname "security certificate"
-access all
```

```
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole
security login create -user-or-group-name csuser -application ssh
-authmethod password -role csrole
security login create -user-or-group-name csuser -application http
-authmethod password -role csrole
```

SVM管理**IP** *を使用して追加する場合の権限：

クラスタ管理管理者ユーザがワークロードセキュリティを使用してONTAP SVMデータコレクタにアクセスできない場合は、次のコマンドに示すロールを持つ「csuser」という新しいユーザを作成できます。Workload SecurityデータコレクタでSVM管理IPを使用するように設定する場合は、「csuser」のユーザ名とパスワードを使用します。

新しいユーザを作成するには、クラスタ管理者のユーザ名とパスワードを使用して ONTAP にログインし、ONTAP サーバで次のコマンドを実行します。これらのコマンドをテキストエディタにコピーし、<vservername> を SVM 名に置き換えてから、 ONTAP で次のコマンドを実行します。

```
security login role create -vserver <vservername> -role csrole -cmddirname
DEFAULT -access none
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"network interface" -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
version -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
volume -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
vserver -access readonly
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservername> -role csrole -cmddirname
"volume snapshot" -access all
```

```
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole -vserver <vservername>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrole -vserver <vservername>
```

プロトタイプモード

コレクタの_Advanced Configuration_settingsでこのオプションを有効にすると、ワークロードセキュリティによってFPolicyエンジンがprotobufモードで設定されます。ProtobufモードはONTAPバージョン9.15以降でサポートされています。

この機能の詳細については、を参照して"ONTAPのドキュメント"ください。

protobufには特定の権限が必要です（これらの一部またはすべてがすでに存在する場合があります）。

クラスタモード：

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole
```

SVMモード：

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <svm_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole -vserver <svm_name>
```

ONTAP Autonomous Ransomware Protectionの権限と**ONTAP**へのアクセス拒否

クラスタ管理者のクレデンシャルを使用している場合、新しい権限は不要です。

ユーザに付与された権限でカスタムユーザ（_csuser_など）を使用している場合は、次の手順に従ってワークロードセキュリティにアクセス許可を付与し、ONTAP からARP関連情報を収集します。

詳細については、"ONTAPアクセス拒否との統合"

および "ONTAP によるランサムウェア対策との統合"

データコレクタを設定します

設定の手順

1. Data Infrastructure 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]*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。
3. NetApp SVM のタイルにカーソルを合わせ、 * + 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ます。

フィールド	製品説明
名前	Data Collector の一意の名前
エージェント	リストから設定済みエージェントを選択します。
管理 IP 経由で接続：	クラスタ IP または SVM 管理 IP を選択します
クラスタ / SVM 管理 IP アドレス	上記の選択に応じて、クラスタまたは SVM の IP アドレス。
SVM 名	SVM の名前（このフィールドはクラスタ IP 経由で接続する場合は必須です）
ユーザ名	クラスタ IP を介して追加する場合に SVM / クラスタにアクセスするためのユーザ名。オプションは 1 です。cluster-admin 2.「 csuser 」 3.csuser と同様のロールを持つ ad-user 。SVM IPを使用して追加する場合のオプションは次のとおりです。4.vsadmin 5.「 csuser 」 6.csuser と同様のロールを持つ ad-username 。
パスワード	上記のユーザ名のパスワード

共有 / ボリュームをフィルタリングします	イベントコレクションに共有 / ボリュームを含めるか除外するかを選択します
除外または対象に含める共有名を入力します	イベント収集の対象から除外または対象に含める（必要に応じて）共有をカンマで区切ったリスト
除外または対象に含めるボリュームの完全な名前を入力します	イベント収集の対象から除外または対象に含めるボリュームをカンマで区切ったリスト
フォルダアクセスを監視します	オンにすると、フォルダアクセス監視のイベントが有効になります。このオプションを選択しなくても、フォルダの作成 / 名前変更および削除が監視されることに注意してください。これを有効にすると、監視されるイベントの数が増えます。
ONTAP 送信バッファサイズを設定します	ONTAP FPolicy 送信バッファのサイズを設定します。9.8p7 より前のバージョンの ONTAP を使用していて、 Performance 問題が表示された場合、 ONTAP 送信バッファサイズを変更して ONTAP のパフォーマンスを向上させることができます。このオプションが表示されない場合は、ネットアップサポートにお問い合わせください。

終了後

- Installed Data Collectors ページで、各コレクタの右側にあるオプションメニューを使用してデータコレクタを編集します。データコレクタを再起動したり、データコレクタ設定の属性を編集したりできます。

MetroClusterの推奨構成

MetroClusterの推奨事項は次のとおりです。

1. 2つのデータコレクタをソースSVMに、別のデータコレクタをデスティネーションSVMに接続します。
2. データコレクタは、*Cluster IP*.によって接続する必要があります。
3. あるデータコレクタを実行する必要がある時点であれば、別のデータコレクタでエラーが発生します。

   現在の「実行中」のSVMのデータコレクタは、_RUNNING _と表示されます。現在の「停止」されているSVMのデータコレクタは、_Error_と表示されます。

4. スイッチオーバーが発生すると、データコレクタの状態が「Running」から「Error」に変わり、その逆も同様です。
5. データコレクタがError状態からRunning状態に移行するまでに最大2分かかります。

サービスポリシー

ONTAP *バージョン9.9.1以降*でサービスポリシーを使用している場合、データソースコレクタに接続するには、データservice_data-nfs_、および/または_data-cifs_とともに_data-fpolicy-client_serviceが必要です。

例：

```
Testcluster-1::*> net int service-policy create -policy only_data_fpolicy
-allowed-addresses 0.0.0.0/0 -vserver aniket_svm
-services data-cifs,data-nfs,data,-core,data-fpolicy-client
(network interface service-policy create)
```

9.6.1より前のバージョンのONTAP では、_data -fpolicy-client_need not be set」を実行します。

Data Collectorの再生**-**一時停止

2つの新しい操作がコレクタのkebabメニューに表示されるようになりました(一時停止と再開)。

Data Collectorがin_running_stateの場合は、収集を一時停止できます。コレクターの「3つのドット」メニューを開き、一時停止を選択します。コレクタが一時停止している間は、ONTAPからデータが収集されず、コレクタからONTAPにデータが送信されません。つまり、ONTAPからデータコレクタへ、およびそこからデータインフラストラクチャインサイトへのFPolicyイベントは流れません。

コレクタの一時停止中に新しいボリュームなどがONTAPに作成されると、ワークロードセキュリティでデータが収集されず、それらのボリュームなどがダッシュボードやテーブルに反映されないことに注意してください。

次の事項に注意してください。

- スナップショットのパージは、一時停止中のコレクタに設定されている設定に従って実行されません。
- 一時停止したコレクタでEMSイベント（ONTAP ARPなど）は処理されません。つまり、ONTAPがランサムウェア攻撃を特定した場合、データインフラ分析情報ワークロードセキュリティはそのイベントを取得できません。
- 一時停止中のコレクタについては、ヘルス通知Eメールは送信されません。
- 一時停止中のコレクタでは'手動または自動のアクション(スナップショットやユーザーブロックなど)はサポートされません
- エージェントまたはコレクタのアップグレード、エージェントVMの再起動/再起動、またはエージェントサービスの再起動時に、一時停止したコレクタは_Paused_stateのままになります。
- データコレクタが_Error_stateの場合、コレクタを_Paused_stateに変更することはできません。Pauseボタンは'コレクタの状態が_running_の場合にのみ有効になります
- エージェントが切断されている場合、コレクタを_Paused_stateに変更することはできません。コレクタが_stopped_stateになり、Pauseボタンが無効になります。

永続的ストア

永続的ストアは、ONTAP 9.14.1以降でサポートされます。ボリューム名の手順はONTAP 9.14~9.15では異なります。

永続ストアを有効にするには、コレクタの編集/追加ページでチェックボックスをオンにします。チェックボックスを選択すると、ボリューム名を受け入れるためのテキストフィールドが表示されます。永続的ストアを有効にするには、ボリューム名は必須フィールドです。

- ONTAP 9.14.1では、この機能を有効にする前にボリュームを作成し、_Volume Name_フィールドに同じ名前を指定する必要があります。推奨されるボリュームサイズは16GBです。

- ONTAP 9.15.1では、_Volume Name_フィールドに指定した名前を使用して、16GBのサイズでボリュームが自動的に作成されます。

Persistent Storeには特定の権限が必要です（これらの一部またはすべてがすでに存在する場合があります）。

クラスタモード：

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster-name>
security login rest-role create -role csrestrole -api /api/cluster/jobs/
-access readonly -vserver <cluster-name>
```

SVMモード：

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <vserver-name>
security login rest-role create -role csrestrole -api /api/cluster/jobs/
-access readonly -vserver <vserver-name>
```

トラブルシューティング

トラブルシューティングのヒントについては、ページを参照して"SVMコレクタのトラブルシューティング"ください。

NetApp ONTAP コレクタ用のCloud Volumes ONTAP とAmazon FSXの設定

ワークロードセキュリティでは、データコレクタを使用して、デバイスからファイルとユーザのアクセスデータを収集します。

Cloud Volumes ONTAP ストレージ構成

ワークロードセキュリティエージェントをホストするシングルノード/ HA AWSインスタンスを設定するには、OnCommand Cloud Volumes ONTAPのドキュメントを参照してください。https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html[]

設定が完了したら、次の手順に従ってSVMをセットアップします。https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html[]

サポート対象プラットフォーム

- Cloud Volumes ONTAP は、利用可能なすべてのクラウドサービスプロバイダで利用できます。たとえば、Amazon、Azure、Google Cloudなどです。
- ONTAP Amazon FSXの略

Agent Machine Configuration の略

エージェントマシンは、クラウドサービスプロバイダのそれぞれのサブネットで設定する必要があります。ネットワークアクセスの詳細については、[エージェントの要件]を参照してください。

以下は、AWSでエージェントをインストールする手順です。クラウドサービスプロバイダに応じて、AzureまたはGoogle Cloudでインストールのために同等の手順を実行できます。

AWSでワークロードセキュリティエージェントとして使用するマシンを設定するには、次の手順を実行します。

ワークロードセキュリティエージェントとして使用するマシンを構成するには、次の手順を実行します。

手順

1. AWS コンソールにログインし、 EC2-Instances ページに移動して、 *Launch instance* を選択します。
2. 次のページで説明しているように、適切なバージョンのRHELまたはCentOS AMIを選択します。https://docs.netapp.com/us-en/cloudinsights/concept_cs_agent_requirements.html[]
3. Cloud ONTAP インスタンスが存在する VPC とサブネットを選択します。
4. 割り当てられたリソースとして、 [T2.xlarge _ （ 4 vCPU と 16 GB RAM ）] を選択します。
    a. EC2 インスタンスを作成します。
5. YUM パッケージマネージャを使用して、必要な Linux パッケージをインストールします。
    a. Linux パッケージのインストール _wget_or_unzip_native 。

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ます

1. Data Infrastructure 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. **[Collectors]***に移動し、[Agents]*タブをクリックします。
3. [*+Agent] をクリックし、ターゲットプラットフォームとして RHEL を指定します。
4. [エージェントインストール] コマンドをコピーします。
5. ログインしている RHEL EC2 インスタンスに Agent Installation コマンドを貼り付けます。すべてのが満たされている場合、ワークロードセキュリティエージェントがインストールされます"エージェントの前提条件"。

詳細な手順については、次のリンクを参照してください。https://docs NetApp .com/us-en/cloudinsights/task_cs_add_agent.html#steps-to-install-agent

トラブルシューティング

既知の問題とその解決策を次の表に示します。

問題	解決策

「Workload Security: Failed to Determine ONTAP type for Amazon FxSN data collector」というエラーがData Collectorに表示されます。お客様が新しいAmazon FSxNデータコレクタをワークロードセキュリティに追加できません。エージェントからのポート443上のFSxNクラスタへの接続がタイムアウトしました。ファイアウォールとAWSセキュリティグループでは、通信を許可するために必要なルールが有効になっています。エージェントはすでに導入されており、同じAWSアカウントにも存在します。同じエージェントを使用して、残りのネットアップデバイス（およびすべてのデバイスが動作）を接続および監視します。	この問題 を解決するには、fsxadmin LIFネットワークセグメントをエージェントのセキュリティルールに追加します。ポートについて不明な場合は、すべてのポートを許可します。

ユーザ管理

ワークロードセキュリティユーザアカウントは、Data Infrastructure Insightsを通じて管理されます。

Data Infrastructure Insightsには、アカウント所有者、管理者、ユーザ、ゲストの4つのユーザアカウントレベルが用意されています。各アカウントには、特定の権限レベルが割り当てられます。管理者権限を持つユーザアカウントは、ユーザを作成または変更し、各ユーザに次のいずれかのワークロードセキュリティロールを割り当てることができます。

ロール	ワークロードセキュリティアクセス
管理者	アラート、フォレンジック、データコレクタ、自動応答ポリシー、ワークロードセキュリティ用APIなど、すべてのワークロードセキュリティ機能を実行できます。管理者は、他のユーザーを招待することもできますが、割り当てられるのはワークロードセキュリティロールのみです。
ユーザ	アラートを表示および管理し、フォレンジックを表示できます。ユーザーロールは、アラートステータスの変更、メモの追加、スナップショットの手動作成、ユーザーアクセスの制限を行うことができます。
ゲスト	アラートおよびフォレンジックを表示できます。ゲストロールは、アラートステータスの変更、メモの追加、スナップショットの手動作成、ユーザーアクセスの制限を行うことはできません。

手順

1. Workload Securityにログインします
2. メニューで、 [*Admin] > [User Management] をクリックします

   Data Infrastructure Insightsのユーザ管理ページに移動します。

3. 各ユーザに必要なロールを選択します。

新しいユーザを追加する際には、目的のロール（通常はユーザまたはゲスト）を選択します。

ユーザアカウントとロールの詳細については、Data Infrastructure Insightsのドキュメントを参照して"ユーザロール"ください。

SVMイベントレートチェッカー（エージェントサイジングガイド）

イベントレートチェッカーは、 ONTAP SVM データコレクタをインストールする前に、 SVM での NFS / SMB の組み合わせイベントレートを確認するために使用します。これにより、エージェントマシンで監視可能な SVM 1 の数が表示されます。イベントレートチェッカーは、セキュリティ環境の計画に役立つサイジングガイドとして使用します。

Agentは最大50個のデータコレクタをサポートできます。

要件

- クラスタIP
- クラスタ管理者のユーザ名とパスワード

> このスクリプトを実行するときは、イベント速度を確認する SVM で ONTAP SVM Data Collector を実行していない必要があります。

手順：

1. CloudSecure の指示に従って、 Agent をインストールします。
2. エージェントをインストールしたら、 sudo ユーザとして _server_data_rate_checker.sh_script を実行します。

```
 /opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
. このスクリプトを使用するには、 Linux マシンに _sshpass_to
をインストールする必要があります。インストール方法は 2 種類あります。
```

   a. 次のコマンドを実行します。

```
 linux_prompt> yum install sshpass
.. 表示されない場合は、 Web から Linux マシンに sshpass_to
をダウンロードし、次のコマンドを実行します。
```

```
linux_prompt> rpm -i sshpass
```

3. プロンプトが表示されたら、正しい値を指定します。例については、以下を参照してください。
4. スクリプトの実行には約 5 分かかります。
5. 実行が完了すると、 SVM からイベントレートが出力されます。コンソールの出力では、 SVM ごとのイベントレートを確認できます。

