



ワークロードのセキュリティ Cloud Insights

NetApp
April 16, 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.....	46
フォレンジック	53
自動応答ポリシー	61
許可されたファイルタイプポリシー	63
ONTAP によるランサムウェア対策との統合.....	64
ONTAPアクセス拒否との統合.....	67
ユーザアクセスをブロックしています	69
ワークロードのセキュリティ：攻撃のシミュレーション.....	74
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 ...	78
ワークロードセキュリティAPI	79

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

Cloud Insights のストレージワークロードセキュリティ（旧Cloud Secure）は、内部の脅威に関する実用的な情報で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。



ワークロードセキュリティは、Cloud Insights フェデラルエディションでは使用できません。

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は、Cloud Insights フェデラルエディションでは使用できません。

ワークロードセキュリティシステムは、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	<p>[ワークロードセキュリティ]>[コレクタ]をクリックします。</p> <p>設定するデータコレクタをクリックします。</p> <p>ドキュメントの Data Collector Vendor Reference セクションを参照してください。</p> <p>" ビデオ * : ONTAP SVM 接続"</p>
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。例："[このガイドを参照してください](#)" Splunk と統合し、

ワークロードセキュリティエージェントの要件

実行する必要があります ["エージェントをインストールします"](#) データコレクタから情報を取得します。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。



ストレージワークロードセキュリティは、Cloud Insights フェデラルエディションでは使用できません。

コンポーネント	Linux 要件
オペレーティングシステム	<p>次のいずれかのライセンスバージョンを実行しているコンピュータ。</p> <p>Red Hat Enterprise Linux 7.x、8.x 64ビット、SELinux CentOS 7.x 64ビット、SELinux CentOS 8 Stream、SELinux Ubuntu 20から22 64ビット Rocky 8.x 64ビット、Rocky 9.x 64ビット、SELinux SUSE Linux Enterprise Server 15 SP3、SUSE Linux Enterprise Server 15 SP4、SUSE 15 SP3上のSELinux</p> <p>このコンピュータでは、他のアプリケーションレベルのソフトウェアを実行しないでください。専用のサーバを使用することを推奨します。</p>
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	<p>ディスクスペースは次の方法で割り当てる必要があります。 /opt/netapp 35GB（最小）</p> <p>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。</p> <p>/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。ローカルユーザにこのフォルダへのアクセス権がない場合、エージェントまたはデータコレクタのインストールが失敗する可能性があります。を参照してください "トラブルシューティング" 詳細については、を参照してください。</p>
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）

ワークロードセキュリティエージェントは、Cloud Insights Acquisition UnitやAgent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	<p>50~55 GB</p> <p>Linuxの場合は、次の方法でディスクスペースを割り当てる必要があります。</p> <p>/opt/ネットアップ25~30GB /var/log/netapp 25GB</p>
---------------	--

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	宛先	説明
TCP	443年	ワークロードセキュリティエージェント	<site_name>.cs01.cloudinsights.netapp.com <site_name>.c01.cloudinsights.netapp.com <site_name>.c02.cloudinsights.netapp.com	Cloud Insights へのアクセス
TCP	443年	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・セキュリティ環境の場合：

プロトコル	ポート	ソース	宛先	説明
TCP	443年	ワークロードセキュリティエージェント	<site_name>.cs01-eu-1.cloudinsights.netapp.com <site_name>.c01-eu-1.cloudinsights.netapp.com <site_name>.c02-eu-1.cloudinsights.netapp.com	Cloud Insights へのアクセス
TCP	443年	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	宛先	説明
TCP	443年	ワークロードセキュリティエージェント	<site_name>.cs01-ap-1.cloudinsights.netapp.com <site_name>.c01-ap-1.cloudinsights.netapp.com <site_name>.c02-ap-1.cloudinsights.netapp.com	Cloud Insights へのアクセス
TCP	443年	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	宛先	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年	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
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）。

プロトコル	ポート	ソース	宛先	説明
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

を参照してください ["イベントレートチェッカー"](#) サイジングに関する情報のドキュメント

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。エージェントは環境内のデバイスに接続し、分析のためにワークロードセキュリティSaaSレイヤに送信されるデータを収集します。を参照してください ["エージェントの要件"](#) エージェント VM を設定します。



ワークロードセキュリティは、Cloud Insights フェデラルエディションでは使用できません。

作業を開始する前に

- 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。
- Cloud Insightsのセキュリティについては、 ["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。

Add an Agent



Cloud Secure collects device and user data using one or more Agents installed on local servers. Each Agent can host multiple Data Collectors, which send data to Cloud Secure for analysis.

Which Operating system are you using ?

CentOS

RHEL

Close

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。

Agent Server Requirements

Installation Instructions

Open up a terminal window and run the following commands:

- ```
export https_proxy='USER:PASSWORD@PROXY_SERVER:PORT'
```

- ```
token='eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzU4NCJ9.eyJvbmV0aWw1IjVGR  
rZW5JZCk1Zi05YjU0WFJlLTQwNDYtNDk1Zi05YjU1LTdhYjZlODhmNDVlMy  
IsInJvbnZlclVybyCkBlwU1l0sInNlcnZlclVybyCI6Imh0dHBzOi8vZmc3M  
rZW5JZCk1Zi05YjU0WFJlLTQwNDYtNDk1Zi05YjU1LTdhYjZlODhmNDVlMy  
IsInJvbnZlclVybyCkBlwU1l0sInNlcnZlclVybyCI6Imh0dHBzOi8vZmc3M  
xYmJmLTJhMDI0YjYjMC04ODY2LWYwN2JhMDI0YjYjcwMSIsImh0dHBzOi8vZmc3M
```

Close

- ✔ New agent detected!

