はじめに
Data Infrastructure Insights

NetApp
February 11, 2026

目次

はじめに

ワークロードセキュリティ入門

Workload Security は、ユーザー アクティビティを監視し、ストレージ環境における潜在的なセキュリティ脅威を検出するのに役立ちます。監視を開始する前に、エージェント、データ コレクター、およびディレクトリ サービスを構成して、包括的なセキュリティ監視の基盤を確立する必要があります。

Workload Security システムはエージェントを使用して、ストレージ システムからのアクセス データとディレクトリ サービス サーバーからのユーザー情報を収集します。

データの収集を開始する前に、以下を構成する必要があります。

Task	関連情報
エージェントを構成する	"エージェントの要件" "エージェントを追加"
ユーザーディレクトリコネクタを構成する	"ユーザーディレクトリコネクタの追加"
データコレクターを構成する	ワークロード セキュリティ > コレクター をクリックし、設定するデータ コレクターをクリックします。コレクター情報については、ドキュメントのデータ コレクター ベンダー リファレンス セクションを参照してください。
ユーザーアカウントを作成する	"ユーザーアカウントの管理"

Workload Security は他のツールとも統合できます。例えば、"このガイドをご覧ください" Splunk との統合について。

ワークロード セキュリティ エージェントの要件

ワークロード・セキュリティ・エージェントは、OS、CPU、メモリ、ディスク容量の最小要件を満たす専用サーバーに導入することで、最適な監視および脅威検出パフォーマンスを確保できます。このガイドでは、"Workload Security エージェントのインストール"前に必要なハードウェアおよびネットワーク要件を規定しています。これには、サポート対象のLinuxディストリビューション、ネットワーク接続ルール、システムサイジングのガイダンスが含まれます。

コンポーネント	**Linux** 要件
オペレーティング システム	次のいずれかのライセンス版を実行しているコンピュータ: * AlmaLinux 9.4 (64 ビット) ～ 9.5 (64 ビット)、10 (64 ビット) (SELinux を含む) * CentOS Stream 9 (64 ビット) * Debian 11 (64 ビット)、12 (64 ビット) (SELinux を含む) * OpenSUSE Leap 15.3 (64 ビット) ～ 15.6 (64 ビット) * Oracle Linux 8.10 (64 ビット) 、9.1 (64 ビット) ～ 9.6 (64 ビット) (SELinux を含む) * Red Hat Enterprise Linux 8.10 (64 ビット)、9.1 (64 ビット) ～ 9.6 (64 ビット)、10 (64 ビット) (SELinux を含む) * Rocky 9.4 (64 ビット) ～ 9.6 (64 ビット) (SELinux を含む) * SUSE Linux Enterprise Server 15 SP4 (64 ビット) ～ 15 SP6 (64 ビット)、SELinux を含む * Ubuntu 20.04 LTS (64 ビット)、22.04 LTS (64 ビット)、24.04 LTS (64 ビット) このコンピューターでは、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。専用サーバーをお勧めします。
コマンド	インストールには「unzip」が必要です。さらに、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 su –」コマンドが必要です。
CPU	4つのCPUコア
メモリ	16GBのRAM
使用可能なディスク容量	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 (ファイルシステムの作成後に最低 35 GB の空き領域) 注: ファイルシステムの作成を可能にするために、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少なくとも 35 GB の空き領域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ーである場合は、ローカル ユーザーがこのフォルダーにアクセスできることを確認してください。ローカルユーザーにこのフォルダへの権限がない場合、エージェントまたはデータコレクタのインストールに失敗する可能性があります。"トラブルシューティング"詳細についてはセクションをご覧ください。
ネットワーク	100 Mbps ～ 1 Gbps のイーサネット接続、静的 IP アドレス、すべてのデバイスへの IP 接続、および Workload Security インスタンスへの必要なポート (80 または 443)。

注意: Workload Security エージェントは、Data Infrastructure Insights取得ユニット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がベストプラクティスです。これらを同じマシンにインストールする場合は、以下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容量	50～55 GB Linuxの場合、ディスク容量は次のように割り当てる必要があります: /opt/netapp 25～30 GB /var/log/netapp 25 GB

追加の推奨事項

- **Network Time Protocol (NTP)** または **Simple Network Time Protocol (SNTP)** を使用して、 ONTAPシステムとエージェント マシンの両方の時刻を同期することを強くお勧めします。

クラウドネットワークアクセスルール

*米国ベースの*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	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	Data Infrastructure Insights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	agentlogin.cs01.cloudinsights.netapp.com	認証サービスへのアクセス

*ヨーロッパベースの*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	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	Data Infrastructure Insights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	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	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	Data Infrastructure Insights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	説明
TCP	443	ワークロードセキュリティエージェント	エージェントログイン.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	説明
TCP	389(LDAP) 636 (LDAP / start-tls)	ワークロードセキュリティエージェント	LDAP Server URL	LDAPに接続する
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 管理 IP アドレス (SVM コレクターの構成によって異なります)	ONTAPとのAPI通信
TCP	35000 - 55000	SVM データ LIF IP アドレス	ワークロードセキュリティエージェント	Fpolicy イベントのためのONTAPからWorkload Security Agent への通信。ONTAP がWorkload Security Agent にイベントを送信するには、Workload Security Agent 自体のファイアウォール（存在する場合）も含めてこれらのポートを Workload Security Agent に対して開く必要があります。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。まずは約 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。

プロトコル	ポート	ソース	デスティネーション	説明
TCP	35000-55000	クラスタ管理IP	ワークロードセキュリティエージェント	**EMS** イベント 用のONTAPクラスタ管理 IP 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Workload Security Agent に **EMS** イベント を送信するには、これらのポートを Workload Security Agent に対して開く必要があります。これには、Workload Security Agent 自体のファイアウォール (存在する場合) も含まれます。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。まずは約 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。
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 ユーザーのブロックに必要です。

システムのサイズ設定

参照"イベントレートチェッカー"サイズに関する情報についてはドキュメントを参照してください。

ワークロードセキュリティエージェントの導入

Workload Security エージェントは、ユーザー アクティビティを監視し、ストレージ インフラストラクチャ全体で潜在的なセキュリティ脅威を検出するために不可欠です。このガイドでは、ステップバイステップのインストール手順、エージェント管理のベストプラクティス (一時停止/再開、ピン留め/ピン留め解除機能を含む)、および展開後の構成要件について説明します。始める前に、エージェントサーバーが "システム要件"。

開始前の準備

- 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 ユーザー *cssys* とローカル グループ *cssys* がマシン上に作

成されます。権限設定によりローカル ユーザーの作成が許可されず、代わりに Active Directory が必要な場合は、ユーザー名が *cssys* のユーザーを Active Directory サーバーに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読むことができます"ここをクリックしてください。"。

ベストプラクティス

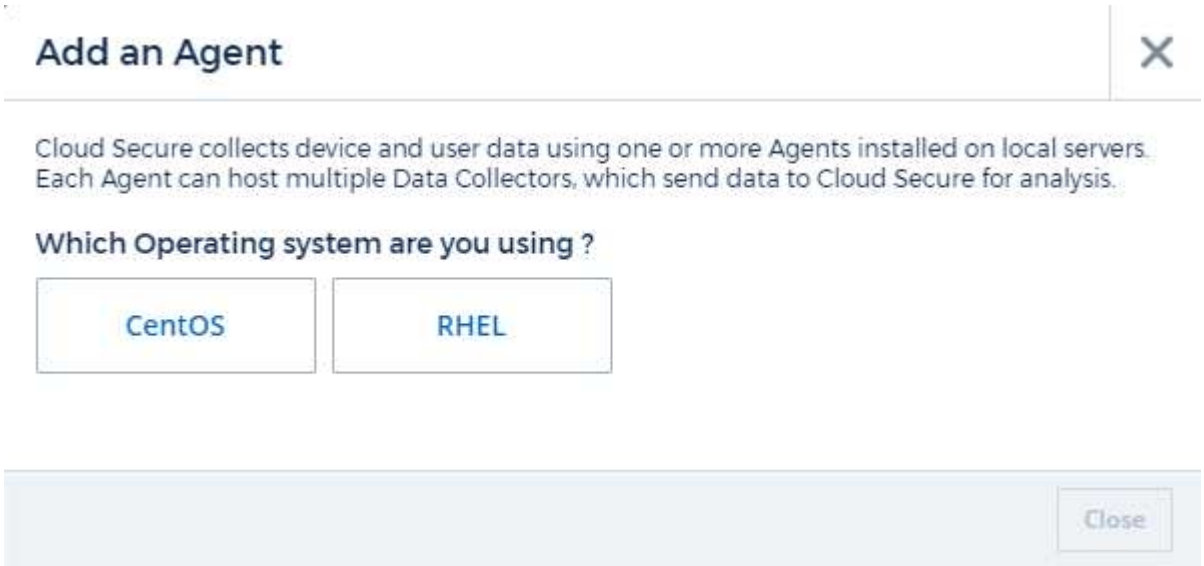
Workload Security エージェントを設定する前に、次の点に留意してください。

一時停止と再開	一時停止: ONTAPから fpolicies を削除します。通常、エージェント VM の再起動やストレージの交換など、かなりの時間を要する可能性がある長時間のメンテナンス アクティビティを顧客が実行する場合に使用されます。再開: fpolicies をONTAPに追加し直します。
ピン留めとピン留め解除	ピンを解除すると、すぐに最新バージョン (利用可能な場合) が取得され、エージェントとコレクターがアップグレードされます。このアップグレード中、fpolicies は切断され、再接続されます。この機能は、自動アップグレードのタイミングを制御したいお客様向けに設計されています。以下を参照ピン留め/ピン留め解除の手順。
推奨されるアプローチ	大規模な構成の場合、コレクターを一時停止するのではなく、Pin と Unpin を使用することをお勧めします。ピンとピン解除の使用中に一時停止したり再開したりする必要はありません。顧客はエージェントとコレクターを固定したままにして、新しいバージョンに関する電子メール通知を受信したら、30 日以内にエージェントを 1 つずつ選択的にアップグレードすることができます。このアプローチにより、fpolicies への遅延の影響が最小限に抑えられ、アップグレード プロセスをより細かく制御できるようになります。

