IBM Security QRadar

WinCollect ユーザー・ガイド V7.2.5

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、 77 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 Security QRadar
WinCollect User Guide V7.2.5

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 製品ライブラリーでより技術的な資料にアクセスする方法については、Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644) 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については、Support and Download Technical Note (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861) 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 V7.2.5 の新機能

WinCollect V7.2.5 では、Microsoft Windows Server 2016 のサポートが導入されました。

第 2 章 WinCollect の概要

WinCollect アプリケーションは、管理者が QRadar での Windows イベント収集のために使用できる Syslog イベント・フォワーダーです。WinCollect アプリケーションは、WinCollect ソフトウェアがインストールされたシステム (ローカル・システム) からのイベントの収集や、その他の Windows システムに対するイベントのリモート・ポーリングを行えます。

WinCollect は、Windows イベントの収集用の数多いソリューションの 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 は 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 QRadar に送信します。

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。

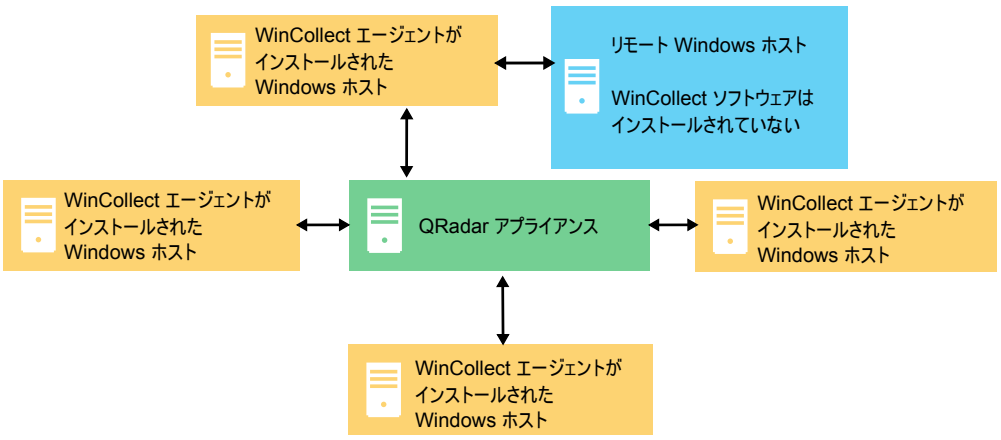

図 *1. WinCollect* 管理対象デプロイメントの例

重要: 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 コンソールまたは QRadar 管理対象ホストによって管理できます。

WinCollect は、管理対象デプロイメントで最大で 500 の Windows エージェントをモニターする場合に最も効率的に機能します。500 を超える Windows ホス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することを、実証済みの方法として推奨します。詳しくは、 69 ページの『第 7 章 スタンドアロン・デプロイメントおよび WinCollect 構成コンソール』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 を超えるホストから 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 ホス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。

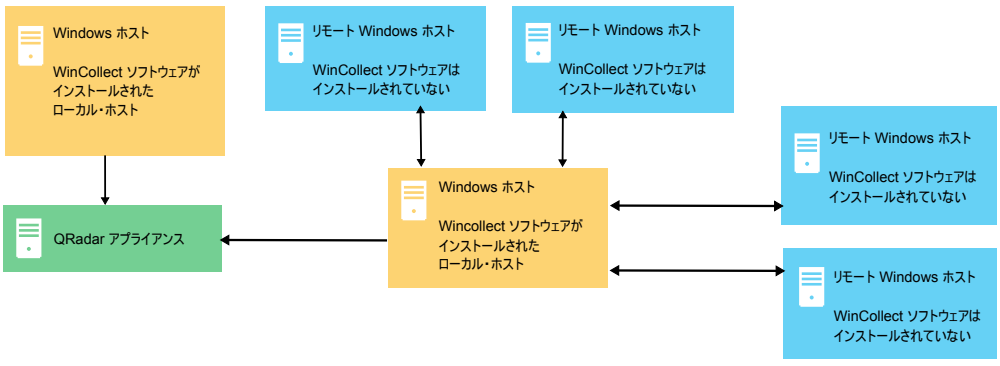

図 2. *WinCollect* スタンドアロン・デプロイメントの例

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が可能。
- 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が可能。
- Adaptive Log Exporter よりも多くのリモート Windows ソースをサポート。
- 仮想マシンのインストールを公式にサポート。