1. を設定する必要があります "User Directory Collector の略"。
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
```

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 <code>/opt/NetApp/cloudsecure/agent/logs/agent.log</code> フォルダが作成されず、 <code>install.log</code> 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、を使用してサービスログに表示されます <code>journalctl -u cloudsecure-agent.service</code> コマンドを実行しますこのコマンドを使用して、問題のトラブルシューティングをさらに行うことができます。
「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。を参照してください "エージェントの要件" 。

問題	解決策：
<p>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：</p> <p>"-bash：unzip：コマンドが見つかりません"</p>	<p>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。</p> <p>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。</p>
<p>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。</p>	<p>Agent マシンに SSH 接続します。を使用して、エージェントサービスのステータスを確認します <code>sudo systemctl status cloudsecure-agent.service</code>。</p> <p>1.ログに「Failed to start Workload Security daemon service」というメッセージが表示されるかどうかを確認します。</p> <p>2. cssys 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。</p> <pre>sudo id cssys sudo groups cssys</pre> <p>3.何も存在しない場合は、中央集中型の監視ポリシーによってcssysユーザが削除されている可能性があります。</p> <p>4. 次のコマンドを実行して、cssys のユーザとグループを手動で作成します。</p> <pre>sudo useradd cssys sudo groupadd cssys</pre> <p>5.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。</p> <pre>sudo systemctl restart cloudsecure-agent.service</pre> <p>6.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。</p>
<p>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。</p>	<p>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で使用できます。</p>
<p>Agent is in not_connected 状態であることが UI に表示されます。</p>	<p>エージェントを再起動する手順。</p> <p>1. エージェントマシンに SSH 接続します。</p> <p>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。</p> <pre>sudo systemctl restart cloudsecure-agent.service</pre> <p>3.からエージェントサービスのステータスを確認します <code>sudo systemctl status cloudsecure-agent.service</code>。</p> <p>4. エージェントは接続状態になります。</p>

問題	解決策：
<p>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。</p>	<p>*.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。</p>
<p>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。</p>	<p>「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。</p> <ol style="list-style-type: none"> 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「トークン=.....」をコピーして貼り付けます。/cloudsecure-agent-install.sh "インストールコマンドを入力し、Enterキーを押します。 4. インストールを続行できるはずです。
<p>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。Cloud Insights のシリアル番号を入力してケースをオープンし、メモしておいたケースにログを添付します。</p>	<p>ログをケースに添付するには、次の手順に従います。</p> <ol style="list-style-type: none"> 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-symptoms.zip)を共有します。 A /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh <p>以下のコマンドをroot権限で1つずつ実行し、出力を共有します。</p> <p>A ID csys B グループcsys c. Cat /etc/os-release</p>

問題	解決策：
<p>cloudsecure-agent-symptom-collector.shスクリプトが次のエラーで失敗します。</p> <pre>[root@machine tmp]#/opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh サービスログを収集しています アプリケーションログを収集しています エージェント設定を収集しています サービスステータスのスナップショットを取得しています エージェントディレクトリ構造のスナップショットを取得しています /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh行52:zip:コマンドが見つかりません エラー：/tmp/ cloudsecure-agent-symptoms.zipを作成できませんでした</pre>	<p>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。</p> <p>次に、cloudsecure-agent-symptom-collector.shを再度実行します。</p>
<p>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</p>	<p>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。</p> <p>回避策では、次のコマンドを使用してcssysユーザを作成し、ログインディレクトリを手動で追加します。</p> <pre>sudo useradd user_name -m -d home_DIR</pre> <p>-m：ユーザのホームディレクトリが存在しない場合は作成します。</p> <p>-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</p> <p>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。</p>

問題	解決策：
<p>エージェントはインストール後に実行されていません。 <code>_systemctl status cloudsecure-agent.service</code> には、次の情報が表示されます。</p> <pre>[root@demo ~]# systemctl status cloudsecure-agent.service agent.service--Workload Security Agent Daemon Service (ワークロードセキュリティエージェントデーモンサービス) loaded: loaded(/usr/lib/systemd/system/cloudsecure-agent.service;有効;ベンダープリセット:無効) アクティブ:アクティブ化(自動再起動)(結果:終了コード) Since Tue 2021-08-03 21:12:26 PDT;2 s ago プロセス: 25889 ExecStart=/bin/bash /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent (code=exited status=126) メインPID: 25889 (コード=終了、ステータス= 126)、</pre> <p>Aug 03 21:12:26 demo systemd[1]: cloudsecure-agent.service: main process exited、code=exited、status=126/n/a Aug 03 21:12:26 demo systemd[1]: Unit cloudsecure-agent.service entered failed state. 8月03日21:12:26デモシステムd[1]: cloudsecure-agent.serviceが失敗しました。</p>	<p>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</p> <p>/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。</p> <p>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。</p> <p>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。</p>
<p>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。</p>	<p>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。</p> <ol style="list-style-type: none"> 1.プロパティファイルを含むフォルダに変更します。 <pre>CD /opt/netapp/cloudsecure/conf</pre> <ol style="list-style-type: none"> 2.お気に入り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。 <pre>agent_proxy_host = scspa1950329001.vm.netapp.com AGENT_PROXY_PORT = 80 agent_proxy_user = pxuser AGENT_PROXY_PASSWORD = pass1234</pre> <ol style="list-style-type: none"> 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。 <pre>sudo systemctl restart cloudsecure-agent.service</pre>

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。

作業を開始する前に

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。

作業を開始する前に

- このタスクを実行するには、Cloud Insights 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、次のいずれかをクリックします。
[Collectors]>[User Directory Collector]>[+ User Directory Collector]*を選択し、[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	説明
名前	ユーザディレクトリの一意の名前。例： <i>GlobalADCollector</i>
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	<p>ディレクトリ構造のフォレストレベル。 フォレスト名では、次の両方の形式を使用できます。</p> <p><i>x.y.z</i>⇒ドメイン名をSVMと同じように直接指定します。 [例：hq.companyname.com]</p> <p><i>dc=x</i>、<i>dc=y</i>、<i>dc=z</i>⇒相対識別名[例：dc=hq、dc=companyname、dc=com]</p> <p>または、次のように指定できます。</p> <p><i>OU=engineering</i>、<i>DC=hq</i>、<i>DC=companyname</i>、<i>DC=com</i>[特定のOU engineeringでフィルタする]</p> <p><i>CN=username</i>、<i>OU=engineering</i>、<i>DC=companyname</i>、<i>DC=netapp</i>、<i>DC=com</i>[OU <engineering>から<username>を使用して特定のユーザだけを取得する場合]</p> <p><i>CN=Acrobat</i>ユーザ、<i>CN=Users</i>、<i>DC=HQ</i>、<i>DC=companyname</i>、<i>DC=com</i>、<i>O=companyname</i>、<i>L=Boston</i>、<i>S=MA</i>、<i>C=US</i>[その組織のユーザ内のすべてのAcrobatユーザを取得するには]</p> <p>信頼されたActive Directoryドメインもサポートされます。</p>
バインド DN	<p>ディレクトリの検索が許可されています。たとえば、<i>username@companyname.com</i> や <i>username@domainname.com</i> などです</p> <p>また、Domain Read Only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。</p>
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、Idaps、Idap-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 (Attributes)	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 (Attributes)	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
国名	共同
状態	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	所属グループ

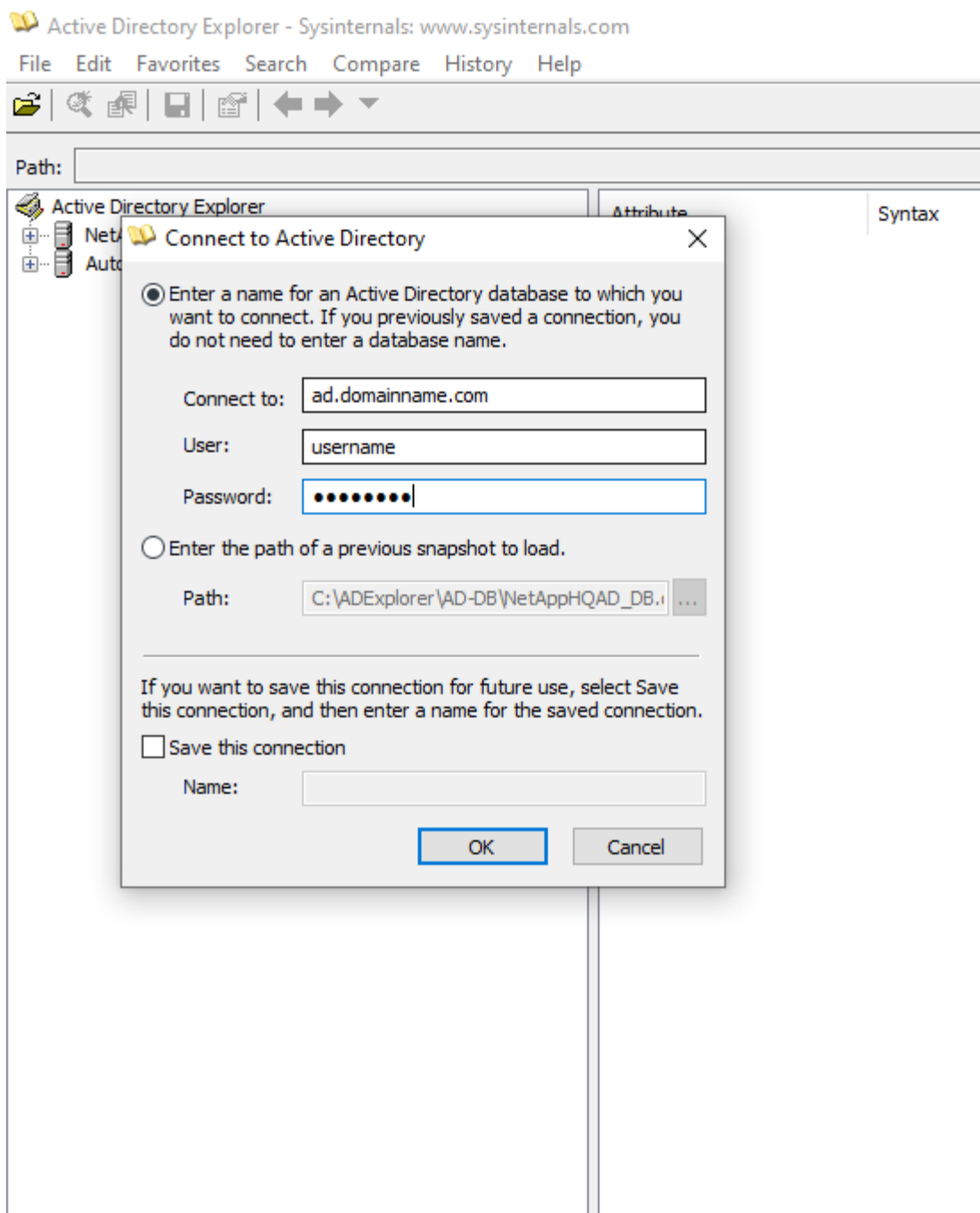
ユーザディレクトリコネクタ設定のテスト

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 Explorer を使用して、AD データベースのナビゲート、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。
 - をインストールします ["AD エクスプローラ"](#) AD サーバに接続できる任意の Windows マシン。
 - AD ディレクトリサーバのユーザ名と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ネクタ設定エラーのトラブルシューティング

次の表に、コネ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。デフォルトのポート値または AD サーバの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？	コレクタの再起動後すぐに AD 同期が行われます。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。
ユーザーデータは、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ィールページに入力されていません。	<p>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。</p> <ol style="list-style-type: none"> 1. Active Directory からユーザの情報を取得している特定の Active Directory コレクタを編集します。 2. オプション属性の下に、Active Directory 属性「telephonenumber」にマッピングされたフィールド名「Telephone Number」があることに注意してください。 4. ここでは、前述の 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、実際にユーザの電話番号を持つ「telephonenumber」という名前の属性があることを確認します。 5. ここでは、Active Directory で「phonenummer」に変更されたとします。 6. 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「phonenummer」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が取得され、ユーザプロフィールページにも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。	<p>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。</p> <p>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。</p> <p>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。</p>
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ります。	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。

作業を開始する前に

- このタスクを実行するには、Cloud Insights 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ネクタの設定手順

1. [Workload Security]メニューで、次のいずれかをクリックします。
[Collectors]>[User Directory Collector]>[+ User Directory Collector]*を選択し、[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	説明
名前	ユーザディレクトリの一意の名前。たとえば、「 <i>GlobalLDAPCollector</i> 」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	<p>LDAPサーバの検索ベース 検索ベースでは、次の両方の形式を使用できます。</p> <p><i>x.y.z</i>⇒ドメイン名をSVMと同じように直接指定します。[例：hq.companyname.com]</p> <p><i>dc=x</i>、<i>dc=y</i>、<i>dc=z</i>⇒相対識別名[例：dc=hq、dc=companyname、dc=com]</p> <p>または、次のように指定できます。</p> <p><i>OU=engineering</i>、<i>DC=hq</i>、<i>DC=companyname</i>、<i>DC=com</i>[特定のOU engineeringでフィルタする]</p> <p><i>CN=username</i>、<i>OU=engineering</i>、<i>DC=companyname</i>、<i>DC=netapp</i>、<i>DC=com</i>[OU <engineering>から<username>を使用して特定のユーザだけを取得する場合]</p> <p><i>CN=Acrobat</i>ユーザー、<i>CN=Users</i>、<i>DC=HQ</i>、<i>DC=companyname</i>、<i>DC=com</i>、<i>O=companyname</i>、<i>L=Boston</i>、<i>S=MA</i>、<i>C=US</i>[その組織のユーザー内のすべてのAcrobatユーザーを取得するには]</p>

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
ー ジョン	ー 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（Attributes）	ディレクトリサーバの属性名
表示名	名前
UNIX ID	uidNumber
ユーザ名	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（Attributes）	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
国名	共同
状態	状態
部門	部門番号
写真	写真
ManagerDN	マネージャー
グループ	所属グループ

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 Explorer をインストールします (<http://ldaptool.sourceforge.net/>) またはJava LDAPエクスプローラ (<http://jxplorer.org/>) LDAPサーバに接続できるすべてのWindowsマシンで使用します。
- 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 ディレクトリコネクタ設定エラーのトラブルシューティング

次の表に、コネ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。

問題	解決策：
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。
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、次のエラーが表示されます。 「Failed to determine the health of the collector within 2 retries、try restarting the collector again（Error Code：AGENT008）」	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 指定し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。

問題	解決策：
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。デフォルトのポート値または AD サーバの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。
コネクタの再起動後、LDAP 同期はいつ行われますか。	コネ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。
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ィールページに入力されていません。	<p>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。</p> <ol style="list-style-type: none"> 1. Active Directory からユーザの情報を取得している特定の Active Directory コネクタを編集します。 2. オプション属性の下に、Active Directory 属性「telephonenumber」にマッピングされたフィールド名「Telephone Number」があることに注意してください。 4. ここでは、前述の 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、実際にユーザの電話番号を持つ「telephonenumber」という名前の属性があることを確認します。 5. ここでは、LDAP ディレクトリで「phonenumber」に変更されたとします。 6. CloudSecure User Directory コネクタを編集します。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 コネクタを保存すると、コネクタが再起動してユーザの電話番号が取得され、ユーザプロフィールページにも同じ番号が表示されます。

問題	解決策：
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。	<p>ユーザーディレクトリコネ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。</p> <p>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。</p> <p>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ネクタが AD に接続されている必要があります。</p>

ONTAP SVM Data Collector の設定

ワークロードセキュリティでは、データコネクタを使用して、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。

作業を開始する前に

- このデータコネクタは、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。
 - NFSプロトコルバージョン4.0以前
 - 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_SOURCE、および_SYNC_destination_のみです。
- エージェント **"を設定する必要があります"** データコネクタを設定する前に、
- 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。
- 最適なパフォーマンスを実現するには、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ます、大文字と小文字が区別されます。
 - SVM 管理 IP、ユーザ名、およびパスワードを使用する
 - フル管理者のクラスタ / SVM 管理ユーザ名とパスワードを使用できない場合は、に記載されている権限よりも少な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」"** セクションを参照してください。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。
 - 以下の「権限に関する注意」セクションで説明されているように、少なくともcsroleの権限を持つ

ロールを持つ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 <vservname> -user-or  
-group-name <username>
```