```
“Svm svm_rate is generating 100 events/sec”.
```

各 ONTAP SVM データコレクタを 1 つの SVM に関連付けることができます。つまり、各データコレクタは、 1 つの SVM が生成するイベント数を受け取ることができます。

次の事項に注意してください。

a）この表は、一般的なサイジングガイドとして使用します。コアまたはメモリの数を増やして、サポートされるデータコレクタの数を増やすことができます（最大50個のデータコレクタ）。

Agent Machine Configuration の略	SVM データコレクタの数	エージェントマシンが処理できる最大イベントレート
4コア、16GB	データコレクタ 10 個	20K イベント / 秒
4コア、32GB	データコレクタ 20 個	20K イベント / 秒

b ）合計イベント数を計算するには、そのエージェントのすべての SVM に対して生成されたイベントを追加します。

c) スクリプトがピーク時に実行されない場合、またはピークトラフィックが予測しにくい場合は、 30% のイベントレートバッファを維持します。

B+C は A 未満でなければなりません。そうしないと、 Agent マシンはモニタできません。

つまり、 1 台のエージェントマシンに追加できるデータコレクタの数は、次の式に準拠する必要があります。

```
 Sum of all Event rate of all Data Source Collectors + Buffer Event rate
of 30% < 20000 events/second
```

その他の前提条件と要件については、ページを参照してlink:concept_cs_agent_requirements.html["エージェントの要件"]ください。

例

ここでは、 1 秒あたり 100 、 200 、および 300 のイベントレートを生成する SMS が 3 つあるとします。

式を適用します。

```
 (100+200+300) + [(100+200+300)*30%] = 600+180 = 780events/sec
780 events/second is < 20000 events/second, so the 3 SVMs can be monitored
via one agent box.
```

コンソール出力は、エージェントマシンの現在の作業ディレクトリにあるファイル名 *fpolicy_stat_<SVM 名 >.log* で確認できます。

次の場合、スクリプトから間違った結果が返されることがあります。

- クレデンシャル、 IP 、または SVM 名が正しくない。
- 同じ名前、シーケンス番号などの既存の FPolicy にはエラーが発生します。
- 実行中はスクリプトは突然停止します。

スクリプトの実行例を次に示します。

```
[root@ci-cs-data agent]#
/opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
```

```
Enter the cluster ip: 10.192.139.166
Enter the username to SSH: admin
Enter the password:
Getting event rate for NFS and SMB events.
Available SVMs in the Cluster
-----------------------------
QA_SVM
Stage_SVM
Qa-fas8020
Qa-fas8020-01
Qa-fas8020-02
audit_svm
svm_rate
vs_new
vs_new2
```