重要: WinCollect 管理対象デプロイメントは、IBM QRadar on Cloud ではサポートされていません。

WinCollect 管理対象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、以下の手順に従います。

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 3 章 WinCollect のインストールの前提条件』を参照してください。
2. Windows ホストをモニターするために使用する QRadar コンソールに WinCollect アプリケーションを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. 認証トークンを作成して、Windows ホストが QRadar に情報を送信できるようにします。詳しくは、 15 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. 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。
   - 15 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』
   - 19 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
   - 27 ページの『WinCollect エージェントの手動による追加』
5. デプロイメント内でドメイン・コントローラーを使用してバルク・ログ・ソースを追加する場合は、 65 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。
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、33 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. WinCollect のインストールを調整するには、 39 ページの『WinCollect ログ・ソースの共通パラメーター』 でイベント・チューニング・プロファイルのセクションを参照してください。
8. QRadar 宛先の 1 つで障害が発生した場合に備えて複数の宛先をセットアップする場合は、 25 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、以下の手順に従います。

1. WinCollect ソフトウェアを、Windows イベントを QRadar に送信する Windows ホスト (複数可) にインストールします。詳しくは、 15 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。
2. WinCollect 構成コンソールまたは WinCollect ソフトウェア更新、あるいはその両方をインストールします。詳しくは、 71 ページの『構成コンソールのインストール』または 72 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。
3. Windows ホストが Windows イベントを送信する宛先、つまり QRadar アプライアンスを構成します。詳しくは、 73 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. リモート・ホストからイベントを収集する場合は、WinCollect がリモート・ホストにログインできるようにするために、資格情報を作成します。 72 ページの『WinCollect 資格情報の作成』を参照してください。
5. Windows イベントを WinCollect に送信するデバイスをセットアップします。詳しくは、 73 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。

第 3 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。

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。WinCollect では、ローカル方式とリモート方式の収集方式を使用できます。

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: ドメイン・コントローラーでのローカル収集は、リモート収集よりも安定しています。これは、ドメイン・コントローラーのイベント/秒 (EPS) レートが、通常、メンバー・サーバーよりも高いためです。

