IBM QRadar

WinCollect ユーザー・ガイド *V7.2.9*

注記

本書および本書で紹介する製品をご使用になる前に、93 ページの『特記事項』に記載されている情報をお読みください。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典：
IBM QRadar
WinCollect User Guide V7.2.9

発行：
日本アイ・ビー・エム株式会社

担当：
トランスレーション・サービス・センター

目次

WinCollect ユーザー・ガイドについて

本書は、WinCollect エージェントをインストールして構成し、Windows ベースのイベント・ソースからイベントを取得するために必要な情報を提供します。WinCollect は、IBM® Security QRadar® SIEM および IBM QRadar Log Manager によってサポートされています。

対象読者

WinCollect のインストールを担当するシステム管理者は、ネットワーク・セキュリティーの概念とデバイスの構成を十分理解している必要があります。

技術資料

すべての翻訳資料を含む IBM Security QRadar 製品資料を Web で見つけるには、IBM ナレッジ・センター (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome) にアクセスしてください。

QRadar 製品ライブラリー内のその他の技術資料にアクセスする方法について詳しくは、QRadar Support – Assistance 101 (https://ibm.biz/qradarsupport) を参照してください。

お客様サポートへのお問い合わせ

お客様サポートへのお問い合わせ方法については、QRadar Support – Assistance 101 (https://ibm.biz/qradarsupport) を参照してください。

適切なセキュリティーの実践に関する注意事項

IT システムのセキュリティーでは、企業の内部と外部からの不正なアクセスの防止、検出、対応により、システムと情報を保護する必要があります。不正なアクセスにより、情報の改ざん、破壊、盗用、悪用が発生したり、使用しているシステムの損傷や、他のシステムに対する攻撃のための利用を含む悪用につながる可能性があります。完全に安全と見なすことができる IT システムまたは IT 製品は存在せず、また単一の製品、サービス、またはセキュリティー対策が、不適切な使用またはアクセスを防止する上で、完全に有効となることもありません。IBM のシステム、製品およびサービスは、合法かつ包括的なセキュリティーの取り組みの一部となるように設計されており、これらには必ず追加の運用手順が伴います。また、最高の効果を得るために、他のシステム、製品、またはサービスを必要とする場合があります。IBM は、何者かの悪意のある行為または違法行為によって、システム、製品、またはサービスのいずれも影響を受けないこと、またはお客様の企業がそれらの行為によって影響を受けないことを保証するものではありません。

第 1 章 WinCollect

WinCollect は、管理者が Windows ログから QRadar にイベントを転送するために使用できる Syslog イベント・フォワーダーです。 WinCollect では、システムからローカルにイベントを収集することも、イベントについて他の Windows システムをリモートでポーリングするように 構成することもできます。

WinCollect の新機能

WinCollect の各リリースにおける新機能について説明します。

V7.2.9 の新機能

WinCollect V7.2.9 には、以下の機能が含まれています。

- イベント転送フィルタリング
- 1 つのログ・ソースへのイベント転送送信のサポート
- デジタル署名が施されたインストーラー
- イベント・ログ収集でのミリ秒時刻形式の使用
- スペイン語とポーランド語で DHCP に対応
- 状況メッセージで CP に対応
- ファイル・フォワーダーで複数行ログに対応
- パッチ・インストーラーによるインストール時の MMC 要件を削除

V7.2.8 の新機能

WinCollect V7.2.8 には、以下の機能が含まれています。

- Microsoft IIS 用 WinCollect プラグインを使用した Microsoft IIS イベントのリモート・ポーリングに対するサポート。
- Microsoft Exchange Server に対するサポート。
- ロギングを単一のファイルに結合する新しいロギング・サブシステム。
- イベントをチャネルごとに毎秒トラックする新しい統計ファイル (イベント・ログ)。

  統計サブシステムの詳細はこちらを参照してください。
- Windows 2016 Core OS に対するサポート。

WinCollect の概要

WinCollect は、管理者が Windows ログから QRadar にイベントを転送するために使用できる Syslog イベント・フォワーダーです。 WinCollect では、システムからローカルにイベントを収集することも、イベントについて他の Windows システムをリモートでポーリングするように 構成することもできます。

WinCollect は、Windows イベントを収集するための数多くあるソリューションの 1 つです。WinCollect に代わるものについて詳しくは、「IBM Security QRadar DSM 構成ガイド」を参照してください。

WinCollect の機能

WinCollect が Windows イベント ログ API を使用してイベントを収集し、それらのイベントを WinCollect が QRadar に送信します。

注 : 管理対象デプロイメントは、クラウド環境の QRadar ではサポートされません。 IBM QRadar on Cloud を使用するお客様は、スタンドアロン WinCollect エージェントを使用する必要があります。

WinCollect 管理対象デプロイメント

WinCollect 管理対象デプロイメントには、モニター対象の Windows ホストにインストールされた WinCollect エージェントと情報を共有する QRadar アプライアンスがあります。Windows ホストは、それ自体、ローカル・ホスト、リモート Windows ホストのいずれからも情報を収集できます。リモート・ホストには WinCollect ソフトウェアはインストールされていません。WinCollect ソフトウェアがインストールされている Windows ホストがリモート・ホストに対してポーリングを行い、イベント情報を QRadar に送信します。

注 : 管理対象デプロイメントは、クラウド環境の QRadar ではサポートされません。 IBM QRadar on Cloud を使用するお客様は、スタンドアロン WinCollect エージェントを使用する必要があります。

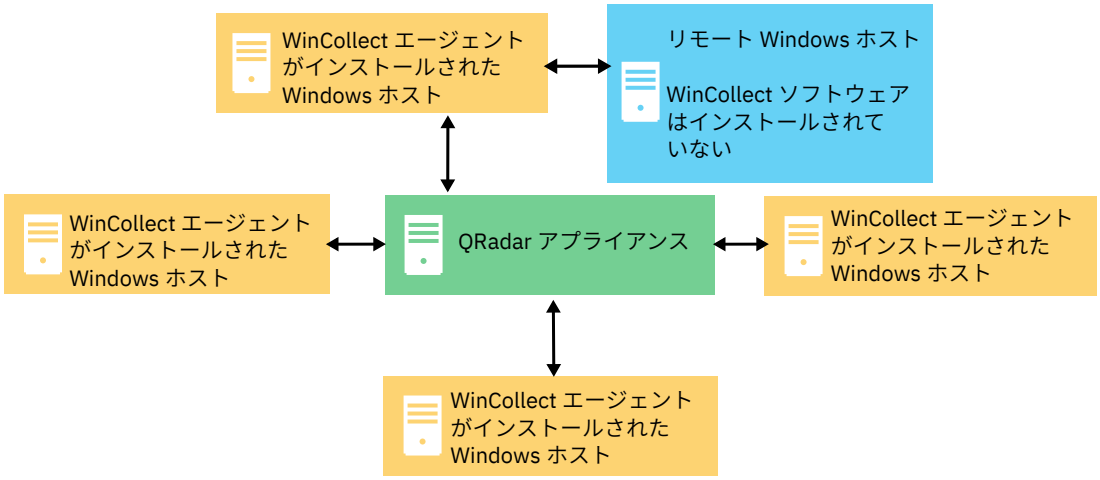


図 *1. WinCollect* 管理対象デプロイメントの例

重要 :

1. 管理対象デプロイメントでは、Windows ホストにインストールされた WinCollect エージェントは、QRadar コンソール、イベント・コレクター、またはイベント・プロセッサーで管理できます。
2. WinCollect 管理対象デプロイメントは、QRadar on Cloud ではサポートされていません。

管理対象デプロイメントにおいて、WinCollect は、コンソールおよび管理対象ホスト 1 台につき最大 500 の Windows エージェントに対応するように設計されています。例えば、コンソール、イベント・プロセッサー (Event Processor)、および Event Collector で構成されるデプロイメントがある場合、それぞれが最大 500 の Windows エージェントに対応できるため、合計 1,500 のエージェントに対応できます。コンソールまたは管理対象ホスト 1 台につき 500 を超える Windows エージェントをモニターする場合は、WinCollect スタンドアロン・デプロイメントを使用してください。

詳しくは、17 ページの『WinCollect のスタンドアロン・インストール』を参照してください。

WinCollect 管理対象デプロイメントには以下の機能があります。

- QRadar コンソールまたは管理対象ホストからの集中管理。
- インストール時のローカル・ログ・ソースの自動生成。
- イベントをもらさず収集するためのイベント・ストレージ。
- Microsoft サブスクリプションから転送されたイベントの収集。
- XPath 照会または除外フィルターを使用したイベントのフィルタリング。
- 仮想マシンのインストールをサポート。
- コンソールからリモート WinCollect エージェントにソフトウェア更新を送信可能。ネットワーク内にエージェントを再インストールする必要がありません。
- 設定したスケジュールに従ってイベントを転送 (ストア・アンド・フォワード)。

WinCollect スタンドアロン・デプロイメント

500 を超えるエージェントから Windows イベントを収集する必要がある場合は、WinCollect スタンドアロン・デプロイメントを使用します。スタンドアロン・デプロイメントとは、WinCollect ソフトウェアがインストールされている、非管理モードの Windows ホストです。Windows ホストは、それ自体、ローカル・ホスト、リモート Windows ホストのいずれからも情報を収集できます。リモート・ホストには WinCollect ソフトウェアはインストールされていません。WinCollect ソフトウェアがインストールされている Windows ホストがリモート・ホストに対してポーリングを行い、イベント情報を QRadar に送信します。500 を超える Windows エージェントを構成する際の時間を節約するために、IBM Endpoint Manager などのソリューションを使用できます。自動化は、スタンドアロン・インスタンスの管理に役立ちます。

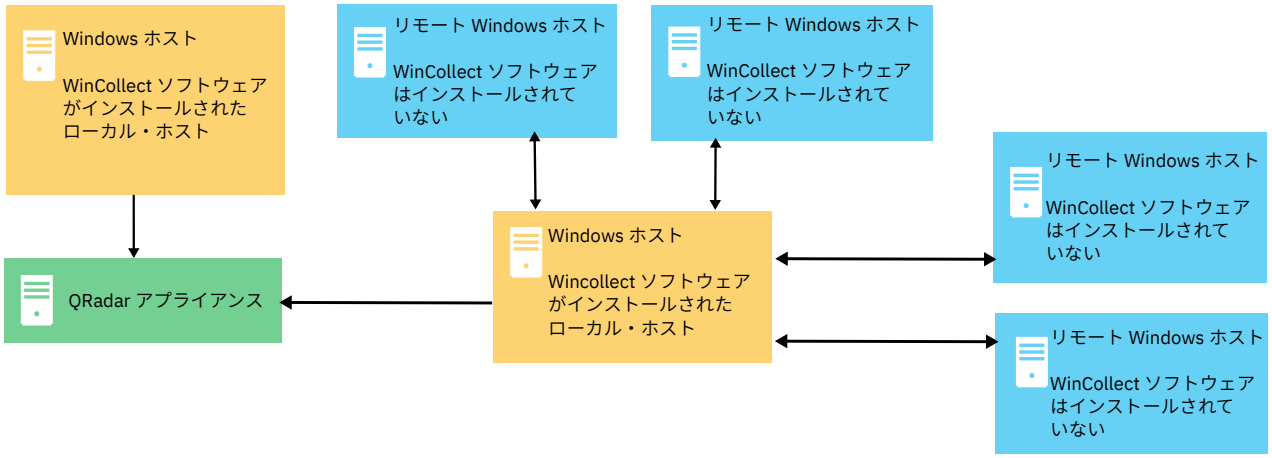


図 *2. WinCollect* スタンドアロン・デプロイメントの例

スタンドアロン WinCollect をデプロイして、1 つの Windows ホストでイベント・データを統合することもできます。WinCollect はこのホストでイベントを収集して QRadar に送信します。

スタンドアロン WinCollect モードには以下の機能があります。

- WinCollect 構成コンソールを使用した各 WinCollect エージェントの構成。
- ソフトウェア更新インストーラーを使用した WinCollect ソフトウェアの更新。
- イベントをもらさず収集するためのイベント・ストレージ。
- Microsoft サブスクリプションから転送されたイベントの収集。
- XPath 照会または除外フィルターを使用したイベントのフィルタリング。
- 仮想マシンのインストールをサポート。
- TLS Syslog を使用した QRadar へのイベントの送信。
- エージェントのインストール時にローカル・ログ・ソースを自動的に作成。

管理対象およびスタンドアロン WinCollect デプロイメントの機能

管理対象またはスタンドアロン WinCollect エージェントの使用時にどの機能を使用できるか理解するために、次の表を確認してください。

表 *1.* 管理対象 *WinCollect* とスタンドアロン *WinCollect* の機能の比較

機能	管理対象 WinCollect	スタンドアロン WinCollect
QRadar コンソールまたは管理対象ホストからの集中管理。	あり	なし
インストール時のローカル・ログ・ソースの自動生成。	あり	あり
イベントをもらさず収集するためのイベント・ストレージ。	あり	あり

表 1. 管理対象 *WinCollect* とスタンドアロン *WinCollect* の機能の比較 (続き)		
機能	**管理対象 WinCollect**	**スタンドアロン WinCollect**
Microsoft サブスクリプションから転送されたイベントの収集。	あり	あり
XPath 照会または除外フィルターを使用したイベントのフィルタリング。	あり	あり
仮想マシンのインストールをサポート。	あり	あり
QRadar コンソールがソフトウェア更新を WinCollect エージェントに送信。	あり	なし
設定したスケジュールに従ってイベントを転送 (ストア・アンド・フォワード)。	あり	なし
WinCollect 構成コンソールを使用した各 WinCollect エージェントの構成。	なし	あり
ソフトウェア更新インストーラーを使用した WinCollect ソフトウェアの更新。	なし	あり
QRadar on Cloud で使用可能。	なし	あり
オンプレミス QRadar で使用可能。	あり	あり

管理対象 WinCollect デプロイメントのセットアップ

管理対象デプロイメントの場合は、以下の手順を実行します。

1. 管理対象 WinCollect の前提条件、使用するポート、必要なハードウェア、アップグレード方法を理解します。詳しくは、7 ページの『第 2 章 WinCollect のインストールの前提条件』を参照してください。
2. WinCollect アプリケーションを QRadar コンソールにインストールします。詳しくは、13 ページの『QRadar アプライアンスでの WinCollect アプリケーションのインストールとアップグレード』を参照してください。
3. 管理対象 WinCollect エージェントが QRadar アプライアンスとデータを交換できるようにするために、認証トークンを作成します。詳しくは、14 ページの『WinCollect エージェントの認証トークンの作成』を参照してください。
4. ログ・ソース・データの転送宛先ホストを構成します。詳しくは、35 ページの『宛先の追加』を参照してください。
5. 管理対象 WinCollect エージェントを Windows ホストにインストールします。詳しくは、以下のオプションのいずれかを参照してください。
   - 21 ページの『WinCollect エージェントを Windows ホストにインストールする』
   - 25 ページの『コマンド・プロンプトからの WinCollect エージェントのインストール』または
   - 33 ページの『WinCollect エージェントの手動による追加』
6. 転送されたイベントまたはイベント・サブスクリプションを構成する場合は、49 ページの『WinCollect エージェントに対する Windows イベント・サブスクリプション』を参照してください。
7. 既存のログ・ソース UI を使用して、単一の WinCollect エージェントがリモート・ポーリングするログ・ソースを一括追加する場合は、83 ページの『リモート・イベント収集用のバルク・ログ・ソース』を参照してください。
8. WinCollect ログ・ソースをチューニングします。詳しくは、54 ページの『Windows ログ・ソースのパラメーター』の『Event Rate Tuning Profile』パラメーターを参照してください。
9. いずれかで障害が発生した場合に備えて、管理対象 WinCollect エージェントが複数の QRadar 宛先に複数の宛先にイベントを送信するようにする場合は、15 ページの『WinCollect エージェントに複数の宛先を追加する』を参照してください。

WinCollect スタンドアロン・デプロイメントのセットアップ

スタンドアロン・デプロイメントの場合は、以下を実行します。

1. スタンドアロン WinCollect の前提条件、使用するポート、必要なハードウェア、アップグレード方法を理解します。詳しくは、7 ページの『第 2 章 WinCollect のインストールの前提条件』を参照してください。
2. スタンドアロン WinCollect エージェントを Windows ホストにインストールします。詳しくは、21 ページの『WinCollect エージェントを Windows ホストにインストールする』を参照してください。
3. エージェントに新しいログ・ソースを追加する場合、または既存のログ・ソースを変更する場合は、WinCollect スタンドアロン構成コンソールをインストールします。 詳しくは、18 ページの『構成コンソールのインストール』または 19 ページの『サイレント・モードでの WinCollect ソフトウェアのインストール、アップグレード、およびアンインストール』を参照してください。
4. Windows ホストが Windows イベントを送信する宛先を構成します。詳しくは、38 ページの『WinCollect 構成コンソールに宛先を追加する』を参照してください。
5. スタンドアロン WinCollect エージェントでリモート・ポーリングを使用して他のデバイスからイベントを収集する場合、WinCollect がリモート・デバイスにログインできるようにするために、WinCollect スタンドアロン構成コンソールで資格情報を作成します。詳しくは、38 ページの『WinCollect 資格情報の作成』を参照してください。
6. スタンドアロン WinCollect エージェントにログ・ソースを追加する場合、WinCollect スタンドアロン構成コンソールを使用して行います。 詳しくは、39 ページの『WinCollect 構成コンソールにデバイスを追加する』を参照してください。

MSEVEN6 プロトコル

MSEVEN6 は、イベント・ログから、タスク、キーワード、命令コードなど、多くの情報を収集する Microsoft のイベント・プロトコルです。また、他のイベント・プロトコルよりも優れたメッセージ・フォーマットを備えています。

MSEVEN プロトコルではポート 445 が使用されます。NETBIOS のポート (137 から 139) を、ホスト名の解決に使用できます。WinCollect エージェントが MSEVEN6 を使用してリモートのイベント・ログをポーリングする場合、リモート・コンピューターとの最初の通信はポート 135 (動的ポートマッパー) を通じて行われ、ここで接続が動的ポートに割り当てられます。動的ポートのデフォルトのポート範囲は、ポート 49152 からポート 65535 ですが、サーバー・タイプによって異なる場合があります。例えば、Microsoft Exchange Server のデフォルトのポート範囲は 6005 から 58321 です。

XPath 照会では、常に MSEVEN6 イベント・プロトコルが使用されます。

管理対象モードで、「**イベント・ログ・ポーリング・プロトコル (Event Log Poll Protocol)**」フィールドを編集し、目的のプロトコルを選択することで、プロトコルを変更できます。アップグレードの場合、アップグレード元の WinCollect のバージョンによっては、ログ・ソースで MSEVEN が継続して使用されます。目的のプロトコルに対して複数のログ・ソースを構成するには、Log Source Management アプリケーションを使用します。

スタンドアロン WinCollect デプロイメントでは、グローバルのデフォルト・イベント・ログ・ポーリング・プロトコルを設定できます。デフォルト値は **MSEVEN6** です。 グローバルのデフォルト・イベント・ログ・ポーリング・プロトコルを使用するように単一の Microsoft Windows イベント・ログ・デバイスを構成するには、そのデバイスの「**基本構成**」ページで「**デフォルト**」を選択します。グローバルのデフォルトを使用しない場合は、「**MSEVEN6**」または「**MSEVEN**」を選択して、グローバルのデフォルト・イベント・ログ・ポーリング・プロトコルをオーバーライドします。

スタンドアロン WinCollect デプロイメントでは、イベント・ログのタイム・スタンプにミリ秒を含めることができます。このオプションは、MSEVEN6 プロトコルを使用しているスタンドアロンの WinCollect デプロイメントにのみ適合しています。 MSEVEN プロトコルではサポートされていません。

第 2 章 WinCollect のインストールの前提条件

WinCollect エージェントをインストールする前に、ご使用のデプロイメント環境がインストール要件を満たしているか検証する必要があります。

サポートされるバージョン

管理者は、IBM WinCollect のサポートされるソフトウェア・バージョンが、最新バージョン (n) と最新バージョンより 1 つ前のバージョン (n-1) であることを認識している必要があります。つまり、WinCollect の 2 つの最新バージョンが、オープンされたサポート・チケット (ケース) で QRadar サポートがフル・サポートを提供するバージョンです。WinCollect の古いバージョンを使用しているお客様は、最小のベスト・エフォートのサポートを受けることになります。問題を防ぐには、新しいバージョンが IBM Fix Central に投稿されたときに、管理者が WinCollect のデプロイメントを常に更新することが重要です。

注 : WinCollect は、ネットワークアドレス変換 (NAT) を使用している Windows サーバーにインストールされたエージェントをサポートしません。管理対象エージェントと同じ NAT 環境にイベント・コレクターを配置した場合、そのエージェントでは、イベント・コレクターを構成サーバーや、状況サーバーとして使用することも、イベントの送信に使用することもできます。ただし、そのイベント・コレクターは NAT を使用するように構成されている必要があります。

WinCollect エージェントの分散オプション

WinCollect エージェントは、リモート収集構成内に分散させることも、ローカル・ホストにインストールすることもできます。

ローカル収集
その WinCollect エージェントがインストールされているホストのイベントのみを収集します。この収集方式は、ビジー状態であるか、または制限付きリソース (ドメイン・コントローラーなど) のある Windows ホストで使用できます。

重要 : ローカル収集の方がリモート収集よりも安定するため、QRadar サポートでは、ドメイン・コントローラーおよびその他の高 EPS サーバーでのローカル収集を推奨しています。潜在的な高 EPS サーバーでログをリモート・ポーリングしている場合、QRadar サポートが、サーバーにエージェントをローカル・インストールするようユーザーに要求することがあります。

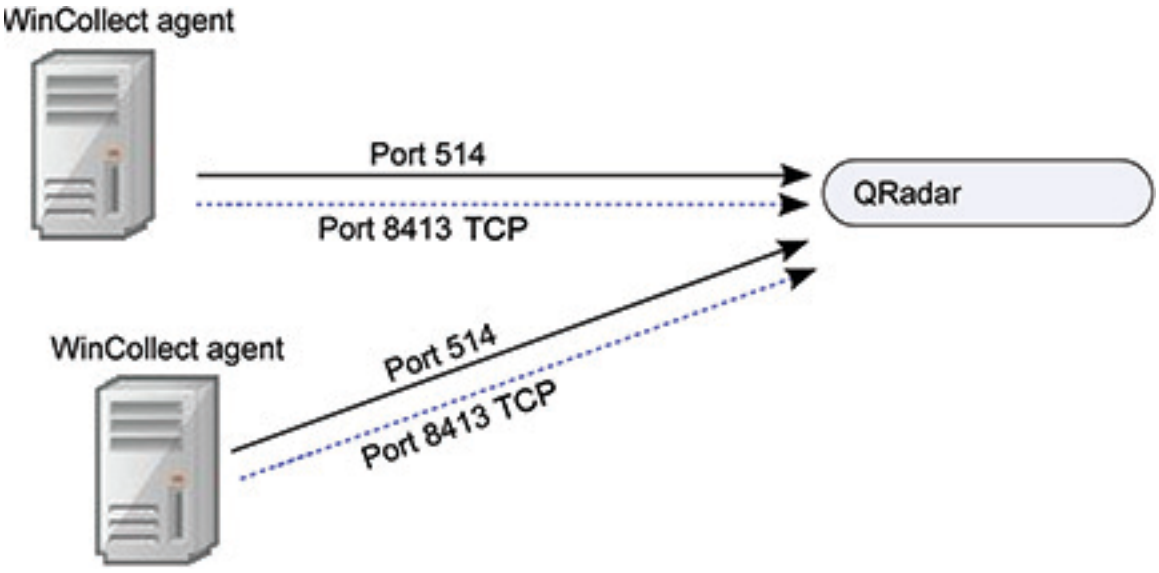


図 *3. WinCollect* エージェントのローカル収集

リモート収集

WinCollect エージェントは単一のホストにインストールされ、複数の Windows システムからイベントを収集します。リモート収集を使用すると、モニター可能な Windows ログ・ソースの数を簡単に調整できます。

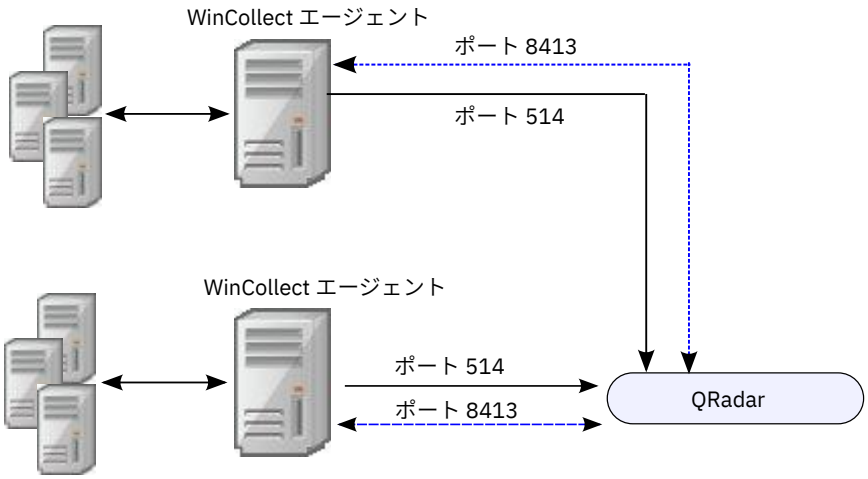


図 *4. WinCollect* エージェントのリモート収集

WinCollect エージェントと QRadar との間の通信

WinCollect エージェントと QRadar ホストとの間のデータ通信、および WinCollect エージェントとそれらがリモートでポーリングを実行するホストとの間のデータ通信には、開いているポートが必要です。

QRadar コンソールおよび Event Collector への WinCollect エージェントの通信

すべての WinCollect エージェントは、QRadar へのイベントの転送と、更新された情報の要求を行う際に、QRadar コンソールおよび Event Collector と通信します。管理対象 WinCollect エージェントは、更新されたコードと構成の変更の要求と受信も行います。 QRadar Event Collector と WinCollect エージェントの間にあるファイアウォールが以下のポートでのトラフィックを必ず許可するようにしてください。

ポート 8413

このポートは、コードと構成の更新を要求および受信する WinCollect エージェントを管理するために必要です。トラフィックは、常に WinCollect エージェントから開始されますが、エージェントが更新を受信するために、このポートは双方向で開いておく必要があります。このトラフィックは TCP を使用して送信され、通信はコンソールの公開鍵とエージェントの `ConfigurationServer.PEM` ファイルを使用して暗号化されます。

ポート 514

このポートは、syslog イベントを QRadar に転送するために WinCollect エージェントによって使用されます。TCP または UDP を使用してイベントを提供するように WinCollect ログ・ソースを構成することができます。WinCollect ログ・ソースごとに、どちらの伝送プロトコルが必要かを決めることができます。ポート 514 のトラフィックは、常に WinCollect エージェントから開始されます。

リモートで Windows イベント・ソースをポーリングする WinCollect エージェント

他の Windows オペレーティング・システムをリモートでポーリングする WinCollect エージェントでは、追加のポートを開く必要があります。これらのポートは、WinCollect エージェント・コンピューター、およびリモート・ポーリング対象のコンピューターで開く必要がありますが、QRadar アプライアンスでは開く必要がありません。以下の表に使用されるポートを示します。

表 *2. WinCollect* のリモート・ポーリングでのポートの使用

ポート	プロトコル	使用
135	TCP	Microsoft エンドポイント マッパー

表 2. *WinCollect* のリモート・ポーリングでのポートの使用 *(続き)*		
ポート	**プロトコル**	**使用**
137	UDP	NetBIOS ネーム・サービス
138	UDP	NetBIOS データグラム・サービス
139	TCP	NetBIOS セッション・サービス
445	TCP	Windows 共有を使用するファイル転送のための Microsoft ディレクトリー・サービス
49152 – 65535 **注 :** Exchange Server は、デフォルトではポート範囲 6005 から 58321 用に構成されています。	TCP	TCP/IP 用のデフォルトの動的ポート範囲

MSEVEN プロトコルではポート 445 が使用されます。NETBIOS のポート (137 から 139) は、ホスト名の解決に使用できます。WinCollect エージェントが MSEVEN6 を使用してリモートのイベント・ログをポーリングする場合、リモート・マシンとの最初の通信はポート 135 (動的ポートマッパー) を通じて行われ、ここで接続が動的ポートに割り当てられます。動的ポートのデフォルトのポート範囲は、ポート 49152 からポート 65535 ですが、サーバー・タイプによって異なる場合があります。 例えば、Exchange Server は、デフォルトではポート範囲 6005 から 58321 用に構成されています。

これらの動的ポート上でのトラフィックを許可するには、ポーリング対象の Windows サーバーで以下の 2 つのインバウンド・ルールを有効化し、許可します。

- リモート イベントのログ管理 (RPC)
- リモート イベント ログ管理 (RPC-EPMAP)

重要 : QRadar に送信されるイベントの数を制限するために、管理者は、イベント ID またはプロセスに基づいて、イベントの除外フィルターを使用できます。WinCollect フィルタリングについて詳しくは、『WinCollect Event Filtering』(http://www.ibm.com/support/docview.wss?uid=swg21672656) を参照してください。

