Hewlett Packard Enterprise

HPE
Security ArcSight SmartConnectors

SmartConnector for Microsoft Windows Event Log - Native

構成ガイド

2017年8月15日

ご注意

保証

Hewlett Packard Enterprise製品、またはサービスの保証は、当該製品、およびサービスに付随する明示的な保証文によってのみ規定されるものとします。ここでの記載は、追加保証を提供するものではありません。
ここに含まれる技術的、編集上の誤り、または欠如について、Hewlett Packard Enterpriseはいかなる責任も負いません。ここに記載する情報は、予告なしに変更されることがあります。
本書の例で使用しているネットワーク情報 (IPアドレスやホスト名を含む) は、説明のみを目的としています。

HPE Security ArcSight製品は高い柔軟性を持ち、お客様の設定に応じて機能します。データのアクセス性、完全性、機密性については、ユーザーが責任を負います。包括的なセキュリティ戦略を実施し、優れたセキュリティ慣習に従ってください。

本書は機密情報です。

権利の制限

機密性のあるコンピューターソフトウェアです。これらを所有、使用、または複製するには、Hewlett Packard Enterpriseからの有効な使用許諾が必要です。商用コンピューターソフトウェア、コンピューターソフトウェアに関する文書類、および商用アイテムの技術データは、FAR12.211および12.212の規定に従い、ベンダーの標準商用ライセンスに基づいて米国政府に使用許諾が付与されます。

著作権について

著作権と承認の完全な表明については、以下のリンク先をご覧ください。
https://community.saas.hpe.com/t5/Discussions/Third-Party-Copyright-Notices-and-License-Terms/td-p/1589228

改訂履歴

日付	説明
2017/08/15	「接続でのSSLの使用 (オプション)」の手順を更新し、"arcsight connectorsetup" コマンドを削除して "runagentsetup" コマンドを追加しました。
2017/07/15	トラブルシューティングに関する説明を追加しました。サポートされるインストールプラットフォームとして、Windows Server 2016を追加しました。
2017/05/15	サポート終了により、Windows 2003を削除しました。インストールプラットフォームとして、Windows 2016のサポートを追加しました。FIPSのサポートを追加しました。
2017/02/15	コネクターのセットアップを変更しました。Active Directoryログイン資格情報に、ユーザー名とパスワードを追加しました。
2016/11/30	インストール手順に、「グローバルパラメーターの設定」を追加しました。これには、優先IPアドレスモードを設定する機能も含まれます。サポートされるバージョンを更新しました。OSレベルでFIPSを無効化する手順を追加しました。
2016/08/30	サポートされるバージョンを更新しました。
2016/05/16	.NET 4.6のサポートを追加しました。「付録C」として、Microsoft Windows Event Log NativeとUnifiedの比較表を追加しました。
2016/03/31	編集上の変更。

日付	説明
2016/02/15	Microsoft Windows 10からのイベント収集のサポート、リモート管理オプションに関する説明、および新しい詳細なコンテナー設定と詳細な共通設定パラメーターを追加しました。パワーユーザーがWindows Vistaワークグループホストから標準のローカルユーザーアカウントを使用してローカルユーザーを設定するための要件を削除しました。
2015/06/30	パラメーターを更新し、フランス語、日本語、および中国語に関するローカリゼーションサポートを追加しました。
2015/02/16	この最新コネクターの一般向け第一版。

サポート

連絡窓口

電話	電話番号の一覧は、HPE Security ArcSightテクニカルサポートページに掲載されています: https://softwaresupport.hpe.com/documents/10180/14684/esp-support-
サポートWebサイト	https://softwaresupport.hpe.com
Protect 724コミュニティ	https://community.saas.hpe.com/t5/ArcSight/ct-p/arcsight

目次

SmartConnector

このガイドでは、SmartConnector (Windows Event Log − Native) のインストールと、デバイスでのイベントログ収集の設定について説明します。

インストールプラットフォーム:

- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

ArcSight SmartConnectorでは、社内のすべてのイベント生成元からすべてのログを監査品質でスケーラブルかつ容易に収集して、リアルタイム分析やフォレンジック分析に利用できます。SmartConnectorは、多数のホストに対応できるように最適化されています。

SmartConnectorのセキュリティイベントのArcSightデータフィールドへのマッピングについては、『SmartConnector for Microsoft Windows Event Log − Native Windows Security Event Mappings』を参照してください。

製品概要

Windowsの操作イベントログやIPv6ホストからのイベント収集およびイベントフィルタリングなどの重要な機能を提供できるように、SmartConnector for Microsoft Windows Event Log − Native (Windows Event Log − Native) によるインフラストラクチャーに改善を加えました。Microsoftプラットフォームのネイティブテクノロジーを活用し、Windowsのイベント機能 (すべてのログタイプでの収集を含む) が最適な形でサポートされています。

注: デフォルトでは、セキュリティイベントは監査されません。監査を行うセキュリティイベントのタイプを必ず指定してください (本書の「Microsoft Windowsイベントログ監査ポリシーの有効化」 (11ページ)」を参照)。

このコネクターは、次の3つの主要なコンポーネントで構成されています。

- SmartConnectorフレームワークベースのイベントプロセッサー
- Microsoft Windowsイベントログからイベントを収集するWindows APIアプリケーション
- 上記の2つのコンポーネント間の通信を円滑にするメッセージキュー

Windows APIのイベント収集とメッセージキューは、コネクターのセットアップ時およびコネクタープロセスの開始時にコネクターによって起動されます。

機能

SmartConnectorの機能には、リアルタイムイベント収集/処理に加えて、データ改良 (正規化、分類、共通イベントフォーマット (CEF)、アグリゲーション、フィルタリング) や効率性 (キャッシュ、一括処理、圧縮、帯域幅管理) などが含まれます。詳細については、『ArcSight SmartConnectorユーザーガイド』を参照してください。Windows Event Log – Nativeコネクターの機能については、以下の各セクションを参照してください。

カスタムログのサポート

非管理用ログ、操作ログ、またはカスタムログからのイベント収集が利用できます。

イベントフィルタリング

イベントソースからコネクターへのイベント収集時に適用されるフィルターがサポートされます。これにより、必要のないイベントを除外し、リソースを有効に利用できます。

グローバルー意識別子 (GUID)

フォレスト内でのGUID (UUIDともいう) の変換とマッピングがサポートされます(フォレストとは、Active Directoryのすべての要素を含むインスタンスです)。コネクターは、グローバルカタログサーバーに問い合わせることで、フォレスト内のGUIDに対してGUID変換を行うことができます。グローバルカタログサーバーでは、Active Directoryのパラメーターが使用されます。コネクターは、デフォルトではGUID変換を行うように設定されていません。GUID変換の詳細については、「SIDおよびGUID変換に関する詳細設定パラメーター」を参照してください。グローバルカタログとActive Directoryは同じマシン上に存在している必要があります。

ホスト参照

ホスト参照は、インストール時にActive Directoryを使用してホストを追加する場合に使用されます。新しいホストがActive Directoryに追加されると、通知が通知先に送信されます。

IPv6

IPv6ホストからのイベント収集とIPv6イベントの解析がサポートされます。

ローカリゼーション

Windows Event Log – Nativeコネクターは、以下の言語でセキュリティイベントのローカリゼーションをサポートしています。

言語	ロケール	エンコーディング
フランス語	fr_CA	UTF-8
日本語	ja_JP	Shift_JIS
簡体字中国語	zh_CN	GB2312
繁体字中国語	zh_TW	Big5