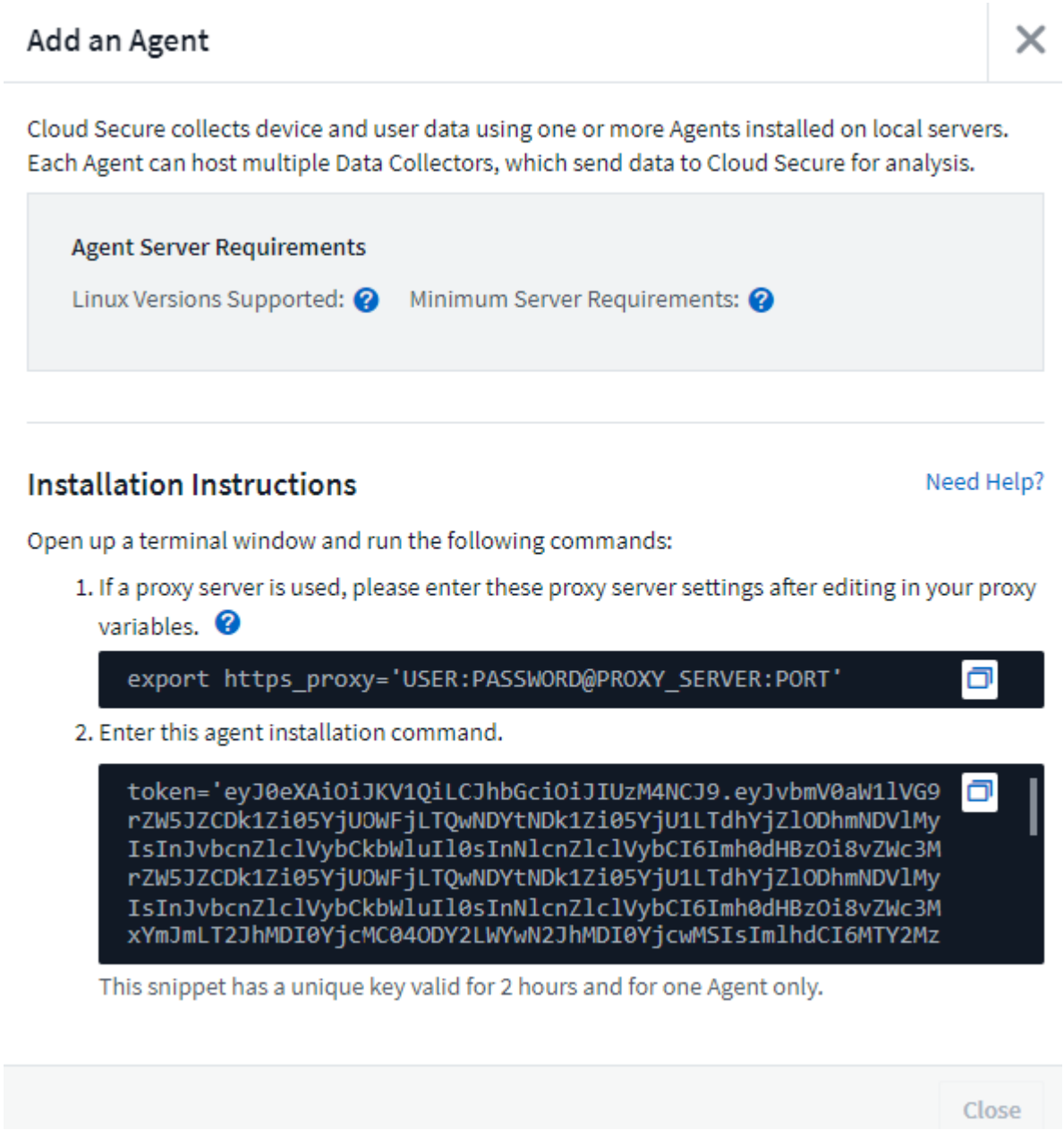
エージェントのインストール手順

1. Workload Security 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. *コレクター > エージェント > +エージェント*を選択

   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 サーバー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 サーバーがサポートされているバージョンの Linux を実行していることを確認するには、[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 サーバー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 サーバーの詳細を設定してください。



6. インストール コマンドをコピーするには、[クリップボードにコピー] アイコンをクリックします。
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. 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ー"。
2. 1 つ以上のデータ コレクターを構成する必要があります。

ネットワーク構成

Workload Security で使用されるポートを開くには、ローカル システムで次のコマンドを実行します。ポート範囲に関してセキュリティ上の懸念がある場合は、*35000:35100* などのより狭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に従ってください。