出力例：

```
Vserver: svmname
```

User/Group Name	Application	Authentication Method	Role Name	Acct Locked	Second Authentication 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。

クラスタシェル：：> vservice cifs show

Vservice 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、この手順を省略します。

クラスタシェル：：> 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、この手順を省略します。

クラスタシェル：：> 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、この手順を省略してください。

クラスタシェル：：> 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。

を参照してください ["エージェントの要件"](#) を参照してください。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

次の点に注意してください。 ["ユーザアクセスブロック"](#)：

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
```

ONTAP ARP統合の権限：

```
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
```

ONTAPアクセス拒否の権限：

```
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
```

注: 1つのrest-role (*arwrole_or_csrestrole*--)がすでに追加されている場合、2つ目のrest-roleを追加する必要はありません。以下の例のように、API権限を追加するだけです。

例: *_csrestrole_*はすでに存在しているため、ランサムウェア対策を有効にし、既存の*_csrestrole_*にAPI権限を付与するだけで済みます。

```
security login rest-role create -role csrestrole -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>
```

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、<vservname> 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 <vservname> -role csrole -cmddirname
DEFAULT -access none
```

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

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

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

ONTAPアクセス拒否の権限：

```
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自律型ランサムウェア対策の権限

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
```

詳細については、["ONTAP によるランサムウェア対策との統合"](#)