ロケールとエンコーディングは、SmartConnectorのインストール時に`event.name`フィールドで指定できます。詳細については、「複数のホストパラメーターの設定」(24ページ) を参照してください。その他の言語のローカリゼーションについては、「Nativeコネクターでのローカリゼーションサポートのカスタマイズ」(39ページ) を参照してください。

イベント収集でサポートされるオペレーティングシステム

SmartConnectorは、以下のMicrosoft OSバージョンが稼働するホストからの、Windowsイベントログのセキュリティ、システム、およびアプリケーションイベントの収集をサポートしています。

- Microsoft Windows Vista
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 10

また、ソースホストからWindowsイベントコレクター (WEC) へ転送されるイベントもサポートしています。

インストール要件

システム要件

このコネクターは、以下のMicrosoft Windows 64ビット版プラットフォームのいずれかにインストールできます。

- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

.NETの要件

- .NET 4.5、4.5.2、4.6、または4.6.1

サポートされるイベント

Windowsイベントログは、以下の解析をサポートしています。

イベントタイプ	イベントヘッダー	イベントの説明
セキュリティ	あり	あり
アプリケーション	あり	なし*
システム (サービスコントロール マネージャーおよびWINSイベントソース)	あり	あり
その他のシステムイベント (リモート アクセスおよびNPSを含む)	あり	なし*

* Flex-Connectorに似たフレームワーク向けにサポートが提供されています。このフレームワークでは、独自のパーサーを作成して展開し、すべてのシステムイベントとアプリケーションイベントのイベントの説明を解析できます。詳細については、「システムイベントおよびアプリケーションイベントに対するカスタムパーサー の作成」を参照してください。すでにサポートされているアプリケーションイベントとシステムイベントについては、「ログパーサーのサポート」を参照してください。

ログパーサーのサポート

SmartConnectorは、以下のログに対する解析をサポートしています。

- セキュリティ
- システム
- アプリケーション (イベントヘッダー)
- 転送済みイベント (転送されたセキュリティ、システム、およびアプリケーション (イベントヘッダー) イベント)

サポートされるアプリケーション

以下のアプリケーションイベントのパーサーのサポートが提供されます。

- Microsoft Active Directory
- Microsoft Exchangeアクセス監査
- Microsoft Forefront Protection 2010
- Microsoft SQL Server Audit
- Oracle監査
- Symantec Mail Security for Exchange

サポートされるシステムイベント

以下のシステムイベントのパーサーのサポートが提供されます。

- Microsoftネットワークポリシーサーバー
- Microsoftリモートアクセス
- Microsoftサービスコントロールマネージャー
- Microsoft WINSサーバー

ホストに対するActive Directoryクエリの使用

収集エンドポイントの読み込みや更新を行う場合、またはWindowsイベントコレクターから収集する場合に転送されるイベントのソースホストのWindows OSバージョンを指定する場合は、Active Directoryクエリを使用できます。コネクターは、Active Directoryに登録されたホストに関する情報を検出して取得します。このホスト情報には、DNS名とホストのOSバージョンが含まれます。コネクターの実行中にActive Directoryに新しいホストが登録されると、新しく検出されたホストをユーザーに通知する内部イベントが送信されます。

Windowsの設定

Microsoft Windowsイベントログ監査ポリシーの有効化

Windowsサーバーによるイベント情報の生成は、有効に設定された監査ポリシーに基づいて行われます。このため、コネクターが情報を収集するWindowsサーバーでは、適切な監査ポリシーを有効にしておく必要があります。デフォルトでは、有効になっているWindows監査機能はありません。

監査対象イベントを計画する際には、監査イベントがメモリ、処理能力、ディスク容量などのシステムリソースを消費することに注意する必要があります。監査対象イベントが多くなるほど、これらのリソースの消費量も増えます。監査対象イベントが多すぎると、サーバーの速度が大幅に低下する可能性があります。

注: 監査ポリシーを設定するには、管理者またはAdministratorsグループのメンバーとしてログオンする必要があります。お使いのコンピューターがネットワークに接続されている場合、ネットワークポリシーの設定により、監査ポリシーを設定できない場合があります。

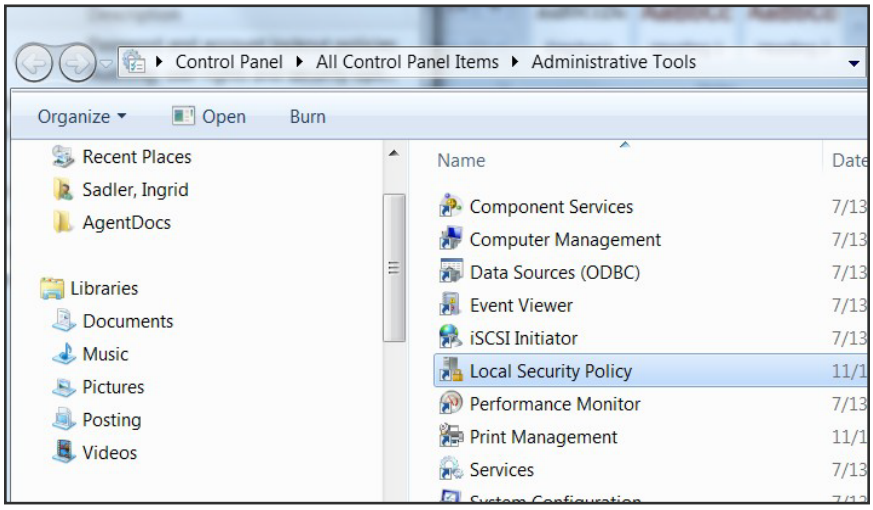
監査ポリシーの作成方法は、ポリシーの作成をメンバーサーバー、ドメインコントローラー、またはスタンドアロンサーバーのいずれで行うかによってやや異なります。

- ドメインコントローラー、メンバーサーバー、またはワークステーションを設定するには、[**Active Directory ユーザーとコンピューター**] を使用します。
- ドメインに参加しないシステムを設定するには、[**ローカル セキュリティ設定**] を使用します。