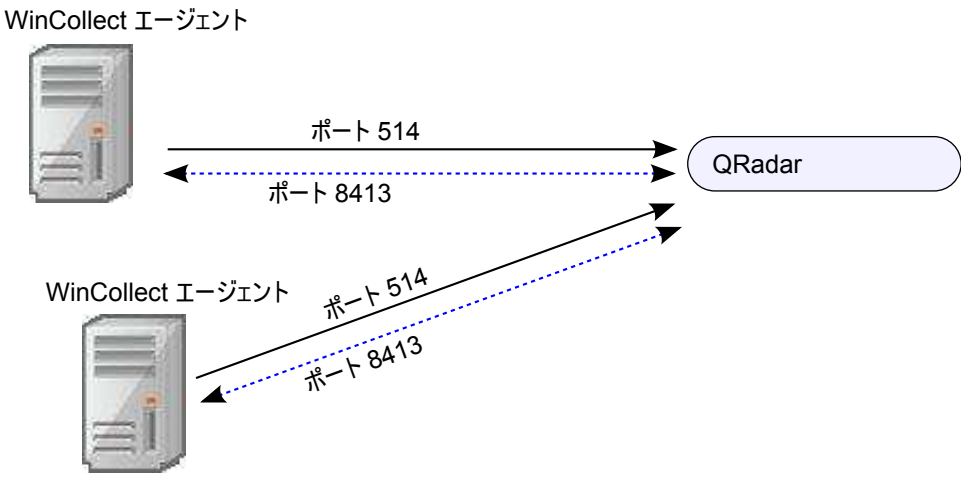

図 3. *WinCollect* エージェントのローカル収集

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。

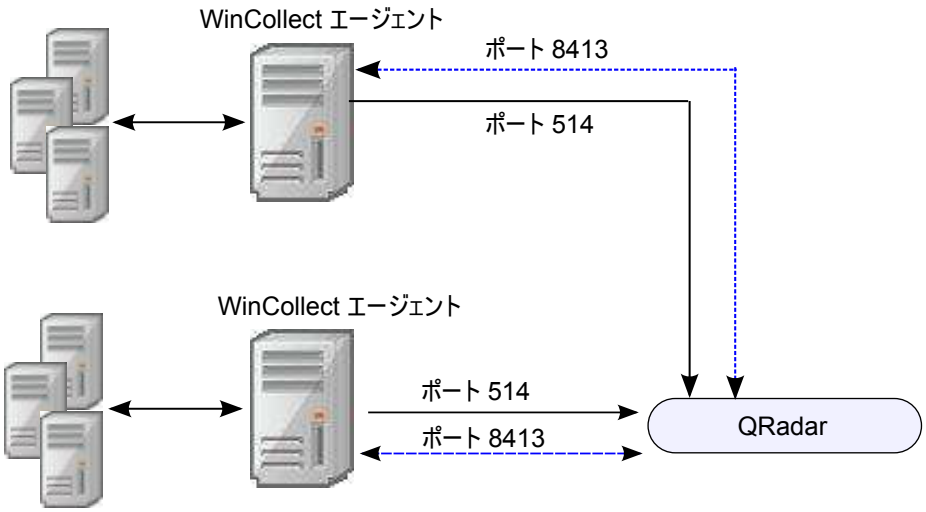

図 *4. WinCollect* エージェントのリモート収集

システム・パフォーマンスとデプロイメントの戦略

以下の戦略により、システム・パフォーマンスへの影響を減らします。

- エージェントの総数を削減するため、1 つのエージェントが多数のエンドポイントをモニターする場合にはリモート収集を使用します。
- WinCollect エージェントのグループをアップデートする場合には、オフピークの稼動時間帯に行います。
- WinCollect エージェントを 100 ずつのグループでデプロイして管理し、問題が発生していないかシステム・パフォーマンスをモニターします。

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。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 WinCollect エージェントの管理に必要です。ポート 8413 は構成の更新などの機能で使用されます。トラフィックは常に WinCollect エージェントから開始されます。このトラフィックは TCP を使用して送信され、通信は暗号化されます。

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・システムのイベントをリモートでポーリングする WinCollect エージェントには、追加のポート要件があります。WinCollect エージェントがリモートで Windows ベースのイベントをポーリングするときは、以下のポートが使用されます。

表 *1. 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
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

リモートの Windows システムをポーリングしてイベントを収集する場合には、動的 RPC が使用されます。動的 RPC を使用するには、WinCollect がイベントのポーリングを試行する Windows システムへのインバウンド・トラフィックをポート 135 で許可する必要があります。ポート 135 は Windows がエンドポイントのマッピングに使用します。

Windows Vista オペレーティング・システム以外の 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場合は、ポート 1024 から ポート 5000 の範囲のポートを許可することが必要な場合があります。古いバージョンの Windows ファイアウォールの場合は、特定のポートに通信を制限するように Windows を構成できます。詳しくは、Windows の資料を参照してください。

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。

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。

以下の表にはハードウェアの最小要件が記載されています。

表 2. *WinCollect* のハードウェア要件

要件	説明
メモリー	8 GB 2 GB (WinCollect エージェント用に確保)
プロセッサー	Intel Core 2 Duo プロセッサー 2.0 GHz
ディスク容量	3 GB (ソフトウェアとログ・ファイルに使用する空きディスク・スペース) 6 GB (スケジュールに基づいてイベントを保管する場合に必要なことがあります)
使用できるプロセッサーのリソース	20%

以下の表には、サポートされるソフトウェアが記載されています。

表 3. 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 2016 Windows Server 2008 (最新) Windows Server 2008 Core Windows Server 2012 (最新) Windows Server 2012 Core Windows 7 (最新) Windows 8 (最新) Windows 10 (最新) Windows Vista (最新)
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。ソフトウェアが延長サポート終了日を過ぎた後でも、製品は予期されると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・システムでの WinCollect の問題を解決するために、コードまたは脆

弱性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 Security 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 エージェントのインストールおよび 1 秒当たりのイベント数