```
-----------------------------
Enter [1/5] SVM name to check (press enter to skip): svm_rate
Enter [2/5] SVM name to check (press enter to skip): audit_svm
Enter [3/5] SVM name to check (press enter to skip):
Enter [4/5] SVM name to check (press enter to skip):
Enter [5/5] SVM name to check (press enter to skip):
Running check for svm svm_rate...
Running check for svm audit_svm...
Waiting 5 minutes for stat collection
Stopping sample svm_rate_sample
Stopping sample audit_svm_sample
fpolicy stats of svm svm_rate is saved in fpolicy_stat_svm_rate.log
Svm svm_rate is generating 100 SMB events/sec and 100 NFS events/sec
Overall svm svm_rate is generating 200 events/sec
fpolicy stats of svm audit_svm is saved in fpolicy_stat_audit_svm.log
Svm audit_svm is generating 200 SMB events/sec and 100 NFS events/sec
Overall svm audit_svm is generating 300 events/sec
```

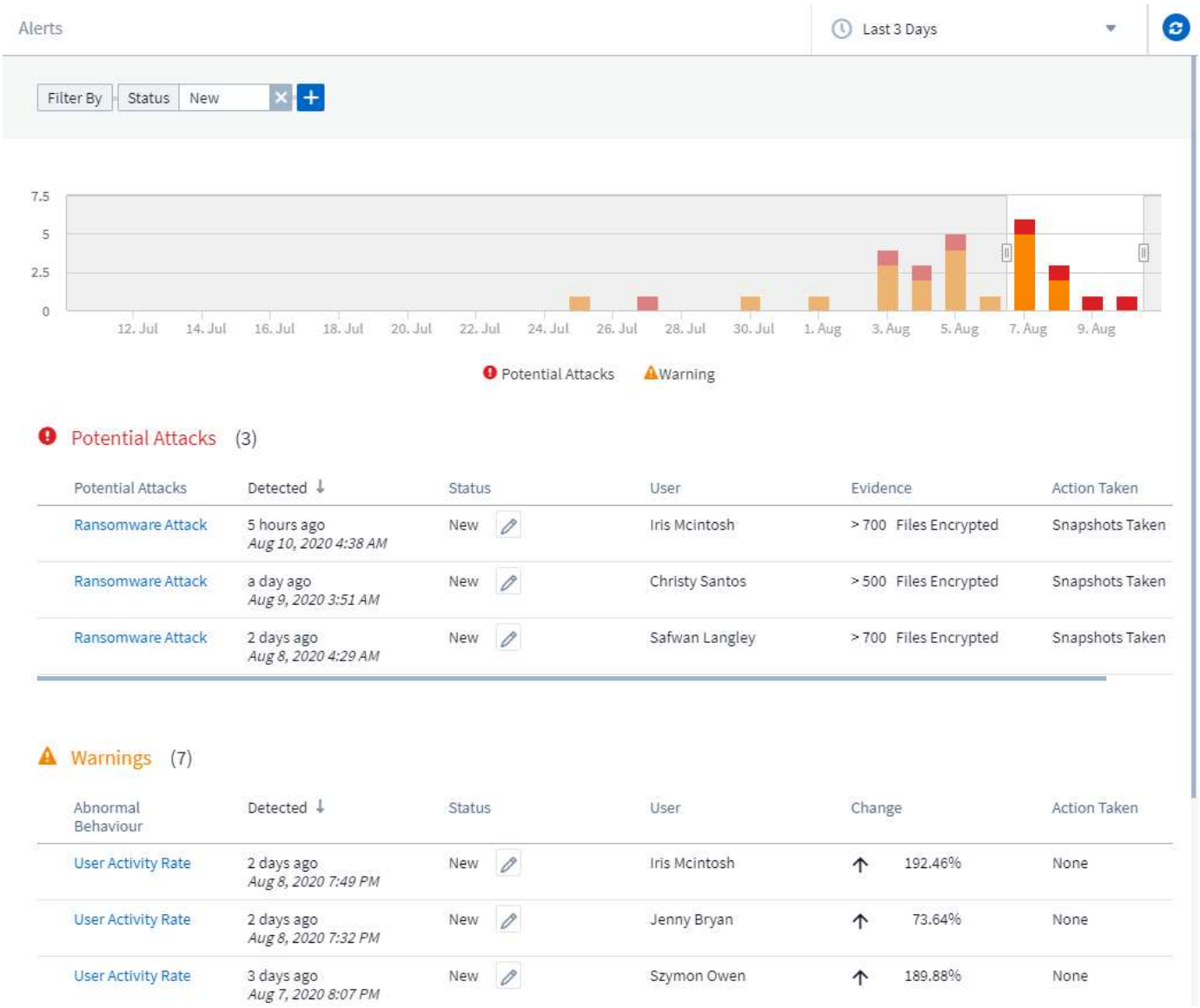
```
[root@ci-cs-data agent]#
```

トラブルシューティング

質問	回答
ワークロードセキュリティ用にすでに設定されているSVMに対してこのスクリプトを実行した場合、SVMの既存のfpolicy設定だけを使用するのか、それとも一時的なfpolicyを設定してプロセスを実行するのか。	ワークロードセキュリティがすでに設定されているSVMであっても、イベントレートチェッカーは問題なく実行できます。影響はありません。
スクリプトを実行できるSVMの数を増やすことはできますか。	はい。スクリプトを編集して、 SVM の最大数を 5 から任意の数に変更するだけです。
SVMの数を増やすと、スクリプトの実行時間は長くなりますか。	いいえ。SVMの数を増やした場合でも、スクリプトは最大5分間実行されます。
スクリプトを実行できるSVMの数を増やすことはできますか。	はい。スクリプトを編集して、 SVM の最大数を 5 から任意の望ましい数に変更する必要があります。
SVMの数を増やすと、スクリプトの実行時間は長くなりますか。	いいえ。SVMの数を増やした場合でも、スクリプトは最大5分間実行されます。
既存のエージェントでEvent Rate Checkerを実行するとどうなりますか？	既存のエージェントに対してイベントレートチェッカーを実行する原因 と、SVMのレイテンシが増加する可能性があります。この増加は、イベントレートチェッカーの実行中は一時的なものです。

アラート

[ワークロードセキュリティアラート]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

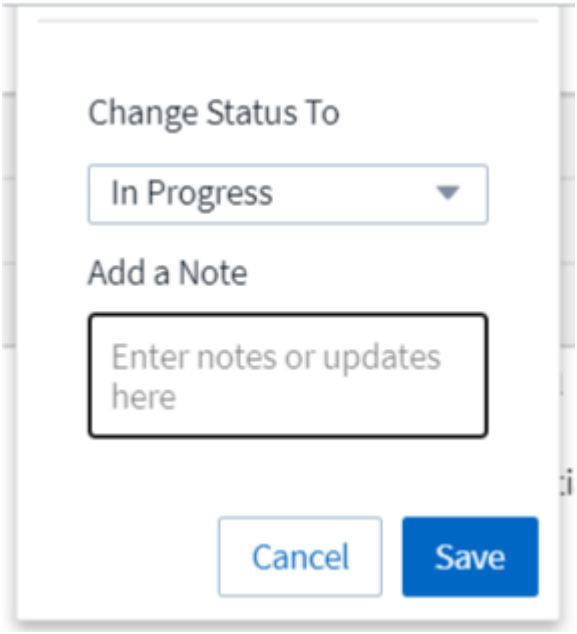
アラートリストには、選択した期間内に発生した攻撃および警告の総数、およびその期間内に発生した攻撃または警告のリストがグラフで表示されます。期間を変更するには、グラフの開始時間と終了時間のスライダを調整します。

アラートごとに次の情報が表示されます。

- 潜在的な攻撃 :*
- 潜在的な攻撃の種類（ランサムウェアや破壊行為など）
- 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です。
  - * 進行中 * ：アラートはチームメンバーまたはメンバーによって調査中です。
  - * 解決済み * ：アラートはチームメンバーによって解決済みとマークされています。

◦ * 却下 * ：アラートは誤検知または予期される動作として却下されました。

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* ）
- 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、進行中など）
- 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（ランサムウェア、被害者）とアラートID（ワークロードセキュリティが割り当て）
- 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）

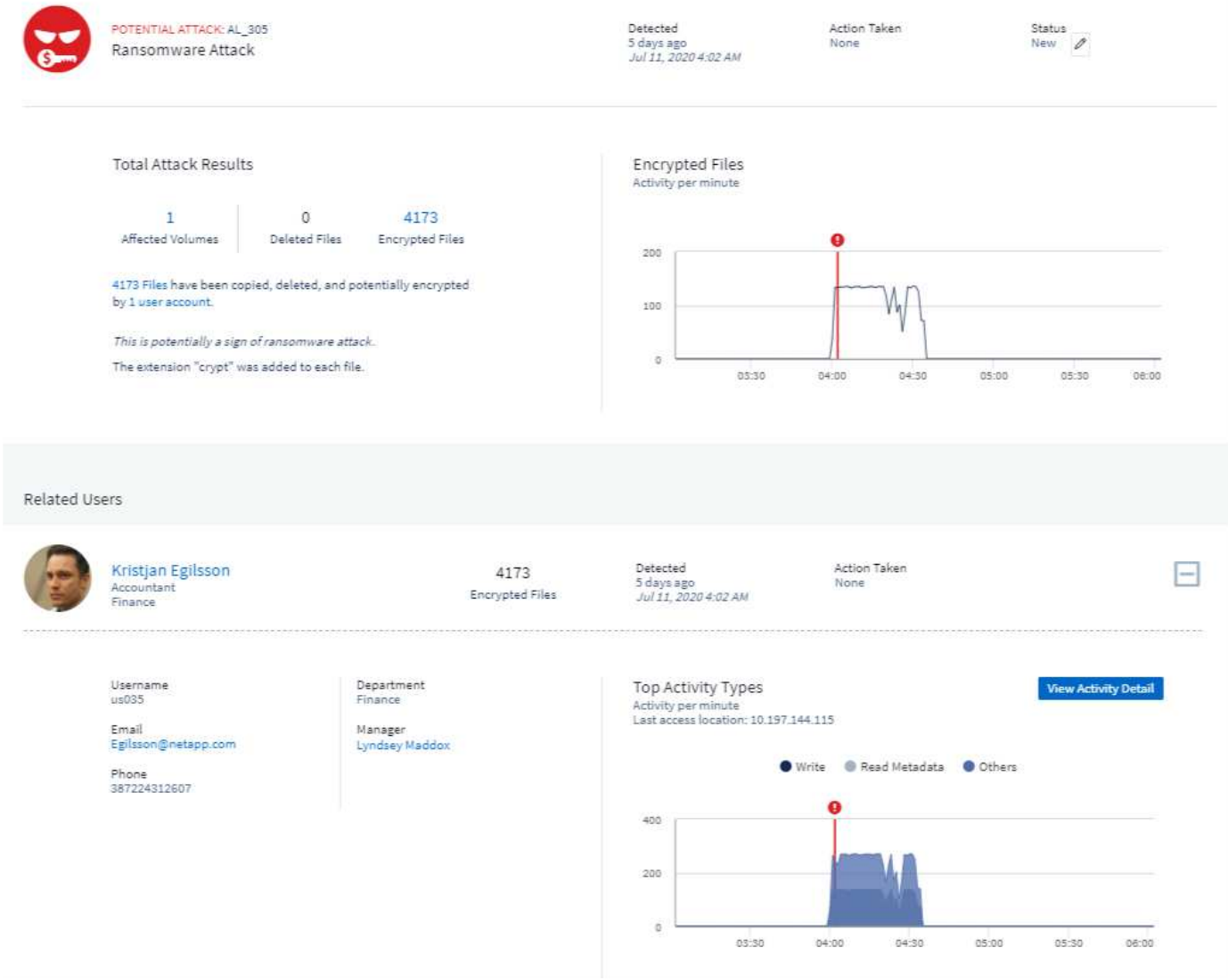
［ 攻撃結果 ］ セクション：

- 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。

詳細ページ（この例はランサムウェア攻撃の可能性を示しています）
：

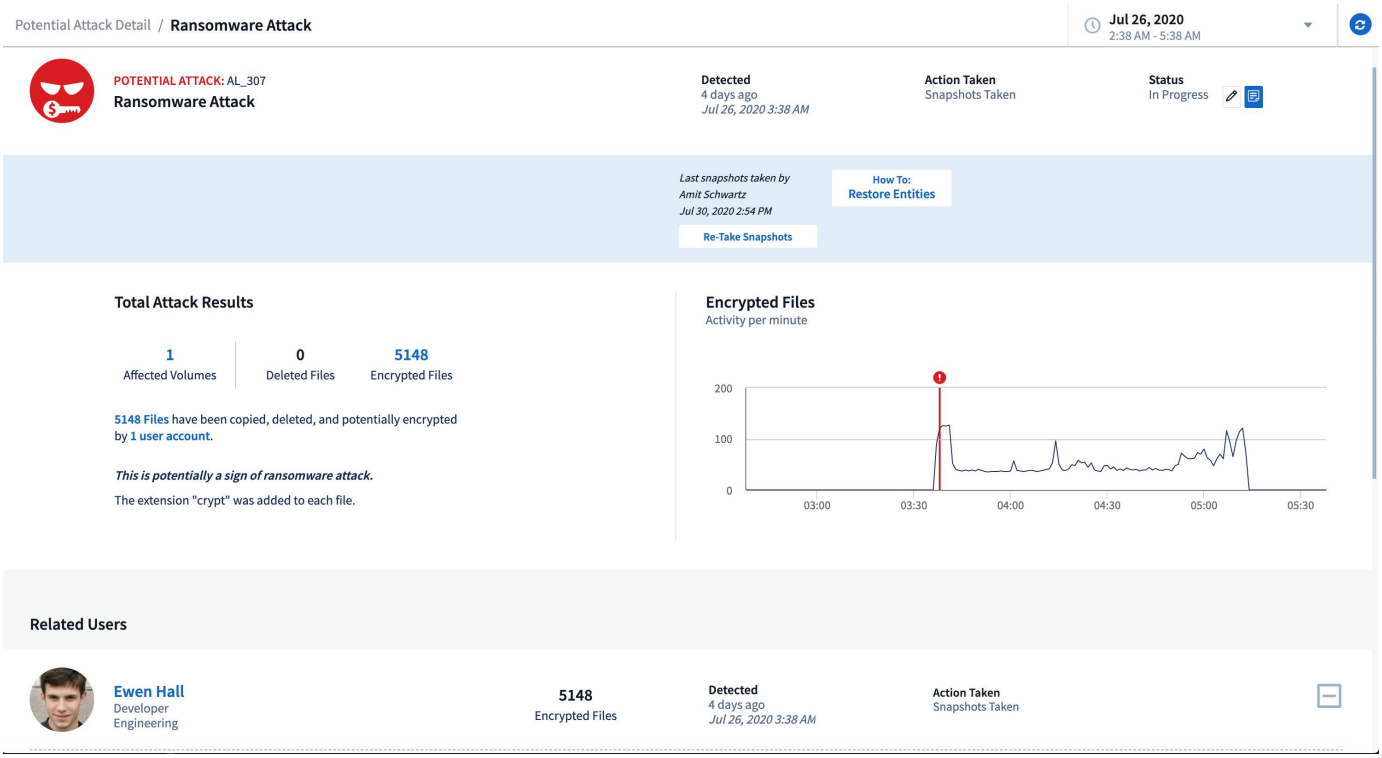


Snapshot_Actionを実行します

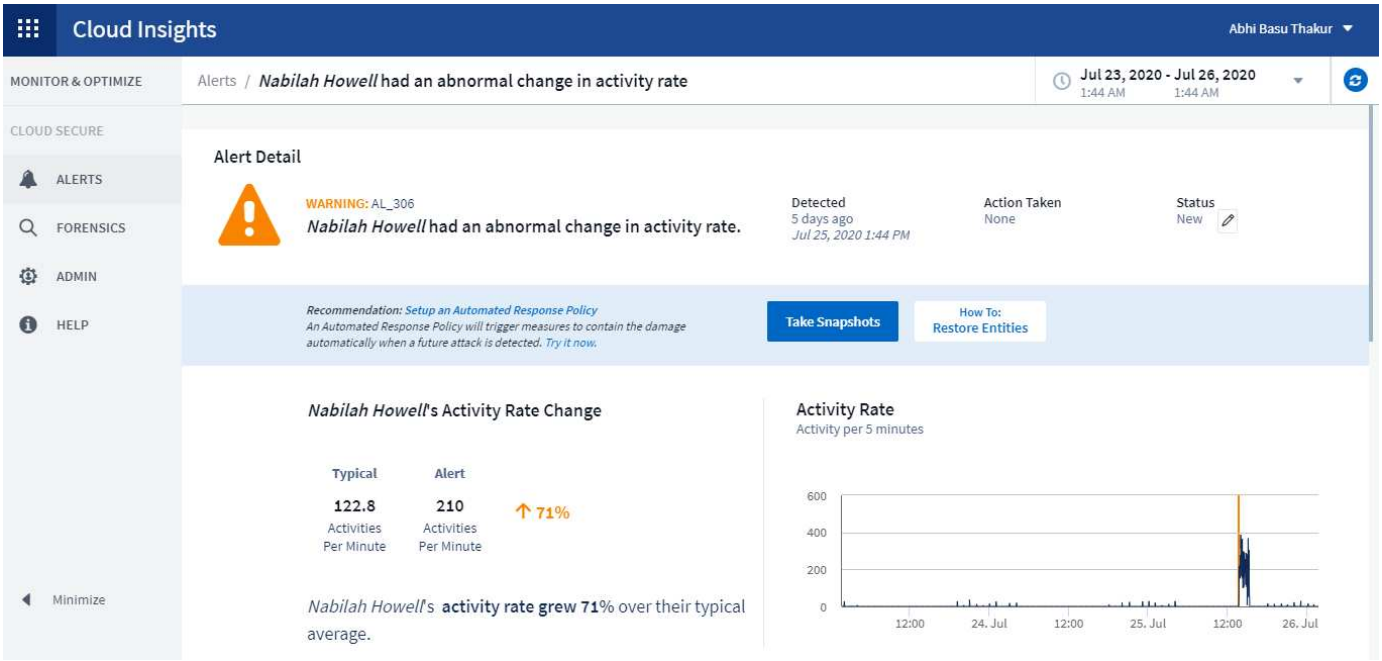
ワークロードセキュリティは、悪意のあるアクティビティが検出されたときにスナップショットを自動的に取得することでデータを保護し、データを安全にバックアップします。

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たときにSnapshotを作成するように定義できます"自動応答ポリシー"。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取得
：



手動スナップショット
：



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。ワークロードセキュリティ環境を削除すると、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
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。ワークロードセキュリティ（WS）スナップショットは影響しますか。WS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？	ワークロードセキュリティスナップショットは、1時間ごとのスナップショットには影響しません。WSスナップショットは時間単位のスナップショット領域を使用しないため、以前と同様に継続する必要があります。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ワークロードセキュリティに表示されます。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のドキュメントを参照してください"Snapshot 削除ポリシーを設定しています"。
ワークロードセキュリティで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ロールに、「https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html#a-note-about-permissions[proper rights assigned」リンクがあ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
ワークロードセキュリティから削除されたSVMでSnapshotを再度追加した場合、古いアラートに対してSnapshot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_disabled_stateである場合に、SVM管理IPを使用してワークロードセキュリティ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、ワークロードセキュリティからtrigger _Take Snapshotを手動で作成します。Snapshot 処理が成功します。

フォレンジック

法医学 - すべての活動

すべてのアクティビティページは'ワークロードセキュリティ環境でエンティティに対して実行されるアクションを理解するのに役立ちます

すべてのアクティビティデータを確認しています

- Forensics > Activity Forensics * をクリックし、 * All Activity * タブをクリックして、 All Activity ページにアクセスします。このページには、テナントのアクティビティの概要が表示され、次の情報が強調表示されます。
- *Activity History*（選択したグローバル時間範囲に基づく）を示すグラフ

  グラフの四角形をドラッグすると、グラフをズームできます。ページ全体がロードされ、ズームした時間範囲が表示されます。ズームインすると、ユーザーがズームアウトできるボタンが表示されます。

- _all Activity_dataのリスト。
- [グループ化]ドロップダウンには、アクティビティをユーザー、パス、エンティティタイプなどでグループ化するオプションが表示されます。
- 一般的なパスボタンは、クリックするとテーブルの上にあり、エンティティパスの詳細を含むスライドアウトパネルを取得できます。

すべてのアクティビティ *_table には、次の情報が表示されます。デフォルトでは、すべての列が表示されるわけではありません。歯車アイコンをクリックすると、表示する列を選択できます。

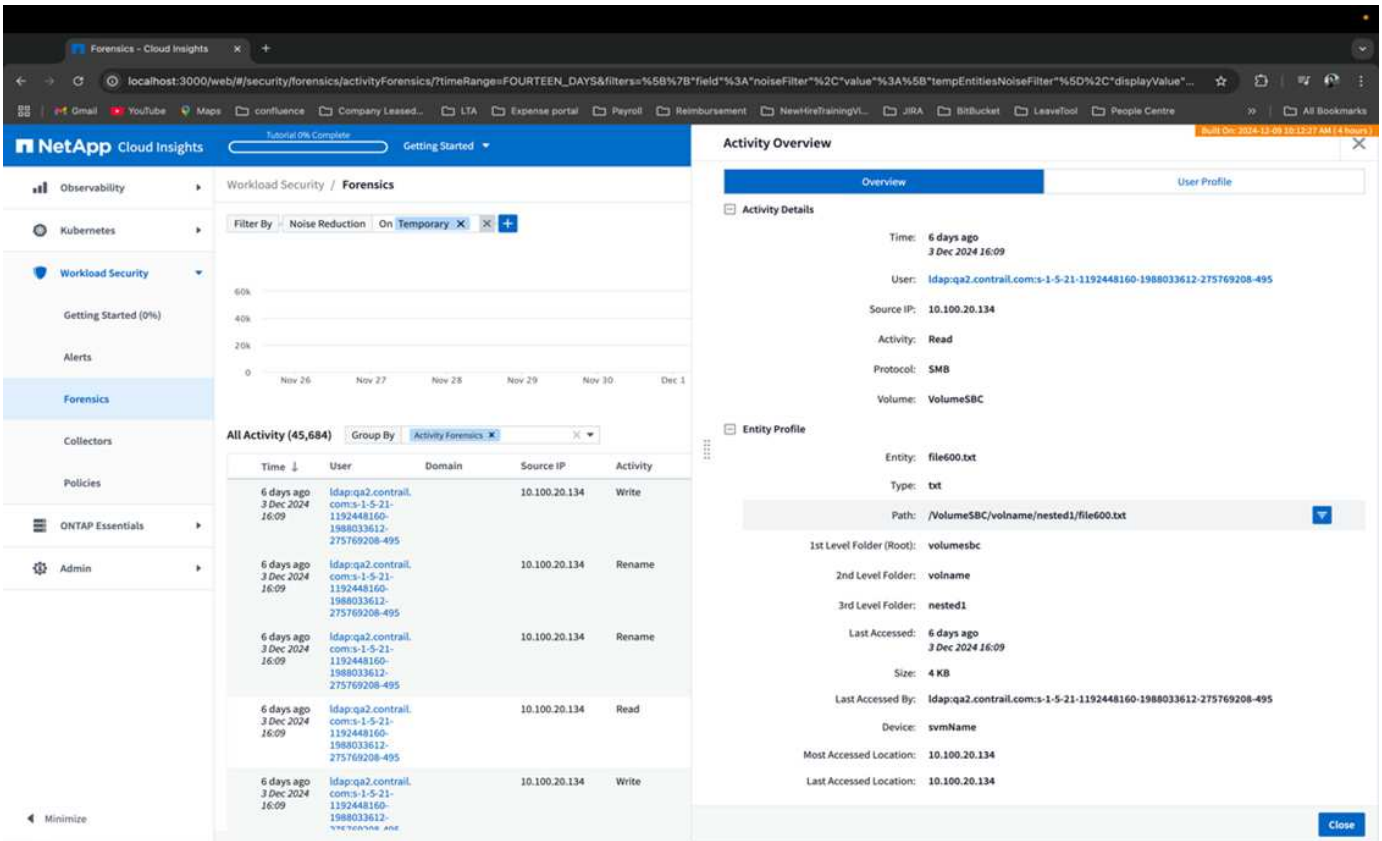
- エンティティがアクセスされた時間（年、月、日、最終アクセス時刻を含む）。
- スライドアウトパネルとしてへのリンクを使用してエンティティにアクセスした*ユーザー*"ユーザ情報"。
- ユーザーが実行した * アクティビティ * 。サポートされるタイプは次のとおりです
  - * グループ所有権の変更 * - グループ所有権はファイルまたはフォルダに変更されています。グループ所有権の詳細については、を参照してください。"リンクをクリックしてください"
  - * 所有者の変更 * - ファイルまたはフォルダの所有権が別のユーザーに変更されています。
  - * アクセス権の変更 * - ファイルまたはフォルダのアクセス権が変更されました。
  - * 作成 * - ファイルまたはフォルダを作成します。
  - * 削除 * - ファイルまたはフォルダを削除します。フォルダを削除すると、そのフォルダおよびサブフォルダ内のすべてのファイルについて、 _delete_events が取得されます。
  - * 読み取り *- ファイルが読み取られています。
  - * 読み取りメタデータ * - フォルダ監視オプションを有効にした場合のみ。Windows でフォルダを開くか、 Linux のフォルダ内で「 ls 」を実行すると、が生成されます。
  - * 名前の変更 * - ファイルまたはフォルダの名前を変更します。
  - * Write * - データはファイルに書き込まれます。
  - * メタデータの書き込み * - ファイルのメタデータが書き込まれます。たとえば、権限が変更された場

合などです。

- * その他の変更 * - 上記に記載されていないその他のイベント。マッピングされていないイベントはすべて、「その他の変更」アクティビティタイプにマッピングされます。ファイルおよびフォルダに適用されます。

- Path * is_entity_path。
- 第1レベルフォルダ（ルート）*は、小文字のエンティティパスのルートディレクトリです。
- *2nd Level Folder*は、小文字のエンティティパスの2番目のレベルのディレクトリです。
- *3rd Level Folder*は、小文字のエンティティパスの3番目のレベルのディレクトリです。
- *4th Level Folder*は、小文字のエンティティパスの4番目のレベルのディレクトリです。
- エンティティ（ファイル）拡張子（.doc、.docx、.tmpなど）を含む*エンティティタイプ*。
- エンティティが存在する*デバイス*。
- イベントの取得に使用される * プロトコル * 。
- 元のファイルの名前を変更したときに名前変更イベントに使用された * 元のパス * 。デフォルトでは、この列はテーブルに表示されません。列セレクタを使用して、この列をテーブルに追加します。
- エンティティが存在するボリューム * 。デフォルトでは、この列はテーブルに表示されません。列セレクタを使用して、この列をテーブルに追加します。

テーブル行を選択すると、スライドアウトパネルが開き、1つのタブにユーザープロファイルが表示され、別のタブにアクティビティとエンティティの概要が表示されます。



Default_Group by_methodは_Activity forensics_です。別の_Group by_method（エンティティタイプなど）を選択すると、entity_Group by_tableが表示されます。何も選択されていない場合は、_Group by _* All *が表示

されます。

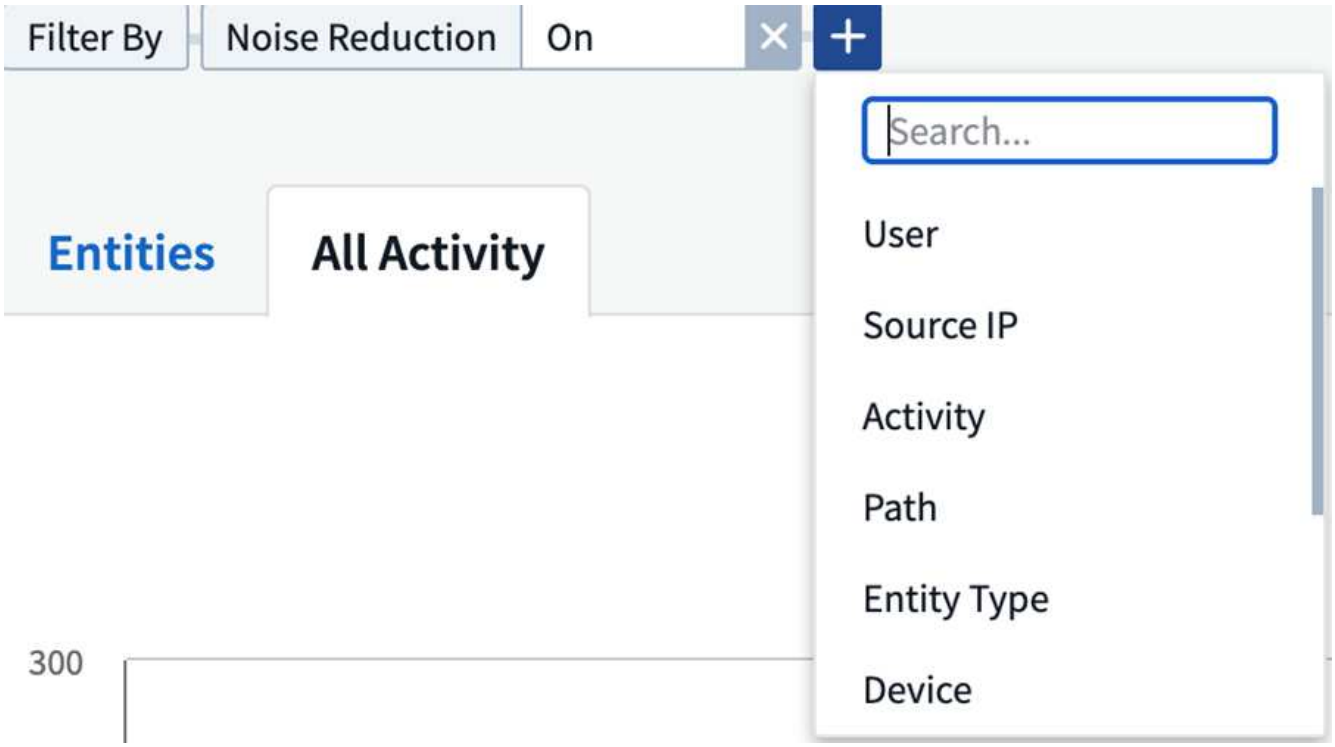
- アクティビティ数はハイパーリンクとして表示されます。これを選択すると、選択したグループがフィルタとして追加されます。アクティビティのテーブルは、そのフィルタに基づいて更新されます。
- フィルタを変更したり、時間範囲を変更したり、画面を更新したりすると、フィルタを再度設定しないとフィルタ結果に戻ることはできません。

フォレンジックアクティビティ履歴データのフィルタリング

データのフィルタリングに使用できる方法は 2 つあります。

- フィルタは、スライドアウトパネルから追加できます。この値は、 top_Filter by_list の適切なフィルタに追加されます。
- 次のフィールドに「 _Filter By_field 」と入力して、データをフィルタリングします。

  [+]* ボタンをクリックして、 [フィルタ基準] ウィジェットから適切なフィルタを選択します。



  検索テキストを入力します

  Enter キーを押すか、フィルタボックスの外側をクリックしてフィルタを適用します。

フォレンジックアクティビティデータは、次のフィールドでフィルタできます。

- * アクティビティ * タイプ。
- * エンティティがアクセスされたソース IP * 。有効な送信元 IP アドレスを二重引用符で囲んで指定する必要があります（例：「 10.1.1.1 」）。「 10.1.1.* 」、「 10.1.. 」などの不完全な IP は機能しません。
- * プロトコル * 。プロトコル固有のアクティビティを取得します。
- * アクティビティを実行しているユーザーのユーザー名 * 。フィルタリングするユーザ名を正確に指定す

る必要があります。部分的なユーザ名で検索したり、プレフィックスやサフィックスの付いたユーザ名の一部を検索したりすることはできません。

- * ユーザーが過去 2 時間に作成したファイルをフィルタリングするためのノイズリダクション * 。また、ユーザがアクセスする一時ファイル（ .tmp ファイルなど）をフィルタするためにも使用されます。
- アクティビティを実行しているユーザーの*ドメイン*。フィルタするには、* exact domain を指定する必要があります。部分ドメイン、または部分ドメインの先頭または末尾にワイルドカード(**")**が付いている部分ドメインを検索することはできません。_None_を指定すると、見つからないドメインを検索できます。

次のフィールドには、特別なフィルタルールが適用されます。

- エンティティタイプ（エンティティ（ファイル）拡張子を使用）-引用符で正確なエンティティタイプを指定することをお勧めします。例：「txt」_。
- エンティティのパス-ディレクトリパスフィルタ（/で終わるパス文字列）のパス*は、より高速な結果を得るために、最大4つのディレクトリの深さが推奨されます。例：*"/home/userX/nested1/nested2/"*。詳細については、次の表を参照してください。
- 第1レベルフォルダ(ルート)-フィルタとしてのエンティティパスのルートディレクトリ。たとえば、エンティティパスが/home/userX/nested1/nested2/の場合、homeまたは"home"を使用できます。
- 2nd Level Folder -エンティティパスフィルタの2ndレベルディレクトリ。たとえば、エンティティのパスが/home/userX/nested1/nested2/の場合、userXまたは"userX"を使用できます。
- 3rd Level Folder -エンティティパスフィルタの3rdレベルディレクトリ。
- たとえば、エンティティパスが/home/userX/nested1/nested2/の場合、nested1または「nested1」を使用できます。
- 第4レベルフォルダ-ディレクトリエンティティパスフィルタの第4レベルディレクトリ。たとえば、エンティティパスが/home/userX/nested1/nested2/の場合、nested2または「nested2」を使用できます。
- *ユーザー*アクティビティの実行-引用符で正確なユーザーを指定することをお勧めします。たとえば、_"Administrator"_などです。
- * エンティティが存在するデバイス * （ SVM ）
- * 体積 * エンティティが存在する場所
- 元のファイルの名前を変更したときに名前変更イベントに使用された * 元のパス * 。

フィルタリングを行う場合、上記のフィールドは次のようになります。

- 正確な値は引用符で囲む必要があります。例： "searchtext"
- ワイルドカード文字列には引用符は含まれていません。例： searchtext 、 * searchtext * は、 'earchtext ' を含む文字列をフィルタします。
- プレフィックスが付いた文字列、たとえば searchtext* は、「 earchtext 」で始まる文字列を検索します。

アクティビティフォレンジックフィルタの例：

ユーザが適用したフィルタ式	予想される結果	パフォーマンス評価	コメント
path="/home/userX/nested1/nested2/"	指定したディレクトリの下にあるすべてのファイルとフォルダの再帰的検索	高速	最大4つのディレクトリの検索が高速になります。
path="/home/userX/nested1/"	指定したディレクトリの下にあるすべてのファイルとフォルダの再帰的検索	高速	最大4つのディレクトリの検索が高速になります。
パス="/home/userX/nested1/test"	指定されたパス正規表現の下にあるすべてのファイルおよびフォルダの再帰的検索（test *はファイルまたはディレクトリ、あるいはその両方を意味する）	遅い	ディレクトリ+ファイル正規表現検索は、ディレクトリ検索と比較して検索に時間がかかります。
path="/home/userX/nested1/nested2/nested3/"	指定したディレクトリの下にあるすべてのファイルとフォルダの再帰的検索	遅い	4つ以上のディレクトリ検索は、検索に時間がかかります。
その他のパスベース以外のフィルタ。UserとEntity Typeのフィルタは引用符で囲むことをお勧めします。例：User="Administrator" Entity Type="txt"		高速	

注：

1. 選択した時間範囲が3日を超える場合、[すべてのアクティビティ]アイコンの横に表示されるアクティビティ数は30分に四捨五入されます。たとえば、_ 9月1日10：15 ~ 9月7日10：15 AM_の時間範囲には、9月1日10：00 ~ 9月7日10：30のアクティビティ数が表示されます。
2. 同様に、選択した期間が3日を超える場合は、[Activity History]グラフに表示されるカウント指標も30分に切り捨てられます。

フォレンジックアクティビティ履歴データのソート

アクティビティ履歴データは、*Time*、*User*、*Source IP*、*Activity*、、_Entity Type _、1st Level Folder（ルート）、2nd Level Folder、3rd Level Folder、4th Level Folderでソートできます。デフォルトでは、テーブルは descending _Time_order でソートされます。つまり、最新のデータが最初に表示されます。_Device_Field と _Protocol_fields に対してソートが無効になっています。

非同期エクスポートのユーザガイド

概要

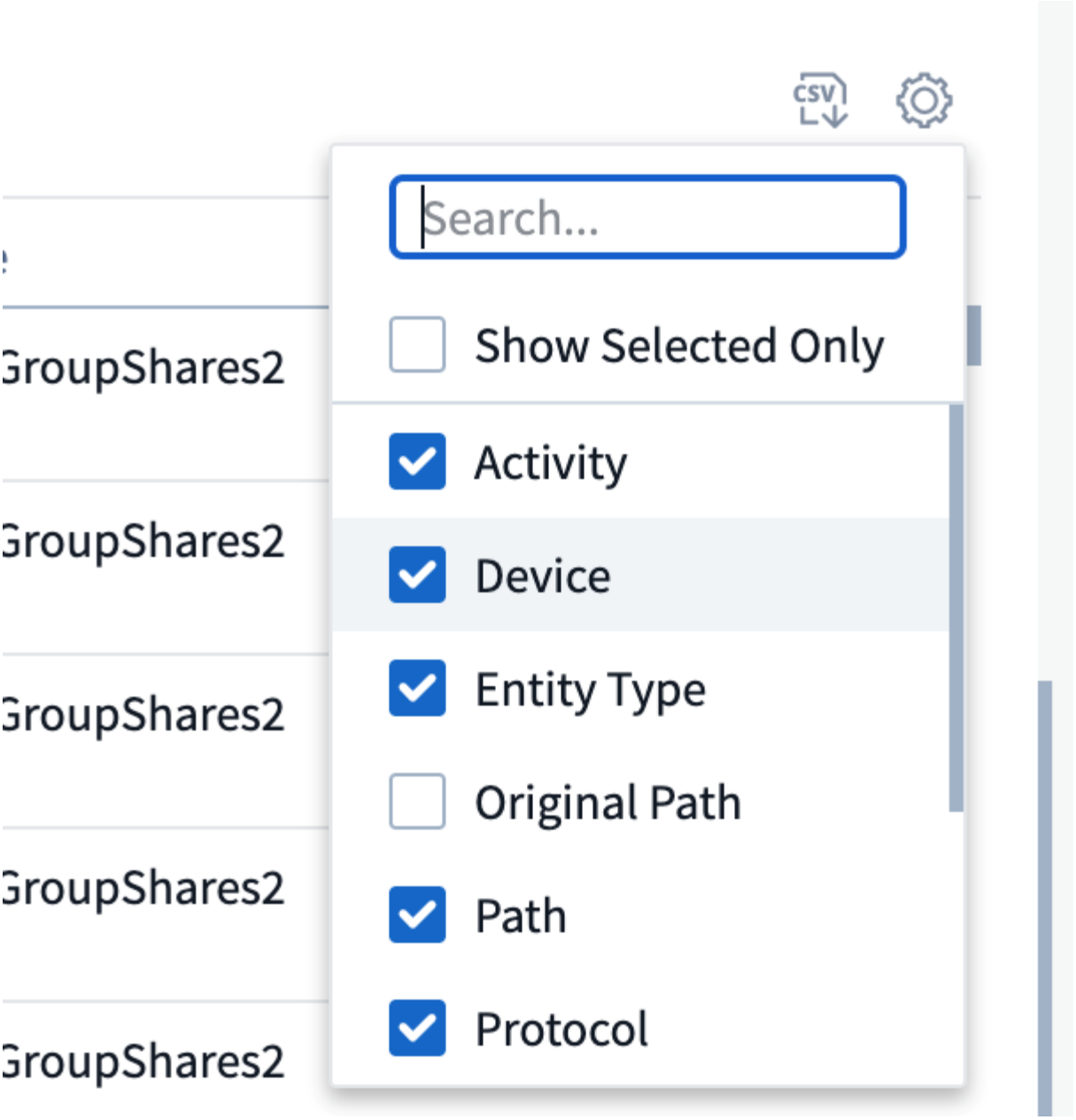
Storage Workload Securityの非同期エクスポート機能は、大規模なデータエクスポートを処理するように設計されています。

1. エクスポートの開始：エクスポートの所要時間とフィルタを選択し、エクスポートボタンをクリックします。
2. エクスポートが完了するのを待ちます：処理時間は数分から数時間の範囲で指定できます。フォレンジックページを数回更新する必要がある場合があります。エクスポートジョブが完了すると、[Download last export CSV file]ボタンが有効になります。