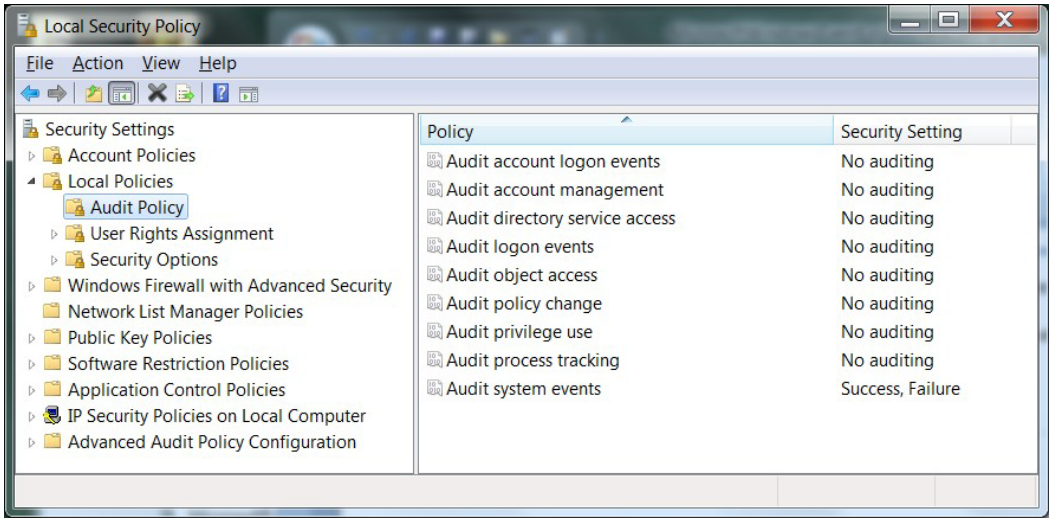
ローカルシステムの監査

ローカルシステムで監査ポリシーを設定するには、次の手順を実行します。

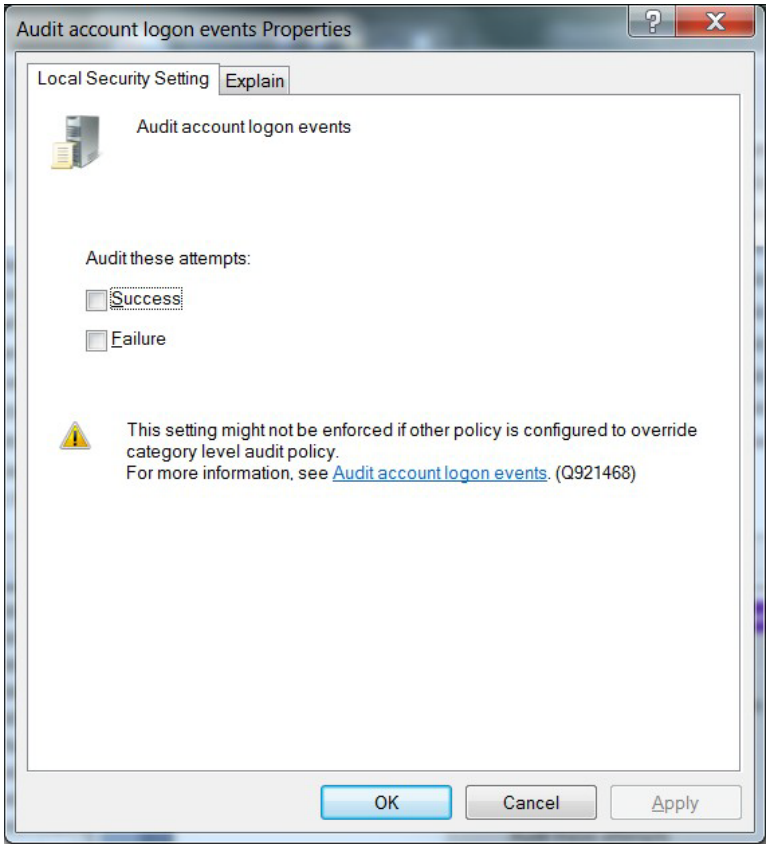
1. **[スタート (Start)] > [コントロール パネル (Control Panel)] > [管理ツール (Administrative Tools)] > [ローカル セキュリティ ポリシー (Local Security Policy)]** を選択します。



2. [**セキュリティの設定 (Security Settings)**] ツリーで [**ローカル ポリシー (Local Policy)**] をダブルクリックして展開します。
3. ツリーから [**監査ポリシー (Audit Policy)**] を選択します。そのシステムの監査情報が表示されます。



4. いずれかの領域に対する監査を有効にするには、その監査のタイプをダブルクリックします。次のようなダイアログボックスが表示され、そのタイプのイベントが [**成功 (Success)**] の場合、または [**失敗 (Failure)**] の場合 (あるいはその両方) に監査を実行するように指定できます。



注: レジストリ、プリンター、ファイル、フォルダーなどのオブジェクトを監査する場合は、オブジェクトアクセスオプションを選択してください。これを行わずに、これらのオブジェクトに対する監査を有効にしようとすると、ローカル監査ポリシー (ドメイン環境の場合はドメイン監査ポリシー) の調整が必要であることを示すエラーが表示されます。

監査を有効に設定したら、システムを確認して、各カテゴリで監査されるイベントのタイプを微調整します。

ドメイン内での監査ポリシーの設定

ドメインコントローラーに対して監査ポリシーを設定するには、次の手順を実行します。

1. **[スタート] > [プログラム] > [管理ツール] > [Active Directory ユーザーとコンピューター]** を選択します。
2. コンソールツリーで目的のドメインに移動します。ドメインを展開します。
3. ドメインの下に [**Computers**] オブジェクトと [**Domain Controllers**] オブジェクトが表示されます。お使いのシステムに応じてオブジェクトを選択し、[**Domain Controllers**] を右クリックします。ドメインコントローラーのプロパティシートが表示されます。
4. [**グループ ポリシー**] タブを選択します。監査ポリシーを適用するグループポリシーを選択し、[**編集**] をクリックします。
5. ツリー内を移動して、**[Default Domain Controllers Policy] > [コンピューターの構成] >**

[Windows の設定] > [セキュリティの設定] > [ローカル ポリシー] > [監査ポリシー] を選択します。

6. [**監査ポリシー**] を選択すると、右側のペインに監査イベントのリストが表示されます。特定のイベントグループを監査する場合は、そのグループをダブルクリックします。ダイアログボックスが表示され、そのイベントグループが [**成功**] の場合、[**失敗**] の場合、またはその両方の場合の監査を有効に設定できます。

イベントグループに対する監査を有効にしたら、監査対象のイベントを正確に微調整します。

ドメインに対する監査ポリシーの設定

ドメインの下のすべてのコンピューターに対して監査を設定するには、次の手順を実行します。

1. **[スタート] > [管理ツール] > [ドメイン セキュリティ ポリシー]** をクリックします。
2. [**既定のドメイン セキュリティの設定**] を開きます。
3. まだ開いていない場合は、[**セキュリティの設定**] を展開します。
4. [**ローカル ポリシー**] を展開し、[**監査ポリシー**] をダブルクリックします。右側のペインに監査イベントのリストが表示されます。
5. 特定のイベントグループを監査する場合は、そのグループをダブルクリックします。ダイアログボックスが表示され、そのイベントグループが [**成功**] の場合、[**失敗**] の場合、またはその両方の場合の監査を有効に設定できます。

標準ユーザーアカウントの設定

コネクターではWindowsホストからセキュリティイベントを収集するのに、ドメイン管理者の特権は必要ありません。システムイベントやカスタムアプリケーションイベントの収集 (転送されたイベントの収集を含む) には、イベントログリーダーの特権が必要です。

標準ユーザーアカウントを使用してターゲットホストのみからセキュリティイベントを収集するようにSmartConnector for Microsoft Windows Event Log − Nativeを設定するには、以下のセクションの手順に従います。

これらの手順では、**arcsight**などのユーザーアカウントを1つだけ作成して、特権の設定と割り当てを行う方法について説明します。また、ユーザーのグループを作成し、この設定で示した手順と同じ手順を用いて、個別ユーザーではなくユーザーグループに対して最小限のすべての特権を割り当てることもできます。

注: 標準ユーザーに適切な特権を割り当てている場合でも、環境内の別のポリシーにより、そのユーザーアカウントではセキュリティイベントログにアクセスできない可能性があります。この問題を識別するには、**[設定] > [コントロール パネル] > [管理ツール] > [ローカル セキュリティ ポリシー] > [セキュリティの設定] > [ローカル ポリシー] > [セキュリティ オプション]** を確認します。この場合に調査が必要なセキュリティポリシーは数多く存在しますが、最初に確認すべきポリシーは、[**ネットワーク アクセス: ローカル アカウントの共有とセキュリティ モデル**] です。これが [**クラシック - ローカル ユーザーがローカル ユーザーとして認証する**] に設定されていることを確認します。