WinCollect エージェントをインストールする前に、WinCollect エージェントで収集可能なイベント数について理解しておくことが重要です。

リモート・イベント収集での EPS レートを向上させるためのエージェントのチューニングは、使用するネットワーク、そのエージェントに割り当てるログ・ソースの数、およびログ・ソースごとに生成されるイベントの数によって異なります。イベントおよびチューニングについて詳しくは、『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。

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 4. 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
QRadar V7.1 (MR2)	WinCollect 7.2.2-2	AGENT-WINCOLLECT-7.1-1018604.noarch
QRadar V7.2.x 以降	WinCollect 7.2.2-2	AGENT-WINCOLLECT-7.2-1018607.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

インストール済み WinCollect エージェントのバージョンは、以下のいずれかの方式で確認できます。

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 4 章 WinCollect のインストール

WinCollect をインストールするには、WinCollect エージェント・バンドルをダウンロードして QRadar システムにインストールし、認証トークンを作成して、イベントの収集対象の各 Windows 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。WinCollect エージェントを Windows ホストにインストールし、そのホストを使用してリモートで他の Windows ホストからイベントを収集することもできます。

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

WinCollect エージェントのデプロイメントを QRadar ユーザー・インターフェースから管理するには、最初に WinCollect エージェント・バンドルを QRadar コンソールにインストールする必要があります。このバンドルには、QRadar システムと管理対象 WinCollect ホスト間で通信を行うために必要なプロトコルが含まれています。WinCollect インストール・ファイルを使用して、最初に WinCollect バンドルを QRadar ホストにインストールしてから、WinCollect エージェントを新しいバージョンにアップグレードすることができます。

このタスクについて

重要: WinCollect バージョン 7.0 または 7.1.0 からのアップグレードについては、www.ibm.com/support (http://www-01.ibm.com/support/docview.wss?uid=swg21698127) を参照してください。

WinCollect エージェント・バンドル・ファイルをアップグレードすると、QRadar アプライアンスからの自動更新の受信が有効になっている WinCollect エージェントが、次の構成ポーリング間隔で新規バージョンにアップグレードされます。新規 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。 WinCollect サービスが再始動すると、引き続きイベント収集の転送が行われます。

重要: WinCollect をインストールした後で QRadar を再インストールした場合は、「**Program Files**」 > 「**IBM**」 > 「**WinCollect**」 > 「**config**」フォルダーの ConfigurationServer.PEM ファイルを削除する必要があります。このファイルを削除しないと、WinCollect が正しく機能しません。

手順

1. WinCollect エージェント・バンドルのインストール・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. WinSCP などのプログラムを使用して、インストール・ファイルを QRadar システムにコピーします。
3. root ユーザーとして QRadar にログインします。

4. 初期インストールのために、/media/patch ディレクトリーを作成します。以下のコマンドを入力します。

   ```
   mkdir /media/patch
   ```

5. インストール・ファイルをマウントするには、以下のコマンドを入力します。

   ```
   mount -t squashfs -o loop Installer_file_name.sfs /media/patch
   ```

   例:

   ```
   mount -t squashfs -o loop 720_QRadar_wincollectupdate-7.2.0.xxx.sfs /media/patch
   ```

6. /media/patch に変更するには、以下のコマンドを入力します。

   ```
   cd /media/patch
   ```

7. WinCollect をインストールするには、以下のコマンドを入力して、その後はプロンプトに従います。

   ```
   ./installer
   ```

8. オプション: 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. 「エージェント」をクリックします。
   e. 「自動更新は有効」列を確認して、値が「**False**」であるエージェントを探します。
   f. 「自動更新は有効」列の値が「**False**」である WinCollect エージェントを選択します。
   g. 「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 WinCollect エージェントが更新され、再始動します。エージェント更新の所要時間は、WinCollect エージェントの構成ポーリング間隔によって異なります。

関連タスク:

15 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』
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。

19 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』
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。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。

この認証トークンは、インストールするすべての WinCollect エージェントに必要です。

認証トークンを使用することで、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。イベントを QRadar ホストに通知するすべての WinCollect エージェント用に、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・ソースの構成変更を受信できなくなります。

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、「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 5. 「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)**	認証トークンの有効期限日付は設定しないでください。