関連概念

5 ページの『MSEVEN6 プロトコル』

MSEVEN6 は、イベント・ログから、タスク、キーワード、命令コードなど、多くの情報を収集する Microsoft のイベント・プロトコルです。また、他のイベント・プロトコルよりも優れたメッセージ・フォーマットを備えています。

Windows でのリモート・ログ管理の有効化

リモート・ログ管理は、リモートで他の Windows オペレーティング・システムをポーリングするようにログ・ソースが構成されている場合にのみ有効にすることができます。Windows 7、Windows Server 2008、Windows 2008 R2、または Windows 2012 R2 で、XPath 照会に対するリモート・ログ管理を有効にすることができます。

手順

1. ご使用のデスクトップで、「**スタート**」 > 「**コントロール パネル**」を選択します。
2. 「**システムとセキュリティ**」アイコンをクリックします。
3. 「**Windows ファイアウォールによるプログラムの許可**」をクリックします。
4. プロンプトが出されたら、「**続行**」をクリックします。
5. 「**設定の変更 (Change Settings)**」をクリックします。
6. 「**許可されたプログラムおよび機能**」ペインで、「**リモート イベントのログ管理**」を選択します。

ご使用のネットワークによっては、他のネットワーク・タイプの修正または選択が必要になることがあります。

7.「**OK**」をクリックします。

WinCollect ホストのハードウェア要件とソフトウェア要件

WinCollect エージェントをホストする Windows ベースのコンピューターが、ハードウェアおよびソフトウェアの最小要件を満たしていることを確認してください。

ハードウェア/仮想マシンの要件

以下の表に、ローカル収集を行う場合のハードウェアの最小要件を示します。

表 *3. WinCollect* を使用してローカル収集を行う場合のハードウェア/仮想マシンの要件

要件	説明
メモリー	1 イベント/秒 (EPS) 以下: 12.5 MB 100 EPS 以下: 27 MB 1,000 EPS 以下: 97 MB 5,000 EPS 以下: 201 MB
プロセッサー	Intel Core i3 または同等品
使用できるプロセッサーのリソース	約 20% (CPU、EPS、およびポーリング対象のエンドポイント数によって異なる)
ディスク容量	ソフトウェア用に 100 MB、さらにファイル用に最大 100 MB。 イベントをディスクに保管する場合、最大 6 GB 必要になることがあります。

注 : WinCollect の CPU およびメモリーに対する負荷は、1 秒間に処理されるイベントの数など、複数の要因によって決まります。

以下の表に、テスト環境で WinCollect によって使用されるリソースを、各種ハードウェア構成および EPS カウントごとに示します。

表 *4. WinCollect* のテスト環境の比較 *(*ローカル・ポーリング*)*

プロファイル	タイプ	OS	RAM	コア数	平均 EPS	使用 RAM	平均 CPU 使用率
高 EPS	VM	Windows 2012 Server	8 GB	8	5,000	200 MB	17%
中程度の EPS	VM	Windows 2012 Server	8 GB	8	300	25 MB	1.3%
低 EPS	Notebook	Windows 7	32 GB	8	<1	10 MB	0.5%

以下の表に、リモート収集を行う場合のハードウェアの最小要件を示します。

表 5. *WinCollect* を使用してリモート収集を行う場合のハードウェア/仮想マシンの要件	
要件	**説明**
メモリー	5 エンドポイント以下: 80 MB 250 エンドポイント以下: 293 MB 500 エンドポイント以下: 609 MB
プロセッサー	Intel Core i3 または同等品
使用できるプロセッサーのリソース	約 20% (CPU、EPS、およびポーリング対象のエンドポイント数によって異なる)
ディスク容量	ソフトウェア用に 100 MB、さらにファイル用に最大 100 MB。 イベントをディスクに保管する場合、最大 6 GB 必要になることがあります。

注 : WinCollect の CPU およびメモリーに対する負荷は、1 秒間に処理されるイベントの数や、ポーリング対象のリモート・エンドポイントの数など、複数の要因によって異なります。

表 6. *WinCollect* のテスト環境の比較 *(*リモート・ポーリング*)*								
プロファイル	**タイプ**	**OS**	**RAM**	**コア数**	**ポーリング対象エンドポイント数**	**平均 EPS**	**使用 RAM**	**平均 CPU 使用率**
高 EPS、デバイス少数	VM	Windows 2012 Server	12 GB	8	6	3,000	78 MB	6.5%
中程度の EPS およびデバイス数	VM	Windows 2016 Server	12 GB	4	250	2,500	290 MB	14%
高 EPS、デバイス多数	VM	Windows 2016 Server	16 GB	8	500	5,000	605 MB	10.75%

ソフトウェア要件

以下の表にソフトウェア要件を示します。

表 7. ソフトウェア要件	
要件	**説明**
オペレーティング・システム	Windows Server 2019 (Core を含む) Windows Server 2016 (Core を含む) Windows Server 2012 (Core を含む) Windows Server 2008 (Core を含む) Windows 10 Windows 8 Windows 7

表 7. ソフトウェア要件 (続き)	
要件	**説明**
配布	各 Windows ホストに 1 つの WinCollect エージェント
インストールのために必要なユーザー・ロール権限	管理者またはローカル管理者 リモート収集については、管理者権限は必要ありません。

重要 : WinCollect は、Microsoft がサポートを終了した Windows のバージョンではサポートされていません。ソフトウェアの延長サポート終了日が過ぎていても、製品が期待どおりに機能することがあります。ただし、IBM は、古いオペレーティング・システムで発生した WinCollect の問題を解決するために、コードまたは脆弱性のフィックスを作成することはありません。例えば、Microsoft Windows Server 2003 R2 および Microsoft Windows XP は、「延長サポート終了日」を過ぎたオペレーティング・システムです。この発表について質問がある場合は、IBM QRadar Collecting Windows Events (`WMI/ALE/WinCollect`) フォーラムで相談できます。詳しくは、https://support.microsoft.com/en-us/lifecycle/search (https://support.microsoft.com/en-us/lifecycle/search) を参照してください。

WinCollect エージェントをアップグレードするための前提条件

WinCollect エージェントをアップグレードする 前に、ご使用のソフトウェアがバージョン要件を満たしていることを確認してください。

WinCollect のバージョンと QRadar のソフトウェアのバージョン

インストールされている WinCollect のバージョンは、実行している QRadar のバージョンによって異なります。

表 8. ソフトウェアのバージョン・マトリックス		
QRadar のバージョン	**WinCollect の最小バージョン**	**RPM の最小バージョン**
V7.2.8	WinCollect 7.2.2-2	AGENT-WINCOLLECT-7.2-1018607.noarch
QRadar V7.3.x	WinCollect 7.2.5	AGENT-WINCOLLECT-7.3-20161123160813.noarch

インストール済み WinCollect エージェントのバージョンの確認する

以下の手順を実行することで、インストールされている WinCollect エージェントのバージョンを確認できます。

1. QRadar で、「**ヘルプ**」 > 「**バージョン情報**」を選択します。
2. 「**追加リリース情報**」リンクを選択します。
3. WinCollect エージェントのリリースを確認する場合は、ssh を使用して、root ユーザーとして QRadar コンソールにログインし、以下のコマンドを実行します。

```
yum list all | grep -i AGENT-WINCOLLECT
```

第 3 章 WinCollect のインストール

WinCollect エージェントは、QRadar によって管理される環境内にインストールすることも、スタンドアロン・エージェントとしてインストールすることも、あるいはこれらの両方を組み合わせてインストールすることもできます。

これで以下のインストールが可能になります。

管理対象 WinCollect の インストール

管理対象 WinCollect を使用するには、 WinCollect Agent SF Bundle をダウンロードして QRadar コンソールにインストールし、認証トークンを作成してから、イベントの収集対象になる各 Windows ホストに管理対象 WinCollect エージェントをインストールします。また、他の Windows ホストからのイベントのリモート収集に使用する Windows ホスト上に管理対象 WinCollect エージェントをインストールすることもできます。

注 : IBM QRadar on Cloud で使用されるデプロイメント・タイプであるスタンドアロン WinCollect では、WinCollect Agent SFS Bundle をダウンロードして QRadar コンソールにインストールする必要はなく、また WinCollect 認証トークンを作成する必要もありません。

QRadar アプライアンスでの WinCollect アプリケーションのインストールとアップグレード

QRadar ユーザー・インターフェースから WinCollect エージェントのデプロイメントを管理するには、最初に WinCollect Agent SFS Bundle を使用して、QRadar コンソールを WinCollect のサポートされているバージョンにアップグレードする 必要があります。このバンドルには、QRadar と Windows ホスト上の管理対象 WinCollect エージェントの通信を可能にするために必要なプロトコルが含まれます。SFS Bundle の新しいバージョンを QRadar コンソールにインストールすることで、QRadar コンソールと管理対象 WinCollect エージェントの両方を WinCollect の新しいバージョンにアップグレードできます。

このタスクについて

重要 :

- WinCollect バージョン v7.0 から v7.2.2 までのアップグレードについて詳しくは、www.ibm.com/support (http://www-01.ibm.com/support/docview.wss?uid=swg21698127) を参照してください。
- WinCollect v7.2.6 以降が QRadar コンソールにインストールされている場合、QRadar を v7.2.8 から v7.3.0 以降にアップグレードすると、QRadar 上の WinCollect のバージョンが v7.2.5 に戻ります。Windows ホストで実行されている管理対象 WinCollect エージェントは現行バージョンのままで、既存の構成情報を使用して、引き続きイベントを QRadar に送信します。ただし、コードや構成の更新は受信しなくなります。QRadar のアップグレード後、現在のエージェントのバージョンと同じか、それよりも新しいバージョンの WinCollect Agent SFS Bundle を QRadar コンソールに再インストールする必要があります。

QRadar コンソールをアップグレードした後、自動更新の受信が有効になっている管理対象 WinCollect エージェントが、次の構成ポーリング間隔で WinCollect の新しいバージョンに自動的にアップグレードされます。新しい WinCollect エージェント・ファイルのダウンロードが可能である場合、エージェントは、更新をダウンロードしてインストールし、必要なサービスを再始動します。イベントはディスクにバッファリングされているため、WinCollect エージェントを更新する際にイベントが失われることはありません。Windows ホスト上の WinCollect サービスが再始動すると、イベント収集の転送が続行されます。

重要 : QRadar をコンソールに再インストールする場合、WinCollect を正常に機能させるには、あらかじめ既存の WinCollect エージェント・インストール済み環境で `Program Files/IBM/WinCollect/config/ConfigurationServer.PEM` ファイルを削除しておく必要があります。

手順

1. WinCollect Agent SFS Bundle インストール・ファイルを IBM Web サイト (http://www.ibm.com/support) からダウンロードします。
2. root ユーザーとして QRadar にログインします。
3. 初期インストールで、/storetmp ディレクトリーおよび /media/updates ディレクトリーが存在しない場合は作成します。次のコマンドを入力します。

```
mkdir /media/updates
mkdir /storetmp
```

4. WinSCP などのプログラムを使用して、ダウンロードした SFS ファイルを QRadar コンソールの /storetmp にコピーします。
5. /storetmp ディレクトリーに移動するために、次のコマンドを入力します。 cd /storetmp
6. SFS ファイルをマウントするために、次のコマンドを入力します。mount -t squashfs -o loop *<Installer_file_name.sfs>* /media/updates

   例: mount -t squashfs -o loop 720_QRadar_wincollectupdate-7.2.0.xxx.sfs /media/updates
7. /media/updates ディレクトリーに移動するために、次のコマンドを入力します。cd /media/updates
8. WinCollect をインストールするために、次のコマンドを入力し、プロンプトに従います。./installer
9. QRadar の管理設定で、「**拡張**」 > 「**すべての構成のデプロイ**」をクリックします。
10. QRadar v7.3.1 以降を使用している場合は、「**拡張**」 > 「**イベント収集サービスの再始動**」をクリックします。
11. WinCollect エージェントがリモート更新を受け入れるように構成されていることを確認します。
    a) QRadar にログインします。
    b) ナビゲーション・メニューで、「**データ・ソース (Data Sources)**」をクリックします。
    c) WinCollect アイコンをクリックします。
    d)「**自動更新は有効**」列を確認し、値が「False」である WinCollect エージェントを選択します。
    e)「**自動更新の有効化/無効化**」をクリックします。

タスクの結果

自動更新が有効になっている管理対象 WinCollect エージェントが更新され、再始動します。管理対象エージェントの更新にかかる時間は、エージェントの構成ポーリング間隔と、コンソールとエージェント間のネットワーク接続の速度によって異なります。

関連タスク

WinCollect エージェントを Windows ホストにインストールする

コマンド・プロンプトからの WinCollect エージェントのインストール

無人インストールでは、コマンド・プロンプトから WinCollect エージェントをインストールできます。WinCollect エージェントを複数のリモート・システムに同時にデプロイするには、サイレント・インストール・オプションを使用します。

WinCollect エージェントの認証トークンの作成

IBM Security QRadar と相互作用するサード・パーティー・アプリケーションまたは外部アプリケーションには、認証トークンが必要です。管理対象 WinCollect エージェントをネットワーク内にインストールする前に、認証トークンを作成する必要があります。

認証トークンは、スタンドアロン WinCollect エージェント (IBM QRadar on Cloud で使用されるエージェントなど) には不要ですが、すべての管理対象 WinCollect エージェントでは認証トークンを使用する必要があります。

認証トークンを使用することで、管理対象 WinCollect エージェントは、QRadar アプライアンスとデータを交換できます。QRadar とイベントをやり取りするすべての管理対象 WinCollect エージェントで使用する認証トークンを 1 つ作成します。認証トークンの有効期限が切れると、WinCollect エージェントは、ログ・ソースの構成変更やコードの更新を受信できなくなります。

このタスクについて

注 : この機能は、IBM QRadar on Cloud では使用できません。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・メニューで、「**システム構成**」をクリックします。
3. 「**許可サービス**」アイコンをクリックします。
4. 「**許可サービスの追加**」をクリックします。
5. 「**許可サービスの管理**」ウィンドウで、パラメーターを構成します。

表 *9.* **「許可サービスの追加」**のパラメーター

パラメーター	**説明**
サービス名	名前は、最大 255 文字までの長さにできます (例えば、`WinCollect Agent`)。
ユーザー・ロール (User Role)	「**WinCollect**」を選択します。 ユーザー・ロールについて詳しくは、「*IBM Security QRadar SIEM* 管理ガイド」を参照してください。
有効期限 (Expiry)	「**期限なし**」を選択します。

6. 「**サービスの作成**」をクリックします。
7. トークン値を記録します。

WinCollect エージェントに複数の宛先を追加する

QRadar アプライアンスで障害が発生した場合に備えて、管理対象 WinCollect のデプロイメント環境で、Windows イベントの宛先として IBM QRadar アプライアンスを追加します。

始める前に

WinCollect エージェントに追加する宛先を作成する必要があります。35 ページの『宛先の追加』を参照してください。

このタスクについて

WinCollect エージェント用に作成した各宛先には、イベント用の専用ディスク・キャッシュが必要です。サイト A で障害が発生し、サイト B が「ターゲット外部宛先」として構成されている場合、サイト B がイベントの受信を継続し、サイト A はイベントをディスクに保管します。両方のサイトで障害が発生した場合は、両方のシステムが個別のディスク・キューにイベントを個別にキャッシュします。エージェントは、各ログ・ソースの接続が回復すると、新しいイベントとキャッシュされたイベント (イベントの数が多すぎるために、または接続の問題のためにキャッシュされたイベント) のバランスを取りながらイベントの送信を実行します。

複数の宛先を使用していることが原因でデプロイメント環境内のログ・ソースの数が多い場合は、デフォルトのディスク・スペースを増やしてください。各エージェントは、6 GB のディスク・スペースを使用してイベントをキャッシュするように構成されています。ただし、50 以上のログ・ソースが存在し、各ログ・ソースが宛先にイベントを送信する場合は、ネットワーク・セグメントで障害が発生すると、各ログ・ソースは、ターゲット内部宛先とターゲット外部宛先上の同じキャッシュに 2 つのイベント・セットを書き込みます。そのため、不安定なセグメントや、停止することが多いセグメントがデプロイメント環境内

に存在する場合は、長時間の停止が発生した場合に備えて、エージェントのデフォルト・ストレージの容量を増やしてください。

手順

1. QRadar で「**管理**」タブをクリックします。
2. ナビゲーション・メニューで、「**データ・ソース (Data Sources)**」をクリックします。
3. 「**WinCollect**」アイコンをクリックします。
4. 「**エージェント**」をクリックし、編集したいエージェントを選択します。
5. 「**ログ・ソース**」をクリックします。
6. 編集するログ・ソースを選択して、「**編集**」をクリックします。
7. 「**ターゲット外部宛先**」チェック・ボックスを選択します。
8. 「**ターゲット外部宛先**」チェック・ボックスの下に表示されているボックスで、エージェントに追加する宛先を選択します。
9. 「**保存**」をクリックします。

QRadar ハードウェアのアップグレード後の WinCollect エージェントのマイグレーション

QRadar ハードウェアのアップグレード後は、WinCollect エージェントの新しい許可トークンを生成して、`install_config` ファイルを更新する必要があります。

このタスクについて

手順

1. 許可トークンを生成します。詳しくは、14 ページの『WinCollect エージェントの認証トークンの作成』を参照してください。

   注 : この機能は、IBM QRadar on Cloud では使用できません。
2. 新しいコンソールの IP アドレスを使用して `¥WinCollect¥config¥install_config.txt` ファイルを更新します。
3. 以下のコマンドを実行します。ここで *<auth_token>* は手順 1 で生成した認証トークンです。

   ```
   C:¥Program Files¥IBM¥WinCollect¥bin¥InstallHelper.exe -T <auth_token> -a
   "C:¥Program Files¥IBM¥WinCollect¥config¥install_config_autocreate.txt"
   ```

   ```
   C:¥Program Files¥IBM¥WinCollect¥bin¥InstallHelper.exe -T xxxxxxxx-xxxx-xxxx-
   xxxx-xxxxxxxxxxxx -a "C:¥Program Files¥IBM¥WinCollect¥config
   ¥install_config_autocreate.txt"
   ```
4. WinCollect エージェントを再始動します。

Adaptive Log Exporter から WinCollect へのマイグレーション

Adaptive Log Exporter (ALE) デプロイメントから WinCollect にマイグレーションするには、Windows ホストに WinCollect エージェントをインストールし、ログ・ソースを作成して、ALE を削除します。ALE 製品は、生産終了 (EOL) となっており、現在はサポートされていません。

手順

1. WinCollect SFS を IBM QRadar SIEM Console にインストールします。
2. 「**管理**」タブをクリックします。
3. 「**データ・ソース**」で「**Wincollect**」を選択します。
4. 「**WinCollect**」ページで「**宛先**」 > 「**追加**」をクリックし、WinCollect 宛先を作成します。
5. WinCollect エージェントを Windows ホストにインストールします。詳しくは、21 ページの『WinCollect エージェントを Windows ホストにインストールする』を参照してください。

   注 : ログ・ソースは、WinCollect インストール・ウィザードから作成できます。
6. WinCollect エージェントが自動的にディスカバーされるのを待ちます。

7. オプション。QRadar で WinCollect ログ・ソースを作成し、Adaptive Log Exporter が使用している既存のログ・ソースと置き換えます。詳しくは、82 ページの『WinCollect エージェントへのログ・ソースの追加』を参照してください。

   注 : WinCollect のインストール時に「**ログ・ソースを作成 (Create Log Source)**」を選択した場合は、ステップ 7 をスキップできます。WinCollect プロトコルを使用するログ・ソースは、個別に作成することも、一括で追加することもできます (リモートでイベントをポーリングする WinCollect エージェントの場合)。
8. 「**ログ・アクティビティー**」タブで、イベントが受信されたことを確認します。
9. Adaptive Log Exporter を以下の手順で削除します。
   a) Windows ホスト上のアクティブなアプリケーションをすべて 閉じます。
   b) Windows コマンド・プロンプトを開きます。
   c) Adaptive Log Exporter のインストール・ディレクトリーに移動します。

      注 : ALE の標準のインストール・ディレクトリーは、`Program Files` ディレクトリーまたは `Program Files (x86)` ディレクトリーです。
   d) 以下のコマンドを入力して、Adaptive Log Exporter をアンインストールします。

```
unins000.exe /SILENT /VERYSILENT
```

WinCollect のスタンドアロン・インストール

スタンドアロン・デプロイメントとは、WinCollect ソフトウェアがインストールされている、非管理モードの Windows ホストです。Windows ホストは、それ自体、ローカル・ホスト、リモート Windows ホストのいずれからも情報を収集できます。リモート・ホストには WinCollect ソフトウェアはインストールされていません。WinCollect ソフトウェアがインストールされている Windows ホストがリモート・ホストに対してポーリングを行い、イベント情報を IBM QRadar に送信します。

WinCollect 構成コンソールの概要

スタンドアロン・デプロイメントでは、WinCollect 構成コンソールを使用して、WinCollect デプロイメントを管理します。WinCollect 構成コンソールを使用して、WinCollect でエージェントを収集するデバイスの追加、および、イベントの送信先の IBM QRadar の宛先の追加を行います。

前提条件 : WinCollect 構成コンソールをインストールするには、その前に以下のことを行う必要があります。

- WinCollect エージェントをスタンドアロン・モードでインストールする。詳しくは、21 ページの『WinCollect エージェントを Windows ホストにインストールする』を参照してください。
- .net framework バージョン 3.5 をインストールする。
- Microsoft 管理コンソール (MMC) 3.0 以降をインストールする。

以下の表で WinCollect 構成コンソールについて説明します。

表 *10. WinCollect* 構成コンソール・ウィンドウ	
セクション	**説明**
グローバル構成 (Global Configuration)	グローバル構成パラメーターを使用して、WinCollect データが保管されるシステムに関する情報を表示、追加、更新できます。
	ディスク・マネージャー (Disk Manager) - イベント・レートがイベント・スロットルを上回った場合に、イベントをディスクにバッファリングするために使用される WinCollect データへのパス。 「**容量**」は、データ・フォルダーの内容に許容される最大容量です。この最大容量に達すると、WinCollect はこのフォルダーには書き込みません。
	インストール情報 (Installation Information) - WinCollect エージェントのインストール済み環境に関する情報を表示します。 **アプリケーション ID** - 状況サーバーに送信されるペイロード・メッセージのヘッダー **状況サーバー (Status Server)** - WinCollect エージェントによって生成されるハートビート・メッセージや警告・エラーなどの、WinCollect エージェント状況イベントの送信先。
	セキュリティー・マネージャー (Security Manager) - リモート・デバイスからのイベントの収集に使用される、集中管理された資格情報。
宛先	「**宛先**」パラメーターは、WinCollect デバイス・データの送信先を定義します。
	「**Syslog TCP**」宛先または「**Syslog UDP**」宛先には以下のパラメーターが含まれます。 **名前** **ホスト名** **ポート** **スロットル (秒当たりのイベント数)** 宛先を展開して、その宛先に割り当てられているすべてのデバイスを表示できます。
デバイス	「**デバイス**」パラメーターには、使用可能なデバイス・タイプが含まれます。各デバイス・タイプの下で、複数のデバイス・パラメーターを表示または更新できます。

構成コンソールのインストール

WinCollect 構成コンソールをダウンロードおよびインストールして、スタンドアロン・デプロイメントを管理します。構成コンソールを必要としない多数の Windows ホストに WinCollect をデプロイする場合は、WinCollect パッチのみをインストールするという選択肢もあります。

始める前に

- 構成コンソールをインストールするには、既存の WinCollect エージェントがスタンドアロン・モードである必要があります。WinCollect エージェントのインストールについて詳しくは、25 ページの『コマンド・プロンプトからの WinCollect エージェントのインストール』を参照してください。
- .NET framework 3.5 機能が必須です。.NET のインストールを確認する方法については、www.ibm.com/support (https://www.ibm.com/support/docview.wss?uid=swg21701063) を参照してください。
- Microsoft 管理コンソール (MMC) 3.0 以降が必須です。
- WinCollect スタンドアロン・パッチ・インストーラーは、以下の Windows ソフトウェアのバージョンをサポートします。
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 (最新)
  - Windows Server 2008 (最新)
  - Windows 10 (最新)
  - Windows 8 (最新)
  - Windows 7 (最新)
  - Windows Vista (最新)

重要 : WinCollect は、Microsoft がサポートを終了した Windows のバージョンではサポートされていません。ソフトウェアの延長サポート終了日が過ぎていても、製品が期待どおりに機能することがあります。ただし、IBM は、古いオペレーティング・システムで発生した WinCollect の問題を解決するために、コードまたは脆弱性のフィックスを作成することはありません。例えば、Microsoft Windows Server 2003 R2 および Microsoft Windows XP は、「延長サポート終了日」を過ぎたオペレーティング・システムです。この発表について質問がある場合は、IBM QRadar Collecting Windows Events (`WMI/ALE/WinCollect`) フォーラムで相談できます。詳しくは、https://support.microsoft.com/en-us/lifecycle/search (https://support.microsoft.com/en-us/lifecycle/search) を参照してください。

手順

1. IBM Support (www.ibm.com/support/fixcentral) から、構成コンソールのインストール先にする Windows ホスト上にパッチ・ソフトウェアをダウンロードします。
2. ご使用のシステムで実行可能ファイルを開きます。
3. インストール・ウィザードの手順に従います。WinCollect 構成コンソールと WinCollect パッチの両方をインストールするか、パッチのみをインストールするかを選択できます。

サイレント・モードでの WinCollect ソフトウェアのインストール、アップグレード、およびアンインストール

インストール・ウィザードを使用するのではなく、コマンドを入力して、WinCollect スタンドアロン・パッチと WinCollect 構成コンソールについて、すべてのインストール・タスクとアップグレード・タスクを実行します。WinCollect エージェントについても、パッチ・インストーラーだけを使用してアップグレードすることができます。

手順

1. IBM サポート (www.ibm.com/support/fixcentral) からパッチ・ソフトウェアをダウンロードします。
2. 以下のコマンドを使用して、WinCollect スタンドアロン・パッチと WinCollect 構成コンソールの両方について、インストールまたはアップグレードを実行します。

   ```
   <setup.exe> /s /v" /qn"
   ```

3. 以下のコマンドを使用して、WinCollect 構成コンソールのインストール・ディレクトリーを変更します。

```
<setup.exe> /s /v" /qn ADDLOCAL=ALL INSTALLDIR=<PATH>"
```

4. 以下のコマンドを使用して、WinCollect スタンドアロン・パッチだけをインストールまたはアップグレードします。

```
<setup.exe> /s /v" /qn ADDLOCAL=WinCollect_StandAlone_Patch"
```

5. WinCollect 構成コンソールをアンインストールする 場合は、以下のコマンドを使用します。

```
<setup.exe> /s /x /v" /qn"
```

スタンドアロン・インストールについて詳しくは、IBM サポート (www.ibm.com/support/docview.wss?uid=swg21698381) を参照してください。

自動インストール中の XPath パラメーターの設定

WinCollect V 7.2.8 以降では、スタンドアロンの WinCollect エージェントのインストール用のコマンド・ライン・インストーラーに XPath パラメーターを追加できます。

手順

1. https://www.base64encode.org/ やその他のエンコード・ツールを使用して、XPath を Base64 エンコードに変換します。

   例えば、Windows PowerShell ログの収集に必要な次の XPath は以下のように変換されます。

```
<QueryList>
<Query Id="0" Path="Windows PowerShell">
<Select Path="Windows PowerShell">*</Select>
</Query>
</QueryList>
```

   上記が変換された結果、次の Base64 が作成されます。
   PFF1ZXJ5TGlzdD4KPFF1ZXJ5IElkPSIwIiBQYXRoPSJXaW5kb3dzIFBvd2VyU2hlbGwiPgo8U2VsZWN0IFBhdGg9IldpbmRvd3MgUG93ZXJTaGVsbCI+KjwvU2VsZWN0Pgo8L1F1ZXJ5Pgo8L1F1ZXJ5TGlzdD4=

2. 次のコードをコマンド・ライン・インストーラーに追加します。

```
c:¥wincollect-7.2.8-91.exe /s /v"/qn STATUSSERVER=<valid IP address>
LOG_SOURCE_AUTO_CREATION_
ENABLED=True
LOG_SOURCE_AUTO_CREATION_PARAMETERS=""Component1.AgentDevice=DeviceWindowsLog&Component1.
Action=create&
Component1.LogSourceName=%COMPUTERNAME%&Component1.LogSourceIdentifier=%COMPUTERNAME%&
Component1.Dest.Name=QRadar&Component1.EventLogPollProtocol=MSEVEN6&Component1.Dest.Hostname=
<valid IP address>&
Component1.Dest.Port=514&Component1.Dest.Protocol=TCP&Component1.Log.Security=true&Component1
.Log.System=true&
Component1.Log.Application=true&Component1.Log.DNS+Server=false&Component1.Log.File
+Replication+
Service=false&
Component1.Log.Directory+Service=false&Component1.RemoteMachinePollInterval=3000&
Component1.MinLogsToProcessPerPass=1250&Component1.MaxLogsToProcessPerPass=2500&
Component1.CustomQuery.Base64=<base64 Xpath>&
Component1.EventRateTuningProfile=High+Event+Rate+Server"""
```