Windows Serverドメインコントローラーの標準ドメインユーザーアカウント

Windows Serverドメインコントローラーで、次の手順を実行します。

1. **[設定] > [コントロール パネル] > [管理ツール] > [Active Directory ユーザーとコンピューター] > [<対象のドメイン>] > [Users]** にアクセスします。
2. **ドメインユーザー** (arcsightなど) を新規に作成します。
3. **[設定] > [コントロール パネル] > [管理ツール] > [Active Directory ユーザーとコンピューター] > [<対象のドメイン>] > [Builtin]** にアクセスします。
4. セキュリティプリンシパル**Event Log Readers**のプロパティを開きます。
5. [**メンバー**] タブで、このセキュリティプリンシパルに新規ドメインユーザーarcsightを追加します。
6. このグループポリシーが有効になるまでに、しばらく時間がかかる場合があります。ポリシーをただちに有効にするには、Windows Serverドメインコントローラーおよびドメインメンバーのコマンドプロンプトで、次のコマンドを実行します。

   ```
   GPUpdate /Force
   ```

   このコマンドを実行すると、このポリシーだけでなく、すべてのグループポリシーに対する変更内容が反映されます。

ドメインメンバーの標準ドメインユーザーアカウント

Windows Serverドメインコントローラーで、次の手順を実行します。

1. **[設定] > [コントロール パネル] > [管理ツール] > [Active Directory ユーザーとコンピューター] > [<対象のドメイン>] > [Users]** にアクセスします。
2. ドメインユーザー (`arcsight`など) を新規に作成します。
3. **[設定] > [コントロール パネル] > [管理ツール] > [グループ ポリシーの管理] > [Default Domain Policy] > [コンピューターの構成] > [ポリシー] > [Windows の設定] > [セキュリティの設定] > [ローカル ポリシー] > [ユーザー権利の割り当て]** にアクセスします。
4. [**監査とセキュリティ ログの管理**] ポリシーを開きます。
5. [**これらのポリシーの設定を定義する**] を有効にし、このポリシーに新規ドメインユーザーarcsightを追加します。
6. このグループポリシーが有効になるまでに、しばらく時間がかかる場合があります。ポリシーをただちに有効にするには、Windows Serverドメインコントローラーおよびドメインメンバーのコマンドプロンプトで、次のコマンドを実行します。

   ```
   GPUpdate /Force
   ```

注: このコマンドを実行すると、このポリシーだけでなく、すべてのグループポリシーに対する変更内容が反映されます。

Windowsワークグループホストの標準ローカルユーザーアカウント

Windowsワークグループホストで、次の手順を実行します。

1. **[設定] > [コントロール パネル] > [管理ツール] > [コンピューターの管理] > [システム ツール] > [ローカル ユーザーとグループ] > [ユーザー]** にアクセスします。
2. **ローカルユーザー** (`arcsight`など) を新規に作成します。
3. **[設定] > [コントロール パネル] > [管理ツール] > [コンピューターの管理] > [システム ツール] > [ローカル ユーザーとグループ] > [グループ]** にアクセスします。
4. **Event Log Readers**グループを開き、このグループに新規ローカルユーザーarcsightを追加します。
5. **[設定] > [コントロール パネル] > [管理ツール] > [ローカル セキュリティ ポリシー] > [セキュリティの設定] > [ローカル ポリシー] > [セキュリティ オプション]** にアクセスします。
6. [**ネットワーク アクセス: ローカル アカウントの共有とセキュリティ モデル**] ポリシーを開きます。
7. このポリシーを [**クラシック - ローカル ユーザーがローカル ユーザーとして認証する**] に設定します。

SSL使用時のセキュリティ証明書の追加

接続プロトコルとしてSSLを使用する場合は、Windowsドメインコントローラーサービス用とActive Directoryサーバー用の両方のセキュリティ証明書が必要です。ドメインコントローラーに有効な証明書をインストールすると、LDAPサービスは、LDAPトラフィックとグローバルカタログトラフィックの両方で、SSL接続をリッスンして自動的に受け入れることができます。

証明書は、コネクターのインストール中にコネクターの証明書ストアにインポートされます。手順については、インストール手順の**ステップ3**を参照してください。

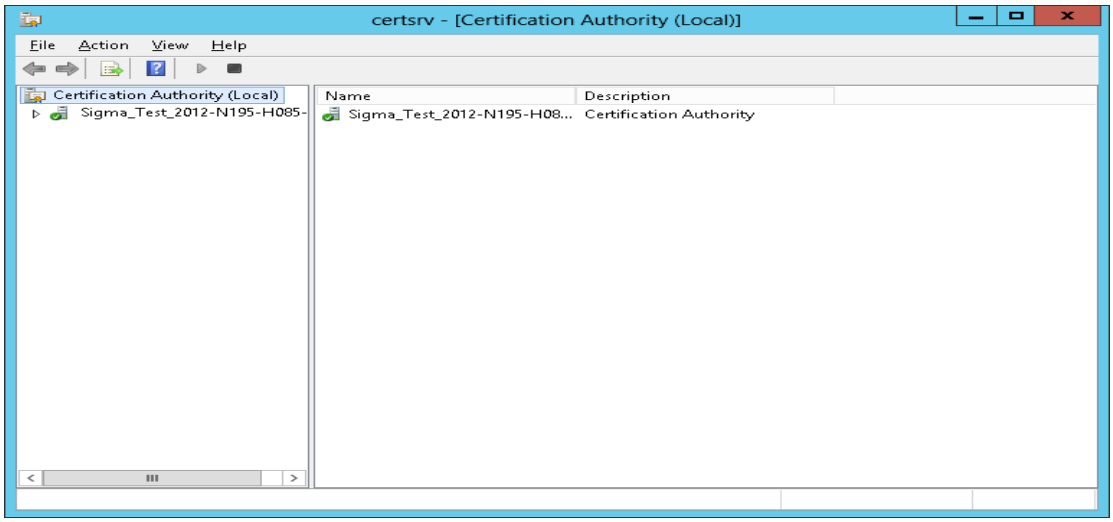
ここでは、Windows 2012の場合の手順を示します。手順は、Windowsバージョンによって異なることがあります。他のWindowsバージョンの詳細な手順については、Microsoftのドキュメントを参照してください。

例: Windows Server 2012

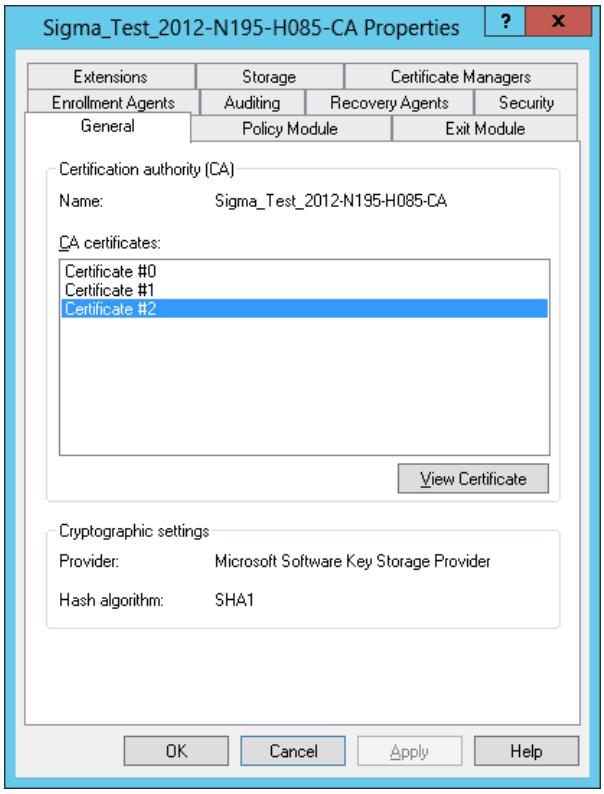
以下の記述はオペレーティングシステムとしてWindows Server 2012を想定しています。