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
```

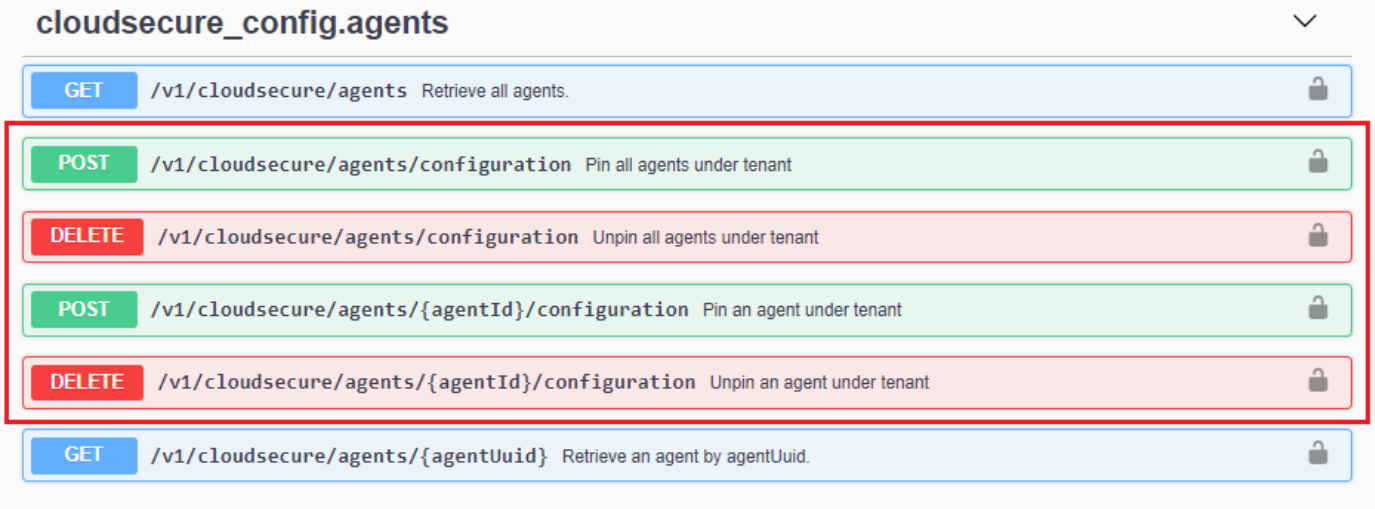
エージェントを現在のバージョンに「固定」する

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。自動更新を一時停止して、次のいずれかが発生するまでエージェントを現在のバージョンのままにすることを希望する顧客もいます。

- 顧客はエージェントの自動更新を再開します。
- 30日が経過しました。 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から始まることに注意してください。

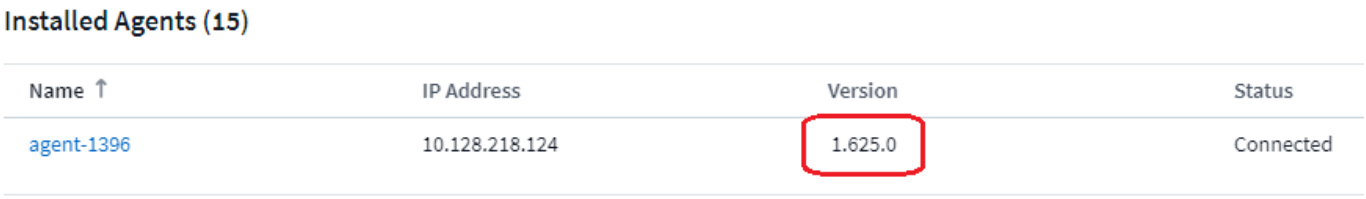
いずれの場合も、エージェントは次回の Workload Security 更新時に更新されます。

自動エージェント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アクションが有効になるまでに最大 5 分かかる場合があることに注意してください。

現在のエージェントのバージョンは、**Workload Security > Collectors** ページの **Agents** 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：
エージェントのインストールで /opt/netapp/cloudsecure/agent/logs/agent.log フォルダの作成に失敗し、install.log ファイルには関連情報が提供されません。	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。エラーはロガーが初期化される前に発生するため、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、サービスログで次のように表示されます。 `journalctl -u cloudsecure-agent.service`指示。このコマンドは、問題をさらにトラブルシューティングするために使用できます。
エージェントのインストールが「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」というメッセージで失敗します。インストールを終了します。	このエラーは、サポートされていないシステムにエージェントをインストールしようとしたときに表示されます。見る"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: コマンドが見つかりません"	unzip をインストールしてから、インストール コマンドを再度実行します。マシンに Yum がインストールされている場合は、「yum install unzip」を実行して unzip ソフトウェアをインストールしてください。その後、エージェントのインストール UI からコマンドを再度コピーし、CLI に貼り付けてインストールを再度実行します。

問題：	解決：

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。	エージェント マシンに SSH で接続します。エージェントサービスのステータスを確認するには、 `sudo systemctl status cloudsecure-agent.service` 。1.ログに「Workload Security デーモン サービスを開始できませんでした」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.エージェント マシンに cssys ユーザーが存在するかどうかを確認します。次のコマンドをルート権限で 1 つずつ実行し、cssys ユーザー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、集中監視ポリシーによって `cssys` ユーザー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、`cssys` ユーザーと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` 6.それでも実行されない場合は、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 50 個を超えるデータ コレクターを追加することはできません。	エージェントに追加できるデータ コレクターは 50 個のみです。これは、Active Directory、SVM、その他のコレクターなど、すべてのコレクター タイプの組み合わせになります。
UI には、エージェントが NOT_CONNECTED 状態にあることが示されます。	エージェントを再起動する手順。1.エージェント マシンに SSH で接続します。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` 3.エージェントサービスのステータスを確認するには、 `sudo systemctl status cloudsecure-agent.service` 。4.エージェントは CONNECTED 状態に移行する必要があります。
エージェント VM は Zscaler プロキシの背後にあり、エージェントのインストールが失敗します。 Zscaler プロキシの SSL 検査により、Workload Security 証明書は Zscaler CA によって署名された状態で提示されるため、エージェントは通信を信頼していません。	*.cloudinsights.netapp.com URL の Zscaler プロキシで SSL 検査を無効にします。 Zscaler が SSL 検査を実行して証明書を置き換えると、Workload Security は機能しなくなります。

問題：	解決：
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。エージェント インストール コマンドが非 root sudo ユーザーによって実行され、作業ディレクトリに別のユーザーに属するファイルがあり、それらのファイルの権限を変更できない場合、コマンドは失敗します。chmod コマンドが失敗したため、インストールの残りの部分は実行されません。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るはずです。
それでもエージェントが Saas に接続できない場合は、 NetAppサポートにケースを開いてください。ケースを開くには、 Data Infrastructure Insights のシリアル番号を提供し、記載されているとおりにログをケースに添付します。	ログをケースに取り付けるには: 1.次のスクリプトをルート権限で実行し、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 2.ルート権限で次のコマンドを1つずつ実行し、出力を共有します。a. id cssys b. groups cssys c. cat /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 エージェント構成を収集しています 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 の作成に失敗しました	Zip ツールがインストールされていません。 「yum install zip」コマンドを実行して、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が useradd で失敗します: ディレクトリ /home/cssys を作成できません	このエラーは、権限不足のためにユーザーのログイン ディレクトリを /home の下に作成できない場合に発生する可能性があります。回避策としては、cssys ユーザーを作成し、次のコマンドを使用してそのログイン ディレクトリを手動で追加します: *sudo useradd user_name -m -d HOME_DIR* -m : ユーザーのホーム ディレクトリが存在しない場合は作成します。 -d : ユーザーのログイン ディレクトリの値として HOME_DIR を使用して新しいユーザーが作成されます。たとえば、*sudo useradd cssys -m -d /cssys* は、ユーザー *cssys* を追加し、ルート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：
インストール後にエージェントが実行されていません。 *Systemctl status cloudsecure-agent.service* は次のように表示します: [root@demo ~]# systemctl status cloudsecure-agent.service agent.service – Workload Security Agent Daemon Service Loaded: loaded (/usr/lib/systemd/system/cloudsecure-agent.service; enabled; vendor preset: disabled) Active: activating (auto-restart) (Result: exit-code) since Tue 2021-08-03 21:12:26 PDT; 2 秒前 プロセス: 25889 ExecStart=/bin/bash /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent (コード = 終了、ステータス = 126) メイン PID: 25889 (コード = 終了、ステータス = 126)、8 月 03 日 21:12:26 demo systemd[1]: cloudsecure-agent.service: メイン プロセスが終了しました。コード = 終了、ステータス = 126/n/a 8 月 03 日 21:12:26 demo systemd[1]: ユニット cloudsecure-agent.service が失敗状態になりました。 8月3日 21:12:26 デモ systemd[1]: cloudsecure-agent.service が失敗しました。	*cssys* ユーザーにインストール権限がない可能性があるため、失敗する可能性があります。 /opt/netapp が NFS マウントであり、*cssys* ユーザーがこのフォルダー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、Workload Security インストーラによって作成されたローカル ユーザーであり、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ります。これを確認するには、*cssys* ユーザーを使用して /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent にアクセスしてみてください。 「Permission denied」が返された場合、インストール権限が存在しません。マウントされたフォルダーの代わりに、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 サーバー経由で接続され、プロキシはエージェントのインストール中に設定されました。プロキシサーバーが変更されました。エージェントのプロキシ構成を変更するにはどうすればよいですか?	agent.properties を編集してプロキシの詳細を追加できます。次の手順に従ってください: 1.プロパティ ファイルが含まれているフォルダーに変更します: cd /opt/netapp/cloudsecure/conf 2.お気に入りのテキストエディターを使用して、*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.netapp.com 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

Workload Security エージェントを削除する場合は、まず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 コレクターを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 コレクターが削除されます。別のエージェントを使用してデータ コレクターを構成する予定の場合は、エージェントを削除する前に、データ コレクター構成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. エージェントに関連付けられているすべてのデータ コレクターが Workload Security ポータルから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ーが STOPPED 状態の場合、この手順は無視してください。

エージェントを削除する手順:

1. エージェント VM に SSH で接続し、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. *ワークロードセキュリティ > コレクター > エージェント*をクリックします

   構成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*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、[削除] をクリックします。

Active Directory (AD) ユーザーディレクトリコレクターの構成

Workload Security は、Active Directory サーバーからユーザー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 サーバーをホストしているサーバーの IP アドレスが必要です。
- ユーザー ディレクトリ コネクタを構成する前に、エージェントを構成する必要があります。

ユーザーディレクトリコレクターを構成する手順

1. Workload Securityメニューで、*コレクター > ユーザーディレクトリコレクター > + ユーザーディレクトリコレクター*をクリックし、*Active Directory*を選択します。

   「ユーザー ディレクトリの追加」画面が表示されます。

次の表に必要なデータを入力して、ユーザー ディレクトリ コレクターを構成します。

Name	説明
Name	ユーザー ディレクトリの一意の名前。例えば_GlobalADCollector_
エージェント	リストから構成済みのエージェントを選択します

サーバーIP/ドメイン名	アクティブ ディレクトリをホストするサーバーの IP アドレスまたは完全修飾ドメイン名 (FQDN)
森林名	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、次の両方の形式が許可されます: *x.y.z* ⇒ SVM にある直接のドメイン名。 [例: hq.companyname.com] *DC=x*、*DC=y*、*DC=z* ⇒ 相対識別名 [例: DC=hq、DC= companyname、DC=com] または、次のように指定することもできます: *OU=engineering*、*DC=hq*、*DC= companyname* 、*DC=com* [特定の OU engineering でフィルタリングする] *CN=username*、*OU=engineering* 、*DC=companyname*、*DC=netapp*、*DC=com* [OU <engineering> から <username> を持つ特定のユーザーのみを取得する] *CN=Acrobat Users*、*CN=Users* 、*DC=hq*、*DC=companyname*、*DC=com*、*O= companyname*、*L=Boston*、*S=MA*、*C=US* [その組織内のユーザー内のすべての Acrobat ユーザーを取得する] 信頼された Active Directory ドメインもサポートされています。
バインドDN	ディレクトリの検索を許可されたユーザー。たとえば、*username@companyname.com* または *username@domainname.com* です。さらに、ドメイン読み取り専用権限が必要です。ユーザーは、セキュリティ グループ 読み取り専用ドメイン コントローラー のメンバーである必要があります。
BINDのパスワード	ディレクトリ サーバーのパスワード (つまり、Bind DN で使用されるユーザー名のパスワード)
プロトコル	ldap、ldaps、ldap-start-tls
ポート	ポートを選択

Active Directory でデフォルトの属性名が変更されている場合は、次のディレクトリ サーバーの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 では変更されません。その場合は、デフォルトの属性名をそのまま使用して続行できます。

属性	ディレクトリサーバーの属性名
表示名	名前
SID	オブジェクトID
ユーザー名	sAMAccountName

次のいずれか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ーの属性名
E メール アドレス	郵便
電話番号	電話番号
ロール	タイトル
国	共同

州	状態
部門	部門
写真	サムネイル写真
マネージャーDN	マネージャー
グループ	memberOf

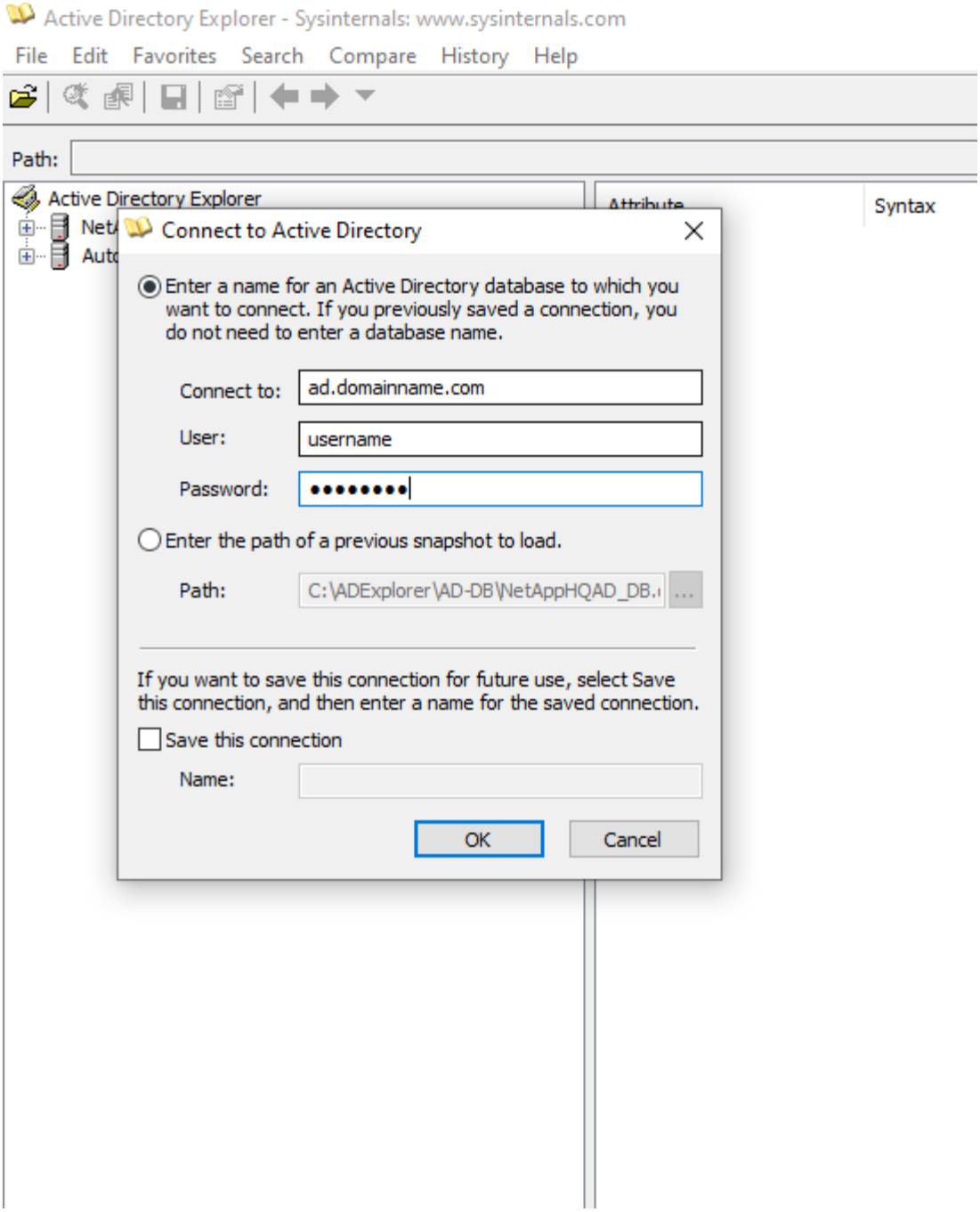
ユーザーディレクトリコレクターの構成のテスト

次の手順を使用して、LDAP ユーザー権限と属性定義を検証できます。

- Workload Security LDAP ユーザー権限を検証するには、次のコマンドを使用します。

```
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 を使用すると、AD データベースをナビゲートしたり、オブジェクトのプロパティと属性を表示したり、権限を表示したり、オブジェクトのスキーマを表示したり、保存して再実行できる高度な検索を実行したりできます。
  - インストール"広告エクスプローラー"AD サーバーに接続できる任意の Windows マシン上。
  - AD ディレクトリ サーバーのユーザー名とパスワードを使用して AD サーバーに接続します。



ユーザーディレクトリコレクターの構成エラーのトラブルシューティング

次の表では、コレクターの構成中に発生する可能性のある既知の問題と解決策について説明します。

問題：	解決：
ユーザー 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 サーバーに無効な資格情報が提供されました」というエラーが表示されます。	間違ったユーザー名またはパスワードが指定されました。正しいユーザー名とパスワードを編集して入力します。