   注 : 以下の項目を有効な IP アドレスに置き換えます。

```
STATUSSERVER=<valid IP address>
Component1.Dest.Hostname=<valid IP address>
```

   STATUSSERVER は WinCollect エージェントからの状況メッセージ (例えば、WinCollect サービスが開始中というメッセージや、いずれかのエージェント・エラー・メッセージ) の送信先です。
   Component1.Dest.Hostname は、エージェントからのイベント・ログの送信先 (例えば、QRadar EC やコンソール) です。

   注 : 次の項目は、ステップ 1 で作成した変換後の Base64 に置き換えます。

```
Component1.CustomQuery.Base64=<base64 Xpath>
```

3. いずれかのコンポーネント、または収集するイベント・ログを追加または削除します。

WinCollect エージェントを Windows ホストにインストールする

ネットワーク環境内のローカル収集またはリモート収集に使用する各 Windows ホストに WinCollect エージェントをインストールします。

始める前に

以下の条件が満たされていることを確認してください。

- 管理対象 WinCollect エージェントの認証トークンが作成されていること。

  注 : 認証トークンは、スタンドアロン WinCollect デプロイメント (IBM QRadar on Cloud で使用されるデプロイメントなど) には不要ですが、すべての管理対象 WinCollect エージェントでは認証トークンを使用する必要があります。

  詳しくは、14 ページの『WinCollect エージェントの認証トークンの作成』を参照してください。
- ご使用のシステムがハードウェア要件およびソフトウェア要件を満たしていること。

  詳しくは、10 ページの『WinCollect ホストのハードウェア要件とソフトウェア要件』を参照してください。
- WinCollect エージェントが QRadar およびリモート・ポーリング対象の Windows コンピューターと通信するために必要なポートが使用可能であること。

  詳しくは、8 ページの『WinCollect エージェントと QRadar との間の通信』を参照してください。
- 管理対象 WinCollect エージェントのログ・ソースを自動的に作成するには、エージェントが QRadar に接続してログ・ソースを作成するために使用できる宛先を最初に作成する必要があります。詳しくは、35 ページの『宛先の追加』を参照してください。

  管理対象 WinCollect エージェントは、Windows イベント・ログを構成済みの宛先に送信します。宛先として、QRadar コンソール、イベント・プロセッサー、またはイベント・コレクターを使用できます。

手順

1. IBM サポート Web サイト (http://www.ibm.com/support) から WinCollect エージェントの .exe ファイルをダウンロードします。
2. WinCollect エージェントの .exe ファイルを右クリックし、「**管理者として実行**」を選択します。
3. インストール・ウィザードのプロンプトに従い、管理対象またはスタンドアロン・エージェントのセットアップ用の次のパラメーターを使用します。

表 *11. WinCollect* 管理対象エージェント・セットアップ・タイプのインストール・ウィザードのパラメーター

パラメーター	説明
ホスト ID	インストールする WinCollect エージェントごとに固有の ID を使用します。このフィールドに入力する名前は、QRadar コンソールの WinCollect エージェント・リストに表示されます。エージェントを Windows ホストに再インストールし、そのエージェントに対して同じホスト ID を使用する場合、最初に QRadar で既存のエージェントの名前を変更する必要があります。ホスト ID は、同じ Windows ホスト上のエージェントのインストールごとに固有です。 デフォルトでは、ホスト ID は Windows ホストのホスト名です。
認証トークン	QRadar で作成した認証トークン (例えば、`af111ff6-4f30-11eb-11fb-1fc117711111`)。
構成サーバー (ホストおよびポート) (Configuration Server (host and port))	QRadar コンソール、イベント・コレクター、またはイベント・プロセッサーの IP アドレスまたはホスト名。例えば、`192.0.2.0` または `myhost`。
ログ・ソースを作成 (Create Log Source)	このチェック・ボックスが選択されている場合は、ログ・ソースとターゲット宛先に関する情報を入力する必要があります。
ログ・ソース名 (Log Source Name)	名前の最大長は 255 文字です。
ログ・ソース ID (Log Source Identifier)	WinCollect エージェントがポーリングするデバイスを識別します。このフィールドでは、ログ・ソースがイベントを収集する Windows ホストのホスト名、IP アドレス、または FQDN を使用する必要があります。
ターゲット宛先	インストール・ウィザードに情報を引き続き入力する前に、QRadar で WinCollect 宛先を構成しておく必要があります。このフィールドには、「**宛先**」ウィンドウに表示される、事前に作成した WinCollect 宛先の名前が含まれている必要があります。
イベント・ログ	ログ・ソースでイベントを収集し QRadar に送信する Windows ログ。
マシンのポーリング間隔 (ミリ秒) (Machine poll interval (msec))	Windows ホストに対する照会の間隔 (ミリ秒単位) を決定するポーリング間隔。 ポーリング間隔の最小値は 300 ミリ秒です。デフォルトは 3000 ミリ秒 (3 秒) です。

表 *11. WinCollect* 管理対象エージェント・セットアップ・タイプのインストール・ウィザードのパラメーター *(続き)*

パラメーター	説明
イベント・レート・チューニング・プロファイル (Event Rate Tuning Profile)	チューニング・プロファイルを以下から選択します。 • デフォルト (エンドポイント) (Default (Endpoint)): 100/150 この設定は、非サーバー OS を実行している Windows エンドポイントに適しています。 • 標準的なサーバー (Typical Server): 500/750 この設定は、ほとんどの Windows Server エンドポイントに適しています。 • イベント・レートが高いサーバー (High Event Rate Server): 1250/1875 この設定は、すべての Windows エンドポイントに適しており、ドメイン・コントローラーおよびその他の潜在的な高 EPS エンドポイントに最適です。 詳しくは、IBM サポート (http://www-01.ibm.com/support/docview.wss?uid=swg21672193) を参照してください。
デフォルトの状況サーバー・アドレス (Default Status Server Address)	WinCollect エージェントからの状況メッセージの送信先である QRadar 管理対象ホスト。これらのメッセージには、アプリケーションのハートビート・メッセージおよび WinCollect エージェントのログ・ファイルからのイベントが含まれます。 デフォルトでは、これは構成済みの構成サーバーと同じ値です。
Syslog 状況サーバー (デフォルトと異なる場合) (Syslog Status Server (if different from default))	WinCollect 状況メッセージを送信する先の代替宛先。デプロイメントのコンソール、イベント・プロセッサー、またはイベント・コレクターを使用できます。

表 *12. WinCollect* スタンドアロン・セットアップ・タイプのインストール・ウィザードのパラメーター

パラメーター	説明
ログ・ソースを作成 (Create Log Source)	このチェック・ボックスが選択されている場合は、ログ・ソースとターゲット宛先に関する情報を入力する必要があります。
ログ・ソース名 (Log Source Name)	名前の最大長は 255 文字です。
ログ・ソース ID (Log Source Identifier)	WinCollect エージェントがポーリングするデバイスを識別します。このフィールドでは、ログ・ソースがイベントを収集する Windows ホストのホスト名、IP アドレス、または FQDN を使用する必要があります。
イベント・ログ	ログ・ソースでイベントを収集し QRadar に送信する Windows ログ。

表 *12. WinCollect* スタンドアロン・セットアップ・タイプのインストール・ウィザードのパラメーター *(続き)*

パラメーター	説明
宛先名 (Destination Name)	WinCollect イベントの送信先を識別します。
ホスト名/IP (Hostname / IP)	宛先のホスト名または IP アドレス。
ポート	WinCollect が宛先との通信に使用するポート。
プロトコル	**TCP** または **UDP**
マシンのポーリング間隔 (ミリ秒) (Machine poll interval (msec))	Windows ホストに対する照会の間隔 (ミリ秒単位) を決定するポーリング間隔。 ポーリング間隔の最小値は 300 ミリ秒です。デフォルトは 3000 ミリ秒 (3 秒) です。
イベント・レート・チューニング・プロファイル (Event Rate Tuning Profile)	チューニング・プロファイルを以下から選択します。 • デフォルト (エンドポイント) (Default (Endpoint)): 100/150 この設定は、非サーバー OS を実行している Windows エンドポイントに適しています。 • 標準的なサーバー (Typical Server): 500/750 この設定は、ほとんどの Windows Server エンドポイントに適しています。 • イベント・レートが高いサーバー (High Event Rate Server): 1250/1875 この設定は、すべての Windows エンドポイントに適しており、ドメイン・コントローラーおよびその他の潜在的な高 EPS エンドポイントに最適です。 詳しくは、IBM サポート (http://www-01.ibm.com/support/docview.wss?uid=swg21672193) を参照してください。
デフォルトの状況サーバー・アドレス (Default Status Server Address)	WinCollect エージェントからの状況メッセージの送信先である IP アドレス宛先。
Syslog 状況サーバー (デフォルトと異なる場合) (Syslog Status Server (if different from default))	WinCollect 状況メッセージを送信する先の代替宛先。デプロイメントのコンソール、イベント・プロセッサー、またはイベント・コレクターを使用できます。QRadar on Cloud デプロイメントでは、データ・ゲートウェイを使用します。
ハートビート間隔 (ミリ秒) (Heartbeat Interval (msecs))	ハートビート状況メッセージが送信される頻度。WinCollect 7.2.8 では、これはミリ秒単位で表示されます。WinCollect 7.2.9 以降では、これは分単位で表示されます。

表 12. *WinCollect* スタンドアロン・セットアップ・タイプのインストール・ウィザードのパラメーター (続き)	
パラメーター	**説明**
ログ・モニター・ソケット・タイプ (Log Monitor Socket Type)	ハートビートと状況メッセージの送信に使用されるプロトコル。 **注 :** このオプションは、スタンドアロンの WinCollect デプロイメントでのみ使用できます。QRadar の今後のリリースで管理対象エージェントにも使用できるようになることが計画されています。

「**コマンド・ライン (config¥cmdLine.txt に保存) (Command Line (will be saved in config ¥cmdLine.txt))**」フィールドには、完了した構成からのコマンド・ラインが表示されます。このコマンドは、サイレント (無人) インストールに使用できます。詳しくは、25 ページの『コマンド・プロンプトからの WinCollect エージェントのインストール』を参照してください。

コマンド・プロンプトからの WinCollect エージェントのインストール

無人インストールでは、コマンド・プロンプトから WinCollect エージェントをインストールできます。WinCollect エージェントを複数のリモート・システムに同時にデプロイするには、サイレント・インストール・オプションを使用します。

このタスクについて

WinCollect インストーラーは、以下のコマンド・オプションを使用します。

表 13. *WinCollect* エージェントのサイレント・インストール・オプション	
オプション	**有効な入力と説明**
`/qn`	サイレント・モードで WinCollect エージェントのインストールを実行します。
`INSTALLDIR`	WinCollect のインストール場所。 インストール・ディレクトリーにスペースが含まれる場合は、引用符の前に円記号 (¥) を追加します。 **例 :** `INSTALLDIR=¥"C:¥Program Files¥IBM ¥WinCollect¥"`
`AUTHTOKEN=token`	管理対象 WinCollect エージェント専用です。QRadar の事前構成済み認証トークンを使用して、管理対象エージェントを許可します。 **例 :** `AUTH_TOKEN=af111ff6-4f30-11eb-11fb-1fc1 17711111`

表 *13. WinCollect* エージェントのサイレント・インストール・オプション *(*続き*)*

オプション	有効な入力と説明
FULLCONSOLEADDRESS=host_address	エージェントを管理する QRadar コンソール、イベント・プロセッサー、またはイベント・コレクターの IP アドレス、ホスト名、または FQDN。 **例 :** • FULLCONSOLEADDRESS=192.0.2.0 • FULLCONSOLEADDRESS=EPqradar • FULLCONSOLEADDRESS=EPqradar.myhost.com
HOSTNAME=host name	**HOSTNAME** フィールドは、WinCollect エージェントに名前を割り当てるために使用されます。このフィールドで使用できる値は、識別可能な名前、ホスト名、または IP アドレスです。ほとんどの場合、管理者は、HOSTNAME=%COMPUTERNAME% を使用して、このフィールドに自動的に値を取り込むことができます。 **例 :** HOSTNAME="windows-%computername%"" HOSTNAME=WindowsSrv1 HOSTNAME= %COMPUTERNAME% WinCollect エージェント・ホストの IP アドレスまたはホスト名にアット・マーク (@) を使用することはできません。
STATUSSERVER	WinCollect の状況メッセージ (ハートビートなど) を送信するための代替宛先 (必要な場合)。
LOG_SOURCE_AUTO_CREATION_ENABLED	必須。True または False。 このオプションを有効にする場合、ログ・ソースのパラメーターを構成する必要があります。 QRadar システムを V7.2.1 パッチ 1 以降に更新する必要があります。
LOG_SOURCE_AUTO_CREATION_ PARAMETERS	各パラメーターが必ず Parameter_Name=value のフォーマットを使用するようにしてください。 各パラメーターは、アンパーサンド (&) で区切ります。 QRadar システムが V7.2.1 パッチ 1 以降に更新されている必要があります。
LOG_MONITOR_SOCKET_TYPE=TCP	TCP を使用して送信されるハートビートと状況メッセージが使用するプロトコルを設定します。 デフォルトのプロトコルは UDP です。 **注 :** このオプションは、スタンドアロンの WinCollect デプロイメントでのみ使用できます。QRadar の今後のリリースで管理対象エージェントにも使用できるようになることが計画されています。

表 *13. WinCollect* エージェントのサイレント・インストール・オプション *(*続き*)*

オプション	有効な入力と説明
Component1.Action	create インストール中に新規ウィンドウのイベント・ログ・ソースを作成します。
Component1.LogSourceIdentifier	エージェントがインストールされているシステムの IP アドレスまたはホスト名。
Component1.Destination.Name	宛先名は、WinCollect ログ・ソースがイベント・データを送信する場所を指定するために使用される英数字の値です。この値は、イベント・データを受信できる QRadar アプライアンス (イベント・プロセッサー、Event Collector、QRadar コンソールなど) である必要があります。 **重要 :** 管理対象デプロイメントでは、この宛先は「内部宛先」でなければならず、その名前は、インストールの前に QRadar ユーザー・インターフェース内に存在している必要があります。存在していないとログ・ソースの構成パラメーターは破棄され、ログ・ソースは自動作成されません。 **内部宛先** イベント・プロセッサー・コンポーネントを含む管理対象ホスト **外部宛先** WinCollect の宛先として構成し、かつ管理対象ホストとしてコンソールに認識されていない宛先
Component1.Dest.Hostname (スタンドアロン・デプロイメントのみ)	WinCollect イベントの送信先 IP アドレスまたはホスト名。
Component1.Dest.Port (スタンドアロン・デプロイメントのみ)	WinCollect が宛先との通信に使用するポート。
Component1.Dest.Protocol (スタンドアロン・デプロイメントのみ)	TCP または UDP
Component1.Dest.MaxPayloadSize (スタンドアロン・デプロイメントのみ)	宛先に送信される最大ペイロード・サイズ (デフォルト値は、UDP では 1020、TCP では 32000 です)。
Component1.Log.Security	必須。True または False。 Windows セキュリティー・ログには、対象オブジェクトの監査ポリシーに定義されているイベントが記録されます。
Component1.Log.System	必須。True または False。 Windows システム・ログでは、オペレーティング・システムによって提供される、デバイス変更、デバイス・ドライバー、システム変更、イベント、および操作についての情報を記録できます。

表 *13. WinCollect* エージェントのサイレント・インストール・オプション *(*続き*)*

オプション	有効な入力と説明
Component1.Log.Application	必須。True または False。 Windows アプリケーション・ログには、オペレーティング・システムではなくソフトウェア・アプリケーションによってトリガーされるイベントが記録されます。このログでは、エラー、情報、および警告の各イベントを記録できます。
Component1.Log.DNS+Server	必須。True または False。 Windows DNS サーバー・ログには、DNS イベントが記録されます。
Component1.Log.File+Replication+Service	必須。True または False。 Windows ファイル複製サービス・ログには、システム上で複製された変更ファイルに関するイベントが記録されます。
Component1.Log.Directory+Service	必須。True または False。 Windows ディレクトリー・サービス・ログには、Active Directory によって書き込まれたイベントが記録されます。
Component1.RemoteMachinePollInterval	Windows ホストに対する照会の間隔 (ミリ秒単位) を決定するポーリング間隔。 ポーリング間隔の最小値は 300 ミリ秒です。デフォルトは 3000 ミリ秒 (3 秒) です。
Component1.EventRateTuningProfile (管理対象デプロイメントのみ)	以下のチューニング・プロファイルのいずれかを選択します。 • Default+(Endpoint) • Typical+Server • High+Event+Rate+Server 詳しくは、IBM サポート (http://www-01.ibm.com/support/docview.wss?uid=swg21672193) を参照してください。

表 *13. WinCollect* エージェントのサイレント・インストール・オプション *(*続き*)*	
オプション	**有効な入力と説明**
Component1.MaxLogsToProcessPerPass (スタンドアロン・デプロイメントのみ)	必須ではありません。 取得対象のイベントがまだ残っている場合に、1 回の受け渡し処理でアルゴリズムが取得するログの最大数 (バイナリー形式)。 **例 :** `Component1.MaxLogsToProcessPerPass=400` **重要 :** このパラメーターを使用すると、イベント収集処理のパフォーマンスが向上しますが、プロセッサーの使用率も高くなります。チューニングについて詳しくは、『WinCollect: Tuning older WinCollect Systems』(http://www.ibm.com/support/docview.wss?uid=swg21699327) を参照してください。
Component1.MinLogsToProcessPerPass (スタンドアロン・デプロイメントのみ)	必須ではありません。 取得対象のイベントがまだ残っている場合に、1 回の受け渡し処理でアルゴリズムが読み取るログの最小数 (バイナリー形式)。 **例 :** `Component1.MinLogsToProcessPerPass=200` **重要 :** このパラメーターを使用すると、イベント収集処理のパフォーマンスが向上しますが、プロセッサーの使用率も高くなります。チューニングについて詳しくは、『WinCollect: Tuning older WinCollect Systems』(http://www.ibm.com/support/docview.wss?uid=swg21699327) を参照してください。
Component1.CoalesceEvents	必須ではありません。 同じイベントが短時間に複数回発生すると QRadar のイベント・カウントが増えます。統合されたイベントを使用することで、「ログ・アクティビティー」タブで、単一のイベント・タイプが発生する頻度を表示し判別できます。このオプションを無効にすると、イベントは個別に表示され、相互にバンドルされません。新規ログ・ソースと自動的にディスカバーされたログ・ソースは、コンソールの「システム 設定」構成から値を継承します。
Component1.StoreEventPayload	必須ではありません。 QRadar のイベント・ペイロードを保管することを指定します。

手順

1. IBM Web サイト (www.ibm.com/support) から、WinCollect エージェント・セットアップ・ファイルをダウンロードします。

2. Windows ホストで、「**管理者として実行**」を使用して、コマンド・プロンプトを開きます。

   重要 : 管理対象デプロイメントでは、ログ・ソースの自動作成中に使用される宛先名は、コマンド・ライン・インストールが実行される前に存在する必要があります。インストールを開始する前に、QRadar ユーザー・インターフェース 内の宛先名を確認します。
3. 以下のコマンドを入力します。

```
wincollect-<Version_number>.x64.exe /s /v" /qn
INSTALLDIR=<"C:¥IBM¥WinCollect">
AUTHTOKEN=<token> FULLCONSOLEADDRESS=<host_address>
HOSTNAME=<hostname> LOG_SOURCE_AUTO_CREATION=<true|false>
LOG_SOURCE_AUTO_CREATION_PARAMETERS=<"parameters"""">
```

   次の例は、スタンドアロン WinCollect エージェントのサイレント・インストールを示しています。

   重要 : この例では、見やすくするために改行しています。実際のコマンドは単一行です。

```
wincollect-<version_number>.x86.exe /s /v"/qn INSTALLDIR=¥"C:¥Program Files
¥IBM¥WinCollect¥" HEARTBEAT_INTERVAL=6000 LOG_SOURCE_AUTO_CREATION_ENABLED=
True LOG_SOURCE_AUTO_CREATION_PARAMETERS=""Component1.AgentDevice=
DeviceWindowsLog&Component1.Action=create&Component1.LogSourceName=
%COMPUTERNAME%-1&Component1.LogSourceIdentifier=
<ip_address>&Component1.Dest.Name=QRadar&Component1
.Dest.Hostname=<ip_address>&Component1.Dest.Port=
514&Component1.Dest.Protocol=TCP&Component1.Log.Security=true&Component1
.Log.System=true&Component1.Log.Application=true
&Component1.Log.DNS+Server=false&Component1.Log.File+Replication+
Service=false&Component1.Log.Directory+Service=false&Component1.
RemoteMachinePollInterval=3000&Component1.EventRateTuningProfile=High+
Event+Rate+Server&Component1.MinLogs
ToProcessPerPass=1250&Component1.MaxLogsToProcessPerPass=1875"""
```

   次の例は、管理対象 WinCollect エージェントのサイレント・インストールを示しています。

   重要 : この例では、見やすくするために改行しています。実際のコマンドは単一行です。

```
 wincollect-<version_number>.x86.exe /s /v"/qn INSTALLDIR=¥"C:¥Program Files
¥IBM¥WinCollect¥" AUTHTOKEN=1111111-aaaa-1111-aaaa-11111111
FULLCONSOLEADDRESS=<ip_address:port> HOSTNAME=%COMPUTERNAME%
 LOG_SOURCE_AUTO_CREATION_ENABLED=True LOG_SOURCE_AUTO_CREATION_PARAMETERS
=""Component1.AgentDevice=DeviceWindowsLog&Component1.Action=create
&Component1.LogSourceName=%COMPUTERNAME%&Component1.LogSourceIdentifier=
%COMPUTERNAME%&Component1.Log.Security=true&Component1.Log.System=false
&Component1.Log.Application=false&Component1.Log.DNS+Server=false
&Component1.Log.File+Replication+Service=false&Component1.Log.
Directory+Service=false&Component1.Destination.Name=Local&
Component1.RemoteMachinePollInterval=3000&Component1.EventRate
TuningProfile=High+Event+Rate+Server"""
```

4. Enter を押します。

コマンド・プロンプトからの WinCollect エージェントのアンインストール

コマンド・プロンプトから WinCollect エージェントをアンインストールできます。

手順

1. デスクトップで、「**スタート**」 > 「**実行**」を選択し、cmd と入力してから「**OK**」をクリックします。

   重要 : コマンド・プロンプトは管理ユーザーとして実行する必要があります。
2. すべてのファイルを削除する場合は、以下のコマンドを入力します。

```
msiexec /x{1E933549-2407-4A06-8EC5-83313513AE4B} REMOVE_ALL_FILES=True /qn
```

3. WinCollect アプリケーションのみを削除し、構成ファイル、保管イベント、およびブックマークは削除しない場合は、以下のコマンドを入力します。

```
msiexec /x{1E933549-2407-4A06-8EC5-83313513AE4B} REMOVE_ALL_FILES=False /qn
```

4. Enter を押します。

制御パネルからの WinCollect エージェントのアンインストール

WinCollect エージェントのアンインストールは、Microsoft Windows のコントロール パネルから実行できます。

手順

1. 「**コントロール パネル**」 > 「**プログラム**」 > 「**プログラムのアンインストール**」をクリックします。
2. プログラム・リストで WinCollect を強調表示して、「**変更**」をクリックします。
3. WinCollect アプリケーション、構成ファイル、保管イベント、およびブックマークを削除する場合は、「**すべてのファイルの削除 (Remove all files)**」チェック・ボックスを選択します。
4. 「**削除**」をクリックします。

第 4 章 インストール後の WinCollect エージェントの構成

管理対象 WinCollect デプロイメントでは、IBM Security QRadar を多様なエージェント構成タスクに使用できます。 スタンドアロン・デプロイメントでは、WinCollect 構成コンソールを使用して、WinCollect デプロイメントを管理します。

WinCollect エージェントの構成作業の中には、エージェントがインストールされている Windows ホストで実行しなければならないものもあります。

管理対象 WinCollect エージェントの構成

管理対象 WinCollect デプロイメントのインストール後は、IBM Security QRadar を使用してデプロイメントを管理します。

WinCollect のエージェント、宛先、およびスケジュールを管理することができます。制限付きポリシーが適用されたシステムの構成オプションも管理できます。

WinCollect エージェントは、個々のログ・ソースとの通信、イベントの解析、および syslog を使用しての QRadar へのイベント情報の転送を担っています。

WinCollect エージェントを Windows ホストにインストールしたら、QRadar が WinCollect エージェントを自動的にディスカバーするまで待機してください。通常、この自動ディスカバリーは完了まで数分かかります。

注 : QRadar ホストへの登録要求は、ご使用のネットワーク内のファイアウォールによってブロックされることがあります。

WinCollect エージェントの手動による追加

WinCollect エージェントを削除した場合、それを手動で再追加することができます。 既存の WinCollect エージェントに再接続するには、そのホスト名がエージェントの削除前に使用したホスト名と完全に一致している必要があります。

WinCollect エージェントを削除すると、IBM Security QRadar コンソール によってエージェント・リストからエージェントが削除され、削除された WinCollect エージェントの管理対象ログ・ソースがすべて無効になります。

以前に自動的にディスカバーされた WinCollect エージェントは、WinCollect では再ディスカバーされません。 削除した WinCollect エージェントを QRadar のエージェント・リストに再追加するには、削除したエージェントを手動で追加する必要があります。

例えば、ホスト ID 名が VMRack1 という WinCollect エージェントを削除します。このエージェントを再インストールし、同じホスト ID 名 VMRack1 を使用します。 WinCollect では、この WinCollect エージェントは自動的にはディスカバーされません。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・メニューで、「**データ・ソース (Data Sources)**」をクリックします。
3. 「**エージェント**」をクリックします。
4. 「**追加**」をクリックします。
5. パラメーターを構成します。

   これらのパラメーターの一部について、次の表で説明します。

表 *14. WinCollect* エージェント・パラメーター	
パラメーター	**説明**
ホスト名	リモート・ホストへの WinCollect エージェントのインストールに使用した方法に応じて、「**ホスト名**」フィールドの値は以下のいずれかの値に一致する必要があります。 • WinCollect エージェントのコマンド・ライン構成の「**HOSTNAME**」フィールド • WinCollect エージェント・インストーラーの「**ホスト ID**」フィールド
説明	オプション。 IP アドレスを WinCollect エージェントの名前として指定した場合は、WinCollect エージェントまたは WinCollect エージェントで管理されているログ・ソースを識別する説明テキストを追加します。
自動更新は有効	構成の更新が WinCollect エージェントに送信されるかどうかを制御します。
ハートビート間隔	このオプションは、WinCollect エージェントがその状況を状況サーバーに通信する頻度を定義します。間隔は 1 分から 20 分の間です。
構成ポーリング間隔	更新されたログ・ソース構成情報またはエージェント・ソフトウェアの更新の有無を調べるために、WinCollect エージェントが QRadar 構成サーバーをポーリングする頻度を定義します。 間隔は 1 分から 20 分の間です。

6. 「**保存**」をクリックします。
7. 「**管理**」タブで、「**変更のデプロイ**」をクリックします。

   WinCollect エージェントがエージェント・リストに追加されます。

関連タスク

WinCollect エージェントの削除

WinCollect エージェントを削除すると、IBM Security QRadar コンソール によってエージェント・リストからエージェントが削除され、削除された WinCollect エージェントの管理対象ログ・ソースがすべて無効になります。

WinCollect エージェントの削除

WinCollect エージェントを削除すると、IBM Security QRadar コンソール によってエージェント・リストからエージェントが削除され、削除された WinCollect エージェントの管理対象ログ・ソースがすべて無効になります。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・メニューで、「**データ・ソース (Data Sources)**」をクリックします。
3. 「**WinCollect**」アイコンをクリックします。
4. 削除するエージェントを選択して、「**削除**」をクリックします。
5. 「**保存**」をクリックします。
6. 「**管理**」タブで、「**変更のデプロイ**」をクリックします。

ヒント : 複数の WinCollect エージェントを削除するには、Ctrl を押しながら複数のエージェントを選択してから、「**削除**」をクリックします。

関連タスク

WinCollect エージェントの手動による追加

WinCollect の宛先

WinCollect の宛先では、WinCollect エージェントが Event Collector または IBM Security QRadar コンソールにイベントを転送する方式に関するパラメーターを定義します。

宛先の追加

デプロイメント内の WinCollect エージェントにイベントの転送先を割り当てるために、WinCollect デプロイメントの宛先を作成できます。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・メニューで、「**データ・ソース (Data Sources)**」をクリックします。
3. 「**WinCollect**」アイコンをクリックします。
4. 「**宛先**」をクリックしてから、「**追加**」をクリックします。
5. パラメーターを構成します。