3. ダウンロード:「最後に作成したエクスポートファイルをダウンロード」ボタンをクリックして、エクスポートされたデータを.zip形式で取得します。このデータは、ユーザーが別の非同期エクスポートを開始するまで、または3日が経過するまで（いずれか早い方）ダウンロードできます。このボタンは、別の非同期エクスポートが開始されるまで有効のままです。
4. 制限事項：
    - 非同期ダウンロードの数は、現在、ユーザあたり1つ、テナントあたり3つに制限されています。
    - エクスポートされるデータは、最大100万レコードに制限されます。

APIを介してフォレンジックデータを抽出するサンプルスクリプトは、NetAppエージェントの_/opt/apl/cloudsecure/agent/export-script /_にあります。スクリプトの詳細については、この場所にあるreadmeを参照してください。

すべてのアクティビティの列を選択します

すべての activity テーブルには ' デフォルトで SELECT カラムが表示されます列を追加、削除、または変更するには、テーブルの右側にある歯車アイコンをクリックし、使用可能な列のリストから選択します。



アクティビティ履歴の保持

アクティビティ履歴は、アクティブなワークロードセキュリティ環境で13カ月間保持されます。

Forensicsページのフィルタの適用性

フィルタ	機能	例	これらのフィルタに適用可能	これらのフィルタには適用されません	結果
*（アスタリスク）	すべての項目を検索できます	Auto * 03172022検索テキストにハイフンまたはアンダースコアが含まれている場合は、角かっこで式を指定します。例：SVM-123の検索には（SVM*）を使用します。	ユーザー、エンティティタイプ、デバイス、ボリューム、元のパス、1stLevelフォルダ、2ndLevelフォルダ、3rdLevelフォルダ、4thLevelフォルダ		「Auto」で始まり「03172022」で終わるすべてのリソースを返します。
？（疑問符）	では、特定の数の文字を検索できます	AutoSabotageUser1_03172022	ユーザー、エンティティタイプ、デバイス、ボリューム、1stLevelフォルダ、2ndLevelフォルダ、3rdLevelフォルダ、4thLevelフォルダ		AutoSabotageUser1_03172022A、AutoSabotageUser1_03172022B、AutoSabotageUser1_031720225などを返します
または	複数のエンティティを指定できます	AutoSabotageUser1_03172022またはAutoRansomUser4_03162022	ユーザ、ドメイン、エンティティタイプ、元のパス		AutoSabotageUser1_03172022またはAutoRansomUser4_03162022のいずれかを返します
ありません	検索結果からテキストを除外できます	NOT AutoRansomUser4_03162022	ユーザー、ドメイン、エンティティタイプ、元のパス、1stLevelフォルダ、2ndLevelフォルダ、3rdLevelフォルダ、4thLevelフォルダ	デバイス	"AutoRansomUser4_03162022 "で始まるものをすべて返します。
なし	すべてのフィールドで NULL 値を検索します	なし	ドメイン		ターゲットフィールドが空の場合に結果を返します

パス/元のパスの検索

検索結果は、の有無によって異なります

"/AutoDir1/AutoFile032420222022"	完全一致検索のみが機能します。正確なパスが/AutoDir1/AutoFile03242022であるすべてのアクティビティが返されます（大文字と小文字は区別されません）。
"/AutoDir1/"	AutoDir1と一致する第1レベルディレクトリを持つすべてのアクティビティを返します（大文字と小文字は区別されません）。
"/AutoDir1/AutoFile03242022 /"	機能します。第1レベルのディレクトリがAutoDir1と一致し、第2レベルのディレクトリがAutoFile03242022と一致するすべてのアクティビティを返します（大文字と小文字は区別されません）。
/AutoDir1/AutoFile03242022または/AutoDir1/AutoFile03242022	壊れています
/AutoDir1/AutoFile03242022ではありません	壊れています
/AutoDir1はありません	壊れています
/AutoFile03242022はありません	壊れています
*	壊れています

ローカルルート**SVM**ユーザアクティビティの変更

ローカルルートSVMユーザが何らかのアクティビティを実行している場合、NFS共有がマウントされているクライアントのIPがユーザ名で考慮されるようになりました。フォレンジックアクティビティとユーザアクティビティの両方のページで、root@<ip-address-of-the-client>と表示されます。

例：

- SVM-1がワークロードセキュリティによって監視されていて、そのSVMのrootユーザがIPアドレスが10.197.12.40のクライアントに共有をマウントした場合、フォレンジックアクティビティページに表示されるユーザ名は_root@10.197.12.40_になります。
- IPアドレスが10.197.12.41の別のクライアントに同じSVM-1がマウントされている場合、フォレンジックアクティビティページに表示されるユーザ名は_root@10.197.12.41_になります。

*•これは、NFS rootユーザーのアクティビティをIPアドレスごとに分離するために行われます。以前は、すべてのアクティビティは_root_userによってのみ実行され、IPの区別はありませんでした。

トラブルシューティング

問題	試してみてください

[すべてのアクティビティ] テーブルの [ユーザー] 列には、「 LDAP: HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817” 」または「 LDAP: デフォルト : 80038003 」というユーザー名が表示されます。	考えられる原因は次のとおりです。 1.ユーザディレクトリコレクタがまだ設定されていません。追加するには、**[ワークロードセキュリティ]>[コレクタ]>[ユーザディレクトリコレクタ]***に移動し、[+ユーザディレクトリコレクタ]*をクリックします。Active Directory_or_LDAP ディレクトリサーバー _ を選択します。2.User Directory Collectorが設定されましたが、停止しているか、エラー状態です。[コレクタ]>[ユーザディレクトリコレクタ]*に移動し、ステータスを確認してください。トラブルシューティングのヒントについては、のマニュアルのセクションを参照して"User Directory Collector のトラブルシューティング"ください。適切に設定すると、 24 時間以内に名前が自動的に解決されます。それでも解決されない場合は、正しい User Data Collector を追加しているかどうかを確認します。追加した Active Directory / LDAP ディレクトリサーバにユーザが実際に含まれていることを確認します。
一部の NFS イベントが UI に表示されません。	次を確認します。 1.POSIX 属性が設定された AD サーバのユーザディレクトリコレクタは、 UI から unixid 属性が有効になっている必要があります。2.NFSアクセスを実行しているすべてのユーザは、UI 3のユーザページで検索したときに表示されます。raw イベント（ユーザがまだ検出されていないイベント）は NFS 4 ではサポートされません。NFS エクスポートへの匿名アクセスは監視されません。5.NFSバージョンがNFS4.1未満で使用されていることを確認します。
Forensics_All Activity_or_Entities_pagesのフィルタにアスタリスク(*)などのワイルドカード文字を含む文字を入力すると、ページのロードに時間がかかります。	検索文字列にアスタリスク（*）を付けると、すべてが検索されます。ただし、*<*searchTerm*> or *<*searchTerm*>*_のような先頭のワイルドカード文字列は、クエリに時間がかかります。パフォーマンスを向上させるには、代わりに<searchTerm>*という形式でプレフィックス文字列を使用します（つまり、検索用語としてアスタリスク***()_after_a***を追加します）。例： testvolume_or_* test * volume__ではなく、文字列_testvolume *_を使用します。ディレクトリ検索を使用して、指定したフォルダの下にあるすべてのアクティビティを再帰的に表示します(階層検索)。たとえば、"/path1/path2/path3/"は、/path1/path2/path3の下にあるすべてのアクティビティを再帰的にリストします。または、[すべてのアクティビティ]タブの[フィルタに追加]オプションを使用します。
パスフィルタを使用すると、「Request failed with status code 500/503」というエラーが発生します。	レコードのフィルタリングには、より小さい日付範囲を使用してみてください。
_path_filterを使用すると、Forensic UIでデータのロードに時間がかかります。	ディレクトリパスフィルタ(/で終わるパス文字列)より高速な結果を得るには、最大4つのディレクトリの深さが推奨されます。たとえば、ディレクトリパスが/Aaa/Bbb/Ccc/Dddの場合は、「/Aaa/Bbb/Ccc/Ddd/」を検索してデータをより高速にロードしてみてください。

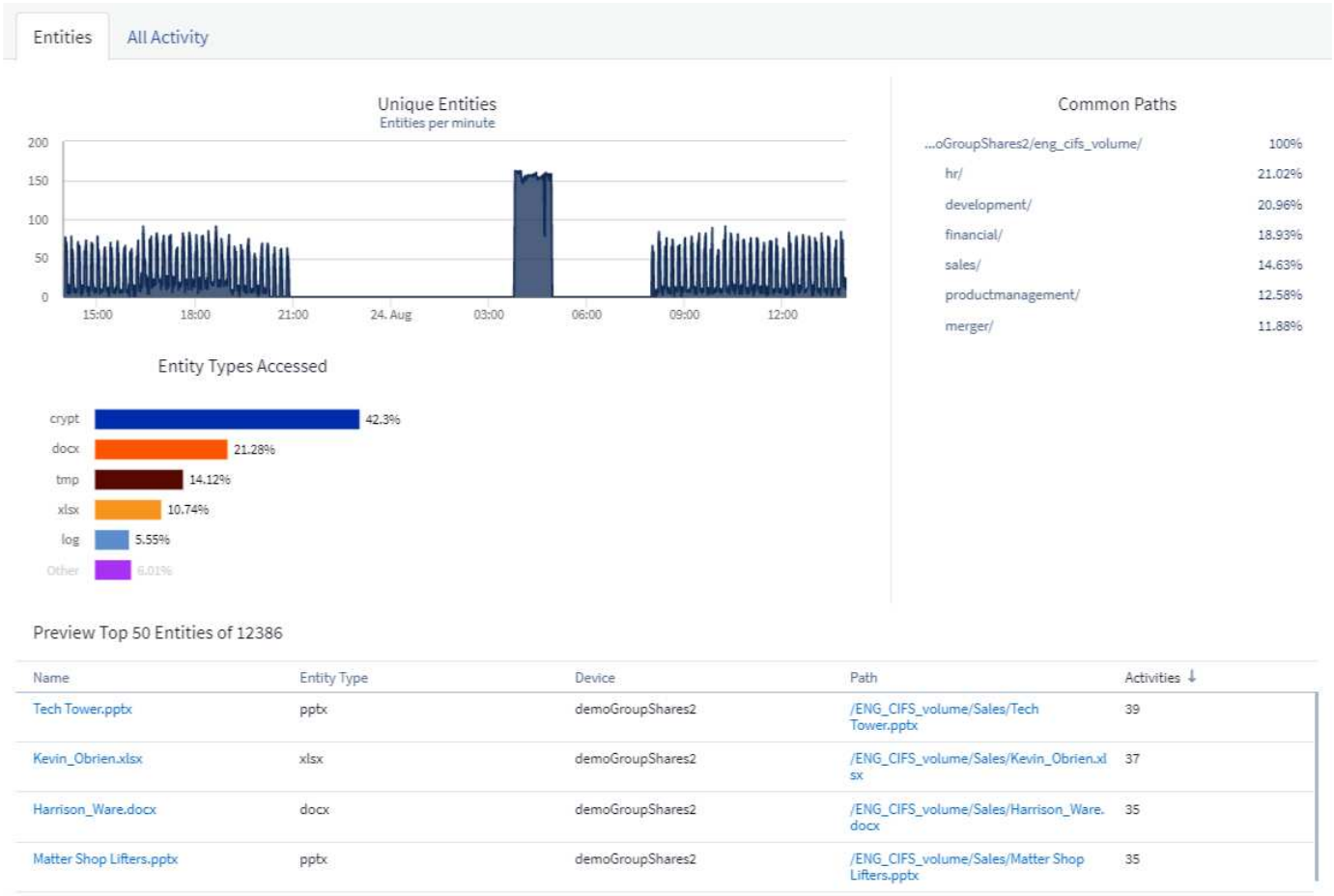
フォレンジックエンティティページ

[Forensics Entities]ページには、テナントのエンティティアクティビティに関する詳細情報が表示されます。

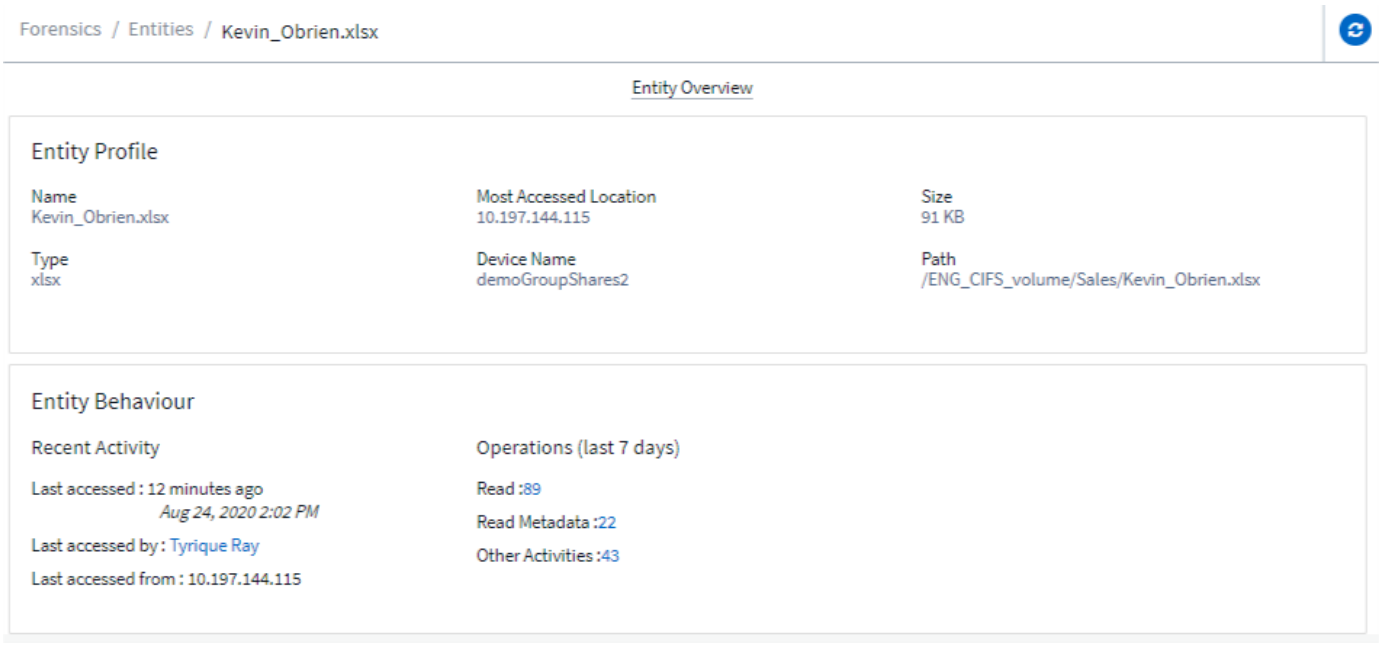
エンティティ情報の検査

- Forensics > Activity Forensics * をクリックし、 *Entities* タブをクリックして Entities ページにアクセスします。

このページには、テナントのエンティティアクティビティの概要が表示され、次の情報が強調表示されます。グラフに**_Unique Entities_accessed per minute *エンティティタイプのグラフaccessed A chart of _ Entity types accessed _* A breakdown of the _Common Paths***エンティティの総数のうち_Top 50 Entities_outのリスト



リスト内のエンティティをクリックすると、エンティティの概要ページが開き、エンティティのプロファイルに名前、タイプ、デバイス名、最もアクセスされる場所の IP 、パスなどの詳細、およびユーザ、 IP 、 エンティティが最後にアクセスされた時刻です。



Forensic User の概要

各ユーザーの情報については、「ユーザー概要」を参照してください。これらのビューを使用して、ユーザの特性、関連付けられたエンティティ、および最近のアクティビティを把握できます。

ユーザプロファイル

ユーザプロファイル情報には、ユーザの連絡先情報と場所が含まれます。プロファイルには次の情報が表示されます。

- ユーザの名前
- ユーザの E メールアドレス
- ユーザーのマネージャー
- ユーザの電話連絡先
- ユーザの場所

ユーザの動作

ユーザの動作情報には、最近実行したアクティビティと処理が含まれます。これには次の情報が含まれ

- 最近のアクティビティ
  - 最終アクセス場所
  - アクティビティグラフ
  - アラート
- 過去 7 日間の処理
  - 処理数

更新間隔

ユーザーリストは 12 時間ごとに更新されます。

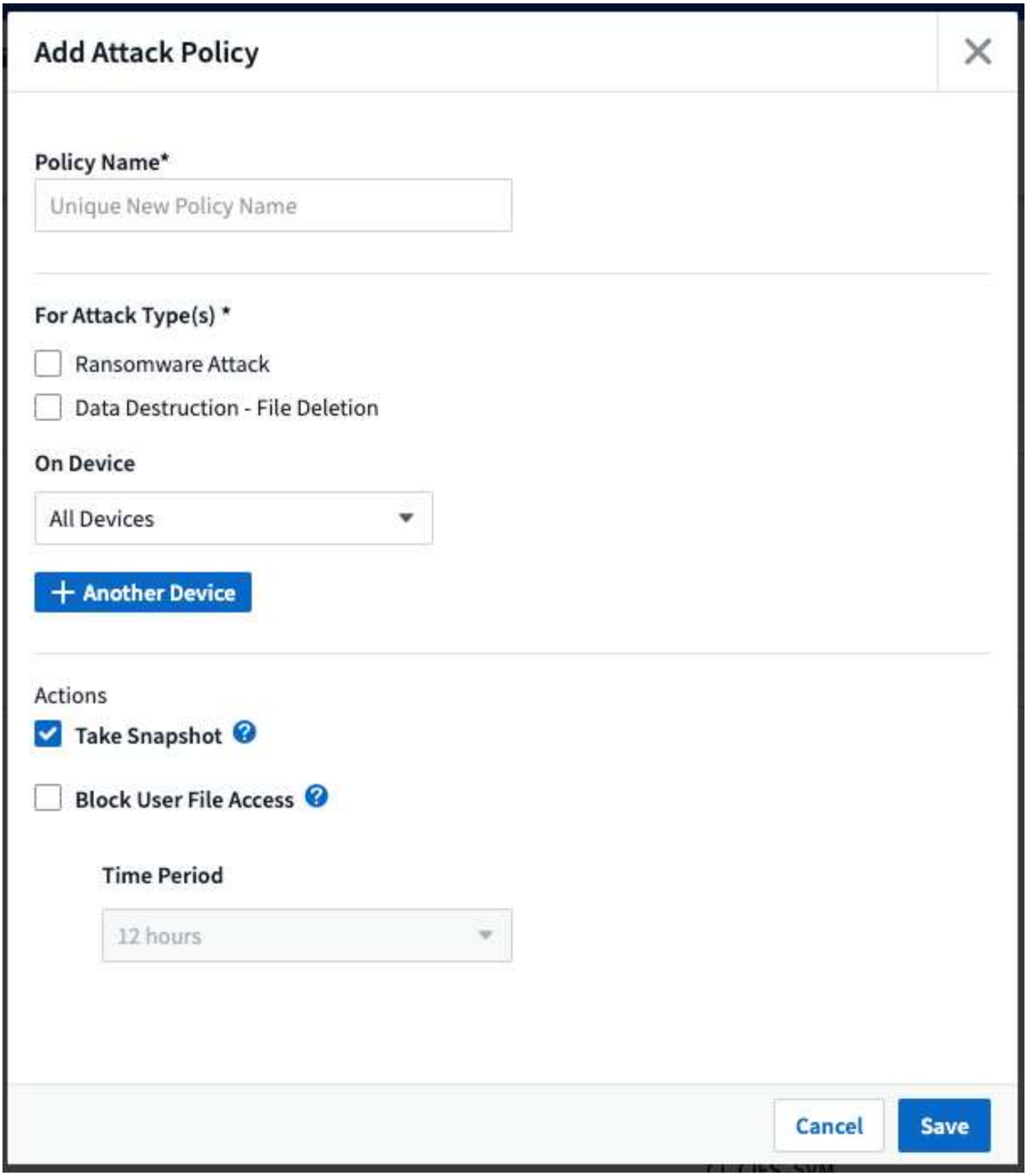
保持ポリシー

再更新されない場合、ユーザリストは 13 カ月間保持されます。13 カ月を過ぎると、データは削除されます。ワークロードセキュリティ環境を削除すると、その環境に関連付けられているすべてのデータが削除されます。

自動応答ポリシー

応答ポリシーは、スナップショットの作成や、攻撃や異常なユーザ動作が発生した場合のユーザアクセスの制限などのアクションをトリガーします。

特定のデバイスまたはすべてのデバイスにポリシーを設定できます。応答ポリシーを設定するには、* Admin > Automated Response Policies を選択し、適切な+ Policy *ボタンをクリックします。攻撃または警告のポリシーを作成できます。



ポリシーは一意の名前で保存する必要があります。

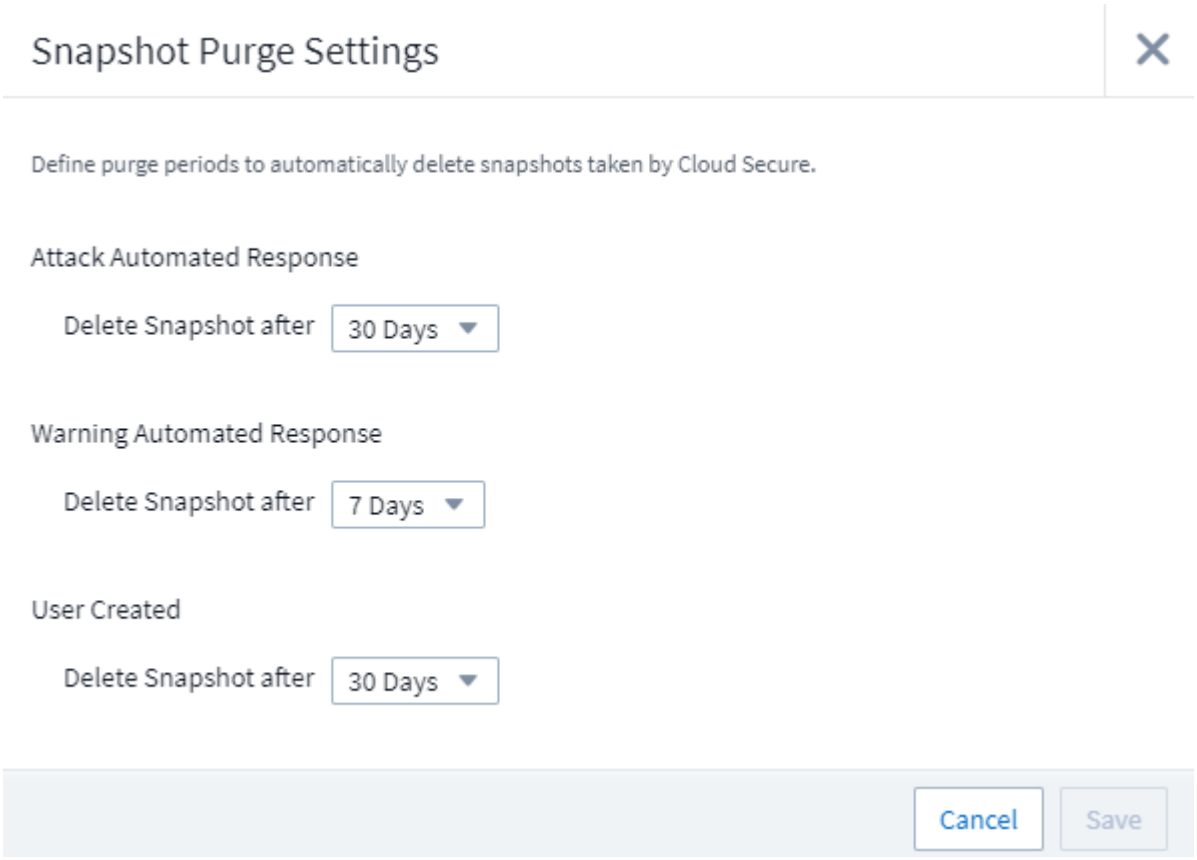
自動応答アクションを無効にする（例： Take Snapshot ）には、アクションをチェック解除してポリシーを保存するだけです。

指定されたデバイス（または選択されている場合はすべてのデバイス）に対してアラートがトリガーされると、自動応答ポリシーによってデータのスナップショットが作成されます。Snapshotのステータスはで確認できます"アラートの詳細ページ"。

IPによるユーザアクセスの制限の詳細については、ページを参照して"ユーザアクセスの制限"ください。

自動応答ポリシーを変更または一時停止するには、ポリシーのドロップダウンメニューでオプションを選択します。

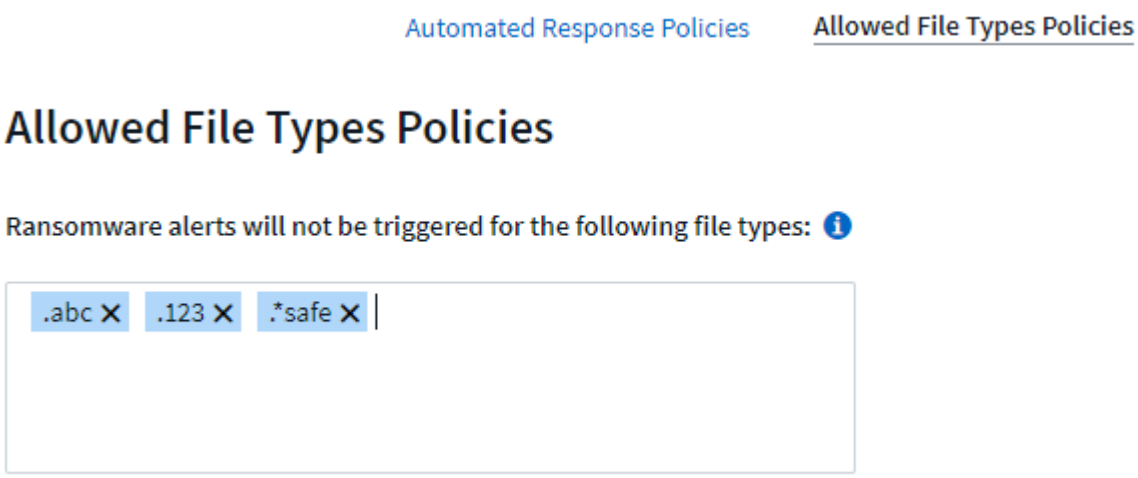
ワークロードセキュリティでは、Snapshotの削除設定に基づいて、Snapshotが1日に1回自動的に削除されます。



許可されたファイルタイプポリシー

既知のファイル拡張子に対するランサムウェア攻撃が検出され、[Alerts]画面でアラートが生成されている場合は、そのファイル拡張子を_allowedファイルtypes_listに追加して不要なアラートを防ぐことができます。

[Workload Security]>[Policies]*に移動し、[_Allowed File Type Policies]タブに移動します。



一度_allowedファイルtypes_listに追加されると、その許可されたファイルタイプに対してランサムウェア攻撃アラートは生成されません。_allowed File types_policyはランサムウェアの検出にのみ適用されることに注意してください。

たとえば、*test.txt_*という名前のファイルが*_test.txt.abc_*に変更され、.abc_拡張子によってランサムウェア攻撃が検出された場合、*.abc_*拡張子を*_allowed*ファイル*types_list*に追加できます。リストに追加されると、拡張子が.abc_のファイルに対するランサムウェア攻撃は生成されなくなります。

許可されるファイルタイプには、完全一致（例：".abc"）または式（例：".**type**"、"**.type**"、または"**type**"）を指定できます。タイプ「. a * c」、「. p * f」の式はサポートされていません。

ONTAP によるランサムウェア対策との統合

ONTAP の自律的ランサムウェア対策（ARP）機能は、NAS（NFSおよびSMB）環境におけるワークロード分析を使用して、ランサムウェア攻撃を示す可能性のある異常なインファイル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。

ARPの詳細とライセンス要件については"ここをクリック"、こちらを参照してください。

ワークロードセキュリティは、ONTAP と統合してARPイベントを受信し、追加の分析と自動応答レイヤを提供します。

ワークロードセキュリティは、ONTAP からARPイベントを受信し、次の処理を行います。

1. ボリューム暗号化イベントとユーザアクティビティを関連付けて、破損の原因となっているユーザを特定します。
2. 自動応答ポリシーを実装する（定義されている場合）
3. フォレンジック機能を提供：
    - お客様がデータ侵害の調査を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に役立ちます。

前提条件

1. ONTAPの最小バージョン：9.11.1
2. ARPが有効なボリューム。ARPのイネーブル化の詳細については、"ここをクリック"を参照してください。ARPは、OnCommand システムマネージャを介して有効にする必要があります。ワークロードセキュリティでARPを有効にすることはできませ
3. ワークロードセキュリティコレクタはクラスタIPを介して追加する必要があります。
4. この機能を使用するには、クラスタレベルのクレデンシャルが必要です。つまり、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。

ユーザ権限が必要です

クラスタ管理者のクレデンシャルを使用している場合、新しい権限は不要です。

ユーザに付与された権限でカスタムユーザ（_csuser_など）を使用している場合は、次の手順に従ってワークロードセキュリティにアクセス許可を付与し、ONTAP からARP関連情報を収集します。

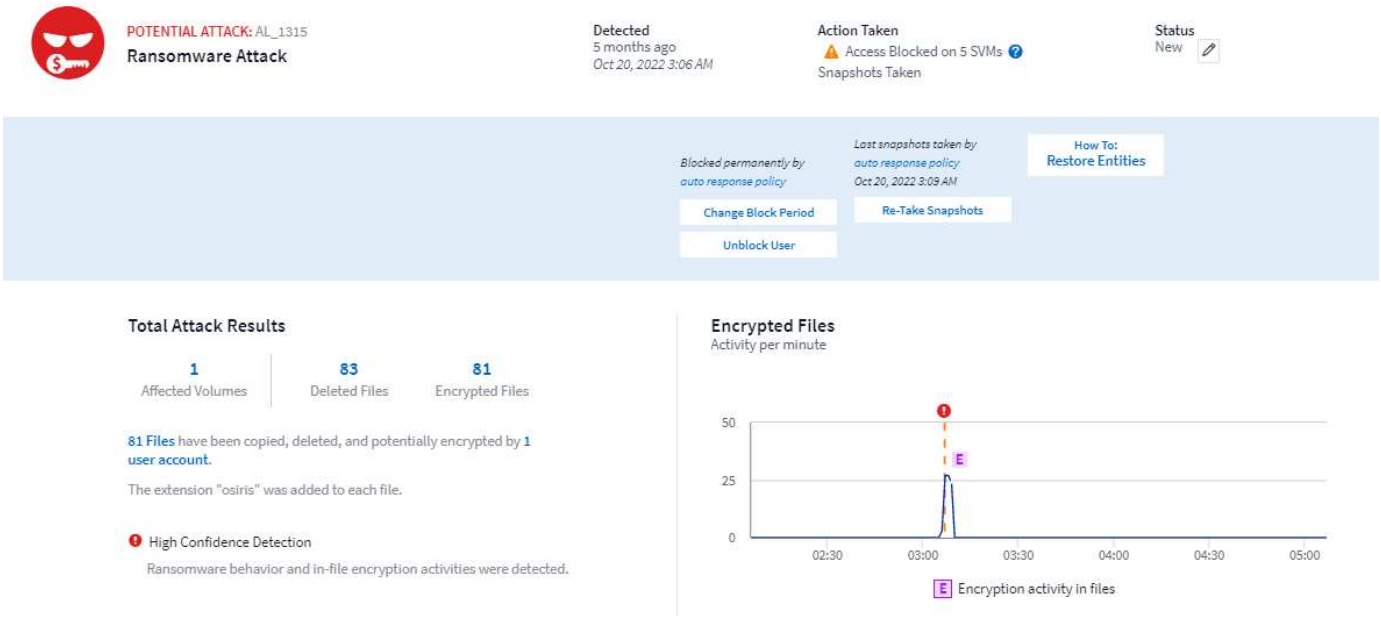
クラスタクレデンシャルを使用する_csuser_withの場合、ONTAP コマンドラインから次の操作を実行します。

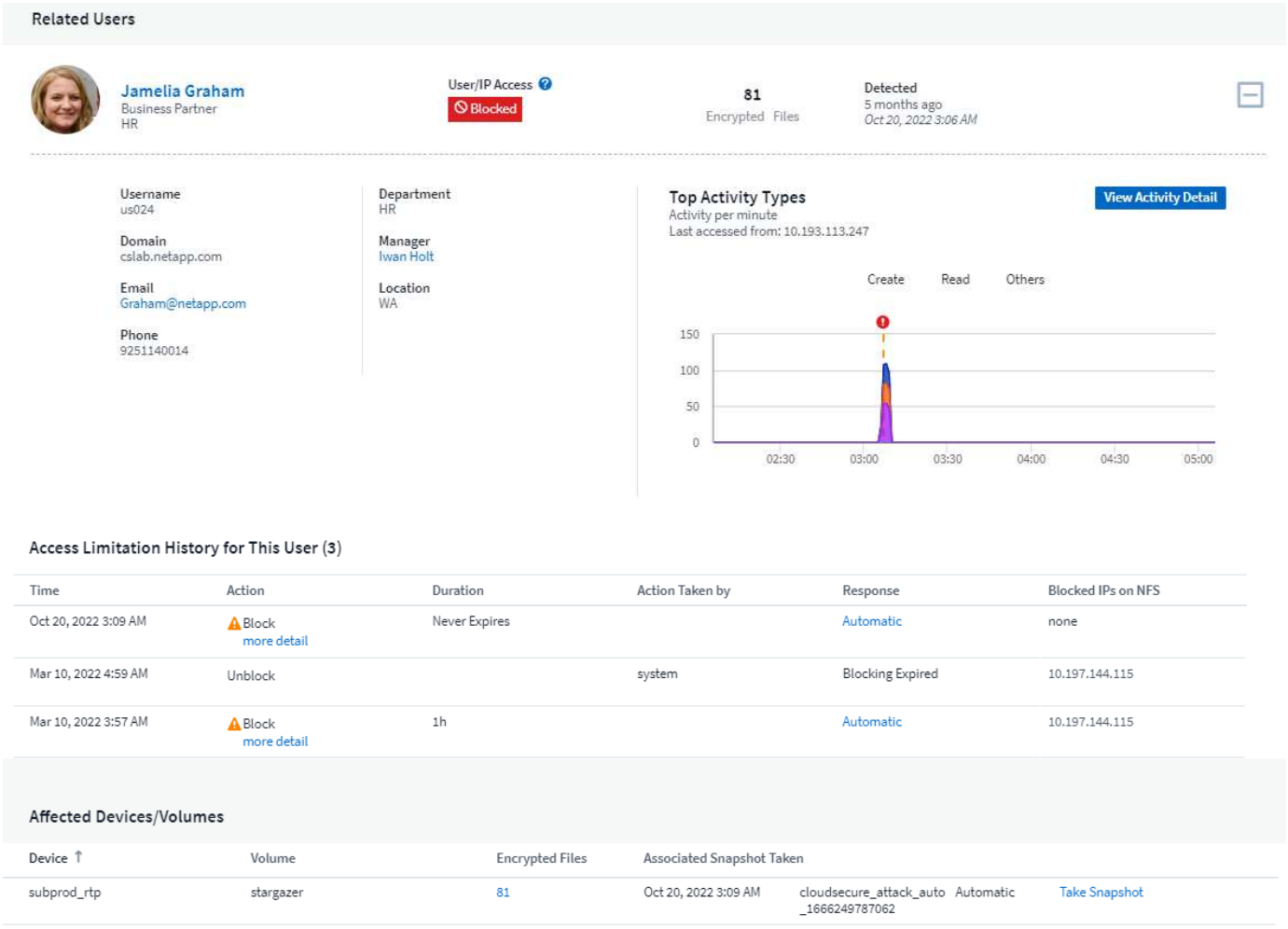
```
security login rest-role create -role arwrole -api /api/storage/volumes
-access readonly -vserver <cluster_name>
security login rest-role create -api /api/security/anti-ransomware -access
readonly  -role arwrole -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role arwrole
```

その他の設定について詳しくは、こちらをご覧ください"ONTAPケンケン"。

アラートの例

ARPイベントにより生成されたアラートの例を次に示します。





信頼性の高いバナーは、攻撃がランサムウェアの挙動とファイル暗号化のアクティビティを示していることを示しています。暗号化ファイルのグラフには、ARP解決策 によってボリューム暗号化アクティビティが検出されたタイムスタンプが示されます。

制限事項

SVMがワークロードセキュリティで監視されていないものの、ONTAP によって生成されたARPイベントがある場合、ワークロードセキュリティはイベントを受信して表示します。ただし、アラートに関連するフォレンジック情報およびユーザーマッピングはキャプチャまたは表示されません。

トラブルシューティング

既知の問題とその解決策を次の表に示します。

問題	解決策：
電子メールアラートは、攻撃が検出されてから24時間後に受信されます。UIでは、その24時間前にData Infrastructure Insights Workload SecurityがEメールを受信するとアラートが表示されます。	ONTAPがData Infrastructure Insights Workload Security（ワークロードセキュリティ）に_Ransomware Detected_Eventを送信すると、Eメールが送信されます。イベントには、攻撃のリストとタイムスタンプが含まれます。Workload Security UIには、攻撃を受けた最初のファイルのアラートタイムスタンプが表示されます。ONTAPは、一定数のファイルがエンコードされると、_Ransomware Detected_EventをData Infrastructure Insightsに送信します。そのため、UIにアラートが表示される時間とEメールが送信される時間が異なる場合があります。

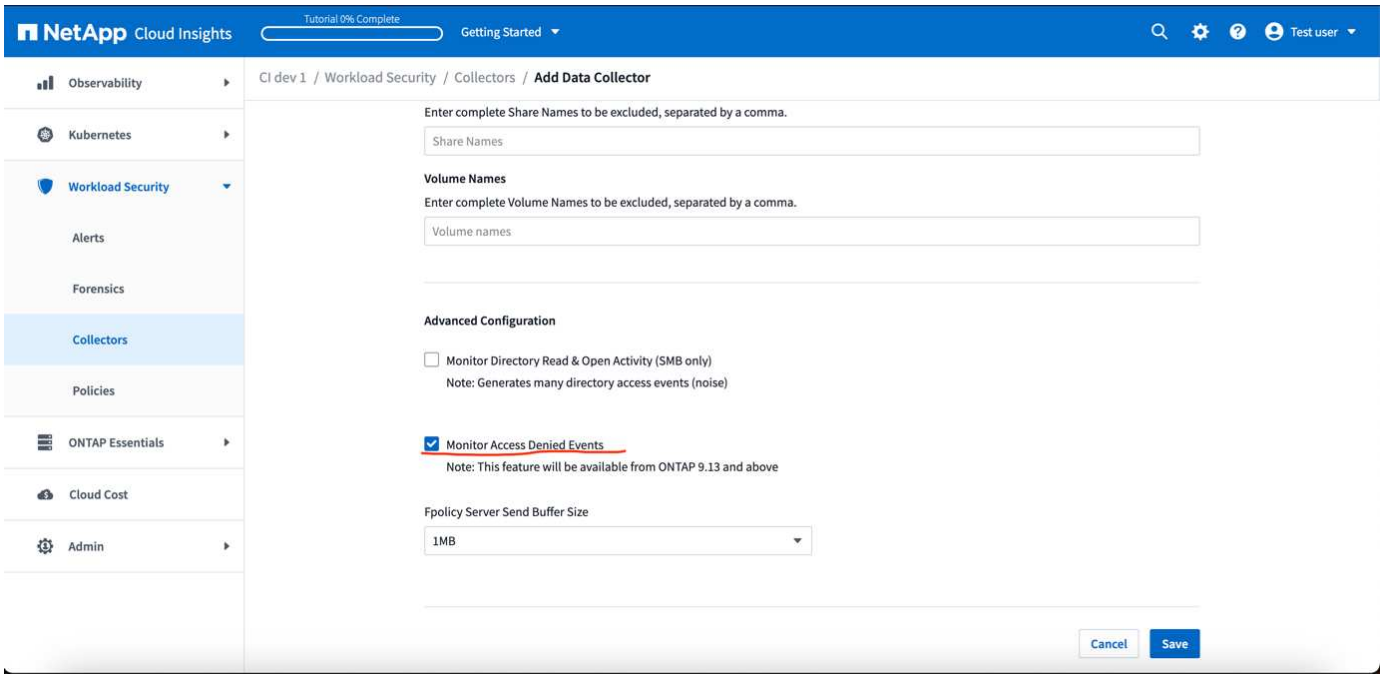
ONTAPアクセス拒否との統合

ONTAPアクセス拒否機能は、NAS環境（NFSおよびSMB）のワークロード分析を使用して、失敗したファイル処理（権限のない処理を実行しようとしているユーザなど）をプロアクティブに検出して警告します。これらのファイル操作の失敗の通知は、特にセキュリティ関連の障害の場合には、初期段階でのインサイダー攻撃のブロックにさらに役立ちます。

データインフラストラクチャインサイトワークロードセキュリティは、ONTAPと統合してアクセス拒否イベントを受信し、追加の分析および自動応答レイヤを提供します。

前提条件

- ONTAPの最小バージョン：9.13.0
- ワークロードセキュリティ管理者は、新しいコレクタの追加時または既存のコレクタの編集時に、[Advanced Configuration]の下にある[*Monitor Access Denied Events*]チェックボックスをオンにして、アクセス拒否機能を有効にする必要があります。



ユーザ権限が必要です

クラスタ管理資格情報を使用してData Collectorを追加する場合、新しい権限は必要ありません。

ユーザに付与された権限を持つカスタムユーザ（_csuser_など）を使用してコレクタを追加する場合は、次の手順に従って、ONTAPでアクセス拒否イベントに登録するために必要な権限をワークロードセキュリティに付与します。

CSUSER WITH_CLUSTER_CREDENTIALの場合は、ONTAPコマンドラインから次のコマンドを実行します。_csrestrole_はカスタムロールで、_csuser_はONTAPカスタムユーザです。