ONTAPアクセスの権限が拒否されました

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、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>
```

詳細については、["ONTAPアクセス拒否との統合"](#)

データコレクタを設定します

設定の手順

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]*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	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	SVM / クラスタにアクセスするためのユーザ名 クラスタ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。 1. クラスタ管理者 2. 「csuser」 3. csuserと同様の役割を持つADユーザ。 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. AD - csuserと同様のロールを持つユーザ名。
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。

完了後

- 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。

Metro Clusterの推奨構成

Metro Cluster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
データコレクタには`_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のサービスポリシーを使用してData Source Collectorに接続するには、Data Service_data-NFS_、および/or _data-cifs_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Cloud Insights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ページは、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、Cloud Insights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。

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。

エラーの場合は、`Status_column` で `_more detail` をクリックしてエラーの詳細を確認します。

Installed Data Collectors

Name	Status	Type	Agent
9.8_vs1	 Error more detail	ONTAP SVM	agent-11

問題	解決策：
<p>Data Collector はしばらくの間実行され、ランダムな時刻の後に停止します。"Error message: connector is in error state" というエラーメッセージが表示されます。サービス名： audit。エラーの理由：外部 FPolicy サーバが過負荷状態です。」</p>	<p>ONTAP からのイベントレートは、[エージェント] ボックスで処理できるイベントレートよりもはるかに高くなっています。そのため、接続が終了しました。</p> <p>切断が発生したときに、CloudSecure でピークトラフィックを確認します。これは、* CloudSecure > Activity Forensics > All Activity * ページで確認できます。</p> <p>集約されたトラフィックのピークが [エージェント] ボックスで処理できるトラフィックよりも大きい場合は、[エージェント] ボックスでのコレクタ展開のサイズ設定方法に関する [イベントレートチェッカー] ページを参照してください。</p> <p>2021年3月4日より前にAgentがAgentボックスにインストールされている場合は、Agentボックスで次のコマンドを実行します。</p> <pre>echo 'net.core.rmem_max=838608'>>/etc/sysctl.conf echo 'net.ipv4.tcp_rmem=4096 2097152 838608'>>/etc/sysctl.conf sysctl -p</pre> <p>サイズ変更後にUIからコレクタを再起動します。</p>

問題	解決策：
<p>コレクタから「No local IP address found on the Connector that can reach the data interfaces of the SVM」というエラーメッセージが報告されます。</p>	<p>その理由としては、ONTAP 側のネットワーク問題が考えられます。次の手順を実行してください。</p> <ol style="list-style-type: none"> 1. SVMデータLIFまたは管理LIFに、SVMからの接続をブロックしているファイアウォールがないことを確認します。 2. クラスタ管理 IP を使用して SVM を追加する場合、Agent VM から SVM のデータ LIF と管理 LIF に ping できることを確認します。問題が発生した場合は、LIF のゲートウェイ、ネットマスク、およびルートを確認してください。 <p>また、クラスタ管理 IP を使用して SSH 経由でクラスタにログインし、エージェント IP に ping を実行することもできます。エージェントIPがping可能であることを確認します。</p> <pre>network ping -vserver <vserver name>-destination <Agent IP>-lif <Lif Name>-show-detail</pre> <p>pingできない場合は、ONTAPのネットワーク設定が正しいことを確認して、エージェントマシンにpingできるようにします。</p> <ol style="list-style-type: none"> 3. クラスタ IP 経由で接続しようとしたが動作しない場合は、SVM IP 経由で直接接続してみます。SVM IP を使用して接続する手順については、上記を参照してください。 4. SVM の IP と vsadmin のクレデンシャルを使用してコレクタを追加するときに、SVM の LIF で Data plus Mgmt ロールが有効になっていることを確認します。この場合、SVM LIF に ping することは可能ですが、SVM LIF への SSH は機能しません。「はい」の場合は、SVM 管理のみの LIF を作成し、この SVM 管理のみの LIF を使用して接続してみてください。 5. まだ機能しない場合は、新しい SVM LIF を作成し、その LIF を介して接続します。サブネットマスクが正しく設定されていることを確認します。 6.高度なデバッグ: <ol style="list-style-type: none"> a) ONTAPでパケットトレースを開始します。 b) CloudSecure UIからSVMにデータコレクタを接続してみます。 c)エラーが表示されるまで待ちます。ONTAP でパケットトレースを停止します。 d) ONTAPからパケットトレースを開きます。この場所で入手できます <pre>\ https : //<cluster_mgmt_ip>/spi /<clustername>/etc/log/packet_traces/</pre>

問題	解決策：
<p>メッセージ： "[hostname:<IP Address>] の ONTAP タイプを特定できませんでした。理由：ストレージシステム <IP アドレス> への接続エラー：ホストに到達できません（ホストに到達できません） "</p>	<p>1. 正しい SVM IP 管理アドレスまたはクラスタ管理 IP が指定されていることを確認します。</p> <p>2. 接続する SVM またはクラスタに SSH で接続します。接続が完了したら、SVM またはクラスタ名が正しいことを確認してください。</p>
<p>エラーメッセージ：「コネクタにエラーがあります。service.name：監査。失敗の理由：外部 FPolicy サーバが終了しました。」</p>	<p>1. 多くの場合、ファイアウォールがエージェントマシンの必要なポートをブロックしています。エージェントマシンが SVM から接続するために、ポート範囲 35000-55000/TCP を開いていることを確認します。また、ONTAP 側からエージェントマシンへの通信をブロックするファイアウォールが有効になっていないことを確認します。</p> <p>2. [エージェント] ボックスに次のコマンドを入力し、ポート範囲が開いていることを確認します。</p> <pre>_sudo iptables -save</pre>

問題	解決策：
<p>grep 3500 * _</p> <p>出力例は次のようになります。</p> <pre>-a in_public_allow -p tcp -m tcp -- dport 35000 -m conntrack -ctstate new -j accept</pre> <p>3.SVMにログインし、次のコマンドを入力して、ONTAPとの通信をブロックするファイアウォールが設定されていないことを確認します。</p> <pre>system services firewall show _ _system services firewall policy show _</pre> <p>"ファイアウォールコマンドをチェックしてください"を選択します。 ONTAP</p> <p>4. 監視する SVM / クラスタに SSH で接続します。SVMデータLIFから[Agent]ボックスにpingを送信し（CIFSプロトコルとNFSプロトコルをサポート）、pingが動作していることを確認します。</p> <pre>_network ping -vserver <vserver name>-destination <Agent IP>-lif <Lif Name>-show-detail</pre> <p>pingできない場合は、ONTAPのネットワーク設定が正しいことを確認して、エージェントマシンにpingできるようにします。</p> <p>5. 1つのSVMを2つのデータコレクタを使用してテナントに2回追加すると、このエラーが表示されます。UIを使用して、いずれかのデータコレクタを削除します。次に、UIを使用して他のデータコレクタを再起動します。次に、データコレクタのステータスが「running」と表示され、SVMからのイベントの受信が開始されます。</p> <p>基本的に、テナントでは、1つのデータコレクタで1つのSVMを追加します。1つのSVMを2つのデータコレクタを使用して2回追加しないで</p> <p>6.同じSVMが2つの異なるワークロードセキュリティ環境（テナント）に追加された場合は、最後の1つが常に成功します。2つ目のコレクタは、独自のIPアドレスでFPolicyを設定し、最初のIPアドレスから開始します。そのため、最初のデータ収集ツールはイベントの受信を停止し、その「監査」サービスはエラー状態になります。</p> <p>これを回避するには、各SVMを1つの環境に設定します。</p> <p>7.このエラーは、サービスポリシーが正しく設定されていない場合にも発生する可能性があります</p>	<p>アクティビティページにイベントは表示されません。</p>

問題	解決策：
<p>1. ONTAP コレクタが「実行中」の状態かどうかを確認します。「はい」の場合は、一部のファイルを開いて、CIFS クライアント VM 上で一部の CIFS イベントが生成されていることを確認します。</p> <p>2. アクティビティが表示されない場合は、SVM にログインして次のコマンドを入力してください。 <code>source fpolicy<SVM> event log show -source fpolicy_ fpolicy</code>に関連するエラーがないことを確認してください。</p> <p>3. アクティビティが表示されない場合は、SVM にログインしてください。次のコマンドを入力します。 <code><SVM> fpolicy show _</code> プレフィックスが「cloudsecure_」であるという名前のFPolicyポリシーが設定され、ステータスが「on」になっているかどうかを確認します。設定されていないと、Agent が SVM でコマンドを実行できない可能性が高くなります。ページの先頭に記載されているすべての前提条件を満たしていることを確認してください。</p>	<p>SVM Data Collector がエラー状態で、エラーメッセージ「Agent failed to connect to the collector」</p>
<p>1. エージェントが過負荷になっており、データソースコレクタに接続できない可能性が高い。</p> <p>2. エージェントに接続されているデータソースコレクタの数を確認します。</p> <p>3. UI の「All Activity」ページでデータフローレートを確認します。</p> <p>4. 1 秒あたりのアクティビティ数が非常に多い場合は、別のエージェントをインストールし、一部のデータソースコレクタを新しいエージェントに移動します。</p>	<p>SVM Data Collector で、「 fpolicy.server.connectError: Node failed to establish a connection with the FPolicy server "12.195.15.146"（reason：Select Timed Out）」というエラーメッセージが表示される</p>
<p>SVM / クラスタでファイアウォールが有効になっています。そのため、FPolicy エンジンが FPolicy サーバに接続できません。 詳細情報の取得に使用できるONTAPのCLIは次のとおりです。</p> <p>event log show -source fpolicyでエラーを表示します event log show -source fpolicy -fields event、action、詳細を表示する説明。</p> <p>"ファイアウォールコマンドをチェックしてください"を選択します。ONTAP</p>	<p>エラーメッセージ：「コネクタはエラー状態です。サービス名：audit。失敗の理由：SVM で有効なデータインターフェイスが見つかりません（ロール：データ、データプロトコル：NFS か CIFS か、両方、ステータス：稼働）。」</p>
<p>動作インターフェイス（データプロトコルおよびデータプロトコルとして CIFS / NFS が設定されている）があることを確認してください。</p>	<p>データコレクタが Error 状態になり、しばらくしてから running 状態になり、Error に戻ります。このサイクルが繰り返されます。</p>

問題	解決策：
<p>これは通常、次のシナリオで発生します。</p> <ol style="list-style-type: none"> 1.複数のデータコレクタが追加されています。 2.このような動作を示すデータコレクタには、これらのデータコレクタにSVMが1つ追加されます。つまり、2つ以上のデータコレクタが1つのSVMに接続されます。 3.1つのデータコレクタが1つのSVMにのみ接続されることを確認します。 4.同じSVMに接続されている他のデータコレクタを削除します。 	<p>コネクタでエラーが発生しています。サービス名：audit。失敗の理由：（SVM SVM名のポリシー）を設定できませんでした。理由：'fpolicy.scope-modify'：'federy'内の'shares-to-include'要素に無効な値が指定されています</p>
<p>共有名は、引用符を付けずに指定する必要があります。ONTAP SVM DSC 設定を編集して共有名を修正します。</p> <p>Include および exclude shares _ は、長い共有名のリストを対象としたものではありません。対象に含める共有や除外する共有が大量にある場合は、ボリュームでフィルタリングします。</p>	<p>クラスタに未使用の既存のポリシーがあります。ワークロードセキュリティをインストールする前に、これらのワークロードに対して何を行う必要がありますか？</p>
<p>切断状態の場合でも、既存の未使用の FPolicy 設定をすべて削除することを推奨します。ワークロードセキュリティで、プレフィックス「cloudsecure_」を付けてFPolicyを作成します。その他の未使用の FPolicy 設定はすべて削除できます。</p> <p>fpolicy listを表示するCLIコマンド：</p> <p><i>fpolicy show</i></p> <p>FPolicy設定を削除する手順は次のとおりです。</p> <p><i>fpolicy disable -vserver <svmname>-policy-name <policy_name></i> <i>fpolicy policy scope delete -vserver <svmname>-policy-name <policy_name></i> <i>fpolicy policy delete -vserver <svmname>-policy-name <policy_name></i> <i>fpolicy policy event delete -vserver <svmname>-event-name <event_list></i> <i>fpolicy policy external-engine delete -vserver <svmname>-engine-name <engine_name></i></p>	<p>ワークロードセキュリティを有効にすると、ONTAPのパフォーマンスが低下します。レイテンシは一時的に上昇し、IOPSは散発的に低下します。</p>
<p>ワークロードセキュリティでONTAPを使用しているときに、ONTAPでレイテンシの問題が発生することがあります。これには、次のようないくつかの理由が考えられます。"1372994"、"1415152"、"1438207"、"1479704"、"1354659"。これらの問題はすべてONTAP 9.13.1以降で解決されています。これらのいずれかのバージョンを使用することを強く推奨します。</p>	<p>データコレクタでエラーが発生し、次のエラーメッセージが表示されます。</p> <p>「エラー：コネクタがエラー状態です。サービス名：audit。失敗の理由：SVM svm_backup でポリシーを設定できませんでした。理由：ZAPI フィールド：イベントに対して値が指定されていません。」</p>

問題	解決策：
<p>NFS サービスのみが設定された新しい SVM から開始します。</p> <p>ワークロードのセキュリティにONTAP SVMのデータコレクタを追加します。ワークロードセキュリティでONTAP SVMデータコレクタを追加する際、CIFSはSVMで許可されるプロトコルとして設定されません。</p> <p>ワークロードセキュリティのデータコレクタでエラーが表示されるまで待ちます。</p> <p>SVMでCIFSサーバが設定されていないため、左側にあるエラーはワークロードのセキュリティに表示されます。</p> <p>ONTAP SVM データコレクタを編集し、許可されたプロトコルとして CIFS のチェックを解除します。データコレクタを保存します。NFS プロトコルのみが有効な状態で実行が開始されます。</p>	<p>Data Collectorに次のエラーメッセージが表示されます。</p> <p>「Error : Failed to determine the health of the collector within 2 retries、try restarting the collector again (Error Code : AGENT008) 」</p>

それでも問題が解決しない場合は、[ヘルプ]>[サポート *] ページに記載されているサポートリンクにアクセスしてください。

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インスタンスの設定については、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. このページに記載されているバージョンに応じて、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. 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. **[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。
これにより、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、すべてのが提供されます **"エージェントの前提条件"** 達成された。

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 クラスター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、Cloud Insights を使用して管理されます。

Cloud 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あります。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

Cloud Insights の User Management ページに転送されます。

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、Cloud Insights を参照してください ["ユーザロール"](#) ドキュメント

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 `_sshpassto` 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 `sshpassto` 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	10 個のデータコレクタ	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

を参照してください

xref:{relative_path}concept_cs_agent_requirements.html["エージェントの要件"]
ページで、その他の前提条件と要件を確認してください。

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。

$(100+200+300) + [(100+200+300)*30\%] = 600+180 = 780\text{events/sec}$
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]#
```