証明書をエクスポートするには、次の手順を実行します。

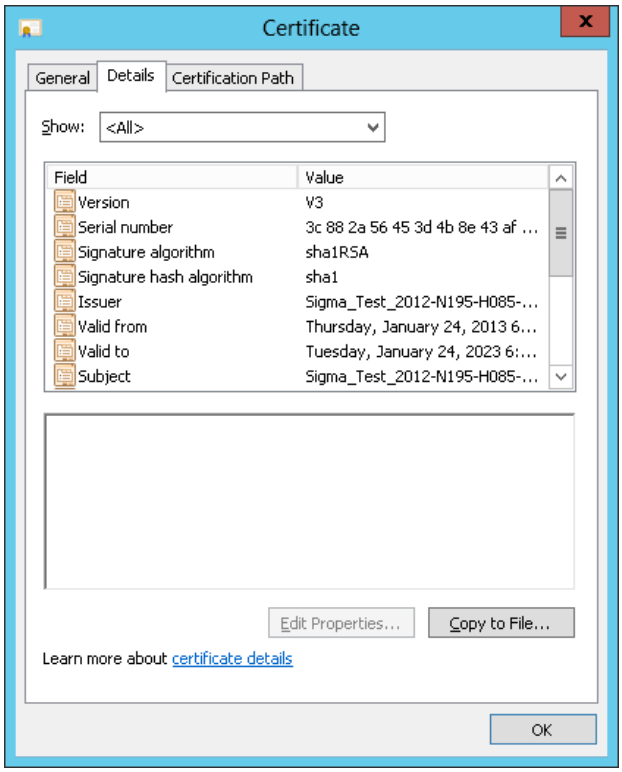
1. Windowsの [**スタート**] メニューから、[**管理ツール**] を選択します。
2. [**証明機関**] を選択してダブルクリックします。1つ以上のドメイン証明機関サーバーが表示されます。



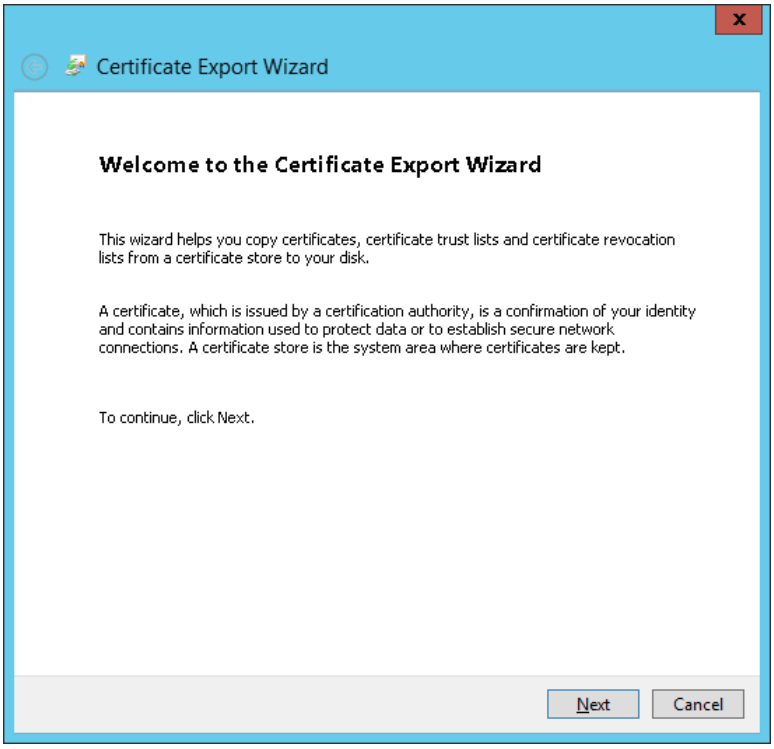
3. Active Directoryサーバーが属しているドメインのドメイン証明機関サーバーを選択して右クリックし、[**プロパティ (Properties)**] を選択して [**プロパティ (Properties)**] ウィンドウを開きます。



4. [**証明書の表示 (View Certificate)**] をクリックします。
5. [**詳細 (Details)**] タブをクリックして、[**ファイルにコピー... (Copy to File...)**] をクリックします。



6. [**証明書のエクスポート ウィザード (Certificate Export Wizard)**] の手順に沿ってエクスポートを完了します。



転送されたイベントの収集

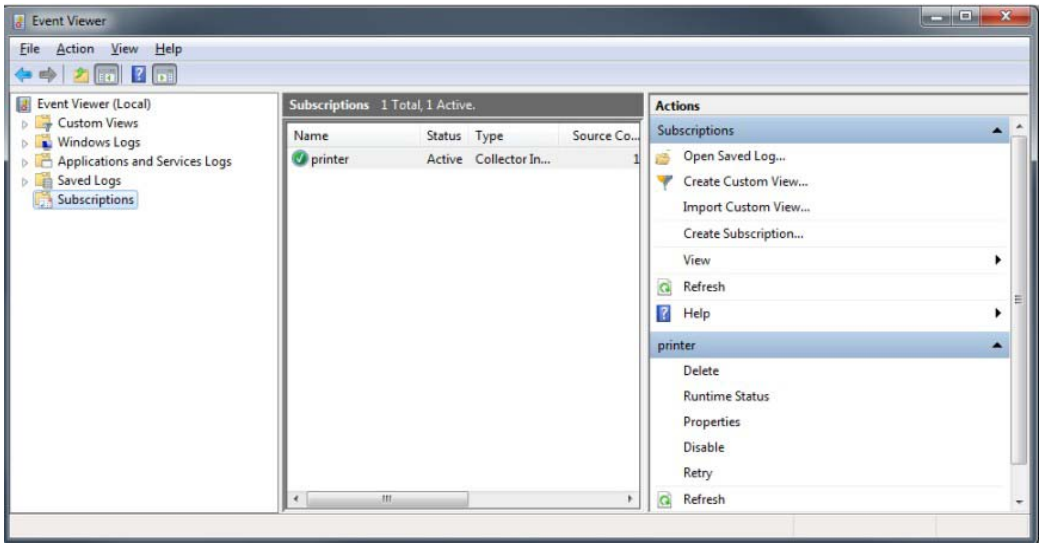
コネクターには、Windowsイベントコレクターホストに転送されたイベントを読み取る機能が用意されています。Windowsイベント収集は、Windowsホストで複数のソースからイベントを収集するためのMicrosoftの機能です。複数のソースからイベントを収集するため、転送されたイベントの収集は通常のイベント収集とはやや異なります。

Microsoft Windowsイベントコレクター (WEC) では、任意の数のリモートコンピューター (イベントソース) から転送されるイベントをローカルコンピューター (イベントコレクター) で受信して保管するようにサブスクライブできます。この機能を使用する際には、前もってMicrosoft Windowsのドキュメントを参照し、Windowsイベントコレクターの仕組みについて理解しておいてください。

注: Windowsイベント収集 (WEC) を設定する場合、Microsoftのデフォルト設定では、イベントのテキスト形式の説明であるRenderingInfoセクションがすべての転送されたイベントに追加されます。この余分なセクションが追加されると、WECマシンのリソース使用量とコネクターのパフォーマンスに悪影響をもたらします。そのため、HPEでは、RenderingInfoセクションを無効にすることを推奨しています。
これを行うには、Windowsコマンドコンソールから以下のコマンドを実行します。

```
wecutil ss <サブスクリプション名> /cf:events
```

ここで、サブスクリプション名は、イベント転送用に作成したWEC設定です。これは、**[イベント ビューアー (Event Viewer)] > [サブスクリプション (Subscriptions)]** フォルダーで確認できます (下記を参照)。



