はじめに
Data Infrastructure Insights

NetApp
December 19, 2024

目次

はじめに . . . 1
- ワークロードセキュリティの導入 . . . 1
- ワークロードセキュリティエージェントの要件 . . . 1
- 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 . . . 5
- ワークロードセキュリティエージェントの削除 . . . 11
- Active Directory （ AD ）ユーザディレクトリコレクタの設定 . . . 12
- LDAP Directory Server Collector の設定 . . . 17
- ONTAP SVM Data Collector の設定 . . . 22
- NetApp ONTAP コレクタ用のCloud Volumes ONTAP とAmazon FSXの設定 . . . 30
- ユーザ管理 . . . 32
- 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） . . . 33

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。

コンポーネント	**Linux** 要件
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"
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

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	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
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"。

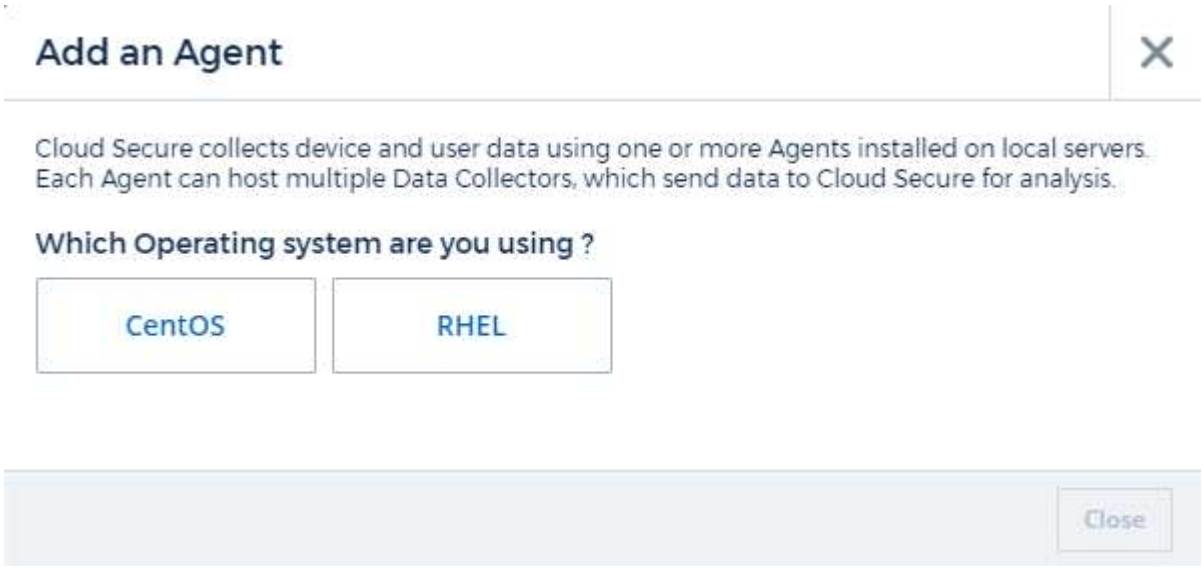
開始する前に

- 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。

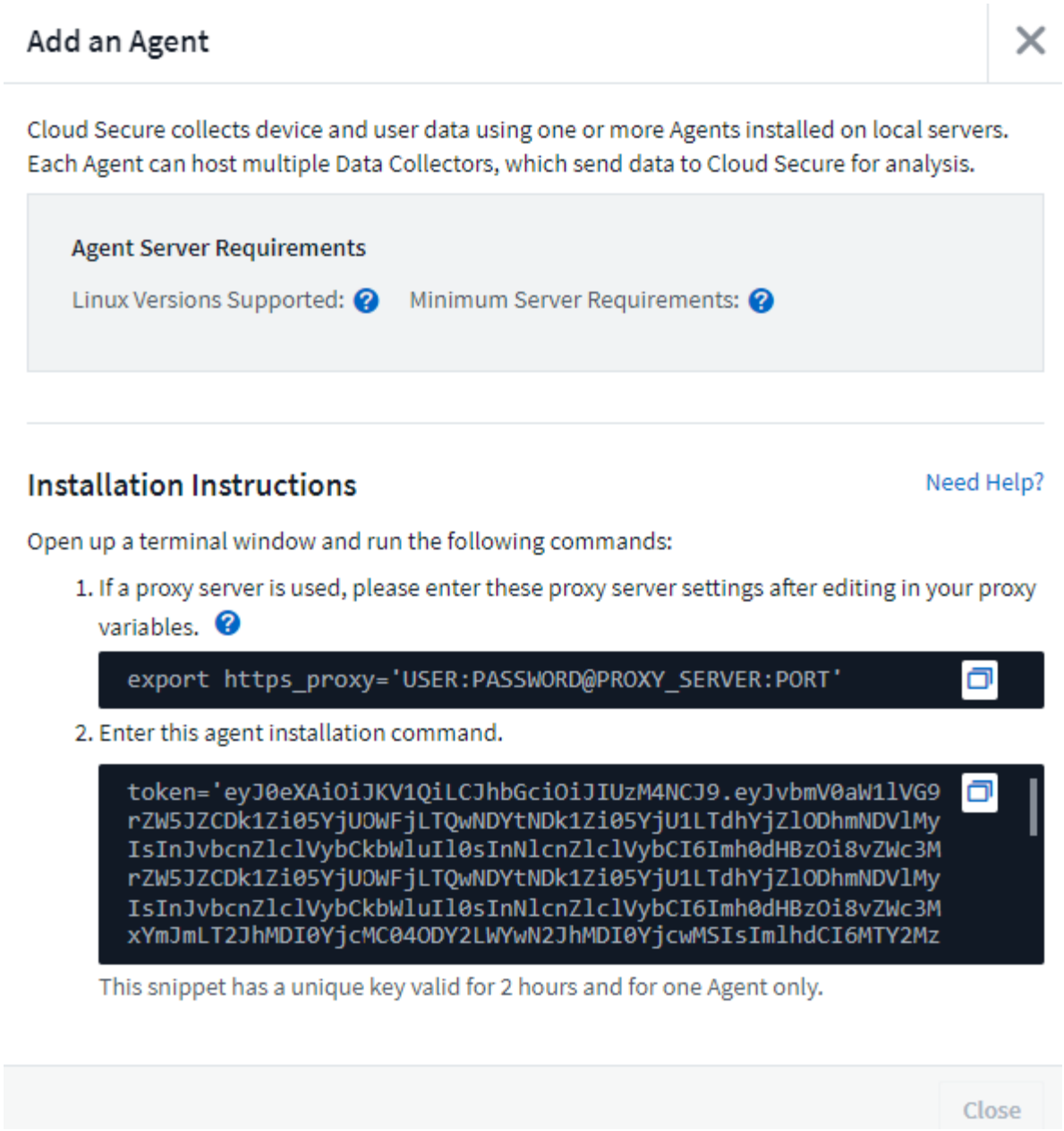
エージェントをインストールする手順

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
```

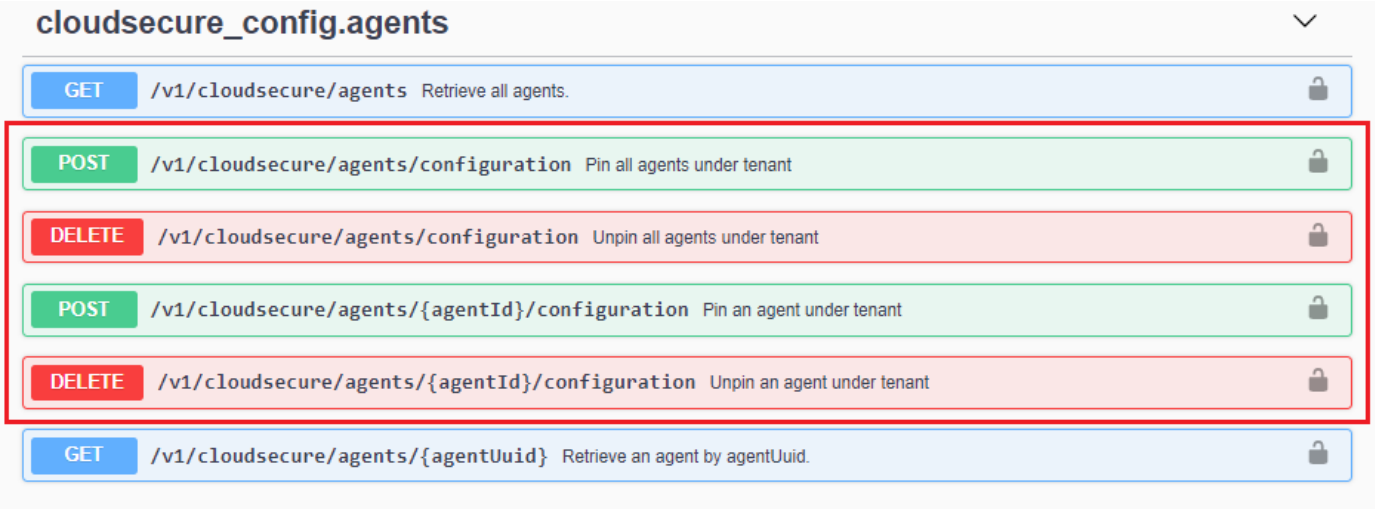
現在のバージョンでエージェントを「固定」する

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。