   これらのパラメーターの一部について、次の表で説明します。

表 *15.* 宛先パラメーター

パラメーター	説明
名前	ログ・ソースを作成するためにエージェント側で使用されます。 **重要 :** 宛先名は、ログ・ソースの自動作成中に使用され、インストールが実行される前に存在する必要があります。インストールを開始する前に、QRadar 内の宛先名を確認します。
ホスト名	宛先 IBM QRadar アプライアンスのホスト名または IP アドレス。
ポート	IBM Security QRadar は、WinCollect エージェントから送信されたイベントをポート 514 (UDP または TCP) で受信します。 TLS プロトコルの場合、デフォルト・ポートは 6514 です。
プロトコル	IBM Security QRadar および WinCollect エージェント間の通信チャネル。「**UDP**」、「**TCP**」、または「**TCP/TLS (暗号化)**」を選択します。
スロットル (秒当たりのイベント数)	WinCollect エージェントが 1 秒当たりに送信できるイベント数の制限を定義します。

表 15. 宛先パラメーター (続き)	
パラメーター	**説明**
スケジュール・モード	「**イベントの転送**」オプションを選択すると、WinCollect エージェントはユーザー定義のスケジュール期間中、イベントを転送します。イベントが転送されていない場合、スケジュールが再び実行されるまで、イベントは保管されます。 「**イベントの保管**」オプションを選択すると、WinCollect エージェントはユーザー定義のスケジュール期間中だけ、イベントをディスクに保管します。その後、イベントを指定された宛先に転送します。

6.「**保存**」をクリックします。

関連タスク

WinCollect からの宛先の削除

WinCollect エージェントのイベント転送とイベント・ストレージのスケジューリング

WinCollect からの宛先の削除

宛先を削除すると、WinCollect エージェントからイベント転送パラメーターが削除されます。

宛先はグローバル・パラメーターです。宛先にログ・ソースが割り当てられている場合に宛先を削除すると、WinCollect エージェントはイベントを転送できません。 既存の宛先が削除されると、ログ・ソースに対するイベント収集は停止されます。 処理されなかったディスク上のイベントは、宛先が削除されると破棄されます。

手順

1.「**管理**」タブをクリックします。
2. ナビゲーション・メニューで、「**データ・ソース (Data Sources)**」をクリックします。
3.「**WinCollect**」アイコンをクリックします。
4.「**宛先**」をクリックします。
5. 削除する宛先を選択して、「**削除**」をクリックします。

関連タスク

宛先の追加

デプロイメント内の WinCollect エージェントにイベントの転送先を割り当てるために、WinCollect デプロイメントの宛先を作成できます。

WinCollect エージェントのイベント転送とイベント・ストレージのスケジューリング

WinCollect エージェントのイベント転送とイベント・ストレージのスケジューリング

スケジュールを使用して、WinCollect エージェントを転送したり、イベントをデプロイメント環境内のディスクに保管したりするタイミングを管理します。

スケジュールは必須ではありません。 スケジュールが存在しない場合、WinCollect エージェントはネットワーク制限により遅延が生じた場合にのみ、イベントの転送と保管を自動で行います。

デプロイメント環境内の WinCollect エージェントのイベントを転送するタイミングを割り当てる WinCollect デプロイメント環境のスケジュールを作成できます。 スケジュール期間中に送信できないイベントは、次の使用可能な間隔のキューに自動的に入れられます。

手順

1.「**管理**」タブをクリックします。
2. ナビゲーション・メニューで、「**データ・ソース (Data Sources)**」をクリックします。

3.「**WinCollect**」アイコンをクリックします。
4.「**スケジュール**」をクリックします。
5.「**追加**」をクリックし、「**次へ**」をクリックします。
6. パラメーターを構成し、スケジュールに含める各曜日のチェック・ボックスを選択します。
7.「**次へ**」をクリックします。
8. スケジュールに宛先を追加するには、「**使用可能な宛先**」リストで、宛先を選択し、選択記号 > をクリックします。
9.「**次へ**」をクリックし、「**完了**」をクリックします。

関連タスク

宛先の追加

デプロイメント内の WinCollect エージェントにイベントの転送先を割り当てるために、WinCollect デプロイメントの宛先を作成できます。

WinCollect からの宛先の削除

WinCollect の状況メッセージへのカスタム・エントリーの追加

WinCollect エージェントの状況メッセージにカスタム情報を追加できます。

手順

1. LEEF ログ内で識別する Windows ホストの `wincollect/config` ディレクトリーで、`heartbeat_custom.props` というファイルを作成します。

   重要 : このファイルの作成、更新、または削除を行えるのは、WinCollect デプロイメントが稼働している場合です。ファイルへの更新は、次回のハートビートに対するログで有効になります。
2. `heartbeat_custom.props` ファイルに次の形式で、1 行につき 1 エントリーずつカスタム情報を入力します。

   ```
   keyword=value
   ```

   例 :

   ```
   department=Accounting
   ```

   ```
   group=AC105
   ```

   この例のキーワードおよび値から出力されるログは、以下のようになります。

   ```
   <13>Jul 22 15:02:48 DESKTOP-0F0QKN3 LEEF:1.0|IBM|
   WinCollect|<version_number>.9999|2|src=DESKTOP-0F0QKN3
   os=Windows 10(Build 10240 64-bit)dst= sev=3 log=Code.SSLConfigServerConnection
   department=Accounting group=AC105 msg=ApplicationHeartbeat
   ```

   重要 :

   - `heartbeat_custom.props` は 10 KB を超えてはなりません。
   - カスタム・キーワード・エントリーは、スペースを含めない英数字にする必要があります。
   - カスタム・エントリーに予約済みキーワード (`src`、`os`、`dst`、`sev`、`log`、`msg` など) を使用することはできません。
   - カスタム値に特殊文字 (`= | [ ] { } < > / ¥ ' "` など) を使用することはできません。
   - カスタム値内の複数の空白文字はシングル・スペースに削減されます。

転送されたイベントの ID

Windows イベント・サブスクリプションを使用して転送されたイベントをログ・ソースが収集できるようにした場合、イベントごとに表示されるイベント・ソースを指定できます。転送されたイベントを収集するログ・ソース内での、転送されたイベントの ID を構成します。

転送されたイベントの ID を設定するためのオプションには、以下の 3 つがあります。

送信元
これはデフォルト・オプションです。 転送されたイベントは、イベントを生成したコンピューターの IP アドレスによって識別されます。

WEC
転送されたイベントは、イベントを収集した WinCollect エージェントの名前で識別されます。エージェントが収集したすべてのイベントは、単一のソース ID によってグループ化されます。

その他
イベントの送信元としてカスタムの ID を選択できます。エージェントが収集したすべてのイベントは、この ID によってグループ化されます。

ヒント : カスタム ID には、スペースを含めることはできません。

構成コンソールを使用したスタンドアロンの WinCollect エージェントの構成

スタンドアロン・デプロイメントでは、WinCollect 構成コンソールを使用して、WinCollect デプロイメントを管理します。

WinCollect エージェントの構成作業の中には、エージェントがインストールされている Windows ホストで実行しなければならないものもあります。

WinCollect 資格情報の作成

ログイン情報を含む資格情報を作成します。WinCollect は、資格情報を使用して、デバイスへのログインおよびログの収集を行います。

手順

1. 「**グローバル構成 (Global Configuration)**」パラメーターを展開して、「**セキュリティー・マネージャー (Security Manager)**」を右クリックします。
2. 「**新規資格情報の追加 (Add New Credential)**」を選択します。
3. 「**新規資格情報名 (New Credential Name)**」ボックスに新規資格情報の名前を追加して、「**OK**」をクリックします。
4. 「**セキュリティー・マネージャー (Security Manager)**」の下で新規資格情報をクリックして、その資格情報の「**基本構成 (Basic Configurations)**」ウィンドウを開きます。
5. 新規資格情報に必要なプロパティーを入力します。
6. 「**アクション**」の下に表示されている「**変更のデプロイ**」をクリックします。

WinCollect 構成コンソールに宛先を追加する

IBM QRadar インスタンスを WinCollect データの宛先として追加します。

手順

1. WinCollect 構成コンソールで「**宛先**」パラメーターを展開します。
2. 追加したい宛先に応じて「**Syslog TCP**」パラメーターまたは「**Syslog UDP**」パラメーターを右クリックし、「**新しい宛先の追加 (Add New Destination)**」をクリックします。
3. 「**新しい宛先の名前 (New Destination Name)**」ボックスで、宛先の名前を追加します。「**OK**」をクリックします。

重要 : IP アドレスを含む宛先名を使用してください (例: QRadarEP1_198.x.x.x)。こうしておくと、後でログ・ソースを編集して宛先を変更する場合に、その宛先の IP アドレスを簡単に確認することができます。

4. 「**Syslog TCP**」または「**Syslog UDP**」を展開し、追加した宛先を選択して「**プロパティー**」ウィンドウを表示します。
5. 新しい宛先の「**名前**」、「**ホスト名**」、「**ポート**」、「**スロットル**」を定義します。
6. 「**アクション**」の下に表示されている「**変更のデプロイ**」をクリックします。

WinCollect 構成コンソールでの TLS を使用した宛先の構成

QRadar に送信される Syslog トラフィックを暗号化するには、Transport Layer Security (TLS) 証明書を使用するように WinCollect の宛先を構成します。

手順

1. WinCollect 構成コンソールで「**宛先**」パラメーターを展開します。
2. 「**Syslog TCP**」を右クリックし、「**新しい宛先の追加 (Add New Destination)**」をクリックします。
3. 「**新しい宛先の名前 (New Destination Name)**」フィールドで宛先名を追加し、「**OK**」をクリックします。

   ヒント : IP アドレスを含む宛先名を使用してください (例: 「*<Managed_Host>*_1.2.3.4」)。この宛先名は、後でログ・ソースを編集して宛先を変更する必要がある場合に、宛先の IP アドレスを確認するのに役立ちます。
4. 「**Syslog TCP**」を展開し、ステップ 3 で追加した宛先を選択して「**プロパティー**」ウィンドウを表示します。
5. 「**名前**」と「**ホスト名**」を定義します。
6. 「**ポート**」を 6514 に変更し、「**スロットル**」のレートを設定します。
7. 新しい宛先の TLS 証明書をコピーして「**証明書**」フィールドに貼り付けます。

   注 : TLS 証明書をコピーするときは、「-----BEGIN CERTIFICATE-----」と「-----END CERTIFICATE-----」を必ず含めてください。
8. 「**アクション**」ペインの下に表示されている「**変更のデプロイ**」をクリックします。

WinCollect 構成コンソールにデバイスを追加する

WinCollect がモニターするデバイスを WinCollect 構成コンソールに追加します。

手順

1. 「**デバイス**」の下で、追加したいデバイスのタイプを右クリックして「**新しいデバイスの追加 (Add New Device)**」を選択します。
2. 「**新しいデバイスの追加 (Add New Device)**」ボックスで、宛先デバイスの名前を入力します。
3. 「**基本構成**」ウィンドウで、新しい宛先デバイスのパラメーターを指定します。

   重要 : Microsoft Windows イベント・ログ・デバイス・タイプの「**基本構成**」ページで、グローバルのデフォルト・イベント・ログ・ポーリング・プロトコルを設定できます。デフォルト値は **MSEVEN6** です。

   グローバルのデフォルト・イベント・ログ・ポーリング・プロトコルを使用するように単一の Microsoft Windows イベント・ログ・デバイスを構成するには、そのデバイスの「**基本構成**」ページで「**デフォルト**」を選択します。グローバルのデフォルトを使用しない場合は、「**MSEVEN6**」または「**MSEVEN**」を選択して、グローバルのデフォルト・イベント・ログ・ポーリング・プロトコルをオーバーライドします。

   「**MSEVEN6**」は、イベント・ログからタスク、キーワード、命令コードなど、より多くの情報を収集する Microsoft イベント・プロトコルです。より優れたメッセージ・フォーマットも提供します。
4. 「**アクション**」の下に表示されている「**変更のデプロイ**」をクリックします。

暗号化されたイベントの QRadar への送信

TLS syslog を使用して、暗号化されたイベントを IBM QRadar に送信するように、WinCollect のスタンドアロン・デプロイメント内でログ・ソースを構成します。QRadar バージョン 7.3.1 以降では、WinCollect 管理対象デプロイメントで TLS Syslog のみサポートされています。

始める前に

QRadar で、TLS Syslog プロトコルを使用するユニバーサル DSM を構成します。詳しくは、「*IBM Security QRadar* ログ・ソース・ユーザー・ガイド」を参照してください。

uDSM は、ポートを開き、TLS を使用して通信するために必要な証明書を提供します。uDSM を削除した場合、TLS 通信は停止します。

手順

1. SSH を使用して、root ユーザーとして QRadar にログインします。
2. 証明書を (`-----BEGIN CERTIFICATE-----` および `-----END CERTIFICATE-----` を含めて) `/opt/qradar/conf/trusted_certificates/syslog-tls.cert` から一時的なロケーションにコピーします。この証明書を WinCollect 構成コンソール内に貼り付けます。
3. WinCollect 構成コンソールで、「**宛先**」を展開し、「**宛先の追加 (Add Destination)**」をクリックします。
4. 「**新しい宛先の名前 (New Destination Name)**」ボックスで、宛先の名前を追加し、「**OK**」をクリックします。
5. 新しい宛先を選択し、「**ホスト名**」フィールドにターゲット QRadar アプライアンスの IP アドレスを入力します。
6. 「**ポート**」フィールドに 6514 と入力します。
7. 「**スロットル**」フィールドにデプロイメントの 1 秒当たりのイベント数 (EPS) のレートを入力します。
8. QRadar からコピーした証明書を「**証明書**」フィールド内に貼り付けます。
9. 「**アクション**」の下に表示されている「**変更のデプロイ**」をクリックします。

UDP ペイロード・サイズの増加

UDP Syslog 宛先のペイロード・サイズをエージェント構成ファイルで増加できます。

このタスクについて

UDP 宛先パッケージのデフォルトのペイロード・サイズは 1,024 バイトです。スタンドアロンの WinCollect エージェントのペイロード・サイズを増やすには、エージェント構成ファイルにパラメーターを追加します。

重要 : WinCollect エージェントのペイロード・サイズを変更したら、QRadar の最大 UDP ペイロード・サイズを増やす必要があります。

手順

1. エージェント構成の XML ファイルを開きます。
   このファイルへのデフォルト・パスは `WinCollect¥config¥AgentConfig.xml` です。
2. `UDPSendStage` モジュールに次のパラメーターを追加します。

```
<Parameter name="MaxPayloadSize" value="<desired value>" />
```

このモジュールの例:

```
<Module order="4" service_name="UDPSendStage">
        <Environment>
           <Parameter value="<Destination IP>" name="TargetAddress"/>
           <Parameter value="514" name="TargetPort"/>
           <Parameter name="MaxPayloadSize" value="4096"/>
        </Environment>
    </Module>
```

3. ファイルを保存し、WinCollect エージェントを再始動します。

次のタスク
調整後のペイロード・サイズに対応できるよう、QRadar の最大 UDP ペイロード・サイズを増やします。

イベント・ログのタイム・スタンプへのミリ秒の組み込み

スタンドアロンの WinCollect デプロイメントでは、イベント・ログのタイム・スタンプにミリ秒を含めることができます。

注 : このオプションは、MSEVEN6 プロトコルを使用しているスタンドアロンの WinCollect デプロイメントにのみ適合しています。 MSEVEN プロトコルではサポートされていません。

イベント・ログのペイロード・フィールド **TimeGenerated** および **TimeWritten** では、デフォルトでは秒が使用されます。 「**WinCollect 構成コンソール**」の「**Microsoft Windows イベント・ログ・プロパティー**」ノードで、ミリ秒が使用されるように「**タイム・スタンプ・プロパティー**」を設定できます。

重要 : これは、すべてのログ・ソースに対して設定される、エージェント・レベルでの変更です。

または、パラメーター `&Component1.TimestampFormat=Milliseconds` を使用して、コマンド・ライン・インストールの一部としてこのプロパティーを変更することもできます。また、テンプレートを使用して `AgentConfig.xml` ファイル内の当該属性を変更することもできます。テンプレートの使用について詳しくは、42 ページの『スタンドアロン・デプロイメントにおけるテンプレートを使用した構成変更』を参照してください。

ローカル Windows ログの収集

このユース・ケース・シナリオでは、WinCollect 構成コンソールがインストールされているホストからログを収集して IBM QRadar に送信するために必要な設定について説明します。

手順

1. Windows ログを収集するホストに WinCollect 構成コンソールをインストールします。次に、IBM サポート (www.ibm.com/support/fixcentral) からパッチをダウンロードします。
2. WinCollect 情報の送信先となる QRadar インスタンスの宛先を作成します。38 ページの『WinCollect 構成コンソールに宛先を追加する』を参照してください。
3. モニター対象のローカルの Microsoft イベント・ログ・デバイスを構成します。39 ページの『WinCollect 構成コンソールにデバイスを追加する』を参照してください。

   重要 : 「**デバイス・アドレス (Device Address)**」フィールドに、イベントのポーリングを行うローカル Windows システムの IP アドレスまたはホスト名を入力します。
4. 「**アクション**」の下に表示されている「**変更のデプロイ**」をクリックします。

リモート Windows ログの収集

このユース・ケース・シナリオでは、WinCollect ソフトウェアがインストールされていないホストから Windows ログを収集して IBM QRadar に送信する場合に、WinCollect 構成コンソールで必要になる設定について説明します。

手順

1. ログ情報を収集する Windows マシンに WinCollect 構成コンソールをインストールします。次に、IBM サポート (www.ibm.com/support/fixcentral) からパッチをダウンロードします。
2. リモート・ホストにログインするための資格情報を作成します。 38 ページの『WinCollect 資格情報の作成』を参照してください。
3. Windows イベントの送信先となる宛先 QRadar を作成します。38 ページの『WinCollect 構成コンソールに宛先を追加する』を参照してください。
4. モニター対象のデバイスを構成します。39 ページの『WinCollect 構成コンソールにデバイスを追加する』を参照してください。

重要 :「**デバイス・アドレス (Device Address)**」フィールドで、イベントのポーリングを行うリモート Windows システムの IP アドレスまたはホスト名を入力します。

5.「**アクション**」の下に表示されている「**変更のデプロイ**」をクリックします。

スタンドアロン・デプロイメントにおけるテンプレートを使用した構成変更

サポート対象のバージョン: WinCollect 7.2.8 以上。スタンドアロンのみ。
テンプレートを利用すると、 AgentConfig.xml ファイルに対して手動による、またはスクリプトを使用した編集を加えることなく、エージェント構成を変更できます。

テンプレートを WinCollect のパッチ・ディレクトリーにコピーすると 、エージェントが既存の構成をテンプレートの内容に置き換えます。エージェントは、テンプレートからの変更内容を適用する前に、現行構成のバックアップを patchcheckpoint ディレクトリー内に作成します。 変更が適用された後、エージェントが再開されて、新しい構成が使用されます。

WinCollect V7.2.8 以降では、4 つのサンプル・テンプレートがインストールされます。これらは ¥IBM ¥WinCollect¥templates ディレクトリーに保管されます。

- tmplt_AgentCore.xml
- tmplt_DestinationManager.xml
- tmplt_DeviceWindowsLog.xml
- tmplt_PayloadRouter.xml

注 : これらのテンプレートは、例を示したものにすぎません。ユーザーが独自のテンプレートを作成できるように、すべてのエージェント構成サービス・モジュールがサポートされています。

以降のユース・ケースは、テンプレートを使用してエージェント構成を変更するための方法例を示しています。

ユース・ケース 1: ハートビート間隔の変更

デプロイ済みのすべてのシステムについて、ハートビート間隔を 5 分から 1 時間に変更する必要があります。 以前、これを行うには、agentconfig.xml ファイルを手動で変更するか、スクリプトを使用して変更する必要があり、その後 WinCollect サービスが再開されていました。テンプレートを使用すると、以下のステップを実行することで、この間隔を変更できます。

手順

1. ¥IBM ¥WinCollect¥templates ディレクトリーで tmplt_AgentCore.xml テンプレートを見つけます。このサービスには、ハートビート間隔の構成が含まれています。
2. テンプレートのコピーを作成し、コピーのほうの名前を service_AgentCore.xml に変更します。
3. HeartbeatInterval パラメーターの値を 3,600,000 ミリ秒 (1 時間) に変更します。

```
<Service classification="Static" type="Service" version="7.2.8" module="AgentCore"
name="AgentCore">
        <Environment>
            <Parameter name="HeartbeatInterval" value="3600000"/>
            <Parameter name="ConfigurationCheckInterval" value="300000"/>
            <Parameter name="Enabled" value="true"/>
            <Parameter name="Deleted" value="false"/>
        </Environment>
    </Service>
```

4. service_AgentCore.xml ファイルを ¥IBM¥WinCollect¥patch ディレクトリーに移動します。

   数秒後、ファイルが消え、エージェントが再始動されます。古い agentconfig.xml ファイルはバックアップ・ディレクトリー (patch_checkpoint_*xxxx*) に移されます。

ユース・ケース 2: イベント・データのストレージ構成の変更

このタスクについて

¥programdata¥WinCollect ファイルに保管されるイベント・データの場所と容量を変更する必要があります。イベント・データを C:¥WinCollect¥Data に保管し、容量を 20 GB に変更したいと考えています。この変更を行うためのデフォルトのテンプレートはありませんが、 agentconfig.xml ファイル内の情報を使用することで、簡単にテンプレートを作成できます。以下のサンプルは、既存のサービスを示しています。

```
<Service classification="Service" type="Service" version="7.2.8" module="WinCollectCommon"
 name="DiskManager">
        <Environment>
            <Parameter name="BasePath" value="%ALLUSERSPROFILE%¥WinCollect¥Data"/>
            <Parameter name="Capacity" value="6144"/>
        </Environment>
    </Service>
```

注 : %ALLUSERSPROFILE% は環境変数です。 デフォルト値は C:¥ProgramData です。この値を C:¥WinCollect¥Data に変更する必要があります。

手順

1. 以下の内容を含んだ service_DiskManager.xml という名前の XML ファイルを作成します。

```
<Service classification="Service" type="Service" version="7.2.8" module="WinCollectCommon"
 name="DiskManager">
        <Environment>
            <Parameter name="BasePath" value="c:¥ibm¥WinCollect¥Data"/>
            <Parameter name="Capacity" value="20480"/>
        </Environment>
    </Service>
```

2. このファイルを ¥IBM¥WinCollect¥patch ディレクトリーに移動します。

   数秒後、ファイルが消え、エージェントが再始動されます。これでデータが新しいディレクトリーに書き込まれました。

ユース・ケース 3: UDP 送信から TCP 送信への変更

Syslog データを UDP 経由ではなく TCP 経由で QRadar に送信する必要があります。このオプションは、宛先マネージャーで指定する必要があります。

手順

1. ¥IBM ¥WinCollect¥templates ディレクトリーで tmplt_DestinationManager.xml テンプレートを見つけます。
2. テンプレートのコピーを 作成し、コピーのほうの名前を service_DestinationManager.xml に変更します。
3. <Module order="4" service_name="UDPSendStage"> で、 service_name パラメーターを TCPSendStage に変更します。

```
Service version="7.2.8" classification="Service" type="Service" module="WinCollectPlugin"
 name="DestinationManager">
    <Environment/>
    <InstanceData>
        <Instance name="QRadar">
            <Environment/>
            <Module order="1" service_name="StoreAndForwardStage">
                <Environment>
                    <Parameter name="DataChunkPeriod" value="10"/>
                    <Parameter name="DataProcessingPeriod" value="500000"/>
                    <Parameter name="QueueLowWaterMark" value="750000"/>
                    <Parameter name="QueueHighWaterMark" value="1000000"/>
                    <Parameter name="Schedule.Enable" value="true"/>
                    <Parameter name="Schedule.Invert" value="false"/>
                    <Parameter name="Socket.KeepAlive.Enabled" value="true"/>
                    <Parameter name="Socket.KeepAlive.Time" value="30000"/>
                    <Parameter name="Socket.KeepAlive.Interval" value="4000"/>
```

```
                </Environment>
            </Module>
            <Module order="2" service_name="SimpleEventThrottle">
                <Environment>
                    <Parameter name="EventThrottleInEPS" value="5000"/>
                </Environment>
            </Module>
            <Module order="3" service_name="SyslogHeaderStage">
                <Environment/>
            </Module>
            <Module order="4" service_name="TCPSendStage">
                <Environment>
                    <Parameter name="TargetAddress" value="172.18.X.X"/>
                    <Parameter name="TargetPort" value="514"/>
                </Environment>
            </Module>
        </Instance>
    </InstanceData>
</Service>
```

4. このファイルを ¥IBM¥WinCollect¥patch ディレクトリーに移動します。

   数秒後、ファイルが消え、エージェントが再始動されます。古い agentconfig.xml ファイルはバックアップ・ディレクトリー (patch_checkpoint_*xxxx*) に移されます。

ユース・ケース 4: 既存のログ・ソースへの NSA フィルタリングの追加

既存のログ・ソースに NSA フィルタリングを追加する必要があります。この属性は、tmplt_DeviceWindowsLog.xml テンプレートを使用することで変更できます。

手順

1. tmplt_DeviceWindowsLog.xml テンプレートを見つけます。
2. テンプレートのコピーを作成し、コピーのほうの名前を service_DeviceWindowsLog.xml に変更します。
3. AgentConfig.xml を開き、モジュール DeviceWindowsLog 内に存在する log source の場所を探索します。
4. モデルとインスタンスの情報をコピーして、service_DeviceWindowsLog.xml の内容を、コピーした情報で置き換えます。

   既存のログ・ソースの例:

```
<Service version="7.2.8" classification="Service" type="DeviceType"
module="DeviceWindowsLog" name="DeviceWindowsLog">
    <Environment>
        <Parameter name="DeviceThreadPoolType" value="AdaptiveThreadPool"/>
        <Parameter name="AdaptiveThreadPool.ReaderThreadsMax" value="500"/>
        <Parameter name="AdaptiveThreadPool.ReaderThreadsMin" value="5"/>
        <Parameter name="AdaptiveThreadPool.ReaderBacklogSamplePeriodMillis" value="200"/>
        <Parameter name="MinEventMonitorThreads" value="5"/>
        <Parameter name="MaxEventMonitorThreads" value="250"/>
        <Parameter name="EventLogMonitor.RetryTimeoutMillis" value="60000"/>
        <Parameter name="DefaultThrottleTimeout" value="1500"/>
        <Parameter name="DefaultEventLogPollProtocol" value="MSEVEN6"/>
    </Environment>
    <InstanceData>
        <Instance enabled="true" name="EventLogLocal">
            <Environment>
                <Parameter name="DeviceAddress" value="DESKTOP"/>
                <Parameter name="RemoteMachine" value="DESKTOP"/>
                <Parameter name="Filter.DNS Server.Enabled" value="false"/>
                <Parameter name="EventTypeFilterFailureAudit" value="true"/>
                <Parameter name="EventLogPollProtocol" value="MSEVEN6"/>
                <Parameter name="Log.Security" value="true"/>
                <Parameter name="Filter.Application.Enabled" value="false"/>
                <Parameter name="ADLookup.Enabled" value="false"/>
                <Parameter name="ThrottleTimeout" value="1000"/>
                <Parameter name="Filter.DNS Server.Param" value=""/>
                <Parameter name="Filter.File Replication Service.Enabled" value="false"/>
                <Parameter name="Filter.Application.Type" value="No Filtering"/>
                <Parameter name="Filter.Directory Service.Param" value=""/>
                <Parameter name="Log.Application" value="true"/>
                <Parameter name="Filter.System.Type" value="No Filtering"/>
                <Parameter name="Filter.DNS Server.Type" value="No Filtering"/>
                <Parameter name="Filter.Application.Param" value=""/>
```

```
                <Parameter name="Filter.System.Param" value=""/>
                <Parameter name="Log.Directory Service" value="false"/>
                <Parameter name="ADLookup.DomainControllerName" value=""/>
                <Parameter name="Log.File Replication Service" value="false"/>
                <Parameter name="Filter.Directory Service.Enabled" value="false"/>
                <Parameter name="CustomQuery.Base64" value=""/>
                <Parameter name="Filter.Security.Param" value=""/>
                <Parameter name="EventRateTuningProfile" value="High Event Rate Server"/>
                <Parameter name="Local.System" value="true"/>
                <Parameter name="EventTypeFilterError" value="true"/>
                <Parameter name="EventTypeFilterWarn" value="true"/>
                <Parameter name="EventTypeFilterInfo" value="true"/>
                <Parameter name="Filter.File Replication Service.Param" value=""/>
                <Parameter name="Filter.File Replication Service.Type" value="No Filtering"/>
                <Parameter name="EventTypeFilterSuccessAudit" value="true"/>
                <Parameter name="Filter.Directory Service.Type" value="No Filtering"/>
                <Parameter name="Filter.Security.Type" value="No Filtering"/>
                <Parameter name="Application" value="None"/>
                <Parameter name="Log.System" value="true"/>
                <Parameter name="Log.ForwardedEvents" value="false"/>
                <Parameter name="Filter.Security.Enabled" value="false"/>
                <Parameter name="Filter.System.Enabled" value="false"/>
                <Parameter name="Log.DNS Server" value="false"/>
                <Parameter name="ADLookup.DNSDomainName" value=""/>
                <Parameter name="RemoteMachinePollInterval" value="3000"/>
                <Parameter name="MinLogsToProcessPerPass" value="1250"/>
                <Parameter name="MaxLogsToProcessPerPass" value="1825"/>
                <Parameter name="Login.Handle" value="0"/>
            </Environment>
        </Instance>
    </InstanceData>
</Service>
```