Windowsイベント転送用のイベントコレクター

コネクターが通常アクセスできるコレクターマシン上の任意のログタイプにソースホストからイベントを転送することができます。

注: セキュリティイベントはコレクターマシン上のセキュリティイベントログには転送できませんが、他のログタイプに転送することはできます。

ソースホストのWindows OSバージョン

転送されたイベントを含むログを使用してコネクターを設定している場合、イベントソースホストのWindows OSバージョンは正規化されたイベントに自動的に取り込まれません。この値を取り込むには、Windows OSバージョンをソースホストファイルとして提供するか、Active Directoryを設定する必要があります。Windows OSバージョンがソースホストファイルとActive Directoryの両方で利用できる場合は、Active Directoryの値が優先されます。

Active DirectoryからOSバージョンを取得する場合

コネクターの設定時にこの方法を選択すると、コネクターは設定したActive Directoryからホスト情報 (ホスト名とバージョン) を取得して、イベントソースホストのWindowsバージョン情報を識別します。新しく検出されたホストはルックアップに自動的に追加されます。コネクターを設定し直す必要はありません。

Active Directory情報の確認は、コネクターの起動時および24時間 (86400000ミリ秒) ごとに行われます。この時間設定を変更するには、`$ARCSIGHT_HOME/current/agent`にある`agent.properties`ファイルで、**hostbrowsingthreadsleeptime**パラメーターをホスト参照クエリを行う間隔 (ミリ秒) に設定します。この値は0より大きい値に設定します。この値を0に設定すると、定期的なホスト参照が実行されません。

コネクターがActive Directoryを参照してソースホストのWindowsバージョン情報を取得するには、コネクターがこのActive Directoryと同じフォレスト内に存在している必要があります。

ファイルからOSバージョンを取得する場合

コネクターの設定時にこの方法を選択する場合は、ホスト名とWindows OSバージョンを含むソースホストファイルを.csv形式で作成し、このファイルをコネクターのインストール/設定時にアップロードします (ステップ9のWEFソースホストファイル名)。

注: インストール時にホストテーブルとの間でインポートまたはエクスポートするホストファイルと、[**WEF Source Hosts File Name**] フィールドで指定するソースホストファイルは別のものです。ソースホストファイルには、デバイスバージョンフィールドにバージョンを読み込むためのホスト名とバージョン情報のみが含まれます。

コネクターはイベント内のコンピューター名を使用してバージョン情報を検出するため、ソースホストファイルを作成する際には、Active Directoryに登録されているFQDNを指定する必要があります。以下にソースホストファイルの例を示します。

```
hostsa.domaina.com,Windows 7
hostsb.domainb.com,Windows 8
hostsc.domainb.com,Windows Server 2012
Hostsd.domaind.com,Windows Server 2016
```

ソースホストファイルで使用できる有効なバージョン説明 (大文字と小文字を区別) は、次のとおりです。

```
Windows Vista
Windows Server 2008
Windows Server 2008 R2
Windows Server 2012
Windows Server 2012 R2
Windows Server 2016
Windows 7
Windows 8
Windows 10
```

注: OSバージョン情報は省略できます。OSバージョン情報を省略しても、たいていの場合、イベントは解析できます。

設定後、初めてコネクターを実行したときにソースホストファイルからOSバージョンがロードされます。その次からはソースホストファイルのタイムスタンプが最後に処理されたファイルからロードされたものと異なる場合に、コネクターの起動時に再ロードされます。

デバイスバージョンは正規化されたイベントには読み込まれません。

SmartConnectorのインストール

SmartConnectorをインストールする前に、コネクターが通信を行うArcSight製品が正しくインストール済みであることを確認します (ArcSight ESMやArcSight Loggerなど)。この構成ガイドでは、インストール先として**ArcSight Manager** (**encrypted**) を使用したインストールプロセスについて説明します。

コネクターが通信を行うArcSight製品の詳しい製品情報については、SmartConnectorを新規にインストールする前に、ArcSight製品の『管理者ガイド』と『インストールおよび構成ガイド』を確認してください。

ArcSight Management Center (ArcMC) にコネクターを追加する場合は、『ArcSight Management Center管理者ガイド』の手順を参照し、「グローバルパラメーターの設定 (オプション)」または「コネクターの選択とパラメーター情報の追加」からインストール手順を始めてください。

必要な項目

このSmartConnectorをインストールする際には、以下が必要です。

- SmartConnectorをインストールするマシンへのローカルアクセス。
- そのマシンの管理者パスワード。

インストールに関する注意点

- このSmartConnectorは、64ビット版Windowsプラットフォームにインストールする必要があります。「イベント収集でサポートされるオペレーティングシステム」を参照してください。
- Microsoft Windows Event Log - UnifiedコネクターからMicrosoft Windows Event Log -- Nativeコネクターにアップグレードすることはできません。
- Windows Event Log – Unifiedコネクター用のパーサーオーバーライドは、Windows Event Log – Nativeコネクター用に変更する必要があります。
- 転送されたイベントの収集を使用する場合は、Active Directoryからか、もしくはcsv形式のソースホストファイルから、コンピューターのフルネームとソースホストのOSバージョンを入手できるようにする必要があります。

OSレベルでのFIPSの有効化

1. Windowsの [**スタート**] メニューから、[**ファイル名を指定して実行**] を選択します。
2. 「`gpedit.msc`」と入力します。
3. グループポリシーエディターで、**[コンピューターの構成] > [Windows の設定] > [セキュリティの設定] > [ローカルポリシー] > [セキュリティ オプション]** に移動します。
4. 右側のペインで、[システム暗号化: 暗号化、ハッシュ、署名のための FIPS 準拠アルゴリズムを使う] 設定をクリックします。
5. [**有効**] に設定して [**OK**] をクリックします。
6. コンピューターを再起動します。

コアソフトウェアのインストール

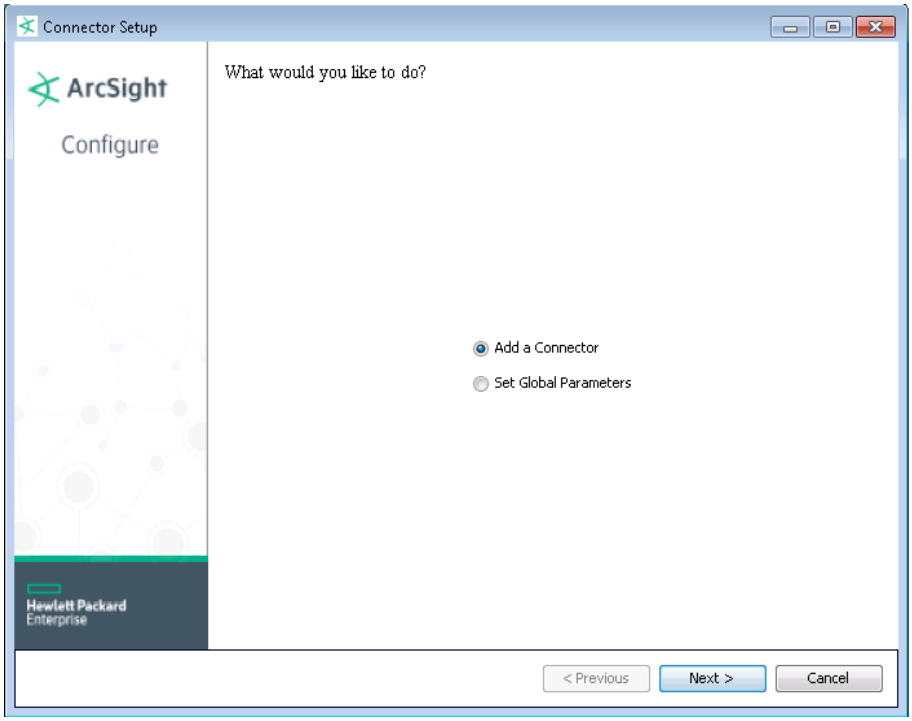
1. HPEソフトウェアサポートサイトから、お使いのオペレーティングシステム用のSmartConnectorの64ビット版実行ファイルをダウンロードします。
2. 実行ファイルを実行してSmartConnectorのインストーラーを起動します。

   インストールウィザードに従って、以下のフォルダー選択タスクを実行します。

   - Introduction
   - Choose Install Folder
   - Choose Shortcut Folder

- Pre-Installation Summary
- Installing...