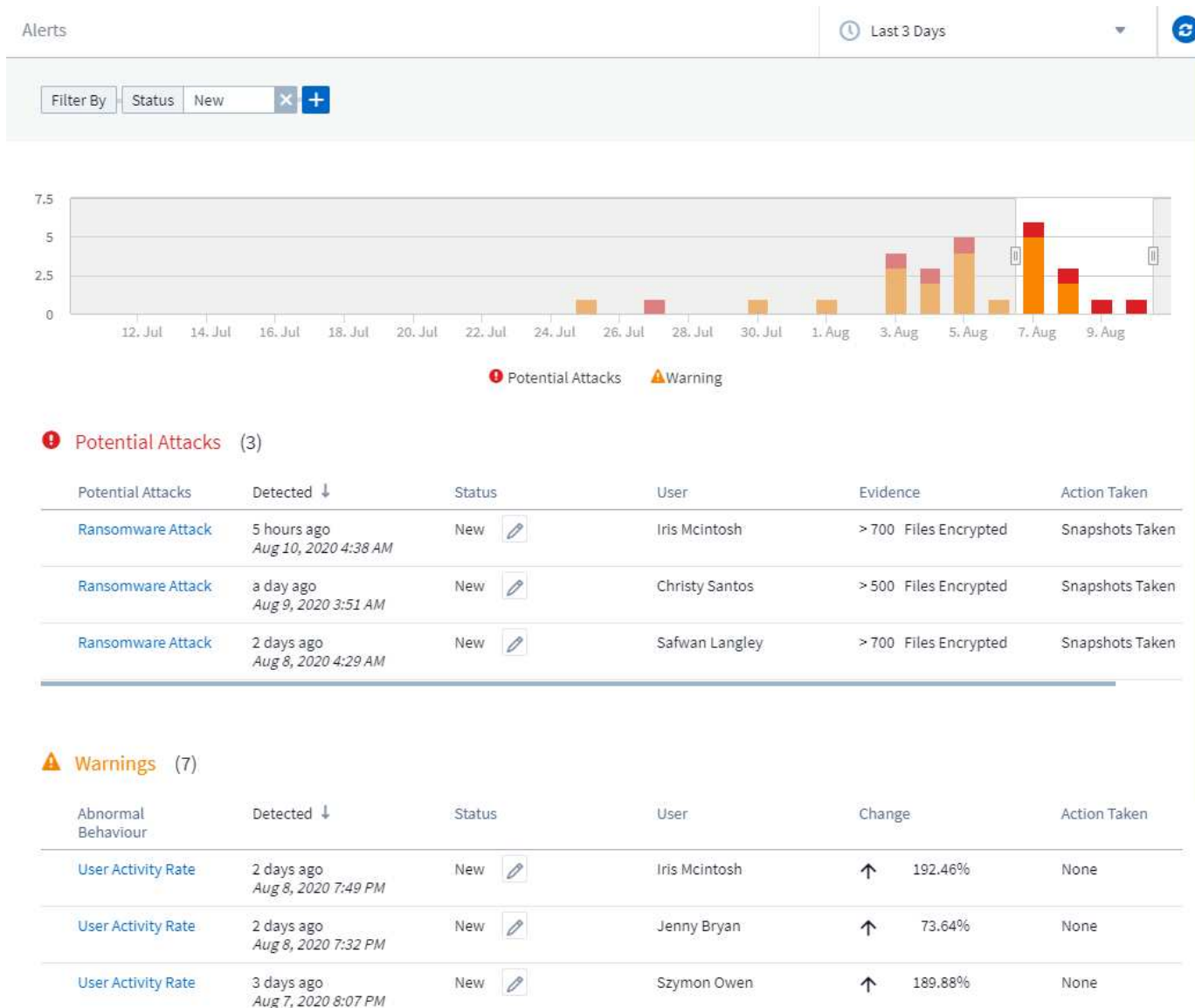
質問	回答
ワークロードセキュリティ用にすでに設定されているSVMに対してこのスクリプトを実行した場合、SVMの既存のfpolicy設定だけを使用するのか、それとも一時的なfpolicyを設定してプロセスを実行するのか。	ワークロードセキュリティがすでに設定されているSVMであっても、イベントレートチェッカーは問題なく実行できます。影響はありません。
スクリプトを実行できるSVMの数を増やすことはできますか。	はい。スクリプトを編集して、SVMの最大数を5から任意の数に変更するだけです。
SVMの数を増やすと、スクリプトの実行時間は長くなりますか。	いいえSVMの数を増やした場合でも、スクリプトは最大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。



ワークロードセキュリティは、Cloud Insights フェデラルエディションでは使用できません。



アラート

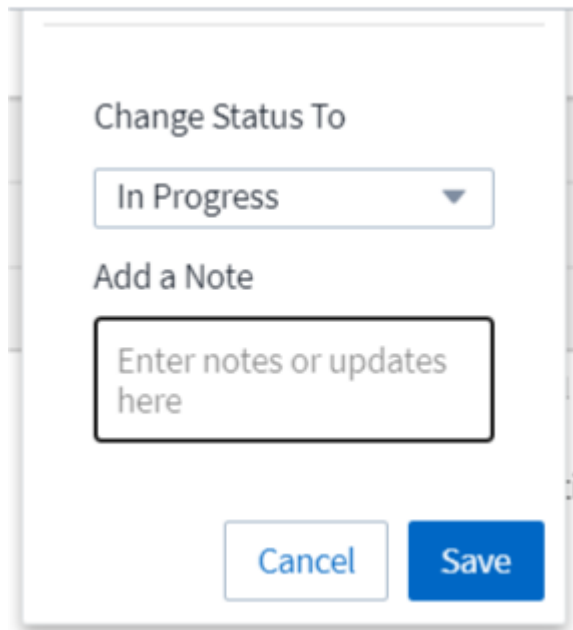
アラートリストには、選択した期間内に発生した攻撃および警告の総数、およびその期間内に発生した攻撃または警告のリストがグラフで表示されます。期間を変更するには、グラフの開始時間と終了時間のスライダを調整します。

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。

A dialog box titled "Change Status To" with a dropdown menu set to "In Progress". Below it is a section titled "Add a Note" with a text input field containing the placeholder "Enter notes or updates here". At the bottom are "Cancel" and "Save" buttons.

Change Status To

In Progress ▼

Add a Note

Enter notes or updates here

Cancel Save

- 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）

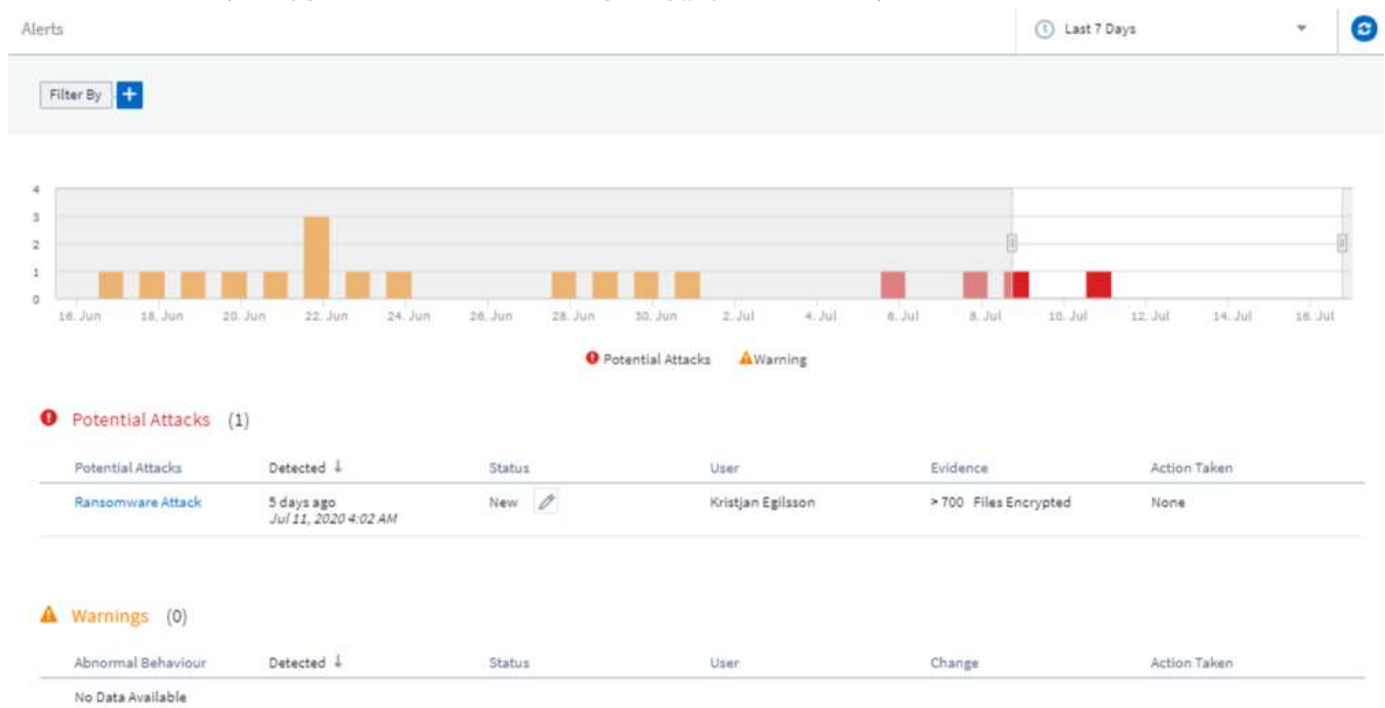
[攻撃結果] セクション：

- 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。

アラートページ（この例ではランサムウェア攻撃の可能性がありますが）：



詳細ページ（この例ではランサムウェア攻撃の可能性を示しています）：



POTENTIAL ATTACK: AL_305
Ransomware Attack

Detected
5 days ago
Jul 11, 2020 4:02 AM

Action Taken
None

Status
New

Total Attack Results

Affected Volumes	Deleted Files	Encrypted Files
1	0	4173

4173 Files have been copied, deleted, and potentially encrypted by 1 user account.

This is potentially a sign of ransomware attack.
The extension "crypt" was added to each file.

Encrypted Files

Activity per minute



Related Users



Kristjan Egilsson
Accountant
Finance

4173
Encrypted Files

Detected
5 days ago
Jul 11, 2020 4:02 AM

Action Taken
None



Username
us035

Email
Egilsson@netapp.com

Phone
387224312607

Department
Finance

Manager
Lyndsey Maddox

Top Activity Types

Activity per minute
Last access location: 10.197.144.115

[View Activity Detail](#)



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。

を定義できます "自動応答ポリシー" ランサムウェア攻撃やその他の異常なユーザアクティビティが検出されるとスナップショットが作成されます。

アラートページから手動で Snapshot を作成することもできます。

自動 Snapshot の作成：

Potential Attack Detail / Ransomware Attack

POTENTIAL ATTACK: AL_307
Ransomware Attack

Detected
4 days ago
Jul 26, 2020 3:38 AM

Action Taken
Snapshots Taken

Status
In Progress

Last snapshots taken by
Amit Schwartz
Jul 30, 2020 2:54 PM

How To:
[Restore Entities](#)

[Re-Take Snapshots](#)

Total Attack Results

1
Affected Volumes

0
Deleted Files

5148
Encrypted Files

5148 Files have been copied, deleted, and potentially encrypted by 1 user account.

This is potentially a sign of ransomware attack.
The extension "crypt" was added to each file.