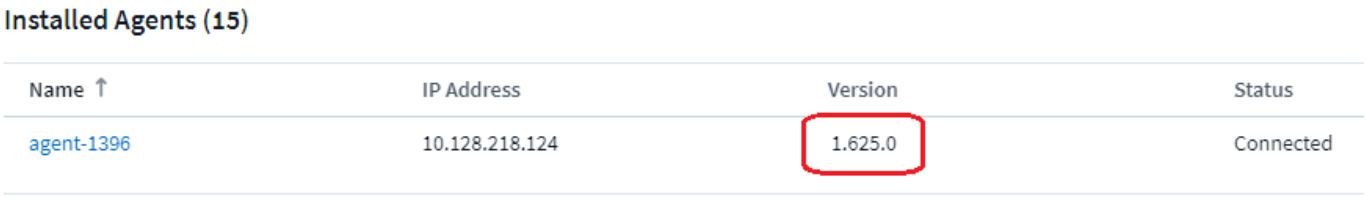
これらのいずれの場合も、エージェントは次回のワークロードセキュリティ更新時に更新されます。

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

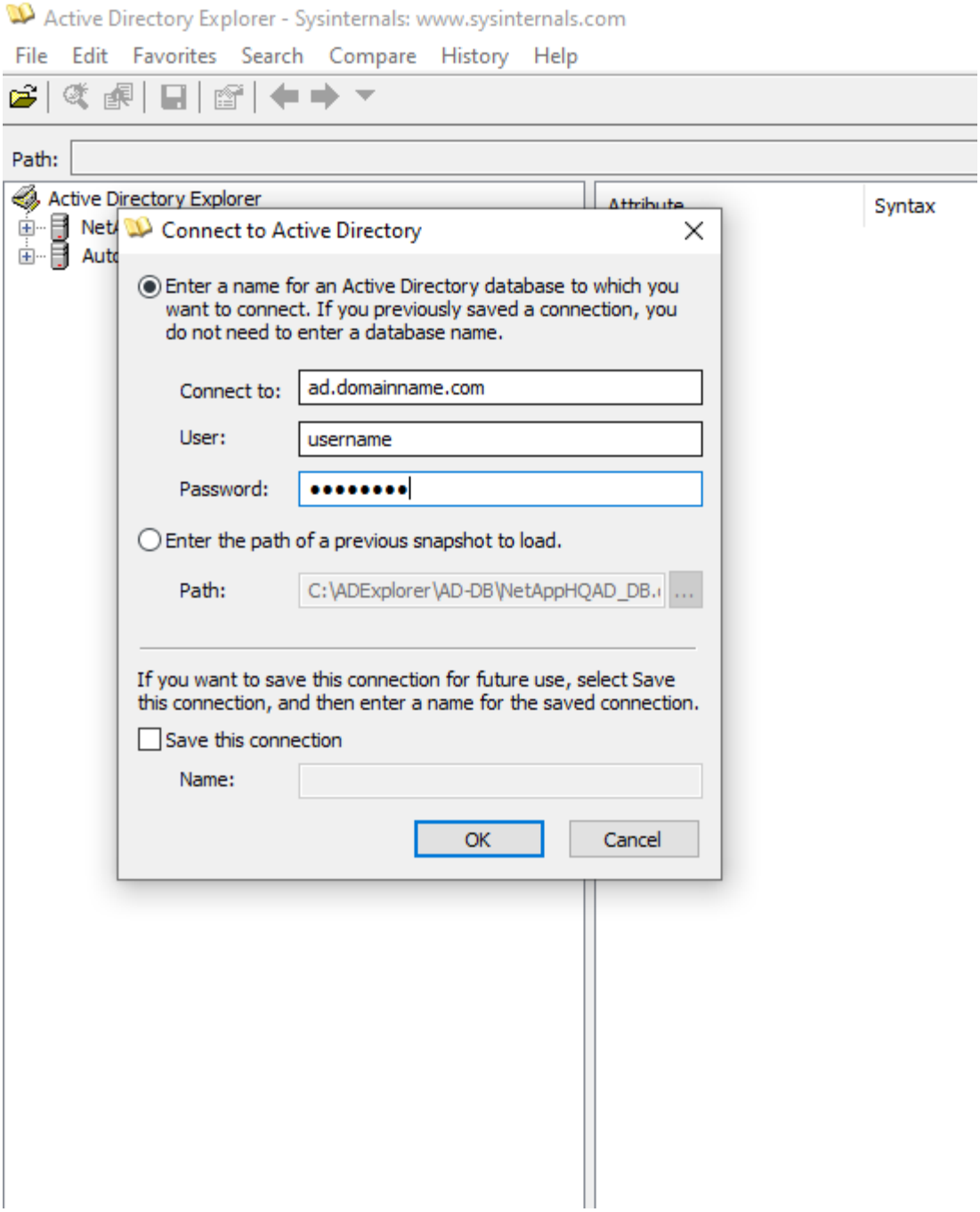
ユーザディレクトリコレクタ設定のテスト

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

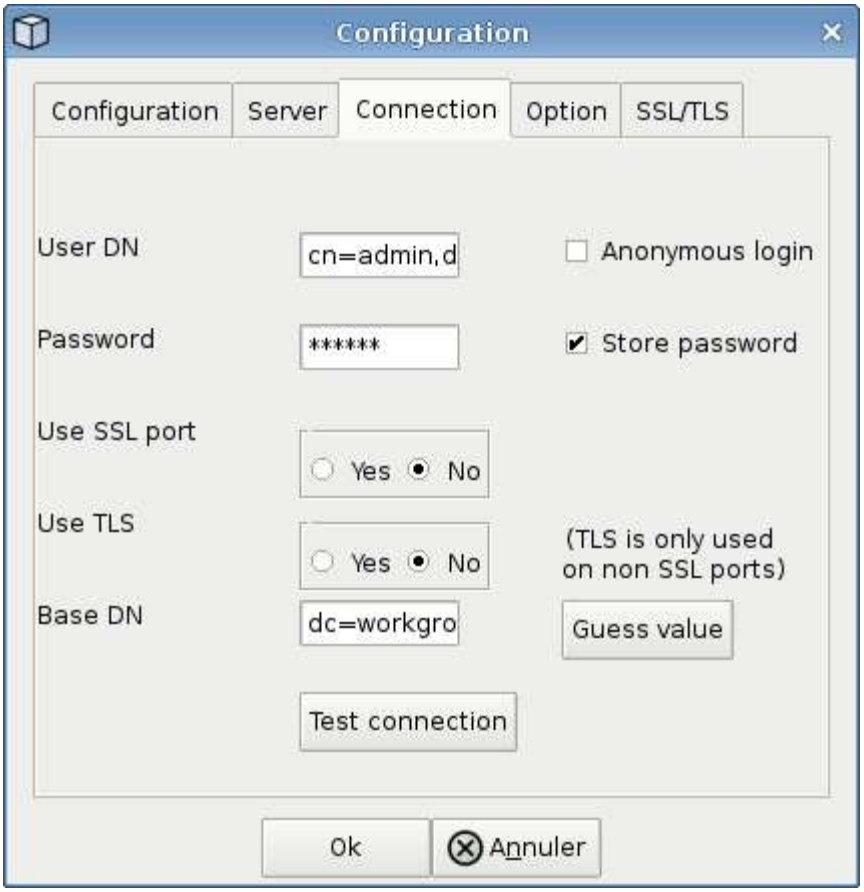
ユーザディレクトリコレクタ設定のテスト

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。

著作権に関する情報

商標に関する情報