問題：	解決：
ユーザー 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。エラーには、「フォレスト名として指定された DN=DC=hq、DC=domainname 、DC=com に対応するオブジェクトを取得できませんでした。」と表示されます。	指定され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属性が、Workload Security 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 に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ていないことが原因であると考えられます。正しいオプション属性名を編集して指定します。
データ コレクターが「LDAP ユーザーの取得に失敗しました」というエラー状態です。失敗の理由: サーバーに接続できません。接続が null です。	*Restart* ボタンをクリックしてコレクターを再起動します。
ユーザー 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 (サーバー、フォレスト名、バインド DN、バインド パスワード) に有効な値を指定していることを確認してください。バインド 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るようにします。
ユーザー ディレクトリ コネクタを追加すると、「再試行」状態になります。 「コレクターの状態を定義できません。理由: java.net.ConnectionException: 接続が拒否されたため、TCP コマンド [Connect(localhost:35012,None,List(),Some(,seconds),true)] が失敗しました。」というエラーが表示されます。	AD サーバーに指定された IP または FQDN が正しくありません。正しい IP アドレスまたは FQDN を編集して入力します。
ユーザー 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 接続を確立できませんでした」というエラーが表示されます。	AD サーバーに指定された IP または FQDN が正しくありません。正しい IP アドレスまたは FQDN を編集して入力します。
ユーザー 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。 「設定の読み込みに失敗しました」というエラーが表示されます。理由: データソース構成にエラーがあります。具体的な理由: /connector/conf/application.conf: 70: ldap.ldap-port のタイプは NUMBER ではなく STRING です	指定されたポートの値が正しくありません。 AD サーバー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。
必須属性から始めましたが、うまくいきました。オプションのものを追加した後、オプションの属性データが AD から取得されません。	これは、CloudSecure に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ていないことが原因であると考えられます。正しい必須またはオプションの属性名を編集して指定します。
コレクターを再起動した後、AD 同期はいつ行われますか?	コレクターが再起動するとすぐに AD 同期が行われます。約 30 万ユーザーのユーザーデータを取得するには約 15 分かかり、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。データはいつ削除されますか?	更新がない場合、ユーザーデータは 13 か月間保持されます。テナントが削除されると、データも削除されます。

問題：	解決：
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。 「コネクタはエラー状態です。サービス名: usersLdap。失敗の理由: LDAP ユーザーの取得に失敗しました。失敗の理由: 80090308: LdapErr: DSID-0C090453、コメント: AcceptSecurityContext エラー、データ 52e、v3839"	指定され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。
ユーザー プロフィール ページに電話番号が入力されません。	これは、Active Directory の属性マッピングの問題が原因であると考えられます。1. Active Directory からユーザーの情報を取得している特定の Active Directory コレクターを編集します。2.オプション属性の下に、Active Directory 属性「telephonenumber」にマップされたフィールド名「電話番号」があることに注意してください。4.ここで、上で説明した Active Directory Explorer 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、実際にユーザーの電話番号を持つ「telephonenumber」という名前の属性があることを確認します。5. Active Directory では「phonenumber」に変更されているとします。6.次に、CloudSecure ユーザー ディレクトリ コレクターを編集します。オプション属性セクションで、「telephonenumber」を「phonenumber」に置き換えます。7. Active Directory コレクターを保存すると、コレクターが再起動し、ユーザーの電話番号を取得して、ユーザー プロファイル ページに表示します。
Active Directory (AD) サーバーで暗号化証明書 (SSL) が有効になっている場合、Workload Security ユーザー ディレクトリ コレクターは AD サーバーに接続できません。	ユーザー ディレクトリ コレクターを構成する前に、AD サーバー暗号化を無効にします。ユーザーの詳細が取得されると、その情報は 13 か月間保存されます。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、AD に新しく追加されたユーザーは取得されません。再度取得するには、ユーザー ディレクトリ コレクターを AD に接続する必要があります。
Active Directory からのデータは CloudInsights Security に存在します。 CloudInsights からすべてのユーザー情報を削除します。	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。ユーザーを削除するには、テナント全体を削除する必要があります。

LDAPディレクトリサーバーコレクターの構成

Workload Security 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 サーバーをホストするサーバーの IP アドレスが必要です。

- LDAP ディレクトリ コネクタを構成する前に、エージェントを構成する必要があります。

ユーザーディレクトリコレクターを構成する手順

1. ワークロード セキュリティ メニューで、コレクター > ユーザー ディレクトリ コレクター > + ユーザー ディレクトリ コレクター をクリックし、**LDAP** ディレクトリ サーバー を選択します。

   「ユーザー ディレクトリの追加」画面が表示されます。

次の表に必要なデータを入力して、ユーザー ディレクトリ コレクターを構成します。

Name	説明
Name	ユーザー ディレクトリの一意の名前。例えば_GlobalLDAPCollector_
エージェント	リストから構成済みのエージェントを選択します
サーバーIP/ドメイン名	LDAP ディレクトリ サーバーをホストするサーバーの IP アドレスまたは完全修飾ドメイン名 (FQDN)
検索ベース	LDAP サーバーの検索ベース検索ベースでは、次の両方の形式が許可されます: *x.y.z* ⇒ SVM にある直接のドメイン名。 [例: hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ 相対識別名 [例: DC=hq,DC=companyname,DC=com] または、次のように指定することもできます: *OU=engineering,DC=hq,DC=companyname,DC=com* [特定の OU engineering でフィルタリングする] *CN=username,OU=engineering,DC=companyname, DC=netapp, DC=com* [OU <engineering> から <username> を持つ特定のユーザーのみを取得する] *CN=Acrobat Users,CN=Users,DC=hq,DC=companyname,DC=com ,O= companyname,L=Boston,S=MA,C=US* [その組織内のユーザー内のすべての Acrobat ユーザーを取得する]
バインドDN	ディレクトリの検索を許可されたユーザー。たとえば、ユーザー john@dorp.company.com の場合、uid=ldapuser、cn=users、cn=accounts、dc=domain、dc=companyname、dc=com uid=john 、cn=users、cn=accounts、dc=dorp、dc=company、dc=com となります。 dorp.company.com
--アカウント	--ユーザー
--ジョン	--アンナ
BINDのパスワード	ディレクトリ サーバーのパスワード (つまり、Bind DN で使用されるユーザー名のパスワード)
プロトコル	ldap、ldaps、ldap-start-tls
ポート	ポートを選択

LDAP ディレクトリ サーバーでデフォルトの属性名が変更されている場合は、次のディレクトリ サーバーの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 LDAP ディレクトリ サーバーで変更されませ

ん。その場合は、デフォルトの属性名でそのまま続行できます。

属性	ディレクトリサーバーの属性名
表示名	名前
UNIXID	uid番号
ユーザー名	uid

次のいずれか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ーの属性名
E メール アドレス	郵便
電話番号	電話番号
ロール	タイトル
国	共同
州	状態
部門	部門番号
写真	写真
マネージャーDN	マネージャー
グループ	memberOf

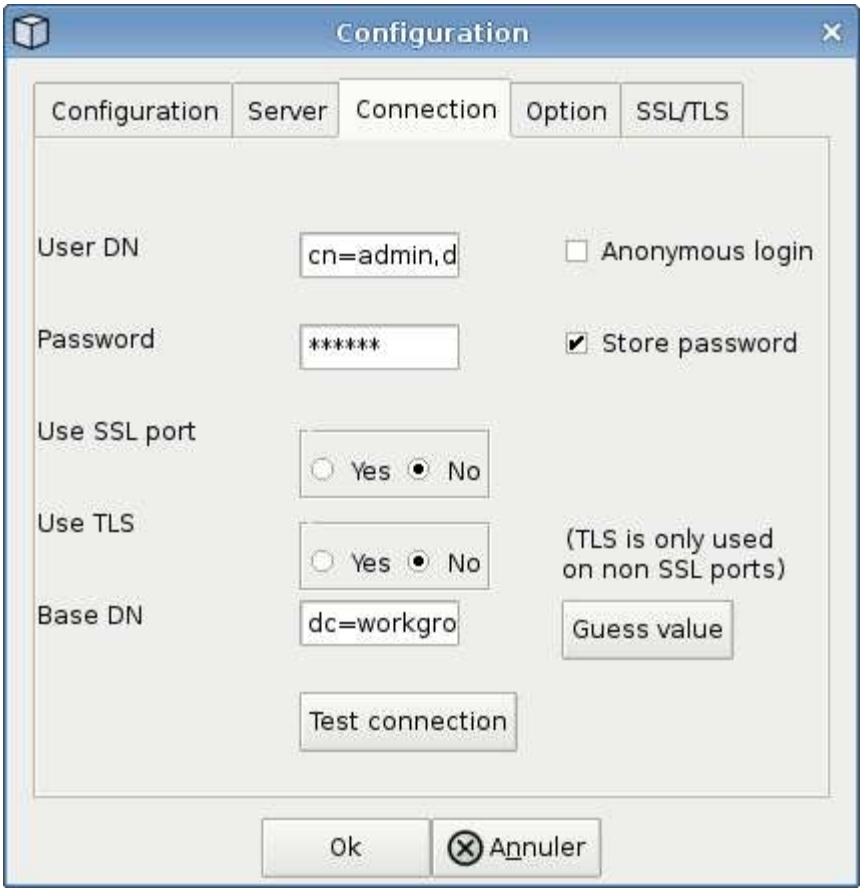
ユーザーディレクトリコレクターの構成のテスト

次の手順を使用して、LDAP ユーザー権限と属性定義を検証できます。

- Workload Security LDAP ユーザー権限を検証するには、次のコマンドを使用します。

```
 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 エクスプローラーを使用すると、LDAP
データベースをナビゲートしたり、オブジェクトのプロパティと属性を表示したり、権限を表示したり、オブジェクトのスキーマを表示したり、保存して再実行できる高度な検索を実行したりできます。
```

  - LDAPエクスプローラーをインストールする(http://ldaptool.sourceforge.net/) または Java LDAP エクスプローラー(http://jxplorer.org/) を、LDAP サーバーに接続できる任意の Windows マシンにインストールします。
  - LDAP ディレクトリ サーバーのユーザー名とパスワードを使用して LDAP サーバーに接続します。



LDAPディレクトリコレクターの設定エラーのトラブルシューティング

次の表では、コレクターの構成中に発生する可能性のある既知の問題と解決策について説明します。

問題：	解決：
LDAP 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 サーバーに無効な資格情報が提供されました」というエラーが表示されます。	指定されたバインド 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。正しい情報を編集して提供してください。
LDAP 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。エラーには、「フォレスト名として指定された DN=DC=hq、DC=domainname 、DC=com に対応するオブジェクトを取得できませんでした。」と表示されます。	間違った検索ベースが指定されました。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属性が、Workload Security 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 に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ていないことが原因であると考えられます。フィールドでは大文字と小文字が区別されます。正しいオプション属性名を編集して指定します。
データ コレクターが「LDAP ユーザーの取得に失敗しました」というエラー状態です。失敗の理由: サーバーに接続できません。接続が null です。	*Restart* ボタンをクリックしてコレクターを再起動します。