Encrypted Files
Activity per minute

Related Users

Ewen Hall
Developer
Engineering

5148
Encrypted Files

Detected
4 days ago
Jul 26, 2020 3:38 AM

Action Taken
Snapshots Taken

手動スナップショット：

Cloud Insights

Abhi Basu Thakur

MONITOR & OPTIMIZE

Alerts / **Nabilah Howell** had an abnormal change in activity rate

Jul 23, 2020 - Jul 26, 2020
1:44 AM 1:44 AM

CLOUD SECURE

ALERTS

FORENSICS

ADMIN

HELP

Alert Detail

WARNING: AL_306
Nabilah Howell had an abnormal change in activity rate.

Detected
5 days ago
Jul 25, 2020 1:44 PM

Action Taken
None

Status
New

Recommendation: Setup an Automated Response Policy
An Automated Response Policy will trigger measures to contain the damage automatically when a future attack is detected. Try it now.

[Take Snapshots](#)

How To:
[Restore Entities](#)

Nabilah Howell's Activity Rate Change

Typical
122.8
Activities Per Minute

Alert
210
Activities Per Minute

↑ 71%

Nabilah Howell's activity rate grew 71% over their typical average.

Activity Rate
Activity per 5 minutes

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 のマニュアルを参照してください "Snapshot 削除ポリシーを設定しています" 。
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。 スナップショットを作成するための適切なアクセス権を持つ <code>_csrole_</code> が作成されていることを確認します。 <code>security login role create -vserver <servername> -role csrole -cmddirname "volume snapshot" -access all</code>
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。
<code>_Alert Details_page</code> では、 <code>_Take Snapshot_Button</code> 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 <code>_disabled_state</code> 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 <code>trigger _Take Snapshot</code> 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。
このページでは、環境内のアクティビティの概要を説明します。次の情報が強調表示されます。

- グラフには、_ アクティビティ履歴 _ (選択したグローバル時間範囲に基づいて、1 分あたり 5 分あたり / 10 分あたりにアクセス) が表示されます。

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。

- アクティビティタイプ _ のチャート。アクティビティタイプ別にアクティビティ履歴データを取得するには、対応する X 軸ラベルリンクをクリックします。
- エンティティタイプ _ 上のアクティビティのグラフ。エンティティタイプ別にアクティビティ履歴データを取得するには、対応する X 軸ラベルリンクをクリックします。
- すべての Activity_data のリスト

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。表示する列を選択するには、「歯車」アイコンをクリックします 。

- 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）。
- へのリンクでエンティティにアクセスした * user * "[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。グループの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。

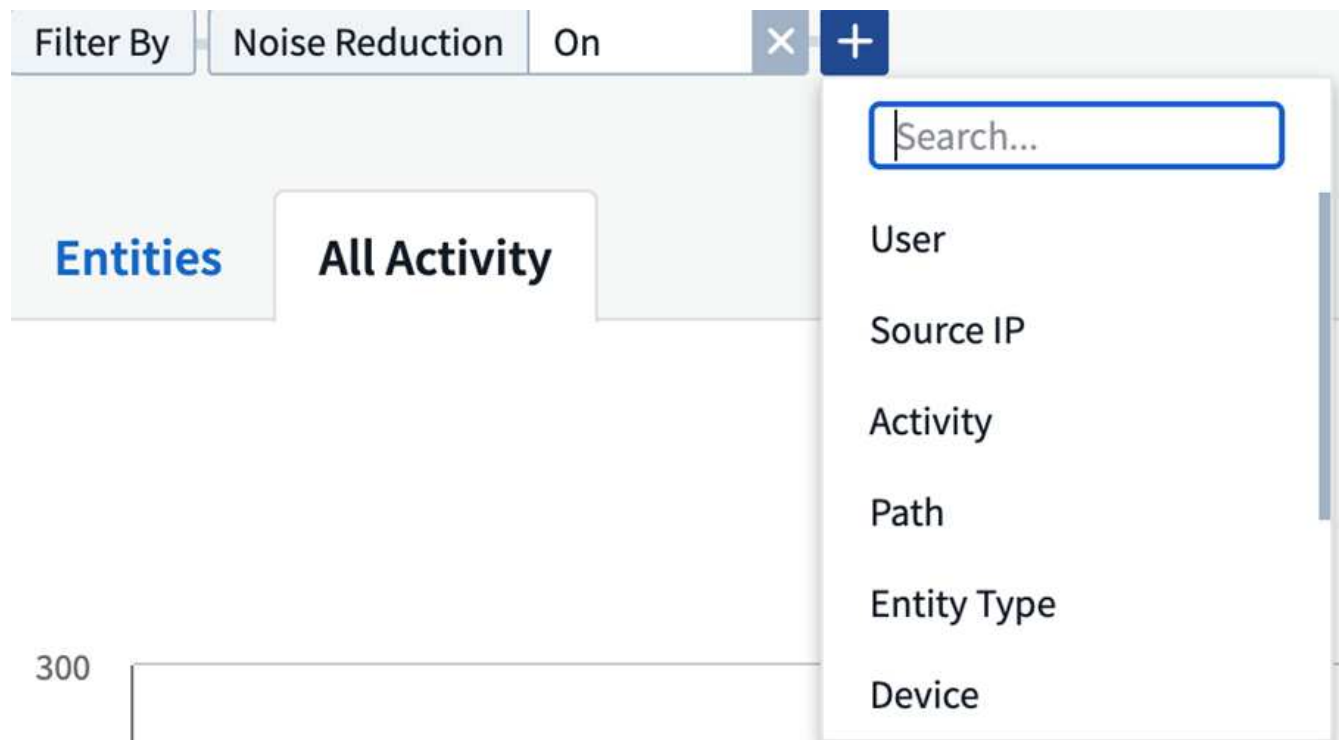
- へのリンクを持つエンティティへの * パス * "[エンティティ詳細データ](#)"
- エンティティタイプ * (エンティティ (ファイル) 拡張子 (.doc、.docx、.tmp など))
- エンティティが存在する * デバイス *
- イベントの取得に使用される * プロトコル *。
- 元のファイルの名前を変更したときに名前変更イベントに使用された * 元のパス *。デフォルトでは、この列はテーブルに表示されません。列セクタを使用して、この列をテーブルに追加します。
- エンティティが存在するボリューム *。デフォルトでは、この列はテーブルに表示されません。列セクタを使用して、この列をテーブルに追加します。

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。

1. テーブルのフィールドにカーソルを合わせ、表示されるフィルタアイコンをクリックします。この値は、top_Filter by_list の適切なフィルタに追加されます。
2. 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ー名を正確に指定する必要があります。部分的なユーザー名で検索したり、プレフィックスやサフィックスの付いたユーザー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、ユーザー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。

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）拡張子を使用します
- * エンティティのパス *
- * ユーザー * アクティビティを実行しています
- * 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。

フォレンジックアクティビティ履歴データのソート

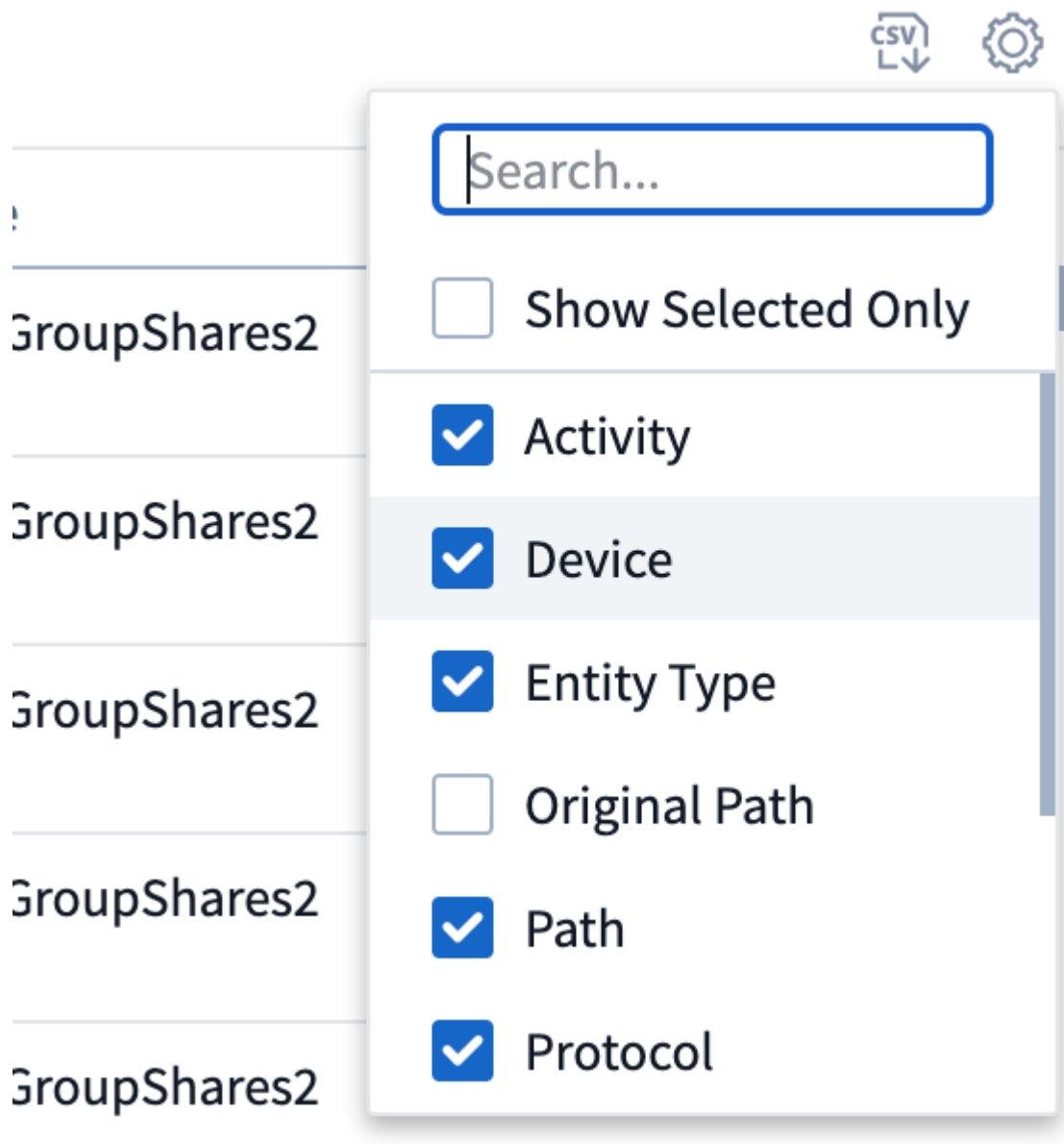
アクティビティ履歴データは、_Time、User、Source IP、Activity、Path_and_Entity Type_でソートできます。デフォルトでは、テーブルは descending _Time_order でソートされます。つまり、最新のデータが最初に表示されます。_Device_Field と _Protocol_fields_ に対してソートが無効になっています。