```
 security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster_name>
 security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole
```

csuser with _svm_credentialsの場合は、ONTAPコマンドラインから次のコマンドを実行します。

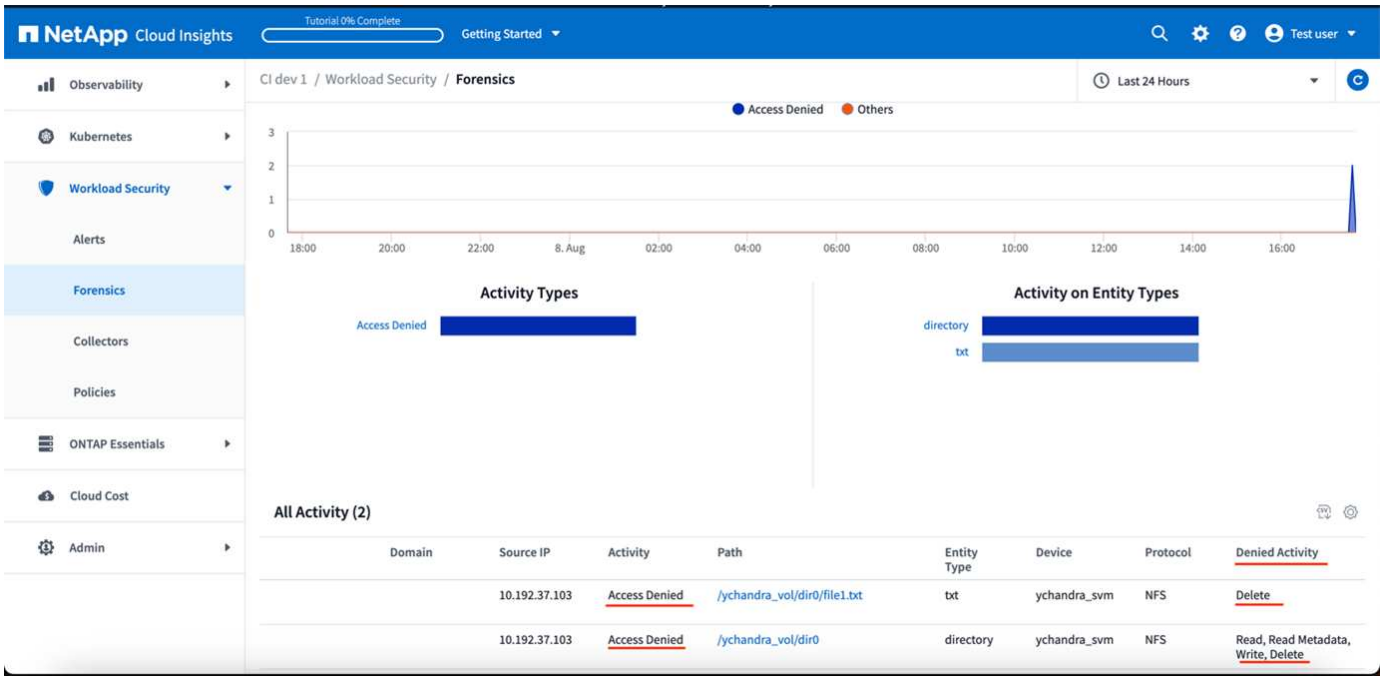
```
 security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <svm_name>
 security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole -vserver <svm_name>
```

その他の設定について詳しくは、こちらをご覧ください"ONTAPケンケン"。

アクセス拒否イベント

ONTAPシステムからイベントが取得されると、[ワークロードセキュリティフォレンジック]ページにアクセス

拒否イベントが表示されます。表示される情報に加えて、歯車アイコンから_desired Activity_columnをテーブルに追加することで、特定の操作で不足しているユーザー権限を表示できます。



ユーザアクセスをブロックしています

攻撃が検出されると、ワークロードセキュリティは、ファイルシステムへのユーザーアクセスをブロックすることで攻撃を停止できます。アクセスは、自動応答ポリシーを使用して自動的にブロックするか、アラートまたはユーザの詳細ページから手動でブロックできます。

ユーザアクセスをブロックする場合は、ブロック期間を定義する必要があります。選択した期間が終了すると、ユーザアクセスが自動的にリストアされます。アクセスブロックは、SMBプロトコルとNFSプロトコルの両方でサポートされています。

SMBおよびホストマシンのIPアドレスに対してユーザが直接ブロックされているため、NFSに対して攻撃がブロックされます。これらのマシンのIPアドレスは、ワークロードセキュリティで監視されているいずれかのStorage Virtual Machine（SVM）へのアクセスがブロックされます。

たとえば、ワークロードセキュリティでは10個のSVMを管理し、自動応答ポリシーでは4つのSVMを設定するとします。攻撃の原因が4つのSVMのいずれかである場合、10個のSVMすべてでユーザのアクセスがブロックされます。元の SVM では引き続き Snapshot が作成されます。

SMB用に設定されたSVMが4つあり、NFS用に設定されたSVMが残り2つのSVMがNFSとSMB両方に対して設定されている場合、4つのSVMのいずれかで攻撃が発生すると、すべてのSVMがブロックされます。

ユーザアクセスブロックの前提条件

この機能を使用するには、クラスタレベルのクレデンシャルが必要です。

クラスタ管理者のクレデンシャルを使用している場合、新しい権限は不要です。

ユーザに付与された権限でカスタムユーザ（_csuser_など）を使用している場合は、次の手順に従ってワークロードセキュリティにユーザをブロックする権限を付与します。

クラスタクレデンシャルを持つ csuser の場合、 ONTAP コマンドラインから次の手順を実行します。