5. 次の行を、太字で示されたサンプル・コードに変更します。

```
<Parameter name="Filter.System.Type" value="NSAlist"/>
<Parameter name="Filter.System.Param" value=
"1,6,12,13,19,104,219,1001,1125,1126,1129,7000,7022,7023,7024,7026,7031,7032,7034,7045"/>
<Parameter name="Filter.System.Enabled" value="true"/>
```

6. service_DeviceWindowsLog.xml ファイルを保存して、これを ¥IBM¥WinCollect¥patch ディレクトリーに移動します。

   数秒後、ファイルが消え、エージェントが再始動されます。古い agentconfig.xml ファイルはバックアップ・ディレクトリー (patch_checkpoint_*xxxx*) に移されます。アップデート後のログ・ソース・サンプル:

```
<Service version="7.2.8" classification="Service" type="DeviceType"
module="DeviceWindowsLog" name="DeviceWindowsLog">
    <Environment>
        <Parameter name="DeviceThreadPoolType" value="AdaptiveThreadPool"/>
        <Parameter name="AdaptiveThreadPool.ReaderThreadsMax" value="500"/>
        <Parameter name="AdaptiveThreadPool.ReaderThreadsMin" value="5"/>
        <Parameter name="AdaptiveThreadPool.ReaderBacklogSamplePeriodMillis" value="200"/>
        <Parameter name="MinEventMonitorThreads" value="5"/>
        <Parameter name="MaxEventMonitorThreads" value="250"/>
        <Parameter name="EventLogMonitor.RetryTimeoutMillis" value="60000"/>
        <Parameter name="DefaultThrottleTimeout" value="1500"/>
        <Parameter name="DefaultEventLogPollProtocol" value="MSEVEN6"/>
    </Environment>
    <InstanceData>
        <Instance enabled="true" name="EventLogLocal">
            <Environment>
                <Parameter name="DeviceAddress" value="DESKTOP"/>
                <Parameter name="RemoteMachine" value="DESKTOP"/>
                <Parameter name="Filter.DNS Server.Enabled" value="false"/>
                <Parameter name="EventTypeFilterFailureAudit" value="true"/>
                <Parameter name="EventLogPollProtocol" value="MSEVEN6"/>
                <Parameter name="Log.Security" value="true"/>
                <Parameter name="Filter.Application.Enabled" value="false"/>
                <Parameter name="ADLookup.Enabled" value="false"/>
                <Parameter name="ThrottleTimeout" value="1000"/>
                <Parameter name="Filter.DNS Server.Param" value=""/>
                <Parameter name="Filter.File Replication Service.Enabled" value="false"/>
                <Parameter name="Filter.Application.Type" value="No Filtering"/>
                <Parameter name="Filter.Directory Service.Param" value=""/>
                <Parameter name="Log.Application" value="true"/>
                <Parameter name="Filter.DNS Server.Type" value="No Filtering"/>
                <Parameter name="Filter.Application.Param" value=""/>
```

```
                <Parameter name="Filter.System.Type" value="NSAlist"/>
                <Parameter name="Filter.System.Param"
value="1,6,12,13,19,104,219,1001,1125,1126,1129,7000,7022,7023,7024,7026,7031,7032,7034,7045"
/>
                <Parameter name="Filter.System.Enabled" value="true"/>
                <Parameter name="Log.Directory Service" value="false"/>
                <Parameter name="ADLookup.DomainControllerName" value=""/>
                <Parameter name="Log.File Replication Service" value="false"/>
                <Parameter name="Filter.Directory Service.Enabled" value="false"/>
                <Parameter name="CustomQuery.Base64" value=""/>
                <Parameter name="Filter.Security.Param" value=""/>
                <Parameter name="EventRateTuningProfile" value="High Event Rate Server"/>
                <Parameter name="Local.System" value="true"/>
                <Parameter name="EventTypeFilterError" value="true"/>
                <Parameter name="EventTypeFilterWarn" value="true"/>
                <Parameter name="EventTypeFilterInfo" value="true"/>
                <Parameter name="Filter.File Replication Service.Param" value=""/>
                <Parameter name="Filter.File Replication Service.Type" value="No Filtering"/>
                <Parameter name="EventTypeFilterSuccessAudit" value="true"/>
                <Parameter name="Filter.Directory Service.Type" value="No Filtering"/>
                <Parameter name="Filter.Security.Type" value="No Filtering"/>
                <Parameter name="Application" value="None"/>
                <Parameter name="Log.System" value="true"/>
                <Parameter name="Log.ForwardedEvents" value="false"/>
                <Parameter name="Filter.Security.Enabled" value="false"/>
                <Parameter name="Log.DNS Server" value="false"/>
                <Parameter name="ADLookup.DNSDomainName" value=""/>
                <Parameter name="RemoteMachinePollInterval" value="3000"/>
                <Parameter name="MinLogsToProcessPerPass" value="1250"/>
                <Parameter name="MaxLogsToProcessPerPass" value="1825"/>
                <Parameter name="Login.Handle" value="0"/>
            </Environment>
        </Instance>
    </InstanceData>
</Service>
```

ドメイン・コントローラー資格情報の制限付きポリシーが適用されるシステムでの構成オプション

適切なリモート・アクセス権を持つユーザーは、ドメイン管理者資格情報を使用せずにリモート・システムからイベントを収集できる場合があります。収集する情報によっては、ユーザーに追加の権限が必要な場合があります。例えば、リモート側でセキュリティー・イベント・ログを収集するには、QRadar ログ・ソースに構成されているユーザーは、エージェントがインストールされているサーバーからのセキュリティー・イベント・ログへのリモート・アクセス権が必要な場合があります。

制約事項:

リモート収集の場合、WinCollect ユーザーは Windows 管理者と連携して、以下の項目に確実にアクセスできるようにする必要があります。

- セキュリティー、システム、およびアプリケーションのイベント・ログ
- リモート・レジストリー
- メッセージ・ストリング情報が含まれている .dll ファイルまたは .exe ファイルが格納されているすべてのディレクトリー

Windows オペレーティング・システムとグループ・ポリシーの特定の組み合わせが配置されている場合、代替構成が不可能なことがあります。

ある Windows ドメイン内でのリモート収集の場合でも、また、ドメインを横断するリモート収集の場合でも、イベントの収集が確実に行われるようにするには、ドメイン管理者資格情報を必要とすることがあります。所属する企業のポリシーによりドメイン管理者資格情報の使用に制約がある場合、WinCollect のデプロイメントには、追加の構成ステップを実行する必要がある場合があります。

WinCollect エージェントがローカル・ホストからイベントを収集する場合、イベント収集サービスは、ローカル・システムのアカウント資格情報を使用してイベントを収集および転送します。ローカル収集を行うには、ローカル収集が発生するホストに WinCollect エージェントをインストールする必要があります。

コマンド・ラインからの WinCollect の構成の変更

Windows ホストのコマンド・ラインから WinCollect エージェントの構成を変更できます。

Windows ホストへの WinCollect エージェントの初期インストール後に、*<WinCollect_installation_path>*/bin にある `installhelper.exe` ファイルを使用して、構成を変更できます。

以下の構成パラメーターを変更できます。

表 *16.* 変更可能な構成パラメーター

パラメーター	**説明**
認証トークン	WinCollect サービスを許可します (例えば、AUTH_TOKEN=af111ff6-4f30-11eb-11fb-1fc1 17711111)。
構成サーバー (ホストおよびポート) (Configuration Server (host and port))	QRadar コンソールの IP アドレスまたはホスト名 (例えば、192.0.2.0 または myhost)。
デフォルトの状況サーバー・アドレス (Default Status Server Address)	WinCollect エージェントからの状況メッセージの送信先である構成サーバーの IP アドレスを表示します。

`installHelper.exe` ファイルには、以下の更新フラグがあります。

表 *17. InstallHelper* の更新フラグ

-h [--help]	`installHelper.exe` の使用法のオプションに関する詳細な情報が表示されます。
-P [--update-password]	AgentConfig.xml 構成ファイルのパスワードを更新します。ログイン・ハンドルと新規パスワードをコロンで区切って指定します。 例: `1:MyNewPassword`。 **注 :** パスワードはプレーン・テキストです。
-F [--update-password-with-file]	外部のファイルを使用して、AgentConfig.xml 構成ファイル内の一連のパスワードを更新します。 ログイン・ハンドルと新規パスワードをコロンで区切って指定します (1 行あたり 1 つ指定します)。 例: `1:MyNewPassword`。 **注 :** 入力ファイルは必ず消去するか、保護された状態にしてください。
-T [--update-auth-token]	構成サーバーと通信するために使用される新しい認証トークン。

例えば、WinCollect エージェントの許可トークンを変更するには、Windows ホストのコマンド・ラインで以下のコマンドを入力します。

```
<WinCollect_installation_path>/bin/installHelper.exe -T <authorization_token>
```

関連概念

ローカル・インストール (リモート・ポーリングを使用しない場合)
リモートでポーリングできないホストのそれぞれに WinCollect をローカルでインストールします。 WinCollect をインストールすると、IBM Security QRadar はエージェントを自動的にディスカバーするので、ユーザーは WinCollect ログ・ソースを作成することができます。

WinCollect エージェントに対する Windows イベント・サブスクリプション
単一の WinCollect エージェントにイベントを提供するには、Windows イベント・サブスクリプションを使用してイベントを転送できます。イベント・サブスクリプションを構成すると、多数の Windows ホストがそれらのイベントを管理者資格情報なしで IBM Security QRadar に転送できます。

関連タスク
リモート・ポーリング対象のレジストリーへのアクセスの構成

ローカル・インストール (リモート・ポーリングを使用しない場合)

リモートでポーリングできないホストのそれぞれに WinCollect をローカルでインストールします。WinCollect をインストールすると、IBM Security QRadar はエージェントを自動的にディスカバーするので、ユーザーは WinCollect ログ・ソースを作成することができます。

ログ・ソースの構成で「ローカル・システム」チェック・ボックスを選択することで、ローカル・システムの使用を指定することができます。

ローカル・インストールは、ドメイン・コントローラーにおける 1 秒当たりのイベント数 (EPS) のレートが高いため、リモートではこのようなシステムからのイベントのポーリング能力が制限される可能性がある場合に適しています。WinCollect エージェントのローカル・インストールでは、ユーザー・アクティビティーのピーク時に送信イベントが一気に増加するビジー状態のシステムでのスケーラビリティーを 実現できます。

関連概念
コマンド・ラインからの WinCollect の構成の変更
Windows ホストのコマンド・ラインから WinCollect エージェントの構成を変更できます。

WinCollect エージェントに対する Windows イベント・サブスクリプション
単一の WinCollect エージェントにイベントを提供するには、Windows イベント・サブスクリプションを使用してイベントを転送できます。イベント・サブスクリプションを構成すると、多数の Windows ホストがそれらのイベントを管理者資格情報なしで IBM Security QRadar に転送できます。

関連タスク
リモート・ポーリング対象のレジストリーへのアクセスの構成

リモート・ポーリング対象のレジストリーへのアクセスの構成

WinCollect ログ・ソースがイベントのポーリングをリモート側で実行できるようにするには、Windows ベース・システムのローカル・ポリシーを構成する必要があります。

リモート・システムのそれぞれでローカル・ポリシーが構成されている場合、単一の WinCollect エージェントが、Windows Event Log API を使用してリモート・レジストリーを読み取り、イベント・ログを取得します。Windows Event Log API には、ドメイン管理者の資格情報は必要ありません。ただし、このイベント API 方式には、リモート・レジストリーおよびセキュリティー・イベント・ログにアクセスできるアカウントが必要です。

この収集方式を使用した場合、ログ・ソースはリモート側で完全なイベント・ログを読み取ることができます。ただし、この方式では、WinCollect がリモート・ホストから取得したイベント・ログ情報を、キャッシュされたメッセージのコンテンツに照らし合わせて解析する必要があります。WinCollect は、リモート・オペレーティング・システムからのバージョン情報を使用して、メッセージのコンテンツが正しく解析されたことを確認してから、イベントを IBM Security QRadar に転送します。

手順

1. リモート側でイベントをポーリングする対象の Windows コンピューターにログオンします。
2. 「**スタート**」 > 「**プログラム**」 > 「**管理ツール**」を選択し、「**ローカル セキュリティ ポリシー**」をクリックします。
3. ナビゲーション・メニューから、「**ローカル ポリシー**」 > 「**ユーザー権利の割り当て**」を選択します。
4. 右クリックして、「**監査とセキュリティ ログの管理**」 > 「**プロパティ**」を選択します。
5. 「**ローカル セキュリティの設定**」タブで、「**ユーザーまたはグループの追加**」をクリックし、WinCollect ユーザーをローカル・セキュリティー・ポリシーに追加します。

6. Windows ホストからログアウトして、WinCollect ログ・ソースに属する Windows ベースのイベントを対象にリモート・ホストをポーリングします。

   WinCollect ログ・ソースのイベントを収集できない場合は、グループ・ポリシーがローカル・ポリシーをオーバーライドしていないことを確認してください。Windows ホストのローカル・ファイアウォールの設定で、リモート・イベント・ログ管理が許可されていることを確認することもできます。

関連概念

コマンド・ラインからの WinCollect の構成の変更
Windows ホストのコマンド・ラインから WinCollect エージェントの構成を変更できます。

ローカル・インストール (リモート・ポーリングを使用しない場合)
リモートでポーリングできないホストのそれぞれに WinCollect をローカルでインストールします。WinCollect をインストールすると、IBM Security QRadar はエージェントを自動的にディスカバーするので、ユーザーは WinCollect ログ・ソースを作成することができます。

WinCollect エージェントに対する Windows イベント・サブスクリプション
単一の WinCollect エージェントにイベントを提供するには、Windows イベント・サブスクリプションを使用してイベントを転送できます。イベント・サブスクリプションを構成すると、多数の Windows ホストがそれらのイベントを管理者資格情報なしで IBM Security QRadar に転送できます。

WinCollect エージェントに対する Windows イベント・サブスクリプション

単一の WinCollect エージェントにイベントを提供するには、Windows イベント・サブスクリプションを使用してイベントを転送できます。イベント・サブスクリプションを構成すると、多数の Windows ホストがそれらのイベントを管理者資格情報なしで IBM Security QRadar に転送できます。

転送されたイベント

収集されるイベントは、イベントを送信するリモート・ホストのイベント・サブスクリプションの構成で定義されます。WinCollect は、ログ・ソースに関してどのイベント・ログのチェック・ボックスが選択されているかにかかわらず、サブスクリプション構成によって送信されるすべてのイベントを転送します。

Windows イベント・サブスクリプション、つまり転送されたイベントは、ローカルやリモートとはみなされません。これらはイベント・リスナーです。WinCollect の「**転送されたイベント**」チェック・ボックスを使用すると、WinCollect ログ・ソースで Windows イベント・サブスクリプションを識別できるようになります。WinCollect エージェントは、ユーザー・インターフェースに 単一のログ・ソースのみを表示しますが、このログ・ソースが、数百件も存在する可能性があるイベント・サブスクリプションについて、イベントを listen し、処理します。エージェント内の 1 つのログ・ソースが、すべてのイベント・サブスクリプションについてイベントをリストします。エージェントは、サブスクリプションによるイベントを認識し、コンテンツを処理して、QRadar に Syslog イベントを送信します。

注 : 転送されたイベントの収集は、「転送されたイベント」チェック・ボックスを使用する方法でのみ実行できます。XPATH は使用できません。

転送されたイベントは `Windows Auth @ <hostname>` または `<FQDN>` として「**ログ・アクティビティー**」タブに表示されます。それに対し、ローカルまたはリモートで収集されたイベントは、`Windows Auth @ <IP address>` または `<hostname>` として表示されます。WinCollect は、ローカルまたはリモートで収集されたイベントを処理するときに、そのイベントを WinCollect イベントとして識別する、追加の Syslog ヘッダーを含むようになります。転送されたイベントはパススルー、つまりリスナーであるため、そのイベントが WinCollect ID を含むことはなく、標準イベントとして表示されます。

重要 : 転送されたイベントは、Windows イベント・ビューアー内に表示されるものだけが WinCollect によって収集されます。

サポートされるソフトウェア環境

イベント・サブスクリプションは、以下の Windows オペレーティング・システム 上で構成された WinCollect エージェントとホストに対してのみ適用されます。

- Windows 8 (最新)
- Windows 7 (最新)

- Windows Server 2008 (最新)
- Windows Server 2012 (最新)
- Windows 10 (最新)
- Windows Server 2016 (Core を含む)
- Windows Server 2019 (Core を含む)

重要 : WinCollect は、Microsoft がサポートを終了した Windows のバージョンではサポートされていません。ソフトウェアの延長サポート終了日が過ぎていても、製品が期待どおりに機能することがあります。ただし、IBM は、古いオペレーティング・システムで発生した WinCollect の問題を解決するために、コードまたは脆弱性のフィックスを作成することはありません。例えば、Microsoft Windows Server 2003 R2 および Microsoft Windows XP は、「延長サポート終了日」を過ぎたオペレーティング・システムです。この発表について質問がある場合は、IBM QRadar Collecting Windows Events (`WMI/ALE/WinCollect`) フォーラムで相談できます。詳しくは、https://support.microsoft.com/en-us/lifecycle/search (https://support.microsoft.com/en-us/lifecycle/search) を参照してください。

イベント・サブスクリプションについて詳しくは、Microsoft の資料か、または Microsoft の技術情報の Web サイト (http://technet.microsoft.com/en-us/library/cc749183.aspx) を参照してください。

イベント・コレクションのトラブルシューティング

Microsoft のイベント・サブスクリプションには、イベント・ソースによるイベントの送信が停止したときにそれを示すアラート・メカニズムがありません。2 つの Windows システム間でサブスクリプションに障害が発生した場合、サブスクリプションはアクティブであるように見えても、サブスクリプションの処理を行うサービスはエラー状態である可能性があります。WinCollect では、イベントが 720 分間 (12 時間) 以内に受信されないときは、リモートでポーリングされるログ・ソースまたはローカルのログ・ソースがタイムアウトになる可能性があります。

関連概念

コマンド・ラインからの WinCollect の構成の変更
Windows ホストのコマンド・ラインから WinCollect エージェントの構成を変更できます。

ローカル・インストール (リモート・ポーリングを使用しない場合)
リモートでポーリングできないホストのそれぞれに WinCollect をローカルでインストールします。WinCollect をインストールすると、IBM Security QRadar はエージェントを自動的にディスカバーするので、ユーザーは WinCollect ログ・ソースを作成することができます。

関連タスク

リモート・ポーリング対象のレジストリーへのアクセスの構成

Microsoft イベント・サブスクリプションの構成

イベントを単一の WinCollect エージェントに転送するように Microsoft イベント・サブスクリプションを構成します。

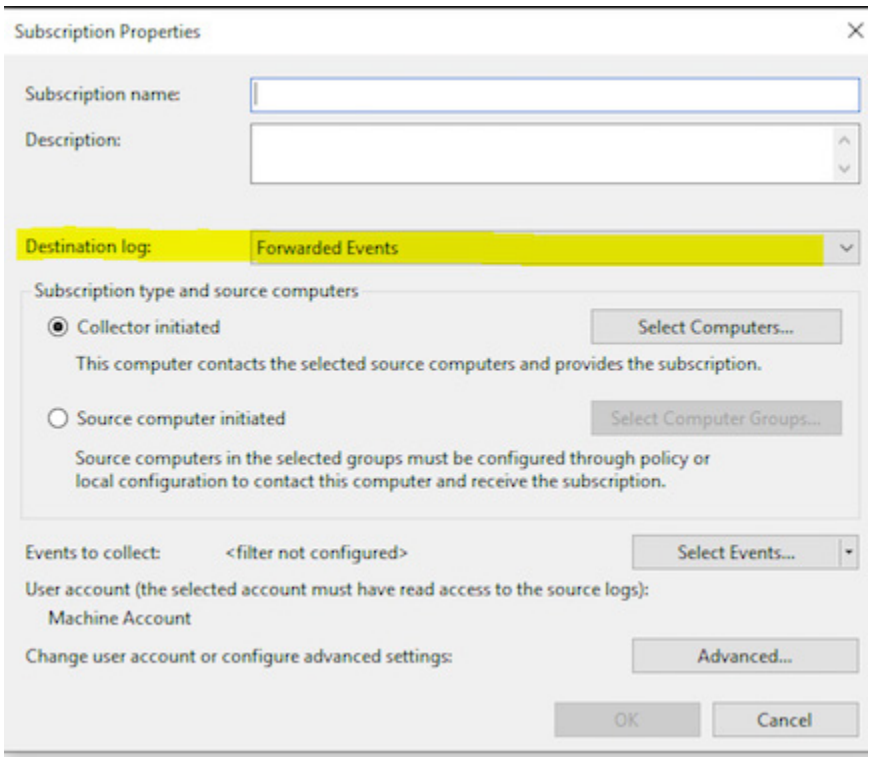
始める前に

WinCollect は、以下のパラメーターを使用したイベント・サブスクリプションをサポートします。

転送されたイベント
サブスクリプションは、転送されたイベント・チャネルにログを送信する必要があります。「**宛先ログ**」リストで選択します (画面キャプチャーを参照してください)。

サブスクリプション (Subscriptions)
ContentFormat: `RenderedText` および **Locale:** `en-US` を使用するように構成されたサブスクリプション。

ロケール
ロケールは、WinCollect がインストールされている Windows コンピューターでは en_US でなければなりません。



注 : ドメイン・コントローラーを使用している場合は、それらのサーバーにローカル WinCollect エージェントをインストールすることを検討してください。生成される可能性のあるイベントの数を考慮して、ドメイン・コントローラーにインストールされているエージェントではローカル・ログ・ソースを使用してください。

手順

1. ご使用の Windows ホストでイベント・サブスクリプションを構成します。

   イベント・サブスクリプションの構成手順については、Microsoft イベント・コレクターの資料を参照してください。 (https://docs.microsoft.com/en-us/windows/desktop/wec/creating-an-event-collector-subscription)
2. イベントを受信する WinCollect エージェントでのログ・ソースを構成します。

   WinCollect ログ・ソースに関して、「**ローカル・システム**」チェック・ボックスおよび「**転送されたイベント**」チェック・ボックスを選択する必要があります。

   注 : IBM サポートは、Microsoft サブスクリプションの作成や保守には対応していません。

関連タスク

WinCollect エージェントへのログ・ソースの追加

WinCollect エージェントに新規ログ・ソースを追加した場合、またはログ・ソースのパラメーターを編集した場合、WinCollect サービスは再始動されます。エージェントで WinCollect サービスが再始動される間、イベントはキャッシュされます。

第 5 章 WinCollect エージェントのログ・ソース

WinCollect エージェントは、ローカル・システムからイベントを収集して転送することや、複数の Windows ベースのログ・ソースとオペレーティング・システムに対してイベントのリモート・ポーリングを行うことができます。

リモート・ポーリングを行う場合は、WinCollect エージェントを通じて通信するログ・ソースを個別に追加できます。それらのログ・ソースに類似の構成が含まれている場合は、複数のログ・ソースを同時に追加したり、ログ・ソースを一括追加したりできます。個別に追加されたログ・ソースに加えられた変更によって更新されるのは、その個別のログ・ソースのみです。ログ・ソースのグループに加えられた変更の場合は、そのログ・ソースのグループ内のすべてのログ・ソースが更新されます。

ローカル収集を行う場合は、ローカルのログ・ソースを追加できます。ログ・ソースが自動作成されない場合は、手動で作成できます。

重要 : デプロイメントの複数のドメインのそれぞれに同じユーザー名を持つユーザー・アカウントがある場合は、WinCollect ログ・ソースを作成するときにドメイン情報を構成してください。

Windows イベント・ログ

Windows エンドポイントからイベント・ログを収集できます。

Windows イベント・ログを照会すると、すべてのイベントがログに記録されます。イベント・ログのフィルター処理または XPath 照会を使用すると、受信するイベントを制限できます。

Windows イベント・ログは以下の言語でサポートされています。

- 中国語 (簡体字)
- 中国語 (繁体字)
- 英語
- フランス語
- ドイツ語
- イタリア語
- 日本語
- 韓国語
- ポルトガル語
- ロシア語
- スペイン語

Windows イベント・ログのフィルター処理

WinCollect エージェントは、Windows イベント・ログから収集された特定のイベントを無視するように構成することも、含めるように構成することもできます。QRadar コンソール に送信される合計 EPS (1 秒あたりのイベント数) はフィルター・タイプを使用して制限できます。

WinCollect エージェントは、ID コードまたはログ・ソースを指定してグローバルにイベントを無視するように構成できます。グローバル除外では、イベント・ペイロードの **EventIDCode** フィールドを使用します。ソースおよび ID による除外では、Windows ペイロードの **Source=field** と **EventIDCode=field** を使用して除外対象の値を判別します。複数のソースはセミコロンを使用して区切ります。以下のログ・ソース・タイプでは、除外、包含、NSA などのイベント・フィルターを使用できます。

- セキュリティー
- システム
- アプリケーション

- DNS サーバー
- ファイル・レプリケーション・サービス
- ディレクトリー・サービス
- 転送されたイベント

WinCollect エージェントは、「ポーリング間隔」フィールドに指定された値が期限切れになるたびに、イベント・コレクション API から使用可能なすべてのイベントを要求します。

除外フィルターの場合、エージェントは、イベント・コレクション API から取得されたすべてのイベントを検査し、管理者が (Windows イベント ID またはソースで) 定義した除外項目に一致するイベントを無視します。次にエージェントは、残りのイベントで **name=value** ペアを集めて、QRadar コンソール または Event Collector アプライアンスにそれらのイベントを転送します。 ただし、包含フィルターの場合、エージェントは、管理者が指定したイベント ID と一致するイベントをプルして、それらのイベントを QRadar コンソール またはイベント・コレクターに転送します。

NSA フィルターは、対応する事前定義のセキュリティー・イベント ID のリストを含む独自のタイプのフィルターです。この ID を、エージェントがセキュリティー、システム、アプリケーション、および DNS の各ログからプルします。これらの事前定義のセキュリティー・イベント ID は、エージェントがコンソールまたはイベント・コレクターに転送するイベントに組み込まれています。

ヒント : 「転送されたイベント」フィルターを 使用する場合は、フィルタリングするイベント ID を括弧で囲み、送信元またはチャネルを特定する必要があります。 区切り文字としてはセミコロンを使用します。例:

```
Application(200-256,4097,34);Security(1);Symantec(1,13)
```

この例では、チャネル・アプリケーションについてはイベント ID 200 から 256、4097 および 34 が、セキュリティーについてはイベント ID 1 が、Symantec という送信元についてはイベント ID 1 および 13 がフィルタリングされます。

Windows ログ・ソースのパラメーター

WinCollect エージェントまたは WinCollect プラグインのログ・ソースを構成する際には、共通パラメーターを使用します。WinCollect プラグインごとに固有の構成オプションのセットもあります。

表 *18. WinCollect* ログ・ソースの共通パラメーター

パラメーター	説明
ログ・ソース ID (Log Source Identifier)	Windows ベースのイベントの収集元となるリモートの Windows オペレーティング・システムの IP アドレスまたはホスト名。ログ・ソース ID は、該当するログ・ソース・タイプで固有でなければなりません。 リモート・ソースのイベントをポーリングするために使用されます。
ローカル・システム (Local System)	ログ・ソースのリモート・イベント収集を無効にします。 ログ・ソースは、ローカル・システムの資格情報を使用して、イベントを収集し、QRadar に転送します。 **注 :** 完全修飾ドメイン名 (FQDN) ログ・ソース ID を使用していて、エージェントがドメイン・コントローラーにインストールされている場合は、このボックスをクリアする必要があります。

表 18. *WinCollect* ログ・ソースの共通パラメーター (続き)

パラメーター	説明
ドメイン	オプション Windows ベースのログ・ソースが含まれるドメイン。 LAB1, server1.mydomain.com は、正しい構文が使用されている例です。¥¥mydomain.com は、誤った構文です。
イベント・レート・チューニング・プロファイル (Event Rate Tuning Profile)	デフォルトのポーリング間隔 3000 ミリ秒の場合、達成可能な 1 秒当たりの概算のイベント数 (EPS) は以下のとおりです。 • **デフォルト (エンドポイント) (Default (Endpoint))**: 33 から 50 EPS • **標準的なサーバー (Typical Server)**: 166 から 250 EPS • **イベント・レートが高いサーバー (High Event Rate Server)**: 416 から 625 EPS ポーリング間隔が 1000 ミリ秒の場合、概算の EPS レートは以下のとおりです。 • **デフォルト (エンドポイント) (Default (Endpoint))**: 100 から 150 EPS • **標準的なサーバー (Typical Server)**: 500 から 750 EPS • **イベント・レートが高いサーバー (High Event Rate Server)**: 1250 から 1875 EPS WinCollect のチューニングについて詳しくは、IBM サポート (http://www.ibm.com/support/docview.wss?uid=swg21672193) を参照してください。
ポーリング間隔 (ms)	WinCollect が新しいイベントをポーリングする間隔 (ミリ秒)。
アプリケーションまたはサービスのログ・タイプ (Application or Service Log Type)	オプション。 XPath 照会に使用します。 イベントを Windows アプリケーション・ログの一部として書き込む製品専用の XPath 照会を指定します。これにより、Windows イベントを、別の製品のログ・ソースに分類されるイベントから分離できます。
イベント・ログ・ポーリング・プロトコル (Event Log Poll Protocol)	QRadar が Windows デバイスと通信するために使用するプロトコル。デフォルトは **MSEVEN6** です。