すべてのアクティビティのエクスポート

アクティビティ履歴テーブルの上にある _エクスポート_ ボタンをクリックすると 'アクティビティ履歴を.csv ファイルにエクスポートできます上位100、000件のレコードのみがエクスポートされることに注意してください。データの量によっては、エクスポートが完了するまでに数秒から数分かかる場合があります。

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	どのフィルタに適用できますか？	どのフィルタにも適用できません	結果
* (アスタリスク)	すべての項目を検索できます	Auto * 03172022	ユーザー、パス、エンティティタイプ、デバイスタイプ、ボリューム、元のパス		"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		AutoSabotageUser1_03172022A、AutoSabotageUser1_03172022AB、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、ユーザ名、パス、エンティティタイプ、デバイス、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	AutoRansomUser4_03162022ではありません	ユーザ、ドメイン、ユーザ名、パス、エンティティタイプ、元のパス、ボリューム	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

検索結果に/が含まれている場合と含まれていない場合は異なります

/AutoDir1/AutoFile	動作します
AutoDir1/AutoFileです	壊れています
/AutoDir1/AutoFile（Dir1）	dir1部分部分文字列が機能しない
"/AutoDir1/AutoFile032420222022"	完全検索が実行されます
Auto * 03242022	壊れています
AutoSabotageUser1_03172022	壊れています
/AutoDir1/AutoFile03242022または/AutoDir1/AutoFile03242022	動作します
/AutoDir1/AutoFile03242022ではありません	動作します
NOT / AutoDir1	動作します
/AutoFile03242022はありません	壊れています
*	すべてのエントリを表示します

問題	試してみてください
<p>[All Activities]テーブルの[User]列には、ユーザ名が次のように表示されます。</p> <p>LDAP：HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817”</p> <p>または</p> <p>「LDAP：デフォルト：80038003」</p>	<p>考えられる原因は次のとおりです。</p> <ol style="list-style-type: none"> 1. ユーザディレクトリコネ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]>[コネクタ]>[ユーザディレクトリコネクタ]*に移動し、[+ユーザディレクトリコネクタ]*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. ユーザディレクトリコネクタは設定されていますが、停止しているか、エラー状態です。[コネクタ]>[ユーザディレクトリコネクタ]*に移動し、ステータスを確認してください。を参照してください "User Directory Collector のトラブルシューティング" <p>トラブルシューティングのヒントについては、ドキュメントのセクションを参照してください。</p> <p>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。</p> <p>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ーにユーザが実際に含まれていることを確認します。</p>
<p>一部の NFS イベントが UI に表示されません。</p>	<p>次の点を確認します。</p> <ol style="list-style-type: none"> 1. POSIX属性が設定されたADサーバーのユーザディレクトリコネクタが、UIからunixid属性を有効にして実行され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からユーザページで検索したときに表示されます 3. 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ではサポートされていません 4. 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。

<p>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。</p>	<p>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、 *<i><searchTerm></i> or *<i><searchTerm></i>*_ 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。</p> <p>パフォーマンスを向上させるには、代わりに<i><searchTerm></i>*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()<i>_after_a</i>を追加します）。</p> <p>例： testvolume_or_ * test * volume__ではなく、文字列_testvolume *を使用します。</p> <p>プレフィックススペースの検索を使用して、特定の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）。例</p> <p>： /path1/path2/path3_or_"/path1/path2/path3"は、すべてのアクティビティを/path1/path2/path3_の下に再帰的にリストします。</p> <p>または、[すべてのアクティビティ（All Activity）]タブの[フィルタに追加（Add to Filter）]オプションを使用します。</p>
<p>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。</p>	<p>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。</p>

フォレンジックエンティティページ

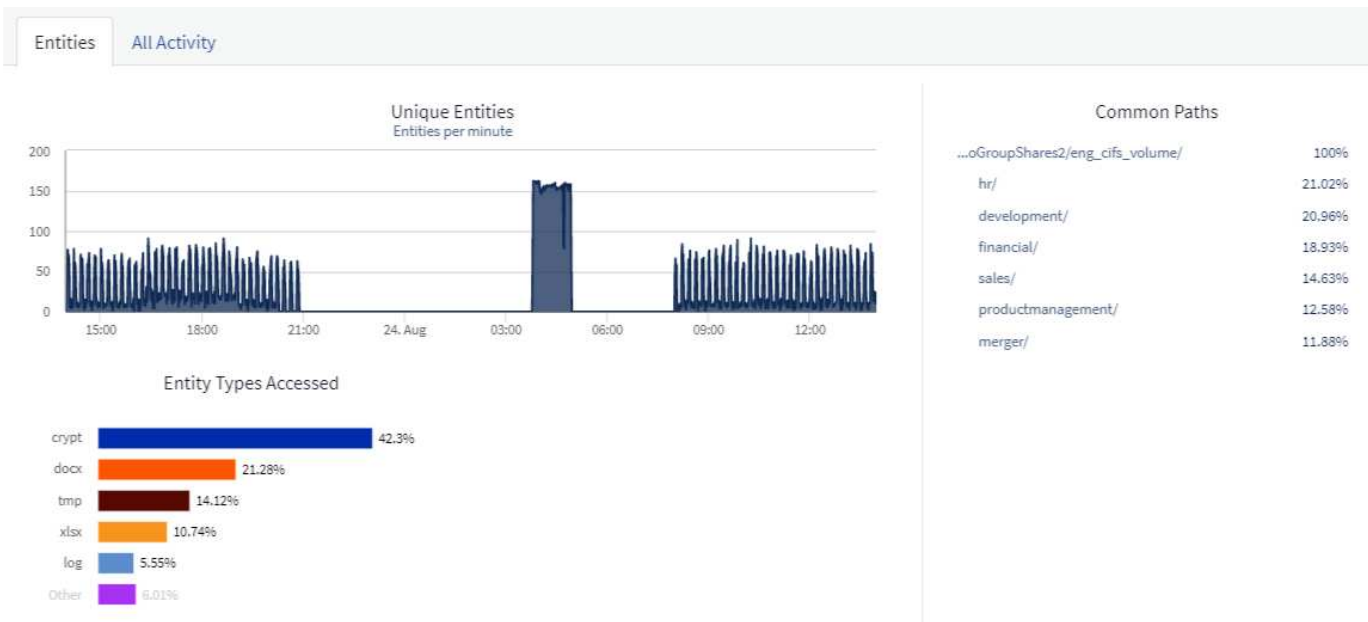
フォレンジックエンティティページには、環境内のエンティティアクティビティに関する詳細情報が表示されます。

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、環境内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。

- * 1分あたりの_unique Entities_accessedを示すグラフ
- * アクセスされたエンティティタイプ_のグラフ
- * _Common Paths_の内訳
- * エンティティの総数のうち_Top 50 Entities_outのリスト



Preview Top 50 Entities of 12386

Name	Entity Type	Device	Path	Activities ↓
Tech Tower.pptx	pptx	demoGroupShares2	/ENG_CIFS_volume/Sales/Tech Tower.pptx	39
Kevin_Obrien.xlsx	xlsx	demoGroupShares2	/ENG_CIFS_volume/Sales/Kevin_Obrien.xlsx	37
Harrison_Ware.docx	docx	demoGroupShares2	/ENG_CIFS_volume/Sales/Harrison_Ware.docx	35
Matter Shop Lifters.pptx	pptx	demoGroupShares2	/ENG_CIFS_volume/Sales/Matter Shop Lifters.pptx	35

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。

Forensics / Entities / Kevin_Obrien.xlsx



Entity Overview

Entity Profile

Name Kevin_Obrien.xlsx	Most Accessed Location 10.197.144.115	Size 91 KB
Type xlsx	Device Name demoGroupShares2	Path /ENG_CIFS_volume/Sales/Kevin_Obrien.xlsx

Entity Behaviour

Recent Activity	Operations (last 7 days)
Last accessed : 12 minutes ago Aug 24, 2020 2:02 PM	Read :89
Last accessed by : Tyrique Ray	Read Metadata :22
Last accessed from : 10.197.144.115	Other Activities :43

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、ユーザーの特性、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。

ユーザプロフィール

ユーザプロフィール情報には、ユーザーの連絡先情報と場所が含まれます。プロフィールには次の情報が表示されます。

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

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、ユーザーリストは 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ー動作が発生した場合のユーザーアクセスの制限などのアクションをトリガーします。



ワークロードセキュリティは、Cloud Insights フェデラルエディションでは使用できません。

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。

Add Attack Policy

Policy Name*

Unique New Policy Name

For Attack Type(s) *

☐ Ransomware Attack

☐ Data Destruction - File Deletion

On Device

All Devices

+ Another Device

Actions

☒ Take Snapshot ?