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。

- WinCollect エージェントに対する認証トークンが作成されていること。

詳しくは、 15 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 エージェントで、QRadar Event Collector との通信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。
- WinCollect エージェントのログ・ソースを自動的に作成するには、Windows ログ・ソースの送信先となる宛先の名前が必要になります。

  インストール時に、WinCollect エージェント・ホストのログ・ソースを自動的に作成するように QRadar を構成できます。ログ・ソース・データの転送先のホストを構成する必要があります。詳しくは、 29 ページの『宛先の追加』を参照してください。WinCollect エージェントは、構成された宛先に Windows イベント・ログを送信します。宛先は、コンソールにすることも、Event Collector にすることもできます。ログ・ソースの自動作成を構成するには、QRadar システムが IBM Security QRadar SIEM V7.2.1 ソフトウェア更新 1 以降に更新されている必要があります。

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・セットアップ・ファイルをダウンロードします。
2. WinCollect エージェントのインストール・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ます。
   - 管理対象インストールについて詳しくは、WinCollect 管理対象セットアップ・タイプのインストール・ウィザードのパラメーターを参照してください。
   - スタンドアロン・インストールについて詳しくは、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を参照してください。

表 6. *WinCollect* 管理対象セットアップ・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 エージェントのリストに表示されます。 「ホスト **ID**」フィールドの値は、QRadar コンソール上にある WinCollect エージェント構成内の「ホスト名」フィールドの値に一致する必要があります。
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 コンソールの IP アドレスまたはホスト名 (例えば、192.0.2.0 または`myhost`)。 これは、ご使用の QRadar コンソールまたは Event Collector のためのパラメーターです。Event Collector を構成サーバーとして使用するには、QRadar システムが V7.2.1ソフトウェア更新 3 以降に更新されている必要があります。
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。
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 に WinCollect 宛先を構成しておく必要があります。
イベント・ログ	ログ・ソースによって収集され、QRadar に送信される必要がある Window イベント・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 6. *WinCollect* 管理対象セットアップ・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
イベント速度チューニング・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 • 標準的なサーバー (Typical Server): 500/750 • イベント速度が高いサーバー (High Event Rate Server): 1250/1875 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構成サーバーの IP アドレスを表示します。
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 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)。

表 7. *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)**	「ログ・ソースの自動作成を有効にする **(Enable Automatic Log Source Creation)**」チェック・ボックスが選択されている場合は必須。WinCollect エージェントがポーリングするリモート・デバイスを識別します。
イベント・ログ	ログ・ソースによって収集され、QRadar に送信される必要がある Window イベント・ログ。
宛先名 **(Destination Name)**	Syslog データを送信する宛先を識別します。
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**

表 7. *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
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。
イベント速度チューニング・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 • 標準的なサーバー (Typical Server): 500/750 • イベント速度が高いサーバー (High Event Rate Server): 1250/1875 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 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)。
ハートビート間隔 **(**ミリ秒**) (Heartbeat Interval (msecs))**	ハートビートの状況メッセージが送信される頻度 (ミリ秒単位)。

「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、『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 *8. 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	WinCollect サービスを許可します (例えば、AUTH_TOKEN=af111ff6-4f30-11eb-11fb-1fc1 17711111)。
FULLCONSOLEADDRESS=host_address	エージェントを管理する QRadar アプライアンスの IP アドレスまたはホスト名。アドレスは、イベントを受信できる QRadar アプライアンスである必要があります。**例:** FULLCONSOLEADDRESS=192.0.2.0 FULLCONSOLEADDRESS=EPqadar.myhost.com Windows ホストと QRadar Event Collector との通信を行うには、QRadar デプロイメント環境内のすべてのシステムを V7.2.1 パッチ 3 以降に更新する必要があります。
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)。

表 8. *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
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。
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:** 宛先名は、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する必要があります。存在しないと、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。
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.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。

表 8. *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.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。
`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 8. *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。

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。

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 Security 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。 29 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。

第 5 章 インストール後の WinCollect エージェントの構成

WinCollect のデプロイメント環境のインストール後は、IBM Security QRadar を使用してデプロイメント環境を管理します。

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 9. *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:

27 ページの『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 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 10. 宛先パラメーター