表 18. *WinCollect* ログ・ソースの共通パラメーター *(続き)*	
パラメーター	**説明**
ログ・フィルター・タイプ (Log Filter Type)	Windows イベント・ログからの特定のイベントを無視するように WinCollect エージェントを構成します。 ID コードまたはログ・ソースを指定してグローバルにイベントを無視するように WinCollect エージェントを構成することもできます。 イベントの除外フィルター を使用できるログ・ソース・タイプは、セキュリティー、システム、アプリケーション、DNS サーバー、ファイル複製サービス、およびディレクトリー・サービスです。 グローバル除外では、イベント・ペイロードの **EventIDCode** フィールドを使用します。ソースおよび ID による除外では、Windows イベント・ペイロードの `Source=` フィールドと `EventIDCode=` フィールドを使用して除外対象の値を判別します。複数のソースはセミコロンを使用して区切ります。 **例 :** 除外フィルターでは、4609, 4616, 6400-6405 のようにコンマおよびハイフンを使用して、単一のイベント ID または範囲をフィルタリングできます。 フィルタリングについて詳しくは、『WinCollect Event Filtering』(http://www.ibm.com/support/docview.wss?uid=swg21672656) を参照してください。
セキュリティー	このチェック・ボックスを選択すると、WinCollect がセキュリティー・ログを QRadar に転送できるようになります。
セキュリティー・ログ・フィルター・タイプ (Security Log Filter Type)	Windows イベント・ログから収集された特定のイベント ID を無視するには、「**除外フィルター (Exclusion Filter)**」を選択します。 Windows イベント・ログで収集された特定のイベント ID を含めるには、「**包含フィルター (Inclusion Filter)**」を選択します。 「**NSA フィルター (NSA Filter)**」オプションを使用すると、国家安全保障局が推奨するイベント ID のリストが「**セキュリティー・ログ・フィルター (Security Log Filter)**」フィールドに設定されます。 デフォルトは、「**フィルタリングなし (No Filtering)**」です。 **注 :** リストからフィルター・タイプを選択すると、「**セキュリティー・ログ・フィルター (Security Log Filter)**」という新しいフィールドが表示されます。含めるまたは除外するイベント ID を指定する必要があります。

表 *18. WinCollect* ログ・ソースの共通パラメーター *(*続き*)*	
パラメーター	**説明**
システム	このチェック・ボックスを選択すると、WinCollect がシステム・ログを QRadar に転送できるようになります。
システム・ログ・フィルター・タイプ (System Log Filter Type)	Windows イベント・ログから収集された特定のイベント ID を無視するには、「**除外フィルター (Exclusion Filter)**」を選択します。 Windows イベント・ログで収集された特定のイベント ID を含めるには、「**包含フィルター (Inclusion Filter)**」を選択します。 「**NSA フィルター (NSA Filter)**」オプションを使用すると、国家安全保障局が推奨するイベント ID のリストが「**システム・ログ・フィルター (System Log Filter)**」フィールドに設定されます。 デフォルトは、「**フィルタリングなし (No Filtering)**」です。 **注 :** リストからフィルター・タイプを選択すると、「**システム・ログ・フィルター (System Log Filter)**」という新しいフィールドが表示されます。含めるまたは除外するイベント ID を指定する必要があります。
アプリケーション	このチェック・ボックスを選択すると、WinCollect がアプリケーション・ログを QRadar に転送できるようになります。
アプリケーション・ログ・フィルター・タイプ (Application Log Filter Type)	Windows イベント・ログから収集された特定のイベント ID を無視するには、「**除外フィルター (Exclusion Filter)**」を選択します。 Windows イベント・ログで収集された特定のイベント ID を含めるには、「**包含フィルター (Inclusion Filter)**」を選択します。 「**NSA フィルター (NSA Filter)**」オプションを使用すると、国家安全保障局が推奨するイベント ID のリストが「**アプリケーション・ログ・フィルター (Application Log Filter)**」フィールドに設定されます。 デフォルトは、「**フィルタリングなし (No Filtering)**」です。 **注 :** リストからフィルター・タイプを選択すると、「**アプリケーション・ログ・フィルター (Application Log Filter)**」という新しいフィールドが表示されます。含めるまたは除外するイベント ID を指定する必要があります。
DNS サーバー	このチェック・ボックスを選択すると、WinCollect が DNS サーバー・ログを QRadar に転送できるようになります。

表 *18. WinCollect* ログ・ソースの共通パラメーター *(*続き*)*	
パラメーター	**説明**
DNS サーバー・ログ・フィルター・タイプ (DNS Server Log Filter Type)	Windows イベント・ログから収集された特定のイベント ID を無視するには、「**除外フィルター (Exclusion Filter)**」を選択します。 Windows イベント・ログで収集された特定のイベント ID を含めるには、「**包含フィルター (Inclusion Filter)**」を選択します。 「**NSA フィルター (NSA Filter)**」オプションを使用すると、国家安全保障局が推奨するイベント ID のリストが「**DNS サーバー・ログ・フィルター (DNS Server Log Filter)**」フィールドに設定されます。 デフォルトは、「**フィルタリングなし (No Filtering)**」です。 **注 :** リストからフィルター・タイプを選択すると、「**DNS サーバー・ログ・フィルター (DNS Server Log Filter)**」という新しいフィールドが表示されます。含めるまたは除外するイベント ID を指定する必要があります。
ファイル・レプリケーション・サービス (File Replication Service)	このチェック・ボックスを選択すると、WinCollect がファイル・レプリケーション・サービス・ログを QRadar に転送できるようになります。
ファイル・レプリケーション・サービス・ログ・フィルター・タイプ (File Replication Service Log Filter Type)	Windows イベント・ログから収集された特定のイベント ID を無視するには、「**除外フィルター (Exclusion Filter)**」を選択します。 Windows イベント・ログで収集された特定のイベント ID を含めるには、「**包含フィルター (Inclusion Filter)**」を選択します。 **注 :** リストからフィルター・タイプを選択すると、「**ファイル・レプリケーション・サービス・ログ・フィルター (File Replication Service Log Filter)**」という新しいフィールドが表示されます。含めるまたは除外するイベント ID を指定する必要があります。
ディレクトリー・サービス	このチェック・ボックスを選択すると、WinCollect がディレクトリー・サービス・ログを QRadar に転送できるようになります。
ディレクトリー・サービス・ログ・フィルター・タイプ (Directory Service Log Filter Type)	Windows イベント・ログから収集された特定のイベント ID を無視するには、「**除外フィルター (Exclusion Filter)**」を選択します。 Windows イベント・ログで収集された特定のイベント ID を含めるには、「**包含フィルター (Inclusion Filter)**」を選択します。 **注 :** リストからフィルター・タイプを選択すると、「**ディレクトリー・サービス・ログ・フィルター (Directory Service Log Filter)**」という新しいフィールドが表示されます。含めるまたは除外するイベント ID を指定する必要があります。

表 *18. WinCollect* ログ・ソースの共通パラメーター *(*続き*)*

パラメーター	説明
転送されたイベント	イベント・サブスクリプションを使用しているリモート Windows イベント・ソースから転送されたイベントを、QRadar で収集できるようにします。 イベント・サブスクリプションを使用する転送イベントは、WinCollect エージェントによって自動的に検出され、syslog イベント・ソースであるかのように転送されます。 Windows システムからのイベント転送を構成する場合は、イベントの事前レンダリングを有効にしてください。 **重要 :** WinCollect は、「転送されたイベント」チャネルからのログのプルのみをサポートしています。あるサブスクリプションから別のチャネルへのイベントの書き込みはサポートされていません。
転送されたイベントのフィルタリング・タイプ	Windows イベント・ログから収集された特定のイベント ID を無視するには、「**除外フィルター (Exclusion Filter)**」を選択します。 Windows イベント・ログで収集された特定のイベント ID を含めるには、「**包含フィルター (Inclusion Filter)**」を選択します。 「**NSA フィルター (NSA Filter)**」オプションを使用すると、国家安全保障局が推奨するすべてのチャネルとそれぞれのフィルターが「**転送されたイベント・フィルター (Forwarded Events filter)**」フィールドに設定されます。 デフォルトは、「**フィルタリングなし (No Filtering)**」です。 **注 :** リストからフィルター・タイプを選択すると、「**転送されたイベント・フィルター (Forwarded Events filter)**」という新しいフィールドが表示されます。含めるまたは除外するイベント ID を指定する必要があります。 「転送されたイベント」フィルターを使用する場合は、フィルタリングするイベント ID を括弧で囲み、送信元またはチャネルを特定する必要があります。区切り文字としてはセミコロンを使用します。例: `Application(200-256,4097,34); Security(1);Symantec(1,13)` この例では、チャネル・アプリケーションについてはイベント ID 200 から 256、4097 および 34 が、セキュリティーについてはイベント ID 1 が、Symantec という送信元についてはイベント ID 1 および 13 がフィルタリングされます。
イベント・タイプ (Event Type)	少なくとも 1 つのイベント・タイプを選択する必要があります。

表 *18. WinCollect* ログ・ソースの共通パラメーター *(続き)*	
パラメーター	**説明**
Active Directory ルックアップの有効化 (Enable Active Directory Lookups)	WinCollect エージェントが、Active Directory ルックアップを担当しているドメイン・コントローラーと同じドメインに属している場合、このチェック・ボックスを選択して、ドメインおよび DNS のオーバーライドのパラメーターを空白にすることができます。 **重要 :** 「**ドメイン・コントローラー名ルックアップ (Domain Controller Name Lookup)**」および「**DNS ドメイン名ルックアップ (DNS Domain Name Lookup)**」パラメーターの値を入力する必要があります。
ドメイン・コントローラー名のオーバーライド (Override Domain Controller Name)	Active Directory ルックアップを担当するドメイン・コントローラーが WinCollect エージェントのドメイン外部にある場合、必須です。 Active Directory ルックアップを担当するドメイン・コントローラーの IP アドレスまたはホスト名。
XPath 照会	Windows イベント・ログからカスタマイズしたイベントを取得するために使用する、構造化 XML 式。 XPath 照会を使用してイベントをフィルターに掛ける場合、その XPath 照会で指定した項目に加えて、「**標準ログ・タイプ (Standard Log Type)**」または「**イベント・タイプ (Event Type)**」で選択したチェック・ボックスの項目も収集されます。 XPath 照会を使用して情報を収集するには、Windows 2008 上では、「**リモート イベントのログ管理**」を有効にする必要があります。
ターゲット内部宛先	内部宛先として、イベント・プロセッサー・コンポーネントがある任意の管理対象ホストを使用します。
ターゲット外部宛先	宛先リストで構成した 1 つ以上の外部宛先に、イベントを転送します。

「アプリケーションとサービス」のログ

「アプリケーションとサービス」のイベント・ログからイベントを収集するには、XPath 照会を使用します。

XPath 照会は、Windows イベント・ログからカスタマイズしたイベントを取得するために使用する構造化 XML 式です。

関連資料

Windows ログ・ソースのパラメーター

WinCollect エージェントまたは WinCollect プラグインのログ・ソースを構成する際には、共通パラメーターを使用します。WinCollect プラグインごとに固有の構成オプションのセットもあります。

カスタム・ビューの作成

Microsoft イベント・ビューアーを使用してカスタム・ビューを作成します。このビューでは、重大度、ソース、カテゴリー、キーワード、特定のユーザーについてイベントをフィルタリングすることができます。

WinCollect のログ・ソースは、XPath フィルターを使用してログから特定のイベントを取り込むことができます。 XPath 照会パラメーターの XML マークアップを作成するには、カスタム・ビューを作成する必要があります。 Microsoft イベント・ビューアーを使用するには、管理者としてログインする必要があります。

注 : 使用する XPath 照会の数が 10 を超えると、XPath および各チャネルで受信するイベントの数によっては WinCollect のパフォーマンスに影響が生じる場合があります。

WinCollect プロトコルを使用する XPath 照会では、TimeCreated 表記の時刻範囲によるイベントのフィルターはサポートされません。 イベントを時刻範囲でフィルターすると、イベントの収集でエラーが発生する可能性があります。

手順

1. ご使用のデスクトップで、「**スタート**」 > 「**ファイル名を指定して実行**」をクリックします。
2. 以下のコマンドを入力します。

   ```
   Eventvwr.msc
   ```
3. 「**OK**」をクリックします。
4. プロンプトが出されたら、管理者パスワードを入力して、Enter を押します。
5. 「**操作**」 > 「**カスタム ビューの作成**」をクリックします。

   カスタム・ビューを作成する場合は、「**ログの日付**」リストから時刻範囲を選択しないでください。「**ログの日付**」リストには、**TimeCreated** エレメントが含まれています。このエレメントは、WinCollect プロトコルの XPath 照会ではサポートされていません。
6. 「**イベント レベル**」で、カスタム・ビューに含めるイベントの重大度のチェック・ボックスを選択します。
7. イベント・ログのソースを選択します。「**イベント ソース**」ドロップダウン・メニューからソースを選択するか、「**イベント ログ**」ドロップダウン・メニューからソースを参照できます。
8. イベント・ソースまたはログ・ソースからフィルターに掛けるイベント ID を入力します。

   ID を区切るにはコンマを使用します。

   次のリストには、個別の ID と範囲が含まれています。4133, 4511-4522
9. 「**タスクのカテゴリ**」リストで、イベント・ソースまたはログ・ソースからフィルターに掛けるカテゴリーを選択します。
10. 「**キーワード**」リストで、イベント・ソースまたはログ・ソースからフィルターに掛けるキーワードを選択します。
11. イベント・ソースまたはログ・ソースからフィルターに掛けるユーザー名を入力します。
12. イベント・ソースまたはログ・ソースからフィルターに掛けるコンピューター (複数可) を入力します。
13. 「**XML**」タブをクリックします。
14. XML をコピーして、WinCollect ログ・ソース構成の「**XPath 照会**」フィールドに貼り付けます。

次のタスク

XPath 照会を使用してログ・ソースを構成します。詳しくは、60 ページの『「アプリケーションとサービス」のログ』を参照してください。

XPath 照会の例

XPath 照会を作成する際の参照として、XPath でイベントをモニターする例、およびログオン資格情報を取得する例を使用してください。

XPath 照会について詳しくは、Microsoft の資料を参照してください。

注 : XPath は、MSEVEN6 イベント・プロトコルのみを使用します。

例: 特定のユーザーに関するイベントのモニター

この例の照会では、すべての Windows イベント・ログから、ゲスト・ユーザーについてのイベントを取得します。

重要 : XPath 照会は、Windows の転送されたイベントをフィルタリングできません。

```
<QueryList>
<Query Id="0" Path="Application">
<Select Path="Application">*[System[(Level=4 or Level=0) and
Security[@UserID='S-1-5-21-3709697454-1862423022-1906558702-501
']]]</Select>
<Select Path="Security">*[System[(Level=4 or Level=0) and
Security[@UserID='S-1-5-21-3709697454-1862423022-1906558702-501
']]]</Select>
<Select Path="Setup">*[System[(Level=4 or Level=0) and
Security[@UserID='S-1-5-21-3709697454-1862423022-1906558702-501
']]]</Select>
<Select Path="System">*[System[(Level=4 or Level=0) and
Security[@UserID='S-1-5-21-3709697454-1862423022-1906558702-501
']]]</Select>

</Query>
</QueryList>.
```

例: Windows 2008 の資格情報ログオン

この例の照会では、セキュリティー・ログから、Windows 2008 のアカウント認証に関連付けられている、通知レベルのイベントについての特定のイベント ID を取得します。

```
<QueryList>
<Query Id="0" Path="Security">
<Select Path="Security">*[System[(Level=4 or Level=0) and
( (EventID &gt;= 4776 and EventID &lt;= 4777) )]]</Select>
</Query>
</QueryList>
```

表 *19.* 資格情報ログオンの例で使用されているイベント *ID*

ID	説明
4776	ドメイン・コントローラーがアカウントの資格情報を検証しようとしました。
4777	ドメイン・コントローラーがアカウントの資格情報の検証に失敗しました。

例: ユーザーに基づくイベントの取得

この例の照会では、イベント ID を検査して、ユーザー・パスワード・データベースが含まれる架空のコンピューター上で作成されたユーザー・アカウントに関する特定のイベントを取得します。

```
<QueryList>
<Query Id="0" Path="Security">
<Select Path="Security">*[System[(Computer='Password_DB') and
(Level=4 or Level=0) and (EventID=4720 or (EventID &gt;= 4722
and EventID &lt;= 4726) or (EventID &gt;= 4741 and EventID
&lt;= 4743) )]]</Select>
</Query>
</QueryList>
```

表 *20.* データベースの例で使用されているイベント *ID*

ID	説明
4720	ユーザー・アカウントが作成されました。

表 20. データベースの例で使用されているイベント ID (続き)	
ID	**説明**
4722	ユーザー・アカウントを有効にしました。
4723	アカウントのパスワードを変更しようとしました。
4724	アカウントのパスワードをリセットしようとしました。
4725	ユーザー・アカウントを無効にしました。
4726	ユーザー・アカウントが削除されました。
4741	ユーザー・アカウントが作成されました。
4742	ユーザー・アカウントが変更されました。
4743	ユーザー・アカウントが削除されました。

例: DNS 分析ログの取得

この例の照会では、DNS 分析ログに収集されたすべてのイベントを取得します。

```
<QueryList>
  <Query Id="0" Path="Microsoft-Windows-DNSServer/Analytical">
    <Select Path="Microsoft-Windows-DNSServer/Analytical">*</Select>
  </Query>
</QueryList>
```

例: Sysinternals Sysmon を使用したイベントの取得

この例の照会では、Sysinternals Sysmon によって収集されたすべてのイベントを取得します。

```
<QueryList>
<Query Id="0" Path="Microsoft-Windows-Sysmon/Operational">
<Select Path="Microsoft-Windows-Sysmon/Operational">*</Select>
</Query>
</QueryList>
```

Microsoft DHCP ログ・ソースの構成オプション

この参照情報を使用して、Microsoft DHCP 用の WinCollect プラグインを構成してください。

制約事項 : WinCollect エージェントのタイム・ゾーンは、ポーリング対象に構成されたリモート DHCP サーバーのタイム・ゾーンと同じである必要があります。

表 21. *Microsoft DHCP* のプロトコル・パラメーター	
パラメーター	**説明**
ログ・ソース・タイプ	**Microsoft DHCP**
プロトコル構成	**WinCollect Microsoft DHCP**
ローカル・システム (Local System)	WinCollect エージェントが Microsoft DHCP サーバーにインストールされている必要があります。 ログ・ソースは、ローカル・システムの資格情報を使用して、イベントを収集し、QRadar に転送します。

表 *22. Microsoft DHCP* イベントのデフォルトのルート・ログ・ディレクトリー・パス.

WinCollect によってモニターされる DHCP イベント・ログは、WinCollect DHCP ログ・ソース内で指定するディレクトリー・パスによって定義されます。

収集タイプ	**ルート・ログ・ディレクトリー**
ローカル	`c:¥WINDOWS¥system32¥dhcp`
リモート	`¥¥DHCP IP address¥c$¥Windows ¥System32¥dhcp`

表 *23. Microsoft DHCP* イベントのログ・フォーマットの例.

WinCollect は、ルート・ログ・ディレクトリー・フォルダーを評価して、イベント・ログに書き込まれる新規 DHCP イベントを自動的に収集します。DHCP イベント・ログ名は、DHCP で開始され、3 文字の曜日の省略形を含み、`.log` ファイル拡張子で終了します。ルート・ログ・ディレクトリー内にある DHCP ログ・ファイルのうち、IPv4 または IPv6 のいずれかの DHCP ログ・フォーマットと一致するすべてのファイルで、WinCollect エージェントによって新規イベントがモニターされます。

ログ・タイプ	**ログ・ファイル・フォーマットの例**
IPv4	`DhcpSrvLog-Mon.log`
IPv6	`DhcpV6SrvLog-Wed.log`

関連資料

Windows ログ・ソースのパラメーター

WinCollect エージェントまたは WinCollect プラグインのログ・ソースを構成する際には、共通パラメーターを使用します。WinCollect プラグインごとに固有の構成オプションのセットもあります。

Microsoft Exchange Server のログ・ソース構成オプション

この参照情報を使用して、Microsoft Exchange Server の WinCollect プラグインを構成してください。

表 *24. Microsoft Exchange Server* のプロトコル・パラメーター

パラメーター	**説明**
ログ・ソース・タイプ	**Microsoft Exchange Server**
プロトコル構成	**WinCollect Microsoft Exchange**
ローカル・システム (Local System)	WinCollect エージェントが Microsoft Exchange Server にインストールされている必要があります。 ログ・ソースは、ローカル・システムの資格情報を使用して、イベントを収集し、QRadar に転送します。

表 *25. Microsoft Exchange Server* イベントの *OWA* のデフォルト・ディレクトリー・パス.

WinCollect によってモニターされる Exchange Server OWA イベント・ログは、WinCollect Exchange Server ログ・ソース内で指定するディレクトリー・パスによって定義されます。

収集タイプ	**ルート・ログ・ディレクトリー**
ローカル	`C:¥inetpub¥logs¥LogFiles¥W3SVC1`
リモート	`¥¥<Exchange Server IP address>¥C$ ¥inetpub¥logs¥LogFiles¥W3SVC1`

表 *26. Microsoft Exchange Server* イベントのメッセージ追跡のデフォルト・ディレクトリー・パス.

WinCollect によってモニターされる Exchange Server のメッセージ追跡のイベント・ログは、WinCollect Exchange Server ログ・ソース内で指定するディレクトリー・パスによって定義されます。

収集タイプ	**ルート・ログ・ディレクトリー**
ローカル	C:¥Program Files¥Microsoft¥Exchange
リモート	¥¥*<Exchange Server IP address>*¥C$ ¥Program Files¥Microsoft¥Exchange

表 *27. Microsoft Exchange Server* イベントの *SMTP*/メールのデフォルト・ディレクトリー・パス.

WinCollect によってモニターされる Exchange Server の SMTP/メールのイベント・ログは、WinCollect Exchange Server ログ・ソース内で指定するディレクトリー・パスによって定義されます。

収集タイプ	**ルート・ログ・ディレクトリー**
ローカル	C:¥Program Files¥Microsoft¥Exchange Server¥V15¥TransportRoles¥Logs¥Hub ¥ProtocolLog
リモート	¥¥*<Exchange Server IP address>*¥C$ ¥Program Files¥Microsoft¥Exchange Server¥V15¥TransportRoles¥Logs¥Hub ¥ProtocolLog

DNS デバッグ・ログ・ソースの構成オプション

この参照情報を使用して、Microsoft Windows DNS デバッグ・ロギング用の WinCollect プラグインを構成してください。

重要 : DNS デバッグ・ロギングでは、DNS サーバーが送受信する情報に関する詳細なデータが表示されるため、システム・パフォーマンスおよびディスク・スペースに影響を与える可能性があります。DNS デバッグ・ロギングを有効にするのは、この情報が必要な場合のみにしてください。

DNS デバッグ・ロギングは、Windows の以下のバージョンでサポートされています。

- Windows Server 2019 (Core を含む)
- Windows Server 2016 (Core を含む)
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008 (32 ビット)

重要 : 「**オプション**」ペインの「**詳細**」は選択しないでください。WinCollect では、現在この機能をサポートしていません。

表 28. DNS デバッグのプロトコル・パラメーター	
パラメーター	**説明**
ファイル・リーダー・タイプ (File Reader Type)	ファイル内容を読み取ります。両方のオプションで、バイト・オーダー・マークに対する基本的な Unicode エンコードがサポートされています。 「**テキスト (ファイルを開いたまま保持) (Text (file held open))**」オプションを選択すると、WinCollect はモニター対象ログ・ファイルに対する共有の読み取りロックおよび書き込みロックを維持します。 「**テキスト (読み取り時にファイルを開く) (Text (file open when reading))**」オプションを選択すると、WinCollect は、ログ・ファイルを読み取るときにのみ共有の読み取りロックおよび書き込みロックを維持します。
ファイル・モニター・タイプ (File Monitor Type)	以下のようにファイルおよびディレクトリーの変更を検出します。 「**通知ベース (ローカル) (Notification-based (local))**」オプションは、Windows のファイル・システム通知を使用して、DNS ログの変更を検出します。 「**ポーリング・ベース (リモート) (Polling-based (remote))**」オプションは、リモートのファイルおよびディレクトリーの変更をモニターします。 エージェントは、リモート DNS ログをポーリングし、そのファイルを前回のポーリング間隔と比較します。ログに新規項目が含まれる場合は、それらの項目が取得されます。
ファイル・パターン	DNS マネージャー内の DNS デバッグ・ログ・ファイル・セットを突き合わせるために必要な正規表現 (regex)。
ルート・ディレクトリー (Root Directory)	WinCollect がファイルをモニターするディレクトリー。このディレクトリーは、ローカル収集の場合はローカル・ファイル・システムであることが必要であり、リモート収集の場合は有効な Microsoft Windows 汎用命名規則 (UNC) パスであることが必要です。 この値は、ご使用の DNS マネージャーで構成されたファイル・パスと一致しなければなりません。 **重要 :** 分散システムの制限により、パスをユーザー・インターフェースで 検証することはできません。

Windows サーバーでの DNS デバッグの有効化

Windows サーバーで DNS デバッグを有効にして、DNS サーバーが送受信する情報を収集します。

始める前に

DNS ロールが Windows サーバーにインストールされている必要があります。

重要 :「**オプション**」ペインの「**詳細**」は選択しないでください。WinCollect では、現在この機能をサポートしていません。

手順

1. 以下のコマンドを使用して DNS マネージャーを開きます。

```
dnsmgmt.msc
```

2. DNS サーバーを右クリックして、「**プロパティ**」をクリックします。
3. 「**デバッグのログ**」タブをクリックします。
4. **「デバッグのためにパケットのログを記録する」**を選択します。
5. ログ・ファイルに、ファイル・パス、ファイル名、および最大サイズを入力します。

   重要 : ファイル・パスおよびファイル名は、Microsoft DNS ログ・ソースを構成したときに指定した **Root Directory** および **File Pattern** と一致している必要があります。
6. 「**適用**」をクリックしてから、「**OK**」をクリックします。

XPath を使用した DNS 分析ログの収集

WinCollect を使用して DNS 分析ログを収集するには、まず分析ログを収集するように Windows を構成し、次に XPath を WinCollect エージェントのログ・ソースに追加してログを収集し、QRadar に送信します。

このタスクについて

DNS サーバー分析ログを収集するように Windows を構成するには、イベント・ビューアーを使用します。

手順

1. イベント・ビューアーを開くには、昇格したコマンド・プロンプトで `eventvwr.msc` と入力し、**Enter** を押します。
2. `Applications and Services Logs¥Microsoft¥Windows¥DNS-Server` に移動します。
3. 「**DNS サーバー**」を右クリックし、「**表示**」 > 「**分析およびデバッグ ログの表示**」をクリックします。
4. 「**分析 (Analytical)**」ログを右クリックし、「**プロパティ**」をクリックします。
5. 「**イベント・ログ・サイズが最大に達した場合 (When maximum event log size is reached)**」セクションで 「**イベントを上書きしない (ログを手動で消去)(Do not overwrite events (Clear logs manually))**」を選択し、「**ロギングを有効にする (Enable logging)**」 を選択してから結果のダイアログ・ボックスで「**OK**」をクリックします。

   重要 : このオプションを選択しない場合、ログが etl 形式で保管されるため、WinCollect エージェントで分析ログを収集できません。詳しくは、https://support.microsoft.com/en-ca/help/2488055/error-when-enabling-analytic-or-debug-event-log を参照してください。
6. 「**OK**」をクリックして DNS サーバー分析イベント・ログを有効にします。

   重要 : イベント・ログが満杯になったら、手動でログを消去し、エージェントを再始動する必要があります。
7. ログ・ソースで、次の XPath を WinCollect エージェントに追加します。

```
<QueryList>
  <Query Id="0" Path="Microsoft-Windows-DNSServer/Analytical">
    <Select Path="Microsoft-Windows-DNSServer/Analytical">*</Select>
  </Query>
</QueryList>
```

ファイル・フォワーダー・ログ・ソースの構成オプション

この参照情報は、ファイル・フォワーダー・ログ・ソース用 WinCollect プラグインを構成する場合に使用します。

このプラグインに固有ではないパラメーターも構成する必要があります。ファイル・フォワーダー・プラグインは、Windows ホストから多くのタイプのログをポーリングするためにユニバーサル DSM とともに使用できます。