☐ Block User File Access ?

Time Period

12 hours

Cancel Save

ポリシーは一意的な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、確認できます ["アラートの詳細ページ"](#)。

を参照してください ["ユーザアクセスの制限"](#) 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。

Snapshot Purge Settings

×

Define purge periods to automatically delete snapshots taken by Cloud Secure.

Attack Automated Response

Delete Snapshot after 30 Days ▼

Warning Automated Response

Delete Snapshot after 7 Days ▼

User Created

Delete Snapshot after 30 Days ▼

Cancel


Save

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。

Allowed File Types Policies

Ransomware alerts will not be triggered for the following file types: 

.abc ✕

.123 ✕

*.safe ✕

|

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に関する詳細およびライセンス要件については、[を参照してください "こちらをご覧ください"](#)。

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. 最小ONTAP バージョン：9.11.1
2. ARPが有効なボリューム。ARPをイネーブルにする方法の詳細は、を参照してください ["こちらをご覧ください"](#)。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ん
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 権限"](#)。

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。



POTENTIAL ATTACK: AL_1315
Ransomware Attack

Detected
5 months ago
Oct 20, 2022 3:06 AM

Action Taken
Access Blocked on 5 SVMs
Snapshots Taken

Status
New

Blocked permanently by
auto response policy

Last snapshots taken by
auto response policy
Oct 20, 2022 3:09 AM

How To:
Restore Entities

Change Block Period

Re-Take Snapshots

Unblock User

Total Attack Results

1 Affected Volumes | 83 Deleted Files | 81 Encrypted Files

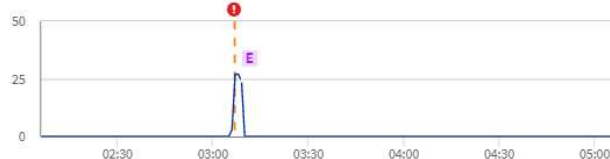
81 Files have been copied, deleted, and potentially encrypted by 1 user account.

The extension "osiris" was added to each file.

High Confidence Detection
Ransomware behavior and in-file encryption activities were detected.

Encrypted Files

Activity per minute



E Encryption activity in files

Related Users



Jamelia Graham
Business Partner
HR

User/IP Access

Blocked

81 Encrypted Files

Detected
5 months ago
Oct 20, 2022 3:06 AM

Username
us024
Domain
cslab.netapp.com
Email
Graham@netapp.com
Phone
9251140014

Department
HR
Manager
Iwan Holt
Location
WA

Top Activity Types

Activity per minute
Last accessed from: 10.193.113.247

View Activity Detail



Access Limitation History for This User (3)

Time	Action	Duration	Action Taken by	Response	Blocked IPs on NFS
Oct 20, 2022 3:09 AM	Block more detail	Never Expires		Automatic	none
Mar 10, 2022 4:59 AM	Unblock		system	Blocking Expired	10.197.144.115
Mar 10, 2022 3:57 AM	Block more detail	1h		Automatic	10.197.144.115

Affected Devices/Volumes

Device ↑	Volume	Encrypted Files	Associated Snapshot Taken
subprod_rtp	stargazer	81	Oct 20, 2022 3:09 AM cloudsecure_attack_auto Automatic _1666249787062 Take Snapshot

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

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にはアラートが24時間前に表示され、その日にCloud Insights ワークロードセキュリティからEメールが受信されます。	ONTAP がCloud Insights ワークロードセキュリティ（ワークロードセキュリティ）に_ランサムウェア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、特定の数のファイルがエンコードされたときに、_ランサムウェアDetected _ EventをCloud 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。

Cloud Insights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。

NetApp Cloud Insights

Tutorial 0% Complete

Getting Started

CI dev 1 / Workload Security / Collectors / Add Data Collector

Enter complete Share Names to be excluded, separated by a comma.

Share Names

Volume Names

Enter complete Volume Names to be excluded, separated by a comma.

Volume names

Advanced Configuration

☐ Monitor Directory Read & Open Activity (SMB only)
Note: Generates many directory access events (noise)

☒ Monitor Access Denied Events
Note: This feature will be available from ONTAP 9.13 and above

Fpolicy Server Send Buffer Size

1MB

Cancel Save

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。

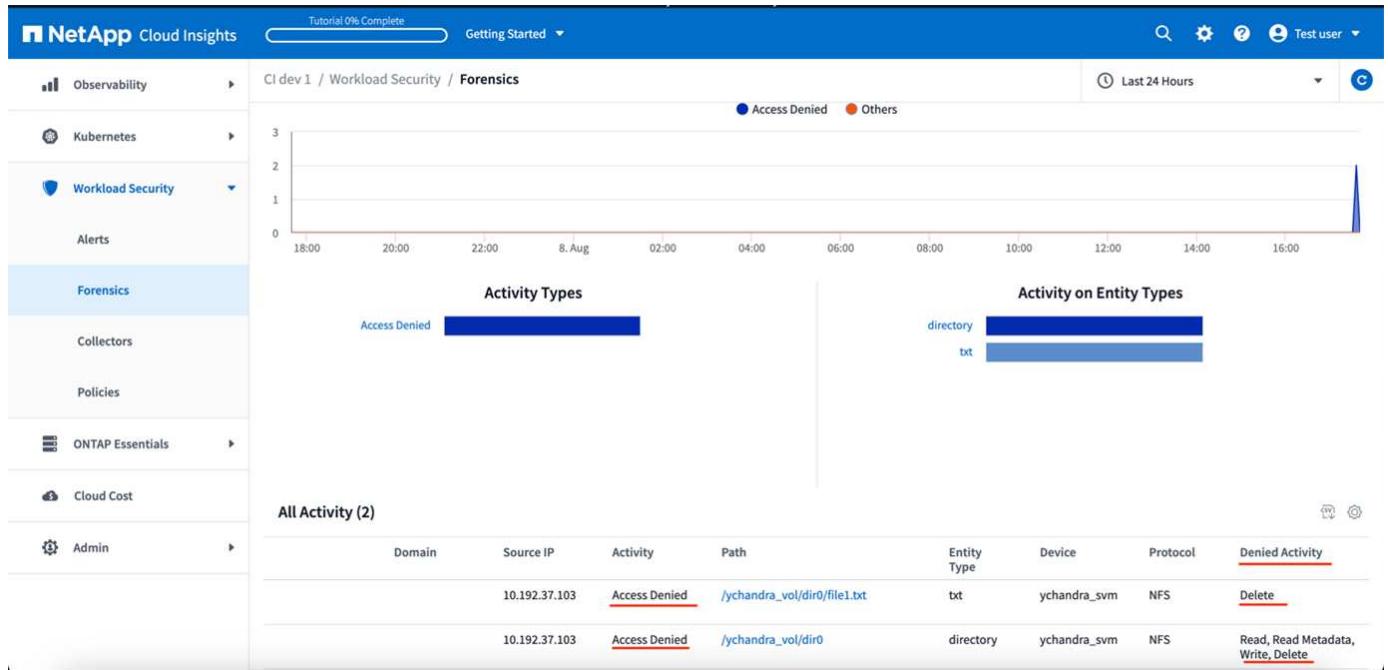
```
security login rest-role create -role csrestrole -api  
/api/protocols/fpolicy -access all -vserver <svm_name>  
security login create -user-or-group-name csuser -application http  
-authmethod password -role csrestrole -vserver <svm_name>
```

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 権限"](#)。

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。



ワークロードセキュリティは、Cloud Insights フェデラルエディションでは使用できません。

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
```

の[Permissions]セクションを確認してください。 ["ONTAP SVM Data Collector の設定"](#) ページも参照してください。

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。

- 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>
```

Vserver	Policy Name	Rule Index	Access Protocol	Client Match	RO Rule
svm0	default	1	nfs3, nfs4, cifs	cloudsecure_rule, 10.11.12.13	never
svm1	default	4	cifs, nfs	0.0.0.0/0	any
svm2	test	1	nfs3, nfs4, cifs	cloudsecure_rule, 10.11.12.13	never
svm3	test	3	cifs, nfs, flexcache	0.0.0.0/0	any

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 クラスター（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:    <vservename>
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。	<p>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。</p> <p>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、ストレージにアクセスできなくなります。</p>

問題	試してみてください
[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。
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」	<p>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。</p> <p>https://docs.netapp.com/us-en/cloudinsights/cs_restrict_user_access.html#prerequisites-for-user-access-blocking</p> <p>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。</p> <pre>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</pre> <p>_csuser_を使用せず、クラスタレベルのadminユーザを使用している場合は、adminユーザにONTAPに対するssh権限があることを確認してください。</p>

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。



ワークロードセキュリティは、Cloud Insights フェデラルエディションでは使用できません。

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）。

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:/svmvoll /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
...
```

ファイルをリストアします

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。



推奨されるオプションは次のとおりです。"コレクターの一時停止" ファイルを作成する前に。]

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、["コレクタの再開"](#)。

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。



ワークロードセキュリティは、Cloud Insights フェデラルエディションでは使用できません。

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Eメール通知は、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 Cloud Insightsドメイン (accounts@service.cloudinsights.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 Cloud Insightsドメインからの外部通知がホワイтли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。



ワークロードセキュリティは、Cloud Insights フェデラルエディションでは使用できません。

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 の簡単な概要情報と使用方法を提供しており、環境内で試すことができます。

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。

トークンを使用すると、お客様の観点から API への汎用アクセスが許可され、環境の範囲内で API へのアクセスが管理されます。

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。

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。