```
security login role create -role csrole -cmddirname "vserver export-policy
rule" -access all
security login role create -role csrole -cmddirname set -access all
security login role create -role csrole -cmddirname "vserver cifs session"
-access all
security login role create -role csrole -cmddirname "vserver services
access-check authentication translate" -access all
security login role create -role csrole -cmddirname "vserver name-mapping"
-access all
```

ページの[Permissions]セクションも確認して"ONTAP SVM Data Collector の設定"ください。

機能を有効にする方法

- [Workload Security]で、**[Workload Security]>[Policies]>[Automated Response Policies]***に移動します。**[**+ Attack Policy]*を選択します。
- [_Block User File Access]を選択（チェック）します。

自動ユーザアクセスブロックの設定方法

- 新しい攻撃ポリシーを作成するか、既存の攻撃ポリシーを編集します。
- 攻撃ポリシーを監視する SVM を選択します。
- [ユーザーファイルアクセスをブロックする]チェックボックスをオンにします。この機能は、このオプションを選択すると有効になります。
- [Time Period]で、ブロッキングを適用する時間を選択します。
- 自動ユーザブロッキングをテストするには、を使用して攻撃をシミュレートします"シミュレートされたスクリプト"。

システム内にブロックされているユーザーがいるかどうかを確認する方法

- アラートリストページでは、ユーザがブロックされた場合に画面上部のバナーが表示されます。
- バナーをクリックすると、[Users]ページが表示され、ブロックされているユーザのリストが表示されます。
- [Users]ページには、「User/IP Access」という名前のカラムがあります。この列には、ユーザブロッキングの現在の状態が表示されます。

ユーザアクセスを手動で制限および管理します

- アラートの詳細画面またはユーザの詳細画面に移動して、これらの画面からユーザを手動でブロックまたは復元できます。

ユーザアクセス制限履歴

［アラートの詳細とユーザーの詳細］ページのユーザーパネルで、ユーザーのアクセス制限履歴（時間、アクション（ブロック、ブロック解除）、期間、実行されたアクション）の監査を表示できます。 手動/自動、およびNFSの影響を受けるIP。

機能を無効にする方法

この機能はいつでも無効にできます。システム内に制限のあるユーザがいる場合は、アクセスを先にリストアする必要があります。

- [Workload Security]で、**[Workload Security]>[Policies]>[Automated Response Policies]***に移動します。**[**+ Attack Policy]*を選択します。
- [_Block User File Access]の選択を解除します（オフにします）。

この機能はすべてのページで非表示になります。

NFSのIPを手動でリストア

ワークロードセキュリティトライアルの期限が切れた場合、またはエージェント/コレクタがダウンした場合に、ONTAP からIPを手動で復元するには、次の手順を実行します。

1. SVM のすべてのエクスポートポリシーをリストします。