問題：	解決：
LDAP 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 (サーバー、フォレスト名、バインド DN、バインド パスワード) に有効な値を指定していることを確認してください。バインド DN 入力が常に uid=ldapuser、cn=users、cn=accounts、dc=domain、dc=companyname、dc=com として提供されるようにします。
LDAP ディレクトリ コネクタを追加すると、「再試行」状態になります。 「コレクターの正常性を判断できなかったため、再試行します」というエラーが表示されます	正しいサーバー IP と検索ベースが提供されていることを確認してください ////
LDAP ディレクトリの追加中に次のエラーが表示されます: 「2 回の再試行でコレクターの正常性を判断できませんでした。コレクターをもう一度再起動してください (エラー コード: AGENT008)」	正しいサーバーIPと検索ベースが提供されていることを確認してください
LDAP ディレクトリ コネクタを追加すると、「再試行」状態になります。 「コレクターの状態を定義できません。理由: java.net.ConnectionException: 接続が拒否されたため、TCP コマンド [Connect(localhost:35012,None,List(),Some(,seconds),true)] が失敗しました。」というエラーが表示されます。	AD サーバーに指定された IP または FQDN が正しくありません。正しい IP アドレスまたは FQDN を編集して入力します。 ////
LDAP 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 接続を確立できませんでした」というエラーが表示されます。	LDAP サーバーに指定された IP または FQDN が正しくありません。正しい IP アドレスまたは FQDN を編集して入力します。または、指定されたポートの値が正しくありません。 LDAP サーバー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 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。 「設定の読み込みに失敗しました」というエラーが表示されます。理由: データ ソース構成にエラーがあります。具体的な理由: /connector/conf/application.conf: 70: ldap.ldap-port のタイプは NUMBER ではなく STRING です	指定されたポートの値が正しくありません。 AD サーバー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。
必須属性から始めましたが、うまくいきました。オプションのものを追加した後、オプションの属性データが AD から取得されません。	これは、CloudSecure に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ていないことが原因であると考えられます。正しい必須またはオプションの属性名を編集して指定します。
コレクターを再起動した後、LDAP 同期はいつ行われますか?	コレクターが再起動するとすぐに LDAP 同期が実行されます。約 30 万ユーザーのユーザーデータを取得するには約 15 分かかり、12 時間ごとに自動的に更新されます。
ユーザーデータは LDAP から CloudSecure に同期されます。データはいつ削除されますか?	更新がない場合、ユーザーデータは 13 か月間保持されます。テナントが削除されると、データも削除されます。

問題：	解決：
LDAP ディレクトリ コネクタが「エラー」状態になります。 「コネクタはエラー状態です。サービス名: usersLdap。失敗の理由: LDAP ユーザーの取得に失敗しました。失敗の理由: 80090308: LdapErr: DSID-0C090453、コメント: AcceptSecurityContext エラー、データ 52e、v3839"	指定され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。
ユーザー プロフィール ページに電話番号が入力されません。	これは、Active Directory の属性マッピングの問題が原因であると考えられます。1. Active Directory からユーザーの情報を取得している特定の Active Directory コレクターを編集します。2.オプション属性の下に、Active Directory 属性「telephonenumber」にマップされたフィールド名「電話番号」があることに注意してください。4.ここで、上で説明した Active Directory Explorer ツールを使用して、LDAP ディレクトリ サーバーを参照し、正しい属性名を確認してください。3. LDAP ディレクトリに、実際にユーザーの電話番号を持つ「telephonenumber」という名前の属性があることを確認します。5. LDAP ディレクトリで「phonenumber」に変更されたとします。6.次に、CloudSecure ユーザー ディレクトリ コレクターを編集します。オプション属性セクションで、「telephonenumber」を「phonenumber」に置き換えます。7. Active Directory コレクターを保存すると、コレクターが再起動し、ユーザーの電話番号を取得して、ユーザー プロファイル ページに表示します。
Active Directory (AD) サーバーで暗号化証明書 (SSL) が有効になっている場合、Workload Security ユーザー ディレクトリ コレクターは AD サーバーに接続できません。	ユーザー ディレクトリ コレクターを構成する前に、AD サーバー暗号化を無効にします。ユーザーの詳細が取得されると、その情報は 13 か月間保存されます。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、AD に新しく追加されたユーザーは取得されません。再度取得するには、ユーザー ディレクトリ コレクターを AD に接続する必要があります。

ONTAP SVMデータコレクターの設定

ONTAP SVM データ コレクターを使用すると、Workload Security はNetApp ONTAPストレージ仮想マシン (SVM) 上のファイルおよびユーザー アクセス アクティビティを監視できます。このガイドでは、 ONTAP環境の包括的なセキュリティ監視を実現するための SVM データ コレクターの構成と管理について説明します。

開始する前に

- このデータ コレクターは以下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、 Data ONTAPバージョン 9.13.1 以降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 4.1 までの NFS バージョン (NFS 4.1 はONTAP 9.15 以降でサポートされます)。
- FlexgroupはONTAP 9.4以降のバージョンでサポートされています
- FlexCache は、 ONTAP 9.7 以降のバージョンの NFS でサポートされます。
- FlexCache は、 ONTAP 9.14.1 以降のバージョンの SMB でサポートされます。
- ONTAP Selectがサポートされています

- データ型 SVM のみがサポートされます。無限ボリュームを持つ SVM はサポートされていません。
- SVM にはいくつかのサブタイプがあります。これらのうち、*default*、*sync_source*、および *sync_destination* のみがサポートされています。
- エージェント"設定する必要があります"データ コレクターを構成する前に。
- ユーザー ディレクトリ コネクタが適切に構成されていることを確認してください。適切に構成されていない場合、「アクティビティ フォレンジック」ページのイベントには、実際のユーザーの名前 (Active Directory に保存されている名前) ではなく、エンコードされたユーザー名が表示されます。
- ONTAP永続ストアは 9.14.1 からサポートされます。
- 最適なパフォーマンスを得るために、FPolicyサーバをストレージ システムと同一のサブネットに設定することを推奨します。
- Workload Security FPolicy設定に関する包括的なベストプラクティスと推奨事項については、"FPolicy ベストプラクティスに関する KB 記事" 。
- 次の 2 つの方法のいずれかを使用して SVM を追加する必要があります。
  - クラスタ IP、SVM 名、クラスタ管理ユーザー名とパスワードを使用します。 これが推奨される方法です。
    - SVM 名はONTAPに表示されているものと完全に一致している必要があり、大文字と小文字が区別されます。
  - SVM Vserver管理IP、ユーザー名、パスワードを使用する
  - 完全な管理者クラスタ/SVM管理ユーザー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、以下に記載されているように、より低い権限を持つカスタムユーザーを作成できます。「権限に関する注意事項」以下のセクションをご覧ください。このカスタム ユーザーは、SVM 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 ユーザーを使用することもできます。また、"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`

  システムは、Vserver 名、CIFS サーバー名、および追加フィールドを返します。

- SVM vsadmin ユーザーのパスワードを設定します。カスタム ユーザーまたはクラスター管理者ユーザーを使用する場合は、この手順をスキップします。clustershell:> `security login password -username vsadmin -vserver svmname`
- 外部アクセス用に SVM vsadmin ユーザーのロックを解除します。カスタム ユーザーまたはクラスター管理者ユーザーを使用する場合は、この手順をスキップします。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「mgmt」（「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てください。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 コレクターを使用するポートの 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。

  見る"エージェントの要件"構成情報については。これは、オンプレミスのエージェントとクラウドにインストールされたエージェントに適用されます。

- Cloud ONTAP SVM を監視するためにエージェントを AWS EC2 インスタンスにインストールする場合、エージェントとストレージは同じ VPC 内に存在する必要があります。別々の VPC にある場合は、VPC 間に有効なルートが必要です。

データコレクターの接続テスト

テスト接続機能 (2025 年 3 月に導入) は、 Data Infrastructure Insights (DII) ワークロード セキュリティでデータ コレクターを設定するときに、エンド ユーザーが障害の具体的な原因を特定できるようにすることを目的としています。これにより、ユーザーはネットワーク通信や役割の不足に関連する問題を自己修正できるようになります。

この機能は、データ コレクターを設定する前に、ネットワーク関連のすべてのチェックが実施されているかどうかをユーザーが確認するのに役立ちます。さらに、 ONTAPでユーザーに割り当てられたONTAP のバージョン、ロール、および権限に基づいて、ユーザーがアクセスできる機能についても通知します。

ユーザーディレクトリコレクターではテスト接続はサポートされていません

接続テストの前提条件

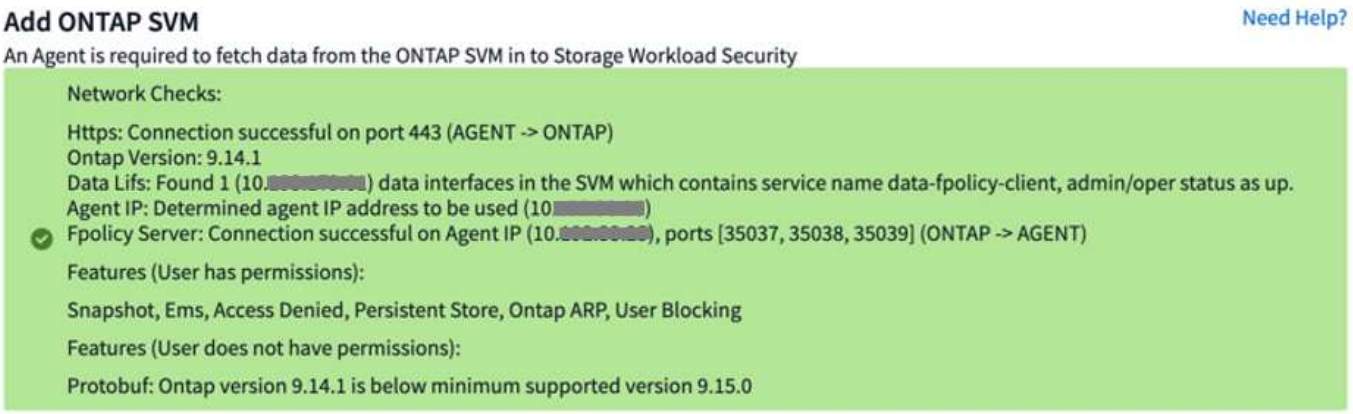
- この機能が完全に動作するには、クラスター レベルの認証情報が必要です。

- SVM モードでは機能アクセス チェックはサポートされていません。
- クラスター管理資格情報を使用している場合は、新しい権限は必要ありません。
- カスタム ユーザー (例: *csuser*) を使用している場合は、使用する機能の必須権限と機能固有の権限を指定します。

必ず確認してください権限以下のセクションも同様です。

接続をテストする

ユーザーはコレクターの追加/編集ページに移動し、クラスター レベルの詳細 (クラスター モードの場合) または SVM レベルの詳細 (SVM モードの場合) を入力して、[接続のテスト] ボタンをクリックできます。Workload Security はリクエストを処理し、適切な成功または失敗のメッセージを表示します。



ONTAP Multi Admin Verify（MAV）の注意事項

スナップショットの作成と削除やユーザー ブロック（SMB）などの一部の機能は、ご使用のバージョンのONTAPに追加されたMAVコマンドによっては機能しない場合があります。

以下の手順に従って、MAV コマンドに除外を追加し、Workload Security がスナップショットを作成または削除したり、ユーザーをブロックしたりできるようにします。

スナップショットの作成と削除を許可するコマンド：

```
multi-admin-verify rule modify -operation "volume snapshot create" -query
"-snapshot !*cloudsecure_*"
multi-admin-verify rule modify -operation "volume snapshot delete" -query
"-snapshot !*cloudsecure_*"
```

ユーザーのブロックを許可するコマンド：

```
multi-admin-verify rule delete -operation set
```

ユーザーアクセスブロックの前提条件

以下の点に留意してください"ユーザーアクセスのブロック":

この機能が動作するには、クラスター レベルの資格情報が必要です。

クラスター管理資格情報を使用している場合は、新しい権限は必要ありません。

ユーザーに権限が付与されたカスタムユーザー（たとえば、*csuser*）を使用している場合は、次の手順に従ってください。"ユーザーアクセスのブロック" Workload Security にユーザーをブロックする権限を与えます。