表 29. ファイル・フォワーダーのプロトコル・パラメーター

パラメーター	説明
ログ・ソース・タイプ	**ユニバーサル DSM**
プロトコル構成	「**WinCollect ファイル・フォワーダー (WinCollect File Forwarder)**」を選択します。
ローカル・システム (Local System)	ログ・ソースのリモート・イベント収集を無効にします。ログ・ソースは、ローカル・システムの資格情報を使用して、イベントを収集し、QRadar に転送します。
ルート・ディレクトリー (Root Directory)	QRadar に転送するログ・ファイルのロケーション。 WinCollect エージェントがリモート側でファイルをポーリングする場合、ルート・ログ・ディレクトリーは、サーバーとログ・ファイルのフォルダー・ロケーションの両方を指定していなければなりません。 **例 :** `¥¥server¥sharedfolder¥remotelogs¥`
ファイル名パターン (Filename Pattern)	ファイル名をフィルターに掛けるために必要な正規表現 (regex)。パターンに一致するすべてのファイル・タイプが処理対象となります。デフォルトのファイル・パターンは .* です。このパターンはルート・ディレクトリー内のすべてのファイルに一致します。
モニター・アルゴリズム (Monitoring Algorithm)	「**継続的モニター (Continuous Monitoring)**」オプションは、データをログ・ファイルに追加するファイル・システムを対象としています。 「**ファイル・ドロップ (File Drop)**」オプションは、1 回読み取られた後は無視される、ルート・ログ・ディレクトリー内のログ・ファイルに使用します。
今日作成されたファイルのみモニター (Only Monitor Files Created Today)	デフォルトでは有効になっています。現在の日より前のファイルをモニターするには、このオプションをクリアします。

表 29. ファイル・フォワーダーのプロトコル・パラメーター (続き)

パラメーター	説明
ファイル・モニター・タイプ (File Monitor Type)	「**通知ベース (ローカル) (Notification-based (local))**」オプションは、Windows のファイル・システム通知を使用して、イベント・ログの変更を検出します。 「**ポーリング・ベース (リモート) (Polling-based (remote))**」オプションは、リモートのファイルおよびディレクトリーの変更をモニターします。 エージェントは、リモート・イベント・ログをポーリングし、そのファイルを前回のポーリング間隔と比較します。イベント・ログに新しいイベントが記録されている場合は、イベント・ログを取得します。
ファイル・リーダー・タイプ (File Reader Type)	「**テキスト (ファイルを開いたまま保持) (Text (file held open))**」オプションを選択すると、イベント・ログを生成するシステムは、常にファイルを開いたままにして、ファイルの終わりにイベントを追加します。 「**テキスト (読み取り時にファイルを開く) (Text (file open when reading))**」オプションを選択すると、イベント・ログを生成するシステムは、前回の既知の位置からイベント・ログを開いてイベントを書き込んだ後、イベント・ログを閉じます。 「**メモリー・マップ・テキスト (ローカルのみ) (Memory Mapped Text (local only))**」オプションは、IBM Professional Services からアドバイスがあった場合にのみ選択してください。このオプションは、イベント・ログを生成するシステムがイベント・ログ末尾の変更をポーリングする場合に使用します。このオプションを使用する場合は、「**ローカル・システム (Local System)**」チェック・ボックスも選択する必要があります。
ファイル・リーダー・エンコード (File Reader Encoding)	BOM を含まないファイルを UTF8 に変換する場合は、「**ANSI**」を選択します。ファイルが既に UTF8 形式で変換が不要の場合は、「**UTF8**」を選択します。
ファイル・パーサー・タイプ (File Parser Type)	ファイルは、単一行 (Single Line) または複数行 (Multi Line) という 2 つの方法で構文解析できます。 **単一行 (Single Line)** ファイルを構文解析し、行ごとにイベントを作成します。 **複数行 (Multi Line)** XML ファイルを構文解析し、指定された開始トークンが構文解析された時点から、次回、指定された開始トークンが構文解析された時点までの、複数行からなるイベントを作成します。 **注 :** 複数行の構文解析では、現在、XML ファイル・タイプのみサポートされています。

表 29. ファイル・フォワーダーのプロトコル・パラメーター (続き)	
パラメーター	**説明**
複数行の「Starts With (次で始まる)」正規表現トークン (Multi Line "Starts With" Regex Token)	複数行ファイル・パーサー・タイプには、「Starts With (次で始まる)」トークンが必要です。「Starts With (次で始まる)」トークンは、複数行イベントの開始行となる行の先頭からのあらゆる文字を識別するために必要とされる正規表現でなければなりません。文字の前にある類似の空白文字が原因でイベントが結合されてしまうようなことがないように、また「Starts With (次で始まる)」トークンが検出されないことが原因でファイルがまったく構文解析されないようなことがないように、できるだけ正確な正規表現にすることが重要です。

複数行パーサー・タイプの XML ファイルの例

XML ファイルが確実に構文解析され、すべての <event> ノードに対してイベントが生成されるようにするには、「¥s*<event>」という複数行「Starts With (次で始まる)」トークンを使用します。

```
<EventList>
    <event>
        <timeStamp=10101010101 payload=example1>
    </event>
    <event>
        <timeStamp=10101010102 payload=example2>
    </event>
    <event>
        <timeStamp=10101010103 payload=example3>
    </event>
    <event>
        <timeStamp=10101010104 payload=example4>
    </event>
</EventList>
```

この複数行ファイル・パーサーは、 個別の単一行イベントを 14 個生成するのではなく、4 つの個別イベントを生成します。 作成される最初のイベントに対するペイロード・メッセージは、次の例のようになります。

```
<event> <timeStamp=10101010101 payload=example1> </event>
```

注 : 「 <event>」という複数行「Starts With (次で始まる)」トークンも機能することは機能します。ただし、タブと空白文字が同じ外観となり、かつ別々のコーディングになります。「¥s*<event>」を使用すると、この両方のタイプの空白文字がカバーされるため、より良い結果が得られます。

関連資料

Windows ログ・ソースのパラメーター

WinCollect エージェントまたは WinCollect プラグインのログ・ソースを構成する際には、共通パラメーターを使用します。WinCollect プラグインごとに固有の構成オプションのセットもあります。

Microsoft IAS ログ・ソースの構成オプション

この参照情報を使用して、Microsoft IAS 用の WinCollect プラグインを構成してください。

表 *30.* サポートされる *Windows* バージョンおよびログ・フォーマット	
Microsoft IAS	**サポートされるバージョン**
Microsoft Windows サポート	Windows Server 2019 Windows Server 2016 Windows Server 2012 R2 Windows Server 2008 R2
NPS® ログ・サーバーのログ・フォーマット	データ変換サービス Open Database Connectivity インターネット認証サービス

重要 : WinCollect では、Microsoft SQL Server に記録されたログ・イベントはサポートされていません。

イベント収集用の Microsoft IAS ディレクトリー構造

WinCollect によってモニターされるイベント・ログは、ログ・ソース内で構成するルート・ディレクトリーによって定義されます。

ルート・ログ・ディレクトリーを指定するときには、Microsoft IAS または NPS のイベントが格納されているフォルダーを指すように WinCollect エージェントを設定する必要があります。ルート・ログ・ディレクトリーは、イベント・ファイルを見つけるためにサブディレクトリーを再帰的に検索しません。

パフォーマンスを向上させるために、IAS および NPS のイベント・ログ用のサブフォルダーを作成できます。例えば、`¥WINDOWS¥System32¥Logfiles¥NPS`。特定のイベント・フォルダーを作成しておくと、エージェントは、イベント・ログを見つけるために多くのファイルを評価する必要がなくなります。

システムが IAS または NPS のイベントを大量に生成する場合は、新規イベント・ログを 1 日間隔で作成するように Windows システムを構成できます。こうしておくと、エージェントは、新規イベントを見つけるために大容量のログを検索する必要がなくなります。

表 *31. Microsoft IAS* のイベント・ログのデフォルトのディレクトリー構造	
イベント・バージョン	**ルート・ログ・ディレクトリー**
Microsoft Windows Server 2019	`¥Windows¥System32¥Logfiles¥`
Microsoft Windows Server 2016	`¥Windows¥System32¥Logfiles¥`
Microsoft Windows Server 2012 R2	`¥Windows¥System32¥Logfiles¥`
Microsoft Windows Server 2008 R2	`¥Windows¥System32¥Logfiles¥`

Microsoft IAS のプロトコル・パラメーター

表 *32. Microsoft IAS* のパラメーター	
パラメーター	**説明**
ログ・ソース・タイプ	**Microsoft IAS サーバー**
プロトコル構成	**WinCollect Microsoft IAS/NPS**

表 32. Microsoft IAS のパラメーター (続き)	
パラメーター	**説明**
ローカル・システム (Local System)	ローカル・イベントを収集するには、WinCollect エージェントが Microsoft DHCP サーバーと同じホストにインストールされている必要があります。 ログ・ソースは、ローカル・システムの資格情報を使用して、イベントを収集し、QRadar に転送します。
ファイル・モニター・ポリシー (File Monitor Policy)	「**通知ベース (ローカル) (Notification-based (local))**」オプションは、Windows のファイル・システム通知を使用して、イベント・ログの変更を検出します。 「**ポーリング・ベース (リモート) (Polling-based (remote))**」オプションは、リモートのファイルおよびディレクトリーの変更をモニターします。 エージェントは、リモート・イベント・ログをポーリングし、そのファイルを前回のポーリング間隔と比較します。イベント・ログに新しいイベントが記録されている場合は、イベント・ログを取得します。
ポーリング間隔 (Polling Interval)	ルート・ログ・ディレクトリーに対して新規イベントを照会する時間間隔。

関連資料

Windows ログ・ソースのパラメーター

WinCollect エージェントまたは WinCollect プラグインのログ・ソースを構成する際には、共通パラメーターを使用します。WinCollect プラグインごとに固有の構成オプションのセットもあります。

WinCollect Microsoft IIS ログ・ソースの構成オプション

Microsoft Internet Information Services (IIS) を使用するようにログ・ソースを構成できます。この WinCollect プラグインでは、Microsoft IIS Web サーバー上の W3C 形式のログ・ファイルを収集する単一ポイントがサポートされます。

Microsoft IIS 用 WinCollect プラグインの概要

WinCollect を使用して Microsoft IIS のログを収集するには、2 つの方法のうちいずれかを使用できます。1 つは、Microsoft IIS サーバーにエージェントをローカルにインストールして、適切に構成する方法です。もう 1 つは、WinCollect 7.2.8 以降を使用して、IIS のログをリモート・ポーリングするように WinCollect エージェントを構成する方法です。それぞれのログ収集方法で使用するディレクトリー・パスの設定については、表 1 を参照してください。

Microsoft IIS 用 WinCollect プラグインは、以下のログのイベントを読み取り、転送することができます。

- Web サイト (W3C) ログ
- ファイル転送プロトコル (FTP) ログ
- Simple Mail Transfer Protocol (SMTP) ログ
- ネットワーク・ニュース転送プロトコル (NNTP) ログ

Microsoft IIS 用 WinCollect プラグインは、W3C、IIS、および NCSA のフォーマットのイベント・ログをモニターできます。ただし、IIS および NCSA のイベント・フォーマットでは、イベント・ペイロードに W3C イベント・フォーマットと同じだけのイベント情報が含まれません。入手可能な情報を最大限収集するた

めに、イベントを W3C フォーマットで書き込むように Microsoft IIS サーバーを構成します。WinCollect は、ASCII および UTF-8 の両方のエンコード方式のイベント・ログ・ファイルを収集できます。

サポートされる Microsoft IIS のバージョン

WinCollect 用の Microsoft IIS プラグインは、以下の Microsoft IIS ソフトウェアのバージョンをサポートします。

- Microsoft IIS サーバー 7.0
- Microsoft IIS サーバー 7.5
- Microsoft IIS サーバー 8.0
- Microsoft IIS サーバー 8.5
- Microsoft IIS サーバー 10

WinCollect Microsoft IIS のパラメーター

表 *33. Microsoft IIS* のパラメーター

パラメーター	**説明**
プロトコル構成	「**WinCollect Microsoft IIS**」を選択します。
ログ・ソース ID	Microsoft IIS サーバーの IP アドレスまたはホスト名。 ログ・ソース・タイプに固有でなければなりません。
ルート・ディレクトリー	Microsoft IIS のログ・ファイルのディレクトリー・パス。 Microsoft 7.0 から 10.0 (全サイト) の場合は、以下を使用します: • ローカル: `%SystemDrive%¥inetpub¥logs¥LogFiles` • リモート: `¥¥HostnameorIP¥c$¥inetpub¥logs¥LogFiles` Microsoft IIS 7.0 から 10.0 (個別サイト) の場合は、以下を使用します。 • ローカル: `%SystemDrive%¥inetpub¥logs¥LogFiles¥site name` • リモート: `¥¥HostnameorIP¥c$¥inetpub¥logs¥LogFiles ¥site name`
ポーリング間隔	ルート・ログ・ディレクトリーに対して新規イベントを照会する時間間隔。 ポーリング間隔のデフォルト値は 5000 ミリ秒です。
FTP	Microsoft IIS からファイル転送プロトコル (FTP) イベントを収集します。
NNTP/ニュース	Microsoft IIS からネットワーク・ニュース転送プロトコル (NNTP) イベントを収集します。
SMTP/メール	Microsoft IIS から Simple Mail Transfer Protocol (SMTP) イベントを収集します。
W3C	Microsoft IIS から Web サイト (W3C) イベントを収集します。
WinCollect エージェント	WinCollect エージェント・ログ・ソースを管理します。

Microsoft ISA ログの構成オプション

この参照情報を使用して、Microsoft ISA 用の WinCollect プラグインを構成してください。

サポートされる Microsoft ISA のバージョン

WinCollect 用の Microsoft ISA プラグインは、以下のソフトウェアのバージョンをサポートします。

- Microsoft ISA Server 2006
- Microsoft Forefront Threat Management Gateway 2010

サポートされる Microsoft ISA または TMG のサーバー・ログ・フォーマット

Microsoft ISA および Forefront Threat Management Gateway のインストール済み環境は、個々のファイアウォールおよび Web プロキシーのイベント・ログを共通ログ・ディレクトリー内に作成します。WinCollect でこれらのイベントを収集するには、イベント・ログをログ・ディレクトリーに書き込むように Microsoft ISA または Microsoft Time Management Gateway を構成する必要があります。

制約事項 : Microsoft SQL Server データベースに記録されたログ・イベントは、WinCollect ではサポートされません。

WinCollect では、以下のイベント・ログ・フォーマットがサポートされています。

- WC3 フォーマットの Web プロキシー・ログ (w3c_web)
- WC3 フォーマットの Microsoft ファイアウォール・サービス・ログ (w3c_fws)
- IIS フォーマットの Web プロキシー・ログ (iis_web)
- IIS フォーマットの Microsoft ファイアウォール・サービス・ログ (iis_fws)

優先されるイベント・ログ・フォーマットは、W3C イベント・フォーマットです。W3C フォーマットには、バージョン情報を示す標準見出しと、イベント・ペイロード内で予期されるすべてのフィールドが含まれます。ファイアウォール・サービス・ログおよび Web プロキシー・ログの W3C イベント・フォーマットをカスタマイズして、イベント・ログのフィールドを組み込んだり除外したりできます。

ほとんどの管理者は、デフォルトの W3C フォーマット・フィールドを使用できます。W3C フォーマットをカスタマイズする場合、イベントを適切に分類するには、以下のフィールドが必須です。

表 *34. W3C* フォーマットの必須フィールド

必須フィールド	**説明**
クライアント IP (c-ip)	送信元 IP アドレス。
アクション	ファイアウォールによって実行されるアクション。
宛先 IP (r-ip)	宛先 IP アドレス。
プロトコル (cs-protocol)	アプリケーション・プロトコル名。例えば、HTTP または FTP。
クライアント・ユーザー名 (cs-username)	ファイアウォール・サービスのデータ要求を行ったユーザー・アカウント。
クライアント・ユーザー名 (username)	Web プロキシー・サービスのデータ要求を行ったユーザー・アカウント。

イベント収集用の Microsoft ISA ディレクトリー構造

WinCollect によってモニターされるイベント・ログは、ログ・ソース内で構成するルート・ディレクトリーによって定義されます。

ルート・ログ・ディレクトリーが指定されると、WinCollect はディレクトリー・フォルダーを評価し、新規イベントがイベント・ログにいつ書き込まれたかを判別するために、サブフォルダーを再帰的に検索し

ます。デフォルトでは、Microsoft ISA 用の WinCollect プラグインは、更新されたイベント・ログがないか、ルート・ログ・ディレクトリーを 5 秒ごとにポーリングします。

表 *35. Microsoft ISA* のイベント・ログのデフォルトのディレクトリー構造

バージョン	**ルート・ログ・ディレクトリー**
Microsoft ISA 2006	%systemroot%¥LogFiles¥IAS¥
Microsoft Threat Management Gateway	<*Program Files*>¥<Forefront Directory>¥ISALogs¥

Microsoft ISA のプロトコル・パラメーター

表 *36. Microsoft ISA* のプロトコル・パラメーター

パラメーター	**説明**
ログ・ソース・タイプ	**Microsoft ISA**
プロトコル構成	**WinCollect Microsoft ISA/Forefront TMG**
ローカル・システム (Local System)	ローカル・イベントを収集するには、Microsoft ISA サーバーまたは Forefront TMG サーバーと同じホストに WinCollect エージェントがインストールされている必要があります。 ログ・ソースは、ローカル・システムの資格情報を使用して、イベントを収集し、QRadar に転送します。
ルート・ディレクトリー (Root Directory)	リモート・ファイル・パスを指定する場合は、コロン (:) ではなくドル記号 ($) を使用してドライブ名を表します。 Microsoft ISA 2006 • ローカル・ディレクトリー・パスには、%systemroot%¥LogFiles¥ISA¥ を使用します。 • リモート・ディレクトリー・パスには、¥<*ISA server IP*>¥%systemroot%¥LogFiles¥ISA¥ を使用します。 Microsoft Threat Management Gateway • ローカル・ディレクトリー・パスには、<*Program Files*>¥<*Forefront Directory*>¥ISALogs¥ を使用します。 • リモート・ディレクトリー・パスには、¥¥<*ISA server IP*>¥<*Program Files*>¥<*Forefront Directory*>¥ISALogs¥ を使用します。

表 36. *Microsoft ISA* のプロトコル・パラメーター *(続き)*	
パラメーター	**説明**
ファイル・モニター・ポリシー (File Monitor Policy)	「**通知ベース (ローカル) (Notification-based (local))**」オプションは、Windows のファイル・システム通知を使用して、イベント・ログの変更を検出します。 「**ポーリング・ベース (リモート) (Polling-based (remote))**」オプションは、リモートのファイルおよびディレクトリーの変更をモニターします。 エージェントは、リモート・イベント・ログをポーリングし、そのファイルを前回のポーリング間隔と比較します。イベント・ログに新しいイベントが記録されている場合は、イベント・ログを取得します。
ポーリング間隔 (Polling Interval)	ルート・ログ・ディレクトリーに対して新規イベントを照会する時間間隔。

関連資料

Windows ログ・ソースのパラメーター

WinCollect エージェントまたは WinCollect プラグインのログ・ソースを構成する際には、共通パラメーターを使用します。WinCollect プラグインごとに固有の構成オプションのセットもあります。

Juniper Steel-Belted Radius ログ・ソースの構成オプション

この参照情報は、Juniper Steel-Belted Radius 用 WinCollect プラグインを構成する場合に使用します。

表 37. *Juniper Steel-Belted Radius* のプロトコル・パラメーター	
パラメーター	**説明**
ログ・ソース・タイプ	**Juniper Steel-Belted Radius**
プロトコル構成	**WinCollect Juniper SBR**
ローカル・システム (Local System)	ローカル・イベントを収集するには、WinCollect エージェントが Juniper Steel-Belted Radius サーバーと同じホストにインストールされている必要があります。ログ・ソースは、ローカル・システムの資格情報を使用して、イベントを収集し、QRadar に転送します。
ルート・ディレクトリー (Root Directory)	モニター対象のファイルが格納されているディレクトリー。QRadar ユーザー・インターフェースは、ルート・ディレクトリーのパスを検証しません。必ず、Windows の有効なローカル・パスを入力してください。

表 37. *Juniper Steel-Belted Radius* のプロトコル・パラメーター *(続き)*	
パラメーター	**説明**
ファイル・モニター・ポリシー (File Monitor Policy)	「**通知ベース (ローカル) (Notification-based (local))**」オプションは、Windows のファイル・システム通知を使用して、イベント・ログの変更を検出します。 「**ポーリング・ベース (リモート) (Polling-based (remote))**」オプションは、リモートのファイルおよびディレクトリーの変更をモニターします。 エージェントは、リモート・イベント・ログをポーリングし、そのファイルを前回のポーリング間隔と比較します。イベント・ログに新しいイベントが記録されている場合は、イベント・ログを取得します。
ポーリング間隔 (Polling Interval)	ルート・ログ・ディレクトリーに対して新規イベントを照会する時間間隔。

Microsoft SQL Server のログ・ソース構成オプション

この参照情報を使用して、Microsoft SQL Server 用の WinCollect プラグインを構成してください。

Microsoft SQL Server のエラー・ログ

エラー・ログは、Microsoft SQL Server の情報およびエラー・メッセージを格納する標準テキスト・ファイルです。WinCollect は、エラー・ログで新規イベントをモニターし、そのイベントを IBM Security QRadar に転送します。エラー・ログは、問題のトラブルシューティングや、潜在的な問題や既存の問題の発見に役立つ有用な情報を提供します。エラー・ログ出力には、メッセージのログが記録された日時、メッセージのソース、およびメッセージの説明が含まれます。エラーが発生した場合、ログには、エラー・メッセージ番号および説明が含まれます。Microsoft SQL Server は、最新の 6 個のエラー・ログ・ファイルのバックアップを保持します。

WinCollect は、Microsoft SQL Server のエラー・ログ・イベントを収集できます。Microsoft SQL Server の監査イベントおよび認証イベントを収集するために、Microsoft SQL Server DSM を構成します。詳しくは、「*IBM Security QRadar DSM* 構成ガイド」を参照してください。

WinCollect エージェントは、Microsoft SQL Server インストール済み環境でのローカル収集およびリモート・ポーリングをサポートします。Microsoft SQL Server イベントをリモートでポーリングするには、管理者資格情報またはドメイン管理者資格情報を指定する必要があります。ネットワーク・ポリシーで管理者資格情報の使用が制限されている場合は、Microsoft SQL Server と同じホスト上に WinCollect エージェントをインストールできます。WinCollect のローカル・インストール済み環境は、イベントを QRadar に転送するために特別な資格情報を必要としません。

WinCollect によってモニターされる Microsoft SQL Server イベント・ログは、WinCollect SQL ログ・ソース内で指定するディレクトリー・パスによって定義されます。以下の表に、ログ・ソース内の**ルート・ログ・ディレクトリー**・フィールドのデフォルトのディレクトリー ・パスをリストします。

表 38. *Microsoft SQL* イベントのデフォルトのルート・ログ・ディレクトリー・パス		
Microsoft SQL のバージョン	**収集タイプ**	**ルート・ログ・ディレクトリー**
2008	ローカル	`C:¥Program Files¥Microsoft SQL Server ¥MSSQL10.MSSQLSERVER¥MSSQL¥Log¥`
2008	リモート	`¥¥SQL IP address¥c$¥Program Files¥Microsoft SQL Server¥MSSQL10.MSSQLSERVER¥MSSQL¥Log¥`

表 38. *Microsoft SQL* イベントのデフォルトのルート・ログ・ディレクトリー・パス (続き)

Microsoft SQL のバージョン	**収集タイプ**	**ルート・ログ・ディレクトリー**
2008R2	ローカル	C:¥Program Files¥Microsoft SQL Server ¥MSSQL10_50.MSSQLSERVER¥MSSQL¥Log
2008R2	リモート	¥¥SQL IP address¥c$¥Program Files¥Microsoft SQL Server¥MSSQL10_50.MSSQLSERVER¥MSSQL¥Log
2012	ローカル	C:¥Program Files¥Microsoft SQL Server ¥MSSQL11.MSSQLSERVER¥MSSQL¥LOG
2012	リモート	¥¥SQL IP address¥c$¥Program Files¥Microsoft SQL Server¥MSSQL11.MSSQLSERVER¥MSSQL¥LOG
2014	ローカル	C:¥Program Files¥Microsoft SQL Server ¥MSSQL12.MSSQLSERVER¥MSSQL¥LOG
2014	リモート	¥¥SQL IP address¥c$¥Program Files¥Microsoft SQL Server¥MSSQL12.MSSQLSERVER¥MSSQL¥LOG
2016	ローカル	C:¥Program Files¥Microsoft SQL Server ¥MSSQL13.MSSQLSERVER¥MSSQL¥LOG
2016	リモート	¥¥SQL IP address¥c$¥Program Files¥Microsoft SQL Server¥MSSQL13.MSSQLSERVER¥MSSQL¥LOG
2017	ローカル	C:¥PROGRAM FILES¥MICROSOFT SQL SERVER ¥MSSQL14.MSSQLSERVER¥MSSQL¥LOG
2017	リモート	¥¥HOSTNAME¥C$¥PROGRAM FILES¥MICROSOFT SQL SERVER¥MSSQL14.MSSQLSERVER¥MSSQL¥LOG
2019	ローカル	C:¥PROGRAM FILES¥MICROSOFT SQL SERVER ¥MSSQL14.MSSQLSERVER¥MSSQL¥LOG
2019	リモート	¥¥HOSTNAME¥C$¥PROGRAM FILES¥MICROSOFT SQL SERVER¥MSSQL14.MSSQLSERVER¥MSSQL¥LOG

SQL イベント・ログ・フォーマットと一致しないログ・ファイルは、解析されず、QRadar に転送されません。

サポートされる Microsoft SQL Server のバージョン

Microsoft SQL Server 用の WinCollect プラグインは、以下の Microsoft SQL ソフトウェアのバージョンをサポートします。

- Microsoft SQL Server 2008
- Microsoft SQL Server 2008R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019

次の表に、Microsoft SQL Server のプロトコル・パラメーターを示します。

表 *39. Microsoft SQL Server* のプロトコル・パラメーター	
パラメーター	**説明**
ログ・ソース・タイプ	**Microsoft SQL**
プロトコル構成	**WinCollect Microsoft SQL**

表 *39. Microsoft SQL Server* のプロトコル・パラメーター *(*続き*)*

パラメーター	説明
ルート・ディレクトリー (Root Directory)	Microsoft SQL 2008 • ローカル・ディレクトリー・パスには、C:¥Program Files ¥Microsoft SQL Server¥MSSQL10.MSSQLSERVER¥MSSQL ¥Log¥ を使用します。 • リモート・ディレクトリー・パスには、¥¥SQL IP address¥c$ ¥Program Files¥Microsoft SQL Server ¥MSSQL10.MSSQLSERVER ¥MSSQL¥Log¥ を使用します。 Microsoft SQL 2008R2 • ローカル・ディレクトリー・パスには、C:¥Program Files ¥Microsoft SQL Server¥MSSQL10_50.MSSQLSERVER ¥MSSQL¥Log を使用します。 • リモート・ディレクトリー・パスには、¥¥SQL IP address¥c$ ¥Program Files¥Microsoft SQL Server ¥MSSQL10_50.MSSQLSERVER¥MSSQL ¥Log を使用します。 Microsoft SQL 2012 • ローカル・ディレクトリー・パスには、 C:¥Program Files ¥Microsoft SQL Server¥MSSQL11.MSSQLSERVER¥MSSQL ¥Log を使用します。 • リモート・ディレクトリー・パスには、¥¥SQL IP address¥c$ ¥Program Files¥Microsoft SQL Server ¥MSSQL11.MSSQLSERVER¥MSSQL¥Log を使用します。 Microsoft SQL 2014 • ローカル・ディレクトリー・パスには、 C:¥Program Files ¥Microsoft SQL Server¥MSSQL12.MSSQLSERVER¥MSSQL ¥Log を使用します。 • リモート・ディレクトリー・パスには、¥¥SQL IP address¥c$ ¥Program Files¥Microsoft SQL Server ¥MSSQL12.MSSQLSERVER¥MSSQL¥Log を使用します。 Microsoft SQL 2016 • ローカル・ディレクトリー・パスには、 C:¥Program Files ¥Microsoft SQL Server¥MSSQL13.MSSQLSERVER¥MSSQL ¥Log を使用します。 • リモート・ディレクトリー・パスには、¥¥SQL IP address¥c$ ¥Program Files¥Microsoft SQL Server ¥MSSQL13.MSSQLSERVER¥MSSQL¥Log を使用します。 Microsoft SQL 2017 • ローカル・ディレクトリー・パスには、C:¥PROGRAM FILES ¥MICROSOFT SQL SERVER¥MSSQL14.MSSQLSERVER¥MSSQL ¥LOG を使用します。 • リモート・ディレクトリー・パスには、¥¥HOSTNAME¥C$¥PROGRAM FILES¥MICROSOFT SQL SERVER¥MSSQL14.MSSQLSERVER ¥MSSQL¥LOG を使用します。

表 39. *Microsoft SQL Server* のプロトコル・パラメーター *(続き)*	
パラメーター	**説明**
ファイル・モニター・ポリシー (File Monitor Policy)	「**通知ベース (ローカル) (Notification-based (local))**」オプションは、Windows のファイル・システム通知を使用して、イベント・ログの変更を検出します。 「**ポーリング・ベース (リモート) (Polling-based (remote))**」オプションは、リモートのファイルおよびディレクトリーの変更をモニターします。 エージェントは、リモート・イベント・ログをポーリングし、そのファイルを前回のポーリング間隔と比較します。イベント・ログに新しいイベントが記録されている場合は、イベント・ログを取得します。