パラメーター	説明
ポート	IBM Security QRadar は、WinCollect エージェントからのイベントを UDP ポートまたは TCP ポート 514 で受信します。
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 10. 宛先パラメーター (続き)

パラメーター	説明
名前 **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。	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。
ホスト名	宛先 IBM Security QRadar アプライアンスのホスト名または IP アドレス。
キュー最高水準点 (バイト)	イベント・キューのサイズの上限を定義します。 この最高水準点制限に達すると、WinCollect エージェントはキューに入っているイベントの数を削減するために、イベントの優先順位付けを試行します。
キュー最低水準点 (バイト) **重要:** QRadar サポートが変更を推奨している場合を除いて、デフォルト値を変更しないでください。	イベント・キューのサイズの下限を定義します。 最高水準点に達したキューが最低水準点以下のレベルに変わると、イベントの優先順位付けは通常の状態に戻ります。
ストレージ間隔 (秒) **重要:** QRadar サポートが変更を推奨している場合を除いて、デフォルト値を変更しないでください。	WinCollect エージェントがイベントをディスクまたはメモリーに書き込むまでの間隔を定義します。
処理期間 (マイクロ秒) **重要:** QRadar サポートが変更を推奨している場合を除いて、デフォルト値を変更しないでください。	WinCollect エージェントが、転送キュー内のイベントとディスク・キュー内のイベントを評価する頻度を定義します。これは、イベント処理を最適化するために使用されます。
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。

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。

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。

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。

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。

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。

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。

転送されたイベントは、「ログ・アクティビティー」タブに *Windows Auth @ IP address* として表示されます。一方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 が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、WinCollect は、そのイベントを WinCollect イベントとして識別する追加の Syslog ヘッダーを含めます。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、この追加ヘッダーが含まれることはなく、標準のイベントと同様に表示され、WinCollect ID は含まれません。

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場合にのみ、WinCollect によって収集されます。

ドメイン・コントローラー

ドメイン・コントローラーがある場合、サーバーにローカルの 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。生成される可能性があるイベント数のため、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に、ローカルのログ・ソースを使用してください。

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 Vista (最新)
- Windows 10 (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。ソフトウェアが延長サポート終了日を過ぎた後でも、製品は予期されると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・システムでの WinCollect の問題を解決するために、コードまたは脆弱性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 Security 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。

Microsoft イベント・サブスクリプションの使用

イベント・サブスクリプションを使用するには、以下の手順を実行する必要があります。

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。

- 「宛先ログ **(Destination log)**」リストで「転送されたイベント」を選択します。
- コンテンツ・フォーマットは `RenderedText` です。
- ロケールは `en_US` です。

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。
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。

WinCollect ログ

WinCollect ログは、デプロイメントについての情報を提供します。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。

WinCollect ログ・タイプについて、以下の表で説明します。

表 *11. WinCollect* ログ・タイプ

サブフォルダー	説明
WinCollect_System.log	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・システムなど)、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、および WinCollect バージョン情報をキャプチャーします。

表 11. *WinCollect* ログ・タイプ (続き)

サブフォルダー	説明
WinCollect_Code.log	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 アドレスとホスト名の情報、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の情報をキャプチャーします。WinCollect 構成を調査するには、このログを使用します。このログは、イベント収集についての情報を提供しません。
WinCollect_Device.log	WinCollect がイベントを収集するときにメッセージをログに記録するため、およびイベント・ログ収集を実行するプロトコルをログに記録するために使用されます。WinCollect_Device.log のログには、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た後で、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。

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。

第 6 章 WinCollect エージェントのログ・ソース

単一の WinCollect エージェントで、ローカル・システムのイベントの管理と転送をしたり、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・ポーリングを行ったりすることができます。

WinCollect エージェントを通じて通信するログ・ソースは、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。

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。

WinCollect ログ・ソースの共通パラメーター

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 12. *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。
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。

表 12. *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
イベント速度チューニング・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 • イベント速度が高いサーバー **(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 • イベント速度が高いサーバー **(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。

表 12. *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。
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。
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 12. *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 セキュリティー・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、「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・ボックスは無視されます。QRadar が収集するイベントは、XPath 照会のコンテンツを使用します。 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。

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。

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 13. 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 *14. 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 *15. 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:

39 ページの『WinCollect ログ・ソースの共通パラメーター』
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。

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 2016
- Windows Server 2012 R2
- Windows Server 2008 R2

表 16. 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。

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、QRadar で 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。

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 17. 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、IBM Security QRadar に転送します。

表 17. 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
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。
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。

表 17. 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・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。

関連資料:

39 ページの『WinCollect ログ・ソースの共通パラメーター』
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 18. 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 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 19. 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 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 20. 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**
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。

表 20. *Microsoft IAS* のパラメーター (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:

39 ページの『WinCollect ログ・ソースの共通パラメーター』
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

Microsoft IIS イベントを収集するには、WinCollect エージェントが Microsoft Server 上にインストールされている必要があります。

制約事項**:** Microsoft IIS イベントのリモート・ポーリングは、Microsoft IIS 用 WinCollect プラグインではサポートされません。

Microsoft には、Web サイトを管理するための幅広い管理機能が含まれています。Web サイトへのアクセスの試行をモニターして、ファイルの読み取りまたは書き込みが試みられたかどうかを判別できます。単一の Microsoft IIS ログ・ソースを作成して、Web サイト・ディレクトリー全体または個々の Web サイトからのイベントを記録できます。

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

Microsofct 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。

制約事項**:** Microsoft 認証プロトコルの NTLMv2 は、Microsoft IIS プロトコルではサポートされません。

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 6.0
- 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 21. 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 IIS 6.0 (個別サイト) の場合は、「%SystemRoot%¥LogFiles¥サイト名」を使用 • Microsoft 7.0-8.0 (全サイト) の場合は、「%SystemDrive%¥inetpub¥logs¥LogFiles」を使用 • Microsoft IIS 7.0-8.0 (個別サイト) の場合は、「%SystemDrive%¥inetpub¥logs¥LogFiles¥サイト名」を使用
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。

表 21. *Microsoft IIS* のパラメーター (続き)

パラメーター	説明
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 22. *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 23. *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 24. *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、IBM Security QRadar に転送します。

表 24. *Microsoft ISA* 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)**	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。
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:

39 ページの『WinCollect ログ・ソースの共通パラメーター』
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 25. 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、IBM Security 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。
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 *26. 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$¥Program Files¥Microsoft SQL Server¥MSSQL10.MSSQLSERVER¥MSSQL¥Log¥
2008R2	ローカル	C:¥Program Files¥Microsoft SQL Server¥MSSQL10_50.MSSQLSERVER¥MSSQL¥Log
2008R2	リモート	¥¥SQL IP address¥c$¥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 Remote ¥¥SQL IP address¥c$¥Program Files¥Microsoft SQL Server¥MSSQL11.MSSQLSERVER¥MSSQL¥LOG
2014	ローカル	Local C:¥Program Files¥Microsoft SQL Server¥MSSQL12.MSSQLSERVER¥MSSQL¥LOG 2014 Remote ¥¥SQL IP address¥c$¥Program Files¥Microsoft SQL Server¥MSSQL12.MSSQLSERVER¥MSSQL¥LOG

表 26. *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
2016	ローカル	C:¥Program Files¥Microsoft SQL Server¥MSSQL13.MSSQLSERVER¥MSSQL¥LOG 2016 Remote ¥¥SQL IP address¥c$¥Program Files¥Microsoft SQL Server¥MSSQL13.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

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 27. *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 27. *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。

表 27. *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:

39 ページの『WinCollect ログ・ソースの共通パラメーター』
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 28. *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 システムにログインするためのアカウント名。
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
- ファイル・タイプ: Windows イベント・ログ (EVT)

XPath ログ・ソースの構成オプション

この参照情報は、イベント・ビューアーで XPath 照会を組み込んだログ・ソースを作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。