3. SmartConnectorコアコンポーネントソフトウェアのインストールが終了すると、以下のウィンドウが表示されます。



グローバルパラメーターの設定 (オプション)

以下の表に示す操作を実行する場合は、コネクターを追加する前に行ってください。コアソフトウェアをインストールすると、以下のパラメーターを設定できます。

グローバルパラメーター	設定
Set FIPS mode	[**Enable**] に設定すると、FIPS準拠モードが有効になります。FIPS Suite Bモードを有効にするには、『SmartConnectorユーザーガイド』の「コネクターのパラメーターの変更」の手順を参照してください。初期状態では、この値は [**Disable**] に設定されています。
Set Remote Management	[**Enable**] に設定すると、ArcSight Management Centerからのリモート管理が有効になります。リモート管理デバイスがクエリを実行するときは、リモート管理を有効にするためにここで指定した値とポート番号が使用されます。初期状態では、この値は [**Disable**] に設定されています。

グローバルパラメーター	設定
Remote management listener port	リモート管理デバイスは、このフィールドで指定したポートをリッスンします。デフォルトのポート番号は9001です。
Preferred IP Version	ローカルホスト (コネクターがインストールされたマシン) で、**IPv4**と**IPv6**の両方のIPアドレスが使用可能な場合に、優先するバージョンを選択できます。両方が使用可能でない場合は、一方のみが表示されます。両方の値が表示される場合、初期設定は**IPv4**になっています。

選択が終わったら、[**Next**] をクリックします。サマリー画面が表示されます。選択内容のサマリーを確認し、[**Next**] をクリックします。[**Continue**] をクリックすると、[Add a Connector] ウィンドウに戻ります。「コネクターの追加」のインストール手順を続けて実行します。

SSL接続の使用 (オプション)

コネクターの接続にSSLを使用する場合は、以下の手順に従います。使用しない場合は、**ステップ4**に進みます。

コネクターの証明書ストアに証明書をインポートするには、[**Cancel**] をクリックしてウィザードを終了します。

1. `$ARCSIGHT_HOME\current\bin`で、**keytool**アプリケーションを実行し、2つの証明書をインポートします (このガイドの「SSL使用時のセキュリティ証明書の追加」を参照)。

   ```
   arcsight agent keytoolgui
   ```

   グラフィカルインターフェイスに、キーストアを開くように求めるメッセージが表示されます。

2. `jre/lib/security/cacerts`を選択してから、[**import cert**] を選択して証明書をインポートします。正しい証明書がインポートされたことを確認します。
3. [**Trust this certificate?**] と表示されたら、[**Yes**] をクリックします。もう1つの証明書についても、この手順を繰り返します。
4. キーストアを保存します。
5. `$ARCSIGHT_HOME\current\bin`から次のコマンドを入力して、インポートされた証明書を確認します。

   ```
   arcsight agent keytool -list -store clientcerts
   ```

   新しい証明書が表示されます。
6. `$ARCSIGHT_ HOME\current\bin`から次のコマンドを入力して、設定ウィザードに戻ります。

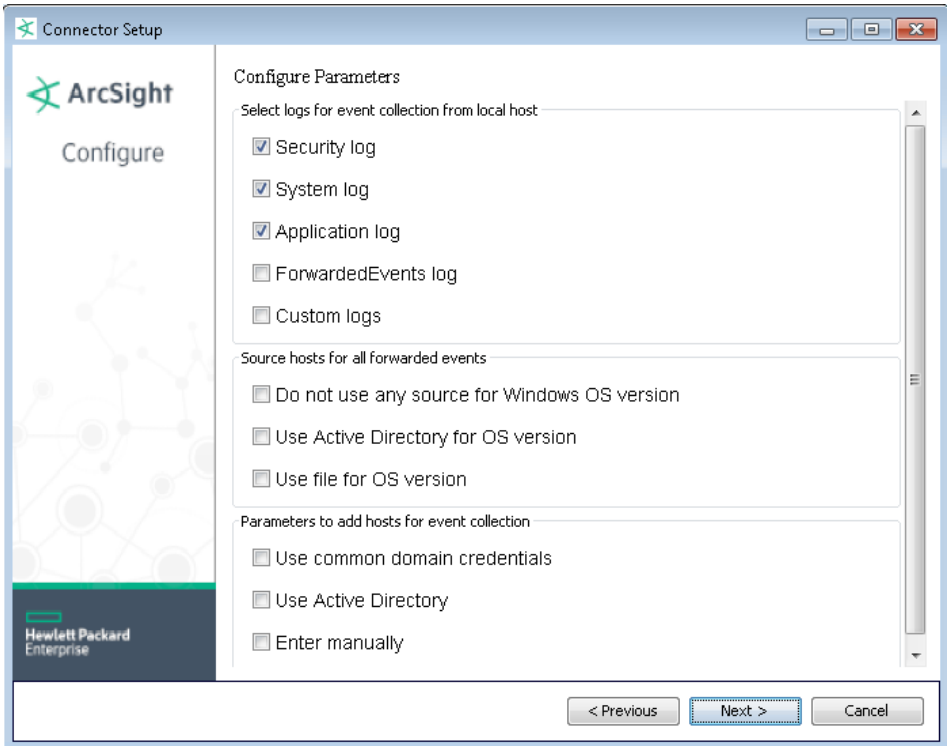
   ```
   runagentsetup
   ```

コネクターの追加

1. [**Add a Connector**] を選択し、[**Next**] をクリックします。
2. 設定ウィザードに、設定可能なSmartConnectorのリストが表示されます。[**Microsoft Windows Event Log – Native**] を選択し、[**Next**] をクリックします。

コネクターの設定

[**Microsoft Windows Event Log – Native**] を選択すると、以下の設定ウィンドウが表示されます。



ローカルホストからイベント収集を行うログの選択

この部分で選択する内容は、ローカルホストに適用されます。ローカルホストのロケールとエンコーディングは、コネクターによって自動的に検出されて設定されるため、ローカルホストでこれらの値を設定する必要はありません。ただし、追加のホストからイベントを収集する場合は、このセクションで後述するように、テーブルパラメーター画面でホストやログを追加して選択できます。

ローカルホストで収集するイベントを生成するログを選択します。デフォルトで選択されている項目は、[**Security log**]、[**System log**]、[**Application log**] です。サポートされるアプリケーションイベントとシステムイベントの一覧については、「ログパーサーのサポート」を参照してください。

- [**ForwardedEvents log**] を選択する場合は、Windowsイベント転送で使用するソースホストファイルの名前を指定する必要があります。「WEFソースホストファイル名」を参照してください。
- [**Custom logs**] を選択する場合は、テーブルパラメーター画面でカスタムログファイル名を指定する必要があります。「複数のホストパラメーターの設定」を参照してください。

すべての転送されたイベントのソースホスト

コネクターを使用して転送された (WEF) ログから収集を行う場合、コネクターはイベントの収集元となるホストのWindows OSバージョンを把握する必要があります。このためには、この情報を含む.csvファイルを用意するか、コネクターがActive Directoryにアクセスしてホストの OSバージョン情報を確認できるようにします。いずれか適切な方法を選択します。