関連資料

Windows ログ・ソースのパラメーター

WinCollect エージェントまたは WinCollect プラグインのログ・ソースを構成する際には、共通パラメーターを使用します。WinCollect プラグインごとに固有の構成オプションのセットもあります。

NetApp Data ONTAP 構成オプション

この参照情報は、NetApp Data ONTAP 用 WinCollect プラグインを構成する場合に使用します。

表 40. *NetApp Data ONTAP* のパラメーター	
パラメーター	**説明**
ログ・ソース・タイプ	NetApp Data ONTAP
プロトコル構成	WinCollect NetApp Data ONTAP
ユーザー名	Windows ドメインまたは Windows システムへのログインに使用するアカウント名。
ドメイン	ユーザー名が属するネットワーク・ドメイン。
ターゲット・ディレクトリー	モニターするファイルが置かれているディレクトリーのネットワーク・パス。このパスは、IBM Security QRadar ユーザー・インターフェースで 検証されません。必ず、NetApp アプライアンスで共有される有効な Windows UNC パスを入力してください。
ポーリング間隔	リモート・ディレクトリーに対して新規イベント・ログ・ファイルを照会する時間間隔。リモート・デバイスが 60 秒未満の期間に新規ファイルを生成しなくても、最適なポーリング間隔は 60 秒未満です。この方法により、WinCollect の再始動時にファイルの収集が確実に再開されます。
WinCollect エージェント	NetApp Data ONTAP イベントの収集に使用する WinCollect エージェント。

バージョンおよびファイル・タイプのサポート

バージョン:

- NetApp Data ONTAP 8
- NetApp Data ONTAP 9.3

ファイル・タイプ: Windows イベント・ログ (EVT)

TLS ログ・ソースの構成

イベントを暗号化して QRadar に送信するには、TLS Syslog プロトコルを使用するようにログ・ソースを構成し、ポート 6514 で QRadar との通信を確立する必要があります。

手順

1. QRadar にログインします。
2. 「**管理**」タブをクリックします。
3. ナビゲーション・メニューで、「**データ・ソース (Data Sources)**」をクリックします。
4. 「**ログ・ソース**」 > 「**追加**」をクリックします。
5. 以下のパラメーターを構成します。

表 *41. Wincollect* 宛先の *TLS* ログ・ソース

パラメーター	説明
ログ・ソース・タイプ	リストから「**ユニバーサル DSM**」を選択します。
プロトコル構成	プロトコル・リストから「**TLS Syslog**」を選択します。
ログ・ソース ID	WinCollect 宛先ホストの IP アドレス。
TLS listen ポート	デフォルトは 6514 です。
認証モード (Authentication Mode)	「**TLS**」を選択します。
最大接続数 (Maximum Connections)	デフォルトは 50 です。「**最大接続数 (Maximum Connections)**」は、500 まで増やすことができます。 **注 :** コレクターあたりのサポートされる WinCollect エージェントの数は、500 です。

6. 「**保存**」をクリックします。

WinCollect エージェントへのログ・ソースの追加

WinCollect エージェントに新規ログ・ソースを追加した場合、またはログ・ソースのパラメーターを編集した場合、WinCollect サービスは再始動されます。エージェントで WinCollect サービスが再始動される間、イベントはキャッシュされます。

始める前に

WinCollect プラグインを使用するログ・ソースを構成する場合は、要件を読んで、サード・パーティー・デバイスを準備する必要があります。詳しくは、WinCollect プラグインの要件を参照してください。

手順

1. 「**管理**」タブをクリックします。
2. ナビゲーション・メニューで、「**データ・ソース (Data Sources)**」をクリックします。
3. 「**WinCollect**」アイコンをクリックします。
4. 「**エージェント**」をクリックします。
5. WinCollect エージェントを選択してから、「**ログ・ソース**」をクリックし、「**追加**」をクリックします。
6. 次のオプションのいずれかを選択してください。

- WinCollect ログ・ソースには、「**ログ・ソース・タイプ**」リストから「**Microsoft Windows セキュリティー・イベント・ログ**」を選択した後、「**プロトコル構成**」リストから WinCollect を選択します。
- WinCollect プラグインの場合は、「**ログ・ソース・タイプ**」リストから WinCollect プラグイン・オプションを選択してから、固有のパラメーターを構成します。これらのパラメーターについて詳しくは、WinCollect プラグインを使用するログ・ソースに対応する構成オプションを参照してください。

7. 汎用ログ・ソース・パラメーターを構成します。
8. 「**保存**」をクリックします。
9. 「**管理**」タブで、「**変更のデプロイ**」をクリックします。

リモート・イベント収集用のバルク・ログ・ソース

バルク・ログ・ソースは、同じプロトコル構成を持つ複数のログ・ソースが存在するシステム用に設計されています。

手順

1. Windows イベントの収集で使用する各 IBM QRadar アプライアンス上に、Windows イベントの宛先を作成します。35 ページの『宛先の追加』を参照してください。

   重要：「Agent1_1.2.3.4」などのように、IP アドレスを含む宛先名を指定することをお勧めします。こうしておくと、後でログ・ソースを編集して宛先を変更する場合に、その宛先の IP アドレスを簡単に確認することができます。また、スロットル値を 5000 EPS に設定してください。これは、WinCollect エージェントの最大 EPS レートです。
2. バルク・ログ・ソースを作成します。83 ページの『リモート収集用にログ・ソースを一括で追加する』を参照してください。
3. 構成情報がリモート・エージェントにプッシュされるまで待ちます。
4. 「**ログ・アクティビティー**」タブで、イベントが受信されていることを確認します。

リモート収集用にログ・ソースを一括で追加する

複数のログ・ソースを一括で IBM QRadar に追加することができます。これらのログ・ソースは、共通の構成プロトコルを共有し、同じ WinCollect エージェントに関連付けられていることが必要です。

IP アドレスまたはホスト名をリストしたテキスト・ファイルをアップロードし、ドメイン・コントローラーに対して照会を実行することで、ホストのリストを取得できます。あるいは、IP アドレスまたはホスト名を 1 つずつ入力して、手動でリストを入力することもできます。

一度に追加する WinCollect ログ・ソースの数によっては、WinCollect エージェントがログ・ソース・リストにアクセスしてすべての Windows イベントを収集するのに時間がかかる場合があります。

始める前に

WinCollect エージェントが Windows イベントを QRadar アプライアンスに送信できるように、必ず宛先を作成しておいてください。また、QRadar Event Collector 16xx アプライアンスまたは 18xx アプライアンスごとに宛先を 1 つずつ作成しておいてください。

WinCollect イベント・ログ・レポート・ツールを使用して、一括収集戦略を計画してください。詳しくは、「GitHub」(https://github.com/ibm-security-intelligence/wincollect) を参照してください。

このタスクについて

管理対象の各 WinCollect エージェントのログ・ソースの最大数は 500 です。また、WinCollect エージェントの EPS は、ローカル収集では 5,000 未満、リモート・ポーリングでは 2,500 未満でなければなりません。Windows システムのイベント・ビューアーで、1 時間ごとに生成される EPS の値を確認することができます。この値を 3600 秒で除算すると、EPS レートを求めることができます。この計算により、インストールしなければならないエージェントの数が分かります。または、24 時間単位でイベントの数を確認して、各 Windows サーバーのビジー状態を調べることもできます。これにより、エージェントをどのようにチューニングすればいいかを判断することができます。また、1 時間ごとに確認する場合にしか表示されない最小 EPS レートと最大 EPS レートを調べる必要がなくなります。

手順

1. 「**管理**」タブのナビゲーション・メニューで「**データ・ソース**」をクリックし、次に「**WinCollect**」アイコンをクリックします。
2. ログ・ソースの割り当て先となる WinCollect エージェントを選択して「**ログ・ソース**」をクリックします。
3. 「**一括アクション**」 > 「**一括追加**」をクリックします。
4. バルク・ログ・ソースの名前を指定します。分かりやすくするため、リモート収集を実行する WinCollect エージェントとして名前を指定してください。
5. 「**ログ・ソース・タイプ**」リスト・ボックスで「**Microsoft Windows セキュリティー・イベント・ログ**」を選択します。
6. 「**プロトコル構成**」リスト・ボックスで「**WinCollect**」を選択します。
7. WinCollect イベント・ログ・レポート・ツールによって指定されたチューニング値を使用して、ログ・ソースを適切にチューニングします。
8. すべての「**標準ログ・タイプ (Standard Log Types)**」チェック・ボックスを選択します。WinCollect エージェントは、これらのリモート・ログを読み取って QRadar に転送します。

   重要 : 「**転送されたイベント**」チェック・ボックスは選択しないでください。「転送されたイベント」は、特殊な場合に使用するオプションです。このオプションを選択すると、複数のログ・ソースが正しく追加されなくなります。
9. すべての「**イベント・タイプ**」チェック・ボックスを選択します。
10. 「**Active Directory ルックアップの有効化 (Enable Active Directory Lookups)**」チェック・ボックスを選択します。このオプションにより、16 進数で表示される Windows イベント内のユーザー名が識別され、人間が読むことのできるユーザー名に解決されます。
11. 「**WinCollect Agent**」リストで、ログ・ソースを管理する Windows ホストを選択します。
12. 「**ターゲット内部宛先**」リストで、Windows イベントを受信して処理する QRadar アプライアンスを選択します。
13. リモートでイベントのポーリングを行う Windows オペレーティング・システムの IP アドレスを追加します。

    IP アドレスまたはホスト名をリストしたテキスト・ファイルをアップロードし、ドメイン・コントローラーに対して照会を実行することで、ホストのリストを取得できます。あるいは、IP アドレスまたはホスト名を 1 つずつ入力して、手動でリストを入力することもできます。

    一度に追加する WinCollect ログ・ソースの数によっては、WinCollect エージェントがログ・ソース・リストにアクセスしてすべての Windows イベントを収集するのに時間がかかる場合があります。
14. 「**保存**」をクリックしてから「**続行**」をクリックします。

次のタスク

構成情報がリモート・エージェントにプッシュされるまで待ちます。「**ログ・アクティビティー**」タブで、イベントが受信されたことを確認します。

関連タスク

WinCollect エージェントへのログ・ソースの追加

WinCollect エージェントに新規ログ・ソースを追加した場合、またはログ・ソースのパラメーターを編集した場合、WinCollect サービスは再始動されます。エージェントで WinCollect サービスが再始動される間、イベントはキャッシュされます。

第 6 章 トラブルシューティング

WinCollect デプロイメント環境に問題が発生した場合は、以下の情報を問題の識別と解決に利用できます。

多くのアセットが関係する複雑な WinCollect デプロイメント環境の場合は、問題の発生源と原因の識別が困難になる場合があります。トラブルシューティングとは、問題を解決するための体系的な方法です。 トラブルシューティングの 目標は、ある部分が予期したように動作しない理由を特定し、問題の解決方法を明確にすることです。

トラブルシューティング・プロセスの最初のステップは、問題を詳しく記述することです。問題記述に よって、ユーザーも、WinCollect サポート担当員も、問題の原因の探索をどこから開始すればよいかが分かります。このステップには、次のような基本的な質問もいくつか含まれています。

- 問題の症状はどのようなものか。
- 問題はどこで発生しているか。
- 問題はいつ発生するか。
- 問題はどのような条件下で発生するか。
- 問題は再現できるか。

これらの質問への回答を確認することで、通常は問題点を適切に記述できるようになるため、問題解決に着手する上で最良の方法になります。明確な記述ができたら、問題の原因と解決策を調査したり、WinCollect サポートに問い合わせて、調査への支援を依頼できます。

サポートの入手先

トラブルシューティングは、問題解決と同じではありませんが、トラブルシューティングの 過程で問題解決に必要な情報が得られることもよくあります。ただし、問題の原因を判別できても、自力では解決できない場合もあります。自力では問題を解決できない場合は、 WinCollect サポートに解決策を問い合わせてください。

また、次のリソースを使用して問題の解決策を調べることもできます。

- WinCollect 101 コミュニティー (https://www.ibm.com/community/qradar/home/wincollect/)
- WinCollect フォーラム (http://ibm.biz/wincollectforums)

よくある問題

以下のトピックでは、WinCollect デプロイメントで発生することがある既知の問題のいくつかについて説明します。

発生した問題に関する説明がここで見つかった場合は、サポートへのお問い合わせ前にその解決策を試してみてください。

QRadar でデフォルトの証明書を置き換えると PEM 無効エラーが生成される

QRadar のデフォルトの証明書を置き換えると、`ConfigurationServer.PEM` ファイルが変更され、デプロイメント内のすべての WinCollect エージェントに影響が及びます。この問題を修正するには、Windows ホスト上の `ConfigurationServer.PEM` ファイルを置き換える必要があります。

このタスクについて

WinCollect エージェントが更新された QRadar アプライアンスと 通信しようとすると、誤った証明書が渡されたことによる拒否メッセージが送信されます。以下のエラー・メッセージがログに出力されます。

```
May 17 17:06:31 ::ffff:IP ADDRESS [ecs-ec] [WinCollectConfigHandler_4]
com.q1labs.sem.semsources. wincollectconfigserver.WinCollectConfigHandler: [ERROR]
[NOT:0000003000] [192.0.2.0/- -] [-/- -]Agent with ip: IP ADDRESS tried to connect
with an invalid PEM
```

通信しようとしているエージェントの IP アドレスが表示されます。WinCollect エージェントからは、証明書が無効であることが原因で通信に問題が発生したことを管理者に通知する LEEF Syslog メッセージも送信されます。この問題を修正するには、Windows ホスト上の ConfigurationServer.PEM ファイルを置き換える必要があります。

注 : このアクションは、Windows 管理者、またはリモートの Windows ホストからファイルを削除する権限を持つユーザーが実行する必要があります。

手順

1. 通信できない WinCollect エージェントへのリモート・デスクトップ接続を開きます。
2. 「**スタート**」 > 「**ファイル名を指定して実行**」をクリックします。
3. services.msc と入力して「**OK**」をクリックします。
4. 「**WinCollect**」サービスを停止します。
5. Windows ホストで WinCollect 構成フォルダーにナビゲートします。
   デフォルトのフォルダー・パスは C:¥ProgramFiles¥IBM¥WinCollect¥config です。
6. ConfigurationServer.PEM を削除します。
7. 「**サービス**」ウィンドウから、「**WinCollect**」サービスを開始します。

タスクの結果

WinCollect サービスが再開されると、エージェントは Windows ホストを管理する QRadar アプライアンスへの接続を試行します。QRadar アプライアンスは ConfigurationServer.PEM ファイルが欠落していることを検出し、既存の証明書を対象に置換を実行します。この操作により、更新済みの証明書を含む新しい ConfigurationServer.PEM ファイルに、以前のファイルが置き換えられます。

統計サブシステム

統計サブシステムは、すべてのログ・ソースおよび宛先から、1 秒あたりのイベント数 (EPS) に関するデータを単一のテキスト・ファイルに収集します。

このシステムは、logs¥Statistics.txt ファイルを作成し、収集した EPS 統計をこのファイルに 5 分ごとに取り込みます。

エージェントが始動すると、このエージェントは、収集した統計の最初のセットを Statistics.txt ファイルの末尾に書き込みます。以前の統計は変更しません。その後は、同じ場所に新しい統計を 5 分ごとに書き込みます。

新しい統計を報告する間隔を変更するには、logconfig.xml ファイルを使用します。ReportEvery パラメーターが、各レポートの間隔を分単位で指定します。デフォルト値は 5 分です。

イベント ID 1003 のメッセージが QRadar で分断される

Windows のイベント ID 1003 が、QRadar に設定されているデフォルトの最大ペイロード・サイズを超えることがあります。これにより、このイベント ID が 2 つの個別のメッセージに分断されます。

このタスクについて

QRadar のデフォルトの最大ペイロード・サイズは 4096 バイトです。イベント ID 1003 のメッセージが分断される場合は、メッセージが分断されないように、最大ペイロード・サイズを増やす必要があります。

最大ペイロード・サイズを増やすには、以下の手順を実行します。

手順

1. コンソールに管理者としてログインします。
2. 「**管理**」タブをクリックします。
3. 「**システム設定**」 > 「**拡張**」をクリックします。
4. 「**設定**」ペインで、「**TCP Syslog ペイロードの最大長**」の値を 8,192 に更新します。

ヒント : ペイロードの値を極端に大きくすると、イベント・パイプラインのパフォーマンスに影響が及びます。IBM サポートへの連絡なしで TCP ペイロード長を 8,192 バイトを超える値に設定しないでください。

5. 「**保存**」をクリックします。
6. 「**管理**」タブで、「**拡張**」 > 「**すべての構成のデプロイ**」をクリックします。

   重要 : 全面デプロイメントを完了すると、すべての QRadar アプライアンス上のすべてのサービスが再開されます。全面デプロイメントを実行すると処理中のレポートが停止されるため、デプロイメントを実行する前に、レポートが実行中であるかどうかを確認してください。これらのレポートは、ユーザーまたは管理者が手動で再開する必要があります。この手順では、サービスの再始動時に、すべてのアプライアンスでイベントおよびフローの収集も一時的に停止されます。これらの問題を防止するには、この変更をメンテナンス・ウィンドウで実行します。
7. 「**続行**」をクリックして全面デプロイメント・プロセスを開始します。

タスクの結果

デプロイメントが完了すると、すべての QRadar 管理対象ホストに、受け入れ可能な TCP ペイロード長を増やすための変更が送信されます。すべての管理対象ホストで、ペイロードが 8,192 バイトを超えなければ、イベント・メッセージが切り捨てられなくなります。

構成のリストア時に WinCollect ファイルがリストアされない

構成リストアの完了時に一部の WinCollect ファイルがリストアされていない場合は、インストール ISO に以前のバージョンの WinCollect が含まれていることが原因になっている可能性があります。

QRadar ISO には、組み込みバージョンの WinCollect が含まれています。その ISO を使用してリストアを実行すると、バックアップからのファイルではなく、その ISO に格納されている WinCollect ファイルがデプロイされます。

この問題を修正するには、構成をリストアする前に、バックアップ内の WinCollect のバージョンと一致する WinCollect SFS をインストールする必要があります。以下のタスクを記載された順序で実行します。

1. QRadar のバックアップを実行します。
2. 新しいハードウェアをオンラインにし、ISO をデプロイします。
3. コンソールで、バックアップ内の WinCollect のバージョンと一致する WinCollect SFS をインストールします。
4. 構成バックアップをリストアします。

構成リストアによって適切な WinCollect ファイルがデプロイされます。

Windows 10 (1803) でセキュリティー・ブックマーク・ファイルを読み取ることができない

Windows 10 build 1803 のログ・ソースで、ホストの再始動後にセキュリティー・ブックマーク・ファイルを読み取ることができません。

これは Windows 10 build 1803 の既知の問題です。WinCollect をインストールしてコンピューターを再始動すると、ログ・ソースでセキュリティー・ブックマーク・ファイルを読み取ることができません。

WinCollect 7.2.5 でこの問題を修正するには、問題が発生しているログ・ソースを、セキュリティー・イベント・ログとモニター対象のその他のチャネルを含む XPath を使用して編集します。

WinCollect 7.2.6 以降でこの問題を修正するには、MSEVEN6 を使用するようにログ・ソースを編集します。

WinCollect の更新後のログ・ソース・エラーを解決する

WinCollect 、IBM QRadar、デバイス・サポート・モジュール (DSM)、プロトコル、または脆弱性情報サービス (VIS) コンポーネントをアップグレードした後にログ・ソースを編集しようとすると、エラー・メッセージが表示されることがあります。キャッシュ・ファイルを削除するために、QRadar Web サービスを再始動して、ブラウザー・キャッシュから QRadar ファイルをクリアしてください。

始める前に

SSH アクセス権限および root アカウント資格情報が必要です。

このタスクについて

以下のメッセージは、Web サーバーが QRadar の更新後に再始動しなかったことを示しています。

エラーが発生しました。ブラウザーを最新表示して（F5 を押して）
アクションを再試行してください。
問題が解消されない場合は、お客様サポートにお問い合わせください。

QRadar Web サービスまたはご使用のデスクトップ・ブラウザーによってファイルがキャッシュされることがあります。QRadar Web サービスを再始動して、デスクトップ上のキャッシュ・ファイルを削除する必要があります。

手順

1. SSH を使用して QRadar にログインします。
2. 以下のコマンドを入力して、QRadar Web サービスを停止します。

   ```
   service tomcat stop
   ```
3. 1 つの Web ブラウザー・ウィンドウを開いたままにします。
4. ブラウザー・キャッシュをクリアするには、Web ブラウザーの設定に移動します。
5. ブラウザーを再始動します。
6. 以下のコマンドを入力して、QRadar Web サービスを再始動します。

   ```
   service tomcat start
   ```

WinCollect ログ・ファイル

WinCollect ログ・ファイルには、デプロイメントに関する情報が記載されます。ログは、問題のトラブルシューティングのための有用な情報を提供します。

WinCollect ログの概要

WinCollect は、インストールおよび構成中にログ・イベント拡張フォーマット (LEEF) メッセージを生成して、これらを単一のログ・ファイルに書き込みます。「**状況サーバー (Status Server)**」フィールドのサーバーは、syslog を通じて LEEF メッセージを受信します。これらのメッセージは、WinCollect サービスの状況、許可トークン、構成などについて報告します。

例 :

以下の例は、管理者へのアラートとなる LEEF メッセージを表示しています。これは、WinCollect エージェントが生成しているイベントの数が、ログ・ソースでチューニングされている数を超えていることを示しています。

```
<13>Sep 22
09:07:56 IPADDRESS LEEF:1.0|IBM|WinCollect|7.2|3|src=MyHost.example.com
dst=10.10.10.10
sev=4 log=Device.WindowsLog.EventLog.MyHost.example.com.System.Read
msg=Reopening event log
due to falling too far behind (approx 165 logs skipped). Incoming
EPS r.avg/max =
150.50/200.00. Approx EPS possible with current tuning = 40.00
```

詳しくは、『Log Source Event Rates and Tuning Profiles』(http://www.ibm.com/support/docview.wss?uid=swg21672193) を参照してください。

syslog メッセージを検索するには、WinCollect エージェントの IP アドレスを使用します。QRadar は、監査ログからの情報を追跡して、ログ・ソースがいつ作成されたか、検索がいつ実行されたかなどを判別します。

WinCollect ログ・タイプ

デフォルトのログ・ディレクトリーは、C:¥Program Files¥IBM¥WinCollect¥logs¥ です。ログ・ファイルの名前は WinCollect.log です。

各ログ項目は、項目のタイプを示す以下の識別子によってタグ付けされます。

- システム
- Code
- Device

```
03-08 11:08:16.306 INFO  Code.PayloadRouter : Using 3 router threads.
03-08 11:08:16.306 INFO  Code.PayloadRouter : Using stats sweep period of 30 seconds.
03-08 11:08:16.306 INFO  System.ComponentFactory : Service PayloadRouter v7.2.8 initialized
03-08 11:08:16.306 INFO  Device.Windows2008EventCollector : Windows2008 Event Collector 7.2.8.58 initialized
03-08 11:08:16.306 INFO  System.ComponentFactory : Service Windows2008EventCollector v7.2.8 initialized
03-08 11:08:16.306 INFO  Device.Service.FileForwarderDevice : Initializing FileForwarder Device Service...
03-08 11:08:16.306 INFO  Device.Service.FileForwarderDevice : FileForwarder Device Service initialized.
```

以下の表に、WinCollect ログ・ファイル内のログ項目のタイプを示します。

表 *42. WinCollect* ログ項目のタイプ

ログ項目のタイプ	説明
システム	システム情報 (エージェントがインストールされているオペレーティング・システム、オペレーティング・システムからの RAM と CPU の情報、サービス開始情報、WinCollect のバージョン情報など) を示します。
Code	スピルオーバーとキャッシュのメッセージ、ファイル・リーダー・メッセージ、許可トークン・メッセージ、ローカル・ホストの IP アドレスまたはホスト名の情報、宛先での問題、ログ・ソースの自動作成、スタンドアロン・モード・メッセージ、およびスレッドまたはプロセスの開始とシャットダウンのメッセージに関する情報を示します。WinCollect の構成を調査するには、これらの項目を使用します。Code 項目では、イベント収集に関する情報は示されません。

表 *42. WinCollect* ログ項目のタイプ *(続き)*	
ログ項目のタイプ	**説明**
Device	WinCollect が、イベントおよびおよびイベント・ログ収集を実行するプロトコルを収集するときに作成されます。Device 項目では以下の問題が記録されます。 プラグインのロード 接続の問題 権限または認証 Windows エラー・コード (オペレーティング・システムによって提供される 16 進値コード、0x000005 アクセス拒否など) ファイル・パスまたはロケーション イベント・ログがポーリング対象として期限切れ イベント・ログ・トランザクション RPC が使用不可 (指定したロケーションが見つからない) 後れが大きすぎるために再オープン (チューニング・メッセージ)

ログ・ファイルのディスク・スペース管理
WinCollect は、ログ・サイズが 20 MB を超えると、「_1」バージョンを生成することにより、ログ用のディスク・スペースを管理します。「_5」バージョンが作成されると、WinCollect は、ログの最も古いバージョンを削除します。

また、WinCollect は、チェックポイント・フォルダーをアーカイブすることにより、ディスク・スペースを管理します。QRadar が新規コードで WinCollect を更新すると、チェックポイント・フォルダーは、置き換えられたコードのバックアップを保管します。WinCollect は、10 個のパッチ・チェックポイント・フォルダーが作成された後で、最も古いフォルダーをアーカイブします。WinCollect は、パッチ・チェックポイント・フォルダー内のファイルのリストを含むアーカイブ・フォルダーと、AgentConfig.xml ファイルの圧縮ファイルを作成します。次に、WinCollect は、アーカイブしたパッチ・チェックポイント・フォルダーを削除します。

InfoX デバッグ・ログ

InfoX デバッグ・ログを使用すると、パフォーマンスに影響を与えずにより簡単に WinCollect をデバッグできます。

デフォルトでは、InfoX は有効になっており、エージェントが実行された最初の 5 分間、イベントをログに記録します (最大 5,000 ログ項目)。その後は、InfoX は、15 分ごとに 1 分間、イベントをログに記録します (最大 200 ログ項目)。InfoX は、ログ・レベルが **info** に設定されていても、デバッグ・ログを生成します。

`logconfig.xml` ファイルに以下のいずれかのパラメーターを追加して、InfoX の構成を編集できます。

表 *43. InfoX* 構成オプション	
パラメーター	**説明**
InfoX.enabled	InfoX を有効または無効にするために使用されます。 例 :`InfoX.enabled=true`

表 *43. InfoX* 構成オプション *(*続き*)*

パラメーター	説明
InfoX.startLen	始動時にエージェントを実行する秒数。この機能を無効にするには、この値を `0` に設定します。 例: `InfoX.startLen=300`
InfoX.startMax	始動時にログに記録できるイベントの最大数。 例: `InfoX.startMax=5000`
InfoX.nextWait	次のロギング期間までの待機秒数。 例: `InfoX.nextWait=900`
InfoX.nextLen	各インターバルで、エージェントを実行する秒数。この機能を無効にするには、この値を `0` に設定します。 例: `InfoX.nextLen=60`
InfoX.nextMax	各インターバルで、ログに記録できるイベントの最大数。 例: `InfoX.nextMax=200`

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。 日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。 本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、または サービスのみが使用可能であることを意味するものではありません。 これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの 評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。 本書の提供は、お客様にこれらの特許権について 実施権を許諾することを意味するものではありません。 実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒 103-8510
東京都中央区日本橋箱崎町 19 番 21 号
日本アイ・ビー・エム株式会社
法務・知的財産
法的財産権ライセンス渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。

IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が 禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。 本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、 改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものでは ありません。 それらの Web サイトにある資料は、この IBM 製品の資料の一部では ありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、 自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムと その他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

本プログラムに関する上記の情報は、適切な使用条件の下で使用すること ができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で 決定されたものです。 そのため、他の操作環境で得られた結果は、異なる可能性があります。 一部の測定が、開発レベルのシステムで行われた可能性がありますが、 その測定値が、一般に利用可能なシステムのものと同じである保証はありません。 さらに、一部の測定値が、推定値である可能性があります。 実際の結果は、異なる可能性があります。 お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、 もしくはその他の公に利用可能なソースから入手したものです。 IBM は、それらの製品のテストは行っておりません。したがって、 他社製品に関する実行性、互換性、またはその他の要求については確証できません。 IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向性および指針に関するすべての記述は、予告なく変更または撤回される場合があります。これらは目標および目的を提示するものにすぎません。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、 現行価格であり、通知なしに変更されるものです。 卸価格は、異なる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。 より具体性を与えるために、それらの例には、個人、企業、ブランド、 あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、 名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は 表示されない場合があります。

商標

IBM、IBM ロゴおよび ibm.com® は、世界の多くの国で登録された International Business Machines Corporation の商標です。 他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。 現時点での IBM の商標リストについては、http://www.ibm.com/legal/copytrade.shtml をご覧ください。

Java™ およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

Microsoft、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。