権限に関する注意事項

*クラスタ管理**IP***経由で追加する場合の権限:

クラスタ管理管理者ユーザーを使用して Workload Security がONTAP SVM データ コレクターにアクセスできるようにできない場合は、以下のコマンドに示すように、ロールを持つ「csuser」という名前の新しいユーザーを作成できます。クラスタ管理 IP を使用するように Workload Security データ コレクターを構成するときは、ユーザー名「csuser」と「csuser」のパスワードを使用します。

注: カスタム ユーザーのすべての機能権限に使用する単一のロールを作成できます。既存のユーザーが存在する場合は、まず次のコマンドを使用して既存のユーザーとロールを削除します。

```
security login delete -user-or-group-name csuser -application *
security login role delete -role csrole -cmddirname *
security login rest-role delete -role csrestrole -api *
security login rest-role delete -role arwrole -api *
```

新しいユーザーを作成するには、クラスタ管理管理者のユーザー名/パスワードを使用してONTAPにログインし、 ONTAPサーバー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 role create -role csrole -cmddirname "cluster application-
record" -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
```

Vserver 管理 **IP** 経由で追加する場合の権限**:**

クラスタ管理管理者ユーザーを使用して Workload Security がONTAP SVM データ コレクターにアクセスできるようにできない場合は、以下のコマンドに示すように、ロールを持つ「csuser」という名前の新しいユーザーを作成できます。 Vserver 管理 IP を使用するように Workload Security データ コレクターを構成するときは、ユーザー名「csuser」と「csuser」のパスワードを使用します。

注: カスタム ユーザーのすべての機能権限に使用する単一のロールを作成できます。既存のユーザーが存在する場合は、まず次のコマンドを使用して既存のユーザーとロールを削除します。

```
security login delete -user-or-group-name csuser -application * -vserver
<vservername>
security login role delete -role csrole -cmddirname * -vserver
<vservername>
security login rest-role delete -role csrestrole -api * -vserver
<vservername>
```

新しいユーザーを作成するには、クラスタ管理管理者のユーザー名/パスワードを使用してONTAPにログインし、 ONTAPサーバーで次のコマンドを実行します。簡単にするために、これらのコマンドをテキスト エディターにコピーし、<vservername> を Vserver 名に置き換えてから、 ONTAPでこれら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>
```

プロトコルバッファモード

このオプションがコレクターの_詳細設定_設定で有効になっている場合、Workload Security は FPolicy エンジンを protobuf モードで設定します。 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、"ONTAPのドキュメント" 。

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既に存在している可能性があります)。

クラスターモード:

```
 security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
Vserver モード:
```

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

ONTAP Autonomous Ransomware Protection および**ONTAP**アクセスの権限が拒否されました

クラスター管理資格情報を使用している場合は、新しい権限は必要ありません。

ユーザーに権限が付与されたカスタム ユーザー (たとえば、*csuser*) を使用している場合は、以下の手順に従って、Workload Security にONTAPから ARP 関連情報を収集する権限を付与します。

詳細については、以下をご覧ください。"ONTAPとの統合アクセスが拒否されました"

そして"ONTAP Autonomous Ransomware Protectionとの統合"

データコレクターを構成する

設定手順

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. ワークロード セキュリティ > コレクター > +データ コレクター をクリックします。

   システムは利用可能なデータ コレクターを表示します。

3. * NetApp SVM タイルにマウスを移動し、+ モニター をクリックします。

   ONTAP SVM 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
Name	データコレクターの一意の名前
エージェント	リストから構成済みの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のいずれかを選択します
クラスタ/SVM管理IPアドレス	上記の選択に応じて、クラスターまたは SVM の IP アドレス。
SVM 名	SVM の名前 (クラスタ IP 経由で接続する場合はこのフィールドが必須です)
ユーザー名	SVM/クラスターにアクセスするためのユーザー名。クラスター IP 経由で追加する場合のオプションは次のとおりです。1.クラスター管理者 2。 「csuser」3. csuser と同様の役割を持つ AD ユーザー。 SVM IP 経由で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 と同様の役割を持つ AD ユーザー名。
パスワード	上記のユーザー名のパスワード
シェア/ボリュームをフィルター	イベント収集に共有/ボリュームを含めるか除外するかを選択します
除外/含める完全な共有名を入力してください	イベント収集から除外または含める共有のコンマ区切りリスト（必要に応じて）
除外/含めるボリューム名を入力してください	イベント収集から除外または含めるボリュームのコンマ区切りリスト（必要に応じて）

フォルダーアクセスを監視する	チェックすると、フォルダー 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、フォルダーの作成/名前変更および削除は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する	ONTAP Fpolicy 送信バッファ サイズを設定します。9.8p7 より前のONTAPバージョンを使用していてパフォーマンスの問題が発生する場合は、 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ず、詳しく知りたい場合は、 NetAppサポートにお問い合わせください。

終了後の操作

- 「インストールされたデータ コレクター」ページで、各コレクターの右側にあるオプション メニューを使用して、データ コレクターを編集します。データ コレクターを再起動したり、データ コレクターの構成属性を編集したりできます。

MetroClusterの推奨構成

MetroClusterには以下が推奨されます。

1. 2 つのデータ コレクターを、1 つをソース SVM に、もう 1 つを宛先 SVM に接続します。
2. データ コレクターは *Cluster IP* によって接続する必要があります。
3. いつでも、現在「実行中」の SVM のデータ コレクターは「実行中」と表示されます。現在「停止」している SVM のデータ コレクターは、*Stopped* として表示されます。
4. 切り替えが発生するたびに、データ コレクターの状態は 実行中 から 停止 に変わり、その逆も同様になります。
5. データ コレクターが 停止 状態から 実行 状態に移行するまで最大 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 ポリシーを使用する場合、データ ソース コレクターに接続するには、データ サービス *data-nfs* や *data-cifs* とともに *data-fpolicy-client* サービスが必要です。

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)
```

ONTAP 9.9.1 より前のバージョンでは、*data-fpolicy-client* を設定する必要はありません。

再生・一時停止データコレクター

データ コレクターが 実行中 状態の場合、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。コレクターが一時停止している間は、 ONTAPからデータは収集されず、コレクターからONTAPにデータは送信されません。つまり、Fpolicy イベントはONTAPからデータ コレクターに流れず、そこからData Infrastructure Insightsに流れません。

コレクターが一時停止中にONTAP上に新しいボリュームなどが作成された場合は、Workload Security はデータを収集せず、それらのボリュームなどは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。

コレクターにユーザーが制限されている場合、コレクターを一時停止することはできません。コレクターを一時停止する前に、ユーザー アクセスを復元します。

次の事項に注意してください。

- 一時停止中のコレクターで構成された設定に従ってスナップショットの消去は実行されません。
- EMS イベント（ONTAP ARP など）は、一時停止中のコレクターでは処理されません。つまり、ONTAP がファイル改ざん攻撃を検知した場合、Data Infrastructure Insights Workload Security 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ーに対しては、ヘルス通知メールは送信されません。
- 一時停止中のコレクターでは、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のブロックなど) はサポートされません。
- エージェントまたはコレクターのアップグレード、エージェント VM の再起動、またはエージェント サービスの再起動が発生すると、一時停止中のコレクターは 一時停止 状態のままになります。
- データ コレクターが *Error* 状態の場合、コレクターを *Paused* 状態に変更することはできません。一時停止ボタンは、コレクターの状態が 実行中 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、コレクターを 一時停止 状態に変更することはできません。コレクターは 停止 状態になり、[一時停止] ボタンは無効になります。

永続ストア

永続ストアはONTAP 9.14.1 以降でサポートされています。ボリューム名の指示はONTAP 9.14 と 9.15 で異なることに注意してください。

コレクターの編集/追加ページでチェックボックスを選択することで、永続ストアを有効にできます。チェックボックスを選択すると、ボリューム名を入力するためのテキスト フィールドが表示されます。ボリューム名は、永続ストアを有効にするための必須フィールドです。

- ONTAP 9.14.1 の場合、機能を有効にする前にボリュームを作成し、[ボリューム名] フィールドに同じ名前を入力する必要があります。推奨ボリュームサイズは 16 GB です。
- ONTAP 9.15.1 の場合、*Volume Name* フィールドに指定された名前を使用して、コレクターによって 16 GB サイズのボリュームが自動的に作成されます。

永続ストア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既に存在している可能性があります)。

クラスターモード:

```
security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "job show" -access
readonly
```

Vserver モード:

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservername> -role csrole -cmddirname
"job show" -access readonly
```

コレクターの移行

Workload Security コレクターをあるエージェントから別のエージェントに簡単に移行できるため、エージェント間でコレクターの負荷を効率的に分散できます。

前提条件

- ソース エージェントは *connected* 状態である必要があります。
- 移行するコレクターは実行中状態である必要があります。

注：

- 移行は、データ コレクターとユーザー ディレクトリ コレクターの両方でサポートされています。
- 手動で管理されるテナントでは、コレクターの移行はサポートされません。

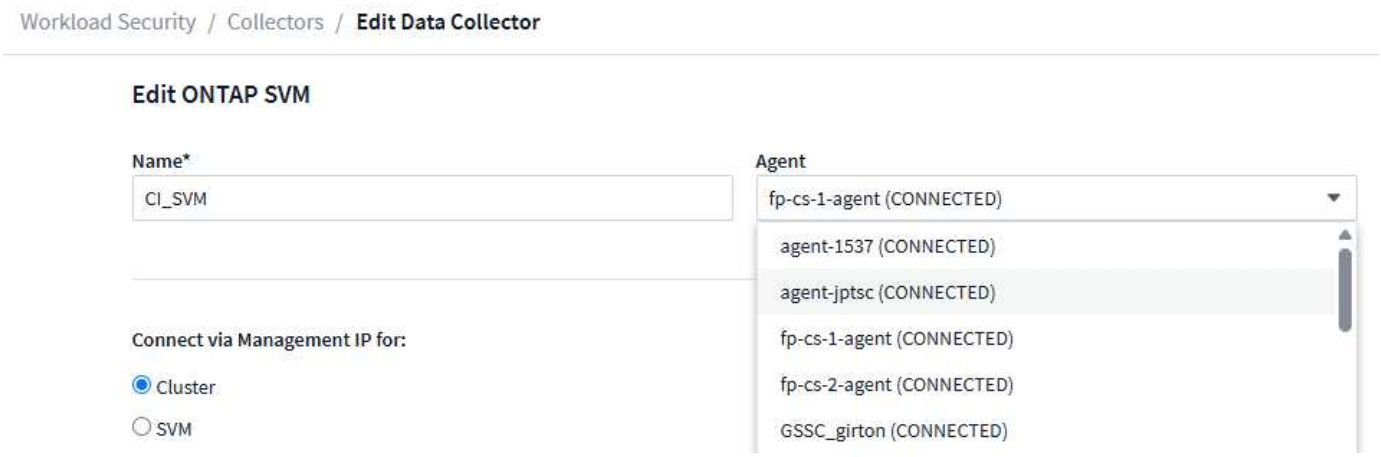
移行コレクター

コレクターを移行するには、次の手順に従います。

1. 「コレクターの編集」ページに移動します。
2. エージェント ドロップダウンから宛先エージェントを選択します。
3. 「コレクターを保存」ボタンをクリックします。