```
contrail-qa-fas8020::> export-policy rule show -vserver <svm name>
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
------------ --------------- ------  -------- --------------------
---------
svm0         default         1       nfs3,    cloudsecure_rule,     never
                                     nfs4,    10.11.12.13
                                     cifs
svm1         default         4       cifs,    0.0.0.0/0             any
                                     nfs
svm2         test            1       nfs3,    cloudsecure_rule,     never
                                     nfs4,    10.11.12.13
                                     cifs
svm3         test            3       cifs,    0.0.0.0/0             any
                                     nfs,
                                     flexcache
4 entries were displayed.
```

2. 「cloudsecure_rule」をクライアント一致として持つSVMのすべてのポリシーのルールを削除するには、対応するRuleIndexを指定します。通常、ワークロードのセキュリティルールは1になります。

```
 contrail-qa-fas8020::*> export-policy rule delete -vserver <svm name>
-policyname * -ruleindex 1
```

.
ワークロードセキュリティルールが削除されていることを確認します（確認のためのオプションの手順）。

```
contrail-qa-fas8020::*> export-policy rule show -vserver <svm name>
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
------------ --------------  ------  -------- --------------------
---------
svm0         default         4       cifs,    0.0.0.0/0             any
                                     nfs
svm2         test            3       cifs,    0.0.0.0/0             any
                                     nfs,
                                     flexcache
2 entries were displayed.
```

SMBのユーザを手動でリストア

ワークロードセキュリティトライアルの期限が切れた場合、またはエージェント/コレクタがダウンした場合に、ONTAP からユーザーを手動で復元するには、次の手順を実行します。

ワークロードセキュリティでブロックされたユーザーのリストは、ユーザーリストページから取得できます。

1. cluster_admin_credentialsを使用してONTAP クラスタ（ユーザのブロックを解除する場所）にログインします。（Amazon FSXの場合、FSXクレデンシャルを使用してログインします）。
2. 次のコマンドを実行して、すべてのSVMのSMBワークロードセキュリティでブロックされているすべてのユーザを表示します。

```
vserver name-mapping show -direction win-unix -replacement " "
```

```
Vserver:   <vservername>
Direction: win-unix
Position Hostname         IP Address/Mask
-------- ---------------- ----------------
1       -                -                    Pattern: CSLAB\\US040
                                         Replacement:
2       -                -                    Pattern: CSLAB\\US030
                                         Replacement:
2 entries were displayed.
```

上記の出力では、2人のユーザーがドメインCSLABでブロックされました（US030、US040）。

1. 上記の出力から位置を特定したら、次のコマンドを実行してユーザーのブロックを解除します。