[**Use file for OS version**] を選択した場合、ソースホストファイル名を指定するウィンドウが表示されます。これは、初期設定ウィンドウの [**Select Logs**] セクションで [**ForwardedEvents log**] を選択したときに表示されるのと同じウィンドウです。「WEFソースホストファイル名」を参照してください。

[**Use Active Directory for OS version**] を選択した場合、ドメイン資格情報とActive Directoryパラメーター情報を入力するウィンドウが表示されます。「ドメイン証明書」と「Active Directoryのパラメーター」を参照してください。

[**Do not use any source for Windows OS version**] を選択した場合、Active Directoryクエリや、イベント転送に関わるすべてのホストとそのWindows OSバージョンをリストするためのCSVファイルは必要ありません。転送ホストからのイベントヘッダーに、Windows OSバージョンは表示されません。

イベント収集用のホストを追加するためのパラメーター

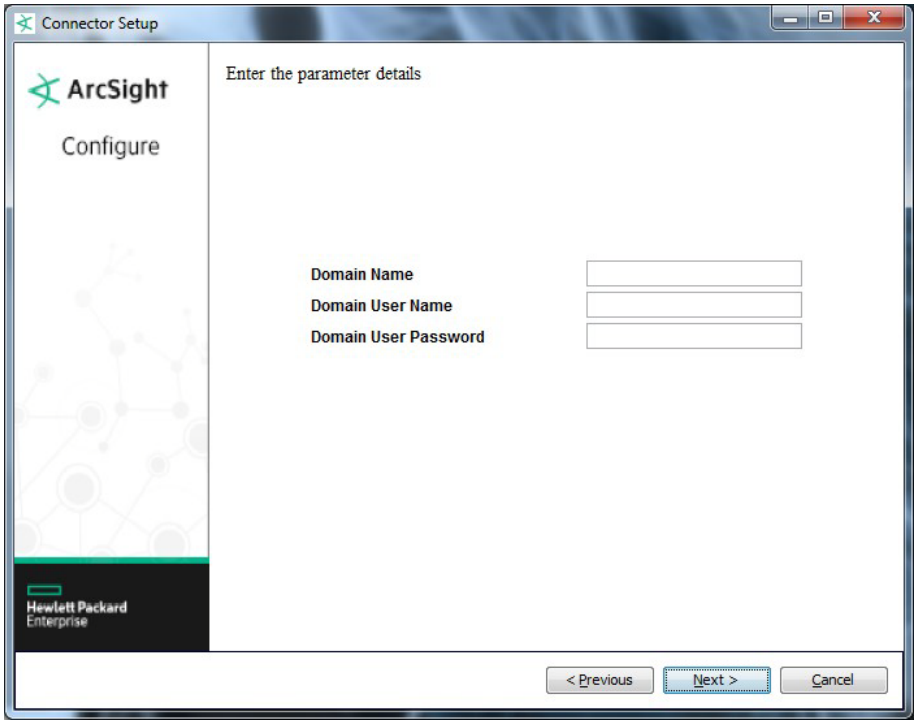
イベント収集用のホストを追加するには、共通のドメイン資格情報を使用するか、Active Directoryを使用するか、またはホスト情報を手動で入力します。

[**Use Active Directory**] をチェックし、Active Directory設定ウィンドウで値を指定している場合は、デフォルトのドメイン名、ユーザー、パスワードが使用されます。それ以外の場合は、ユーザー名、パスワード、ドメイン名を指定します。転送されたイベントの収集を使用する場合は、イベントコレクターホストのみを指定します。

[**Use common domain credentials**] を選択した場合、ドメイン資格情報を入力するウィンドウが表示されます。「ドメイン証明書」を参照してください。

ドメイン資格情報

パラメーター情報を入力して、[**Next**] をクリックします。

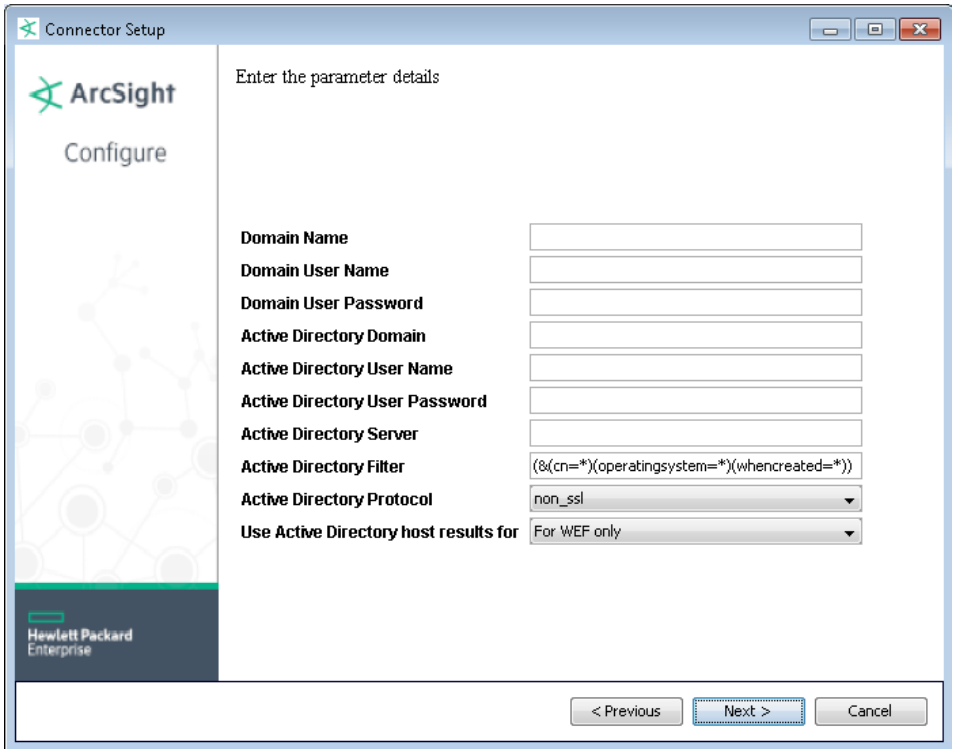


注: ローカルイベントの収集を行う場合、[Domain User Name] と [Domain User Password] を入力する必要はありません。

パラメーター	説明
Domain Name	ホストが属しているドメインの名前を入力します。ワークグループホストとスタンドアロンホストは、テーブルパラメーター入力ウィンドウで手動で追加できます。
Domain User Name	ターゲットホストからWindowsイベントを収集するための適切な特権を持つユーザーアカウントの名前を入力します。ADサーバーがドメインサーバー上に存在し、このドメインユーザー名とパスワードを使用してアクセスできることを想定しています。
Domain User Password	[**Domain User Name**] フィールドで指定したユーザーのパスワードを入力します。

Active Directoryのパラメーター

[**Use Active Directory**] を選択した場合、ドメイン資格情報とActive Directoryパラメーターを指定するための以下のウィンドウが表示されます。これは、初期設定ウィンドウの [**Source hosts for all forwarded events**] (「すべての転送されたイベントのソースホスト」) セクションで [**Use Active Directory for OS version**] を選択したときに表示されるのと同じウィンドウです。



[**Domain Name**]、[**Domain User Name**]、[**Domain User Password**] の説明については、「ドメイン資格情報」を参照してください。

パラメーター情報を入力して、[**Next**] をクリックします。

注:

- ローカルイベントの収集を行う場合、[Domain User Name] と [Domain User Password] を入力する必要はありません。
- ホストのドメインパラメーターがActive Directoryと同じである場