Workload Security がリクエストを処理します。移行が成功すると、ユーザーはコレクター リスト ページにリダイレクトされます。失敗した場合、編集ページに適切なメッセージが表示されます。

注意: 「コレクターの編集」ページで以前に行われた構成の変更は、コレクターが宛先エージェントに正常に移行されたときに適用されたままになります。



トラブルシューティング

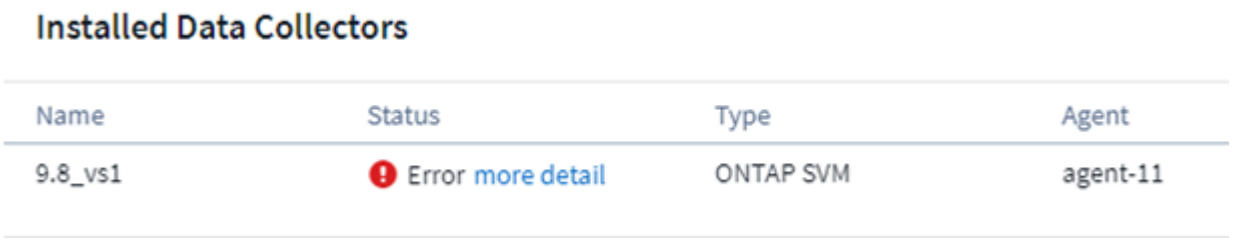
参照"SVMコレクターのトラブルシューティング"トラブルシューティングのヒントのページ。

ONTAP SVM データコレクタのトラブルシューティング

Workload Security はデータ コレクターを使用して、デバイスからファイルおよびユーザー アクセス データを収集します。ここでは、このコレクターに関する問題のトラブルシューティングのヒントを見つけることができます。

参照"SVMコレクターの設定"このコレクターを構成する手順については、このページをご覧ください。

エラーが発生した場合は、「インストールされたデータ コレクター」ページの [ステータス] 列の [詳細] をクリックすると、エラーの詳細が表示されます。



既知の問題とその解決策を以下に説明します。

問題: データ コレクターがしばらく実行され、ランダムな時間の経過後に停止し、次のエラーが発生します: 「エラー メッセージ: コネクタがエラー状態です。サービス名: 監査。失敗の理由: 外部ポリシー サーバーが過負荷です。これを試してください: ONTAPからのイベント レートは、エージェント ボックスが処理できるレートよりもはるかに高かったです。そのため接続は終了しました。

切断が発生したときの CloudSecure のピーク トラフィックを確認します。これは、**CloudSecure >** アクティビティフォレンジック **>** すべてのアクティビティ ページから確認できます。

ピーク集約トラフィックがエージェント ボックスで処理できる量を超える場合は、エージェント ボックスでのコレクター展開のサイズ設定方法について、イベント レート チェッカー ページを参照してください。

2021 年 3 月 4 日より前にエージェントがエージェント ボックスにインストールされていた場合は、エージェント ボックスで次のコマンドを実行します。

```
echo 'net.core.rmem_max=8388608' >> /etc/sysctl.conf
echo 'net.ipv4.tcp_rmem = 4096 2097152 8388608' >> /etc/sysctl.conf
sysctl -p
```

サイズ変更後、UI からコレクターを再起動します。

{空の}

問題: コレクターがエラー メッセージを報告します: 「SVM のデータ インターフェイスに到達できるコネクタにローカル IP アドレスが見つかりません」。 これを試してください: これは、 ONTAP側のネットワークの問題が原因である可能性が最も高いです。次の手順に従ってください。

1. SVM データ LIF または管理 LIF に SVM からの接続をブロックす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 経由で SVM を追加する場合は、SVM のデータ LIF と管理 LIF がエージェント VM から ping 可能であることを確認してください。問題が発生した場合は、LIF のゲートウェイ、ネットマスク、ルートを確認してください。

   クラスター管理 IP を使用して ssh 経由でクラスターにログインし、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。

   ```
   network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
   Name> -show-detail
   ```

   ping できない場合は、エージェント マシンが ping 可能であるように、 ONTAPのネットワーク設定が正しいことを確認します。

3. クラスタ IP 経由で接続しようとしたが機能しない場合は、SVM IP 経由で直接接続してみてください。SVM IP 経由で接続する手順については上記を参照してください。
4. SVM IP および vsadmin 資格情報を使用してコレクターを追加するときに、SVM Lif でデータ プラス Mgmt ロールが有効になっているかどうかを確認します。この場合、SVM Lif への ping は機能しますが、SVM Lif への SSH は機能しません。はいの場合は、SVM 管理専用 Lif を作成し、この SVM 管理専用 Lif 経由で接続してみます。
5. それでも動作しない場合は、新しい SVM Lif を作成し、その Lif を介して接続してみてください。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てください。
6. 高度なデバッグ:
   a. ONTAPでパケット トレースを開始します。
   b. CloudSecure UI からデータ コレクターを SVM に接続してみます。
   c. エラーが表示されるまでお待ちください。 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。この場所で入手可能です

```
 https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/
.. ONTAPからエージェント ボックスへの SYN があることを確認します。
.. ONTAPからの SYN がない場合、それはONTAPのファイアウォールに問題があります。
.. ONTAPでファイアウォールを開き、 ONTAP がエージェント
ボックスに接続できるようにします。
```

7. それでも動作しない場合は、ネットワーク チームに相談して、 ONTAPからエージェント ボックスへの接続が外部ファイアウォールによってブロックされていないことを確認してください。
8. 上記のいずれの方法でも問題が解決しない場合は、"NetApp サポート"さらにサポートが必要な場合はお問い合わせください。

{空の}

問題: メッセージ:「[ホスト名: <IP アドレス>] のONTAPタイプを判別できませんでした。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)" 次を試してください:

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。
2. 接続先の SVM またはクラスターに SSH で接続します。接続したら、SVM またはクラスター名が正しいことを確認します。

{空の}

問題: 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: 監査。失敗の理由: 外部ポリシー サーバーが終了しました。 これを試してみてください:

1. おそらく、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ると考えられます。エージェント マシンが SVM から接続できるように、ポート範囲 35000 ～ 55000/tcp が開かれていることを確認します。また、 ONTAP側でエージェント 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も確認してください。
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。

   ```
   sudo iptables-save | grep 3500*
   ```

   サンプル出力は次のようになります。

   ```
    -A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate
   NEW -j ACCEPT
   . 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。
   ```

```
system services firewall show
system services firewall policy show
```

"ファイアウォールコマンドを確認する"ONTAP側で。

3. 監視する SVM/クラスターに SSH で接続します。 SVM データ LIF (CIFS、NFS プロトコルをサポート) からエージェント ボックスに ping を実行し、ping が機能していることを確認します。

```
network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
Name> -show-detail
```

ping できない場合は、エージェント マシンが ping 可能であるように、 ONTAPのネットワーク設定が正しいことを確認します。

4. 1 つの SVM が 2 つのデータ コレクターを介してテナントに 2 回追加されると、このエラーが表示されます。 UI を通じてデータ コレクターの 1 つを削除します。次に、UI を介して他のデータ コレクターを再起動します。その後、データ コレクターは「実行中」ステータスを表示し、SVM からのイベントの受信を開始します。

基本的に、テナントでは、1 つのデータ コレクターを介して 1 つの SVM を 1 回だけ追加する必要があります。 1 つの SVM を 2 つのデータ コレクター経由で 2 回追加しないでください。

5. 同じ SVM が 2 つの異なる Workload Security 環境 (テナント) に追加された場合には、最後の SVM が常に成功します。 2 番目のコレクターは独自の IP アドレスを使用して fpolicy を設定し、最初のコレクターを排除します。したがって、最初のコレクター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。これを防ぐには、各 SVM を単一の環境で構成します。
6. サービス ポリシーが正しく構成されていない場合にも、このエラーが発生する可能性があります。 ONTAP 9.8 以降では、データ ソース コレクターに接続するには、データ サービス data-nfs や data-cifs とともに、data-fpolicy-client サービスが必要です。さらに、data-fpolicy-client サービスは、監視対象 SVM のデータ lif に関連付けられている必要があります。

{空の}

問題: アクティビティ ページにイベントが表示されません。 これを試してみてください:

1. ONTAPコレクターが「RUNNING」状態であるかどうかを確認します。はいの場合は、いくつかのファイルを開いて、CIFS クライアント VM 上でいくつかの CIFS イベントが生成されていることを確認します。
2. アクティビティが見られない場合は、SVM にログインして次のコマンドを入力してください。

```
<SVM>event log show -source fpolicy
```

fpolicy に関連するエラーがないことを確認してください。

3. アクティビティが見られない場合は、SVM にログインしてください。次のコマンドを入力します。

```
<SVM>fpolicy show
```

プレフィックス「cloudsecure_」で名前が付けられた fpolicy ポリシーが設定されており、ステータスが「オン」になっているかどうかを確認します。設定されていない場合、エージェントは SVM でコマンドを実行できない可能性が高くなります。ページの冒頭に記載されているすべての前提条件が満たされていることを確認してください。

{空の}

問題: SVM データ コレクターがエラー状態にあり、エラー メッセージは「エージェントがコレクターへの接続に失敗しました」です。 次の操作を試してください:

1. おそらく、エージェントが過負荷になっており、データ ソース コレクターに接続できない状態です。
2. エージェントに接続されているデータ ソース コレクターの数を確認します。
3. また、UI の「すべてのアクティビティ」ページでデータ フロー レートを確認します。
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 コレクターを新しいエージェントに移動します。

{空の}

問題: SVM データ コレクターに「fpolicy.server.connectError: ノードは FPolicy サーバー「12.195.15.146」との接続を確立できませんでした (理由:「選択がタイムアウトしました」)」というエラー メッセージが表示されます。 次のことを試してください: SVM/クラスターでファイアウォールが有効になっています。そのため、fpolicy エンジンは fpolicy サーバーに接続できません。詳細情報を取得するために使用できるONTAPの CLI は次のとおりです。

```
event log show -source fpolicy which shows the error
event log show -source fpolicy -fields event,action,description which
shows more details.
```

"ファイアウォールコマンドを確認する"ONTAP側で。

{空の}

問題: 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:監査。失敗の理由: SVM に有効なデータ インターフェイス (ロール: データ、データ プロトコル: NFS または CIFS またはその両方、ステータス: アップ) が見つかりません。 次のことを試してください: 動作可能なインターフェース (データとしての役割と CIFS/NFS としてのデータ プロトコルを持つ) があることを確認します。

{空の}

問題: データ コレクターがエラー状態になり、しばらくすると実行状態になり、その後再びエラー状態に戻ります。このサイクルが繰り返されます。 これを試してみてください: これは通常、次のシナリオで発生します。

1. 複数のデータコレクターが追加されています。
2. このような動作を示すデータ コレクターには、1 つの SVM が追加されます。つまり、2 つ以上のデータ コレクターが 1 つの SVM に接続されます。
3. 1 つのデータ コレクターが 1 つの SVM にのみ接続す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 コレクターを削除します。