```
 vserver name-mapping delete -direction win-unix -position <position>
```

. コマンドを実行して、ユーザがブロックされていないことを確認します。

```
vserver name-mapping show -direction win-unix -replacement " "
```

以前にブロックしたユーザに対しては、エントリは表示されません。

トラブルシューティング

問題	試してみてください
一部のユーザーは制限されていませんが、攻撃があります。	1.SVMのData CollectorとAgentがin_running_stateであることを確認します。Data CollectorとAgentが停止している場合、ワークロードセキュリティはコマンドを送信できません。2.これは、ユーザが以前に使用されていない新しいIPを持つマシンからストレージにアクセスした可能性があるためです。制限は、ユーザがストレージにアクセスする際に使用するホストの IP アドレスを介して行われます。UI （ Alert Details > Access Limitation History for this User > Affected IP ）で、制限されている IP アドレスのリストを確認します。IP が制限された IP と異なるホストからストレージにアクセスしている場合、ユーザは制限されていない IP を介してストレージにアクセスできます。IP が制限されているホストからアクセスしようとすると、ストレージにアクセスできなくなります。
[Restrict Access] を手動でクリックすると、「このユーザの IP アドレスはすでに制限されています」というメッセージが表示されます。	制限する IP はすでに別のユーザから制限されています。
ポリシーを変更できませんでした。理由：このコマンドは許可されていません。	csuserを使用している場合は、上記のようにユーザに権限が与えられているかどうかを確認します。

問題	試してみてください
NFSのユーザ（IPアドレス）ブロックが機能しますが、SMB / CIFSの場合、次のエラーメッセージが表示されます。「SIDからドメイン名への変換に失敗しました。理由タイムアウト：ソケットが確立されていません」	これは、is_csuser_doesにsshを実行する権限がありません。（クラスタレベルで接続してから、ユーザがsshを実行できることを確認してください）。_csuser_roleには、これらの権限が必要です。https://docs.netapp.com/us-en/cloudinsights/cs_restrict_user_access.html#prerequisites-for-user-access-blockingcsuser_に対してクラスタのクレデンシャルを使用する場合は、ONTAPコマンドラインから次の操作を実行します。security login role create -role csrole -cmddirname set -access all security login role create -role csrole -cmddirname "vserver cifs session"-access all security login role create -role csrole csrole csrole -cmddirname " authentication role " vserver access-cmddirname " vserver services -mapping role ONTAP "
エラーメッセージ_SID変換に失敗しました。_Reason：255：Error：command failed：not authorized for that commandエラー："access-check" is not a recognized command、when a user should have been blocked.	これは、_csuser_に正しい権限がない場合に発生する可能性があります。詳細については、を参照してください "ユーザアクセスブロックの前提条件" 。権限を適用したら、ONTAPデータコレクタとユーザディレクトリデータコレクタを再起動することをお勧めします。必要な権限コマンドを次に示します。---- security login role create -role csrole -cmddirname "vserver export-policy rule"-access all security login role create -role csrole -cmddirname set -access all security login role create -role csrole -cmddirname "vserver cifs session"-access all security login role create -role csrole csrole -cmddirname "vserver services access-check authentication translate"-access role create -role csrole -cmddirname "vserver name-mapping"-access all ----

ワークロードのセキュリティ：攻撃のシミュレーション

このページの手順を使用して、付属のランサムウェアシミュレーションスクリプトを使用して、ワークロードセキュリティをテストまたは実証する攻撃をシミュレートできます。

始める前に注意してください

- ランサムウェアシミュレーションスクリプトは Linux でのみ動作します。
- このスクリプトは、Workload Securityエージェントのインストールファイルとともに提供されます。ワークロードセキュリティエージェントがインストールされているすべてのマシンで使用できます。
- このスクリプトは、Workload Securityエージェントマシン自体で実行できます。他のLinuxマシンを準備する必要はありません。ただし、スクリプトを別のシステムで実行する場合は、スクリプトをコピーしてそこで実行するだけです。

サンプルファイルを 1 、 000 個以上用意してください

このスクリプトは、暗号化するファイルが格納されたフォルダを含む SVM で実行する必要があります。フォルダとサブフォルダには、少なくとも 1 、 000 個のファイルを含めることをお勧めします。ファイルは空にできません。ファイルを作成したり、同じユーザを使用して暗号化したりしないでください。ワークロードセキュリティでは、これはリスクの低いアクティビティとみなされるため、アラートは生成されません（つまり、同じユーザが作成したファイルを変更した場合）。

の手順については、以下を参照してください"プログラムによって空でないファイルを作成します"。

シミュレータを実行する前のガイドライン：

1. 暗号化されたファイルが空でないことを確認します。
2. 必ず50を超えるファイルを暗号化してください。少数のファイルは無視されます。
3. 同じユーザで何度も攻撃を実行しないでください。数回後、ワークロードセキュリティはこのユーザの動作を学習し、それがユーザの通常の動作であると想定します。
4. 同じユーザが作成したファイルは暗号化しないでください。ユーザが作成したばかりのファイルを変更しても、リスクのあるアクティビティとは見なされません。別のユーザが作成したファイルを使用するか、ファイルの作成から暗号化まで数時間かかります。

システムを準備

まず、ターゲットボリュームをマシンにマウントします。NFS マウントまたは CIFS エクスポートをマウントできます。

Linux で NFS エクスポートをマウントするには、次の手順を実行

```
mount -t nfs -o vers=4.0 10.193.177.158:/svmvol1 /mntpt
mount -t nfs -o vers=4.0 Vserver data IP>:/nfsvol /destinationlinuxfolder
```

NFS バージョン 4.1 はマウントしないでください。 FPolicy ではサポートされていません。

Linux で CIFS をマウントするには、次の手順を

```
 mount -t cifs //10.193.77.91/sharedfolderincluster
/root/destinationfolder/ -o username=raisa
```

次に、 `Data Collector` をセットアップします。

1. ワークロードセキュリティエージェントがまだ構成されていない場合は構成します。
2. SVM データコレクタが設定されていない場合は設定します。

ランサムウェアシミュレータスクリプトを実行します

1. ワークロードセキュリティエージェントマシンにログイン（ssh）します。
2. /opt/NetApp/cloudsecure/agent/install_に 移動します

3. パラメータを指定せずにシミュレータスクリプトを呼び出し、使用状況を確認します。

```
# pwd
/opt/netapp/cloudsecure/agent/install
# ./ransomware_simulator.sh
Error: Invalid directory  provided.
Usage: ./ransomware_simulator.sh [-e] [-d] [-i <input_directory>]
       -e to encrypt files (default)
       -d to restore files
       -i <input_directory> - Files under the directory to be encrypted
```

```
Encrypt command example: ./ransomware_simulator.sh -e -i
/mnt/audit/reports/
Decrypt command example: ./ransomware_simulator.sh -d -i
/mnt/audit/reports/
```

テストファイルを暗号化します

ファイルを暗号化するには、次のコマンドを実行します。

```
# ./ransomware_simulator.sh -e -i /root/for/
Encryption key is saved in /opt/netapp/cloudsecure/cloudsecure-agent-
1.251.0/install/encryption-key,
which can be used for restoring the files.
Encrypted /root/for/File000.txt
Encrypted /root/for/File001.txt
Encrypted /root/for/File002.txt
...
```

ファイルのリストア

復号化するには、次のコマンドを実行します。

```
[root@scspa2527575001 install]# ./ransomware_simulator.sh -d -i /root/for/
File /root/for/File000.txt is restored.
File /root/for/File001.txt is restored.
File /root/for/File002.txt is restored.
...
```

スクリプトを複数回実行します

ユーザがランサムウェア攻撃を受けた場合は、別のユーザに切り替えて攻撃を受けます。Workload Securityはユーザの動作を学習し、同じユーザに対してランサムウェア攻撃が繰り返し発生してもアラートを生成しません。

プログラムでファイルを作成します

ファイルを作成する前に、データコレクタの処理を停止または一時停止する必要があります。データコレクタをエージェントに追加する前に、次の手順を実行します。データコレクタをすでに追加している場合は、データコレクタを編集し、無効なパスワードを入力して保存します。これにより、データコレクタが一時的にエラー状態になります。注意：元のパスワードを必ずメモしてください。

ファイルを作成する前にをお勧めし"コレクターの一時停止"ます</Z1>.]</</Z1>

シミュレーションを実行する前に、暗号化するファイルを追加する必要があります。暗号化するファイルを手動でターゲットフォルダにコピーするか、スクリプト（以下の例を参照）を使用してプログラムでファイルを作成することができます。どちらの方法を使用した場合も、 1 、 000 個以上のファイルをコピーしてください。

プログラムでファイルを作成する場合は、次の手順を実行します。

1. [エージェント] ボックスにログインします。
2. Filer の SVM から Agent マシンに NFS エクスポートをマウントします。CD をそのフォルダに移動します。
3. このフォルダに、 createfiles.sh という名前のファイルを作成します
4. 次の行をそのファイルにコピーします。

```
for i in {000..1000}
do
   echo hello > "File${i}.txt"
done
echo 3 > /proc/sys/vm/drop_caches ; sync
```

5. ファイルを保存します。
6. ファイルに対する実行権限を確認します。

```
 chmod 777 ./createfiles.sh
```

. スクリプトを実行します。

```
./createfiles.sh
```

現在のフォルダには 1000 個のファイルが作成されます。

7. データコレクタを再度有効にします

   手順 1 でデータコレクタを無効にした場合は、データコレクタを編集し、正しいパスワードを入力して保存します。データコレクタが running 状態であることを確認します。

8. これらの手順を実行する前にコレクタを一時停止した場合は、を確認して"コレクタの再開"ください。

アラート、警告、およびエージェント / データソースコレクタの状態に関する電子メール通知の設定

ワークロードセキュリティアラートの受信者を設定するには、[*Admin]>[Notifications]をクリックし、受信者ごとに適切なセクションに電子メールアドレスを入力します。

潜在的な攻撃アラートと警告

Attack_alert 通知を送信するには、 _Send Potential Attack Alerts_Section に受信者の電子メールアドレスを入力します。アラートに対するすべてのアクションについて、 E メール通知がアラート受信者リストに送信されます。

警告通知を送信するには、 _ 警告通知の送信 _ セクションに受信者の電子メールアドレスを入力します。

エージェントおよび **Data Collector** のヘルスモニタリング

通知を使用して、エージェントとデータソースの状態を監視できます。

エージェントまたはデータソースコレクタが機能していない場合に通知を受信するには、 _Data Collection Health Alerts_Section に受信者の電子メールアドレスを入力します。

次の事項に注意してください。

- ヘルスアラートは、エージェント / コレクタが少なくとも 1 時間レポートを停止した後にのみ送信されます。
- エージェントまたはデータコレクタが長時間切断されている場合でも、指定された 24 時間以内に目的の受信者に送信される電子メール通知は 1 通だけです。
- エージェントに障害が発生した場合は、 1 つのアラートが送信されます（コレクタごとに送信されるアラートではありません）。E メールには影響を受けるすべての SVM のリストが記載されます。
- Active Directory による収集エラーは警告として報告されますが、ランサムウェアによる検出には影響しません。
- [はじめに] セットアップリストに、新しい _ 電子メール通知の構成 _ 段階が追加されました。

エージェントおよび**Data Collector**のアップグレード通知を受信しています

- [Data Collection Health Alerts]にEメールIDを入力します。
- [Enable upgrade notifications]チェックボックスが有効になります。
- エージェントおよびData Collectorのアップグレードの通知は、予定されているアップグレードの1日前にEメールIDに送信されます。

トラブルシューティング

* 問題： *	* これを試みなさい：*
「Data Collector Health Alerts」にEメールIDが表示されていますが、通知を受信していません。	通知メールは、NetApp Data Infrastructure Insightsドメイン（*accounts@service.clou dinsights.jp NetApp .com*）から送信されます。一部の企業は、外部ドメインからの受信メールをブロックします。NetApp Data Infrastructure Insightsドメインからの外部通知がホワイトリストに登録されていることを確認します。

ワークロードセキュリティ**API**

ワークロードセキュリティAPIにより、ネットアップのお客様と独立系ソフトウェアベンダー（ISV）は、ワークロードセキュリティをCMDBや他のチケット発行システムなどの他のアプリケーションと統合できます。

API アクセスの要件：

- API アクセストークンモデルを使用してアクセスが許可されます。
- APIトークン管理は、管理者ロールを持つワークロードセキュリティユーザが実行します。

API ドキュメント（ **Swagger** ）

最新のAPI情報は、Workload Securityにログインし、* Admin > API Access に移動することで確認できます。**[API Documentation]** リンクをクリックします。APIドキュメントはSwaggerベースです。APIの簡単な説明と使用方法が記載されており、テナントで試すことができます。

Forensics Activity APIを呼び出す場合は、cloudsecure_forensics.activities.* v2 * APIを使用します。このAPIに複数の呼び出しを行う場合は、呼び出しが並列ではなく連続して実行されるようにしてください。複数の並行呼び出しが発生すると、APIがタイムアウトする可能性があります。

API アクセストークン

ワークロードセキュリティAPIを使用する前に、1つ以上の* APIアクセストークン*を作成する必要があります。アクセストークンは読み取り権限を付与します。各アクセストークンの有効期限を設定することもできます。

アクセストークンを作成するには：

- **[Admin] > [API Access]** をクリックします
- [*+API アクセストークン *] をクリックします
- 「 * トークン名 * 」と入力します
- トークンの有効期限 * を指定します

トークンは、クリップボードにコピーして作成プロセス中に保存する場合にのみ使用できます。トークンは作成後に取得できないため、トークンをコピーして安全な場所に保存することを強くお勧めします。トークンの作成画面を閉じる前に、 [API アクセストークンのコピー] ボタンをクリックするよう求められます。

トークンを無効化、有効化、および取り消しできます。無効になっているトークンを有効にできます。

トークンは、顧客の視点からAPIへの汎用アクセスを付与し、APIへのアクセスを自身のテナントのスコープで管理します。

アプリケーションは、ユーザがアクセスの認証と許可に成功した後、ターゲット API を呼び出すときにアクセストークンをクレデンシャルとして渡します。渡されたトークンは、トークンのベアラに対して API へのアクセスが許可されていることを API に通知し、許可中に付与されたスコープに基づいて特定のアクションを実行します。

アクセストークンが渡される HTTP ヘッダーは * X-CloudInsights - apiKey ： * です

たとえば、次のようにしてストレージアセットを取得します。

```
 curl https://<tenant_host_name>/rest/v1/cloudsecure/activities -H 'X-
CloudInsights-ApiKey: <API_Access_Token>'
_<API_Access_Token> _ は、 API アクセスキーの作成時に保存したトークンです。
```

詳細については、 _API Documentation_link の * Admin > API Access * を参照してください。

API経由でデータを抽出するスクリプト

ワークロードセキュリティエージェントには、要求された時間範囲を小さなバッチに分割することで、v2 API への並行呼び出しを容易にするエクスポートスクリプトが含まれています。

スクリプトは_/ opt/ NetApp / cloudsecure/agent/export-script_にあります。使用方法については、同じディレクトリにあるREADMEファイルを参照してください。

スクリプトを呼び出すコマンドの例を次に示します。

```
python3 data-export.py --tenant_url <tenant
id>.cs01.cloudinsights.netapp.com --access_key %ACCESS_KEY% --path_filter
"<dir path>" --user_name "<user>" --from_time "01-08-2024 00:00:00"
--to_time "31-08-2024 23:59:59" --iteration_interval 12 --num_workers 3
```

キーパラメータ:-: `--iteration_interval 12`要求された時間範囲を12時間の間隔に分割します。 `--num_workers 3`-: 3つのスレッドを使用して、これらの間隔を並行してフェッチします。

著作権に関する情報

商標に関する情報