表 29. XPath のプロトコル・パラメーター

パラメーター	説明/アクション
ログ・ソース・タイプ	**Microsoft Windows** セキュリティー・イベント・ログ
プロトコル構成	「**WinCollect**」を選択します。
標準ログ・タイプ **(Standard Log Types)**	ログ・タイプのチェック・ボックスがすべて選択解除されていることを確認します。 XPath 照会が、ログ・ソースのログ・タイプを定義します。
転送されたイベント	このチェック・ボックスは選択しないでください。
イベント・タイプ **(Event Type)**	「イベント・タイプ **(Event Type)**」チェック・ボックスは選択しないでください。 XPath 照会が、ログ・ソースのログ・タイプを定義します。
XPath 照会	Microsoft イベント・ビューアーで定義した XPath 照会。 XPath 照会を使用して情報を収集するには、Windows 2008 以降で「リモート イベントのログ管理」オプションを有効にしなければならない場合があります。
WinCollect エージェント	このログ・ソースを管理する WinCollect エージェント。

関連資料:

39 ページの『WinCollect ログ・ソースの共通パラメーター』
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。

XPath 照会の作成

XPath 照会とは、照会が Windows 2008 以降のイベント・ログと通信するときに特定のイベントをフィルターに掛けるログ・ソース・パラメーターのことです。

XPath 照会では XML 表記を使用します。XPath 照会は、WinCollect プロトコルを使用してイベントを取得するときに、QRadar で使用できます。

1. Microsoft イベント・ビューアーを使用して XPath 照会を作成します。
2. Microsoft イベント・ビューアーでカスタム・ビューを作成します。特殊なイベントを対象に作成するカスタム・ビューでは、XPath 通知を生成できます。
3. XPath 照会で生成した XPath 通知をコピーします。XPath 通知をコピーすると、特定のイベント・データの入力ログ・ソース・イベントがフィルターに掛けられます。

注**:** 独自の XPath 照会を手動で作成するには、XPath 1.0 および XPath 照会に習熟している必要があります。

Windows 7 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 で、XPath 照会のリモート・ログ管理を有効にすることができます。

Windows 7 で、XPath 照会のリモート・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。

Windows 2008 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 Server 2008 で、XPath 照会のリモート・ログ管理を有効にすることができます。

Windows Server 2008 で、XPath 照会のリモート・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. 「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. 「例外」タブで、「リモート イベントのログ管理」を選択し、「**OK**」をクリックします。

Windows 2008 R2 および Windows R2 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 2008 R2 および Windows 2012 R2 で、XPath 照会のリモート・ログ管理を有効にすることができます。

Windows 2008 R2 および Windows 2012 R2 で、XPath 照会のリモート・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. 「**Windows** ファイアウォール」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」チェック・ボックスを選択します。

   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。

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 では、XPath 照会でイベント・ログを 10 個まで選択できます。この制限には、抑制されているイベント ID は含まれません。

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。

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・ソースを選択します。
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。

    注**:** ログ・ソースの XPath 照会を指定すると、照会で指定されたイベントのみが WinCollect プロトコルによって取得され、IBM Security QRadar に転送されます。「標準のログ・タイプ」または「イベント・タイプ」から選択するチェック・ボックスは、ログ・ソース構成では無視されます。

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『XPath ログ・ソースの構成オプション』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。

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 <= 4777) )]]</Select>
</Query>
</QueryList>
```

表 *30.* 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 <= 4726) or (EventID &gt;= 4741 and EventID
<= 4743) )]]</Select>
</Query>
</QueryList>
```

表 31. 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。
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。

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 Security QRadar アプライアンス上に、Windows イベントの宛先を作成します。 29 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。『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 Security 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:

42 ページの『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 7 章 スタンドアロン・デプロイメントおよび WinCollect 構成コンソール

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 Security 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 (非管理対象デプロイメントとも呼ばれます) 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 Security 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、 15 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 32. *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。以下のパラメーターを持ちます。 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

- WinCollect 構成コンソールのすべてのバージョンをアンインストールします。詳しくは、 24 ページの『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』を参照してください。
- 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、 19 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 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。ソフトウェアが延長サポート終了日を過ぎた後でも、製品は予期されると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・システムでの WinCollect の問題を解決するために、コードまたは脆弱性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 Security 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. パッチ・ソフトウェアを、IBM サポート (www.ibm.com/support/fixcentral) から、構成コンソールのインストール場所である Windows ホストに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。

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 Security 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**:** 「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。
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。
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 Security 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。TLS Syslog は、管理対象 WinCollect デプロイメントではサポートされていません。

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。

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 Security 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。73 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。 73 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 Security 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。 72 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。 73 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。 73 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。

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。