{空の}

問題: コネクタがエラー状態です。サービス名: 監査。失敗の理由: SVM svmname のポリシーの設定に失敗しました。理由: 'fpolicy.policy.scope-modify: "Federal" 内の 'shares-to-include' 要素に無効な値が指定されました。 次を試してください: *共有名は引用符なしで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。

共有を含めるおよび除外する は、共有名の長いリストを対象としていません。含めるまたは除外する株式が多数ある場合は、代わりに数量によるフィルタリングを使用します。

{空の}

問題: クラスター内に未使用の既存の fpolicies が存在します。 Workload Security をインストールする前に、これらに対して何をすべきでしょうか? これを試してください: 切断状態であっても、既存の未使用の fpolicy 設定をすべて削除することをお勧めします。 Workload Security は、プレフィックス「cloudsecure_」を持つ fpolicy を作成します。その他の未使用の fpolicy 構成はすべて削除できます。

fpolicy リストを表示する CLI コマンド:

```
 fpolicy show
```

fpolicy 構成を削除する手順:

```
fpolicy disable -vserver <svmname> -policy-name <policy_name>
fpolicy policy scope delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy event delete -vserver <svmname> -event-name <event_list>
fpolicy policy external-engine delete -vserver <svmname> -engine-name
<engine_name>
```

{空の}

問題: Workload Security を有効にすると、 ONTAP のパフォーマンスに影響が出ます。レイテンシが散発的に

高くなり、IOPS が散発的に低くなります。 これを試してください: ONTAP をWorkload Security とともに使用している場合、 ONTAPで遅延の問題が発生することがあります。これには、次に示すように、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 以降で修正されているため、これらの新しいバージョンのいずれかを使用することを強くお勧めします。

{空の}

問題: データ コレクターに次のエラー メッセージが表示されます:「エラー: 2 回の再試行でコレクターの状態を判別できませんでした。コレクターをもう一度再起動してください (エラー コード: AGENT008)」。 これを試してみてください:

1. 「データ コレクター」ページで、エラーが発生しているデータ コレクターの右までスクロールし、3 つのドット メニューをクリックします。 編集_を選択します。データコレクターのパスワードをもう一度入力してください。 _*Save* ボタンを押してデータ コレクターを保存します。データ コレクターが再起動し、エラーが解決されるはずです。
2. エージェント マシンに十分な CPU または RAM の余裕がないため、DSC が失敗する可能性があります。マシン内のエージェントに追加されているデータ コレクターの数を確認してください。 20 を超える場合は、エージェント マシンの CPU および RAM 容量を増やしてください。 CPU と RAM が増加すると、DSC は自動的に初期化状態になり、その後実行状態になります。サイズガイドをご覧ください"このページ"。

{空の}

問題: SVM モードを選択すると、データ コレクターでエラーが発生します。 これを試してください: SVM モードで接続しているときに、SVM 管理 IP ではなくクラスター管理 IP を使用して接続すると、接続でエラーが発生します。正しい SVM IP が使用されていることを確認してください。

{空の}

問題: アクセス拒否機能が有効になっている場合、データ コレクターに次のエラー メッセージが表示されます:「コネクタはエラー状態です。サービス名: 監査。失敗の理由: SVM test_svm で fpolicy を設定できませんでした。理由: ユーザーは承認されていません。 これを試してください: ユーザーにアクセス拒否機能に必要な REST 権限がない可能性があります。以下の指示に従ってください"このページ"権限を設定します。

権限が設定されたら、コレクターを再起動します。

{空の}

問題: コレクターがエラー状態にあり、次のメッセージが表示されます: コネクタがエラー状態です。 失敗の理由: SVM <SVM 名> で永続ストアを構成できませんでした。 理由: SVM "<SVM Name>" 内のボリューム "<volumeName>" に適したアグリゲートが見つかりません。 理由: 集計 "<aggregateName>" のパフォーマンス情報は現在利用できません。サービス名: 監査。失敗の理由: SVM に永続的ストアを設定できませんでした。<svm name=""></svm>理由:ボリューム「」に適したアグリゲートが<volumename>SVM「<svm name="">」</svm>に</volumename>見つかりません。理由: アグリゲート「」のパフォーマンス情報<aggregatename>は現在使用できません。</aggregatename>数分待ってからもう一度コマンドを実行して

ください。

次の操作を試してください: 数分待ってからコレクターを再起動します。

{空の}

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。

Cloud Volumes ONTAPとAmazon FSx for NetApp ONTAPコレクターの構成

Cloud Volumes ONTAPおよびAmazon FSx for NetApp ONTAP用の Workload Security データコレクターを構成して、クラウド ストレージ インフラストラクチャ全体のファイルとユーザー アクセスを監視します。このガイドでは、AWS にエージェントをデプロイし、クラウド ストレージ インスタンスに接続するための手順を段階的に説明します。

Cloud Volumes ONTAPストレージ構成

Workload Security Agent をホストするための単一ノード/HA AWS インスタンスを構成するには、OnCommand Cloud Volumes ONTAP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 プロバイダーでサポートされています。例: Amazon、Azure、Google Cloud。
- ONTAP Amazon FSx

エージェントマシン構成

エージェント マシンは、クラウド サービス プロバイダーのそれぞれのサブネット内に構成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 でのエージェントのインストール手順です。インストールには、クラウド サービス プロバイダーに応じて、Azure または Google Cloud で同等の手順に従うことができます。

AWS では、次の手順に従って、マシンを Workload Security エージェントとして使用するように設定します。

Workload Security Agent として使用するマシンを設定するには、次の手順に従います。

手順

1. AWS コンソールにログインし、EC2 インスタンス ページに移動して、[インスタンスの起動] を選択します。

2. このページに記載されている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. 割り当てリソースとして *t2.xlarge* (4 個の vCPU と 16 GB の 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 マネージャーを使用して必要な Linux パッケージをインストールします。
   a. ネイティブ Linux パッケージ *wget* および *unzip* をインストールします。

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する

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** に移動し、**Agents** タブをクリックします。
3. *+エージェント*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 インスタンスにエージェント インストール コマンドを貼り付けます。これにより、Workload Securityエージェントがインストールされ、"エージェントの前提条件"満たされます。

詳細な手順については、こ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
データコレクターによって「Workload Security: Amazon FxSN データコレクターのONTAPタイプを判別できませんでした」というエラーが表示されます。お客様は、新しい Amazon FSxN データコレクターを Workload Security に追加できません。エージェントからポート 443 上の FSxN クラスターへの接続がタイムアウトしています。ファイアウォールと AWS セキュリティグループには、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デプロイされており、同じ AWS アカウントに存在します。この同じエージェントは、残りのNetAppデバイス (すべて動作中) への接続と監視にも使用されます。	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。ポートが不明な場合は、すべてのポートを許可します。

ユーザー管理

Workload Security ユーザー 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、ユーザー、ゲストの 4 つのユーザー 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ーアカウントは、ユーザーを作成または変更し、各ユーザーに次のいずれかの Workload Security 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 コレクター、自動応答ポリシー、および Workload Security の API など、すべての Workload Security 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、割り当てることができるのは Workload Security のロールのみです。
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 ロールでは、アラートのステータスを変更したり、メモを追加したり、スナップショットを手動で取得したり、ユーザー アクセスを制限したりできます。
ゲスト	アラートとフォレンジックを表示できます。ゲスト ロールでは、アラート ステータスを変更したり、メモを追加したり、スナップショットを手動で取得したり、ユーザー アクセスを制限したりすることはできません。

手順

1. ワークロードセキュリティにログイン
2. メニューで*管理>ユーザー管理*をクリックします

   Data Infrastructure Insights のユーザー管理ページに転送されます。

3. 各ユーザーに対して希望するロールを選択します。

新しいユーザーを追加するときは、希望するロール (通常はユーザーまたはゲスト) を選択するだけです。

ユーザーアカウントとロールの詳細については、Data Infrastructure Insightsをご覧ください。"ユーザ ロール" ドキュメント。

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

データコレクタを導入する前に、SVM によって生成される NFS および SMB イベントレートを測定することで、最適な Agent マシンのサイジングを決定します。Event Rate Checker スクリプトは、容量制限（Agent あたり最大 50 のデータコレクタ）を理解し、Agent インフラストラクチャが予想されるイベント量を処理して信頼性の高い脅威検出を実現できることを確認するのに役立ちます。

要件：

- クラスターIP
- クラスター管理者のユーザー名とパスワード

このスクリプトを実行するときは、イベント レートを決定する SVM に対してONTAP SVM データ コレクターが実行されていない必要があります。

手順：

1. CloudSecure の指示に従ってエージェントをインストールします。
2. エージェントがインストールされたら、sudo ユーザーとして *server_data_rate_checker.sh* スクリプトを実行します。

```
 /opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
. このスクリプトを実行するには、Linux マシンに _sshpass_
がインストールされている必要があります。インストール方法は 2 つあります。
```

   a. 次のコマンドを実行します。

```
 linux_prompt> yum install sshpass
.. それでも問題が解決しない場合は、Web から Linux マシンに _sshpass_
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入力してください。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、スクリプトは SVM からのイベント レートを出力します。コンソール出力で 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 コレクターは単一の SVM に関連付けることができます。つまり、各データ コレクターは単一の SVM が生成するイベントの数を受信できるようになります。

次の事項に注意してください。

A) この表を一般的なサイズガイドとして使用してください。コア数やメモリ数を増やすと、サポートされるデータ コレクターの数を最大 50 個まで増やすことができます。

エージェントマシン構成	SVMデータコレクターの数	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人のデータ収集者	20Kイベント/秒
4コア、32GB	20人のデータ収集者	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間帯に実行されない場合、またはピークトラフィックを予測することが難しい場合は、イベント レート バッファを 30% に維持します。

B + C は A より小さくなければなりません。そうでない場合、エージェント マシンは監視に失敗します。

つまり、単一のエージェント マシンに追加できるデータ コレクターの数は、次の式に従う必要があります。

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

参照link:concept_cs_agent_requirements.html["エージェントの要件"]追加の前提条件と要件については、ページをご覧ください。

例

それぞれ 1 秒あたり 100、200、300 イベントのイベント レートを生成する 3 つの SVMS があるとします。

次の式を適用します。

```
 (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。

次の場合には、スクリプトによって誤った結果が返される可能性があります。

- 不正な資格情報、IP、または SVM 名が指定されています。
- 同じ名前、シーケンス番号などを持つ既存の fpolicy はエラーになります。
- スクリプトは実行中に突然停止します。

スクリプトの実行例を以下に示します。

```
[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

Workload Security 用にすでに設定されている SVM でこのスクリプトを実行すると、SVM 上の既存の fpolicy 設定がそのまま使用されるのでしょうか、それとも一時的な設定が設定されてプロセスが実行されるのでしょうか?	イベント レート チェッカーは、すでに Workload Security 用に設定されている SVM でも正常に実行できます。影響はないはずです。
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?	○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も長くなりますか?	いいえ。SVM の数が増えても、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?	○スクリプトを編集し、SVM の最大数を 5 から任意の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も長くなりますか?	いいえ。SVM の数が増えても、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イベント レート チェッカー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と、SVM のレイテンシが増加する可能性があります。イベント レート チェッカーの実行中、この増加は一時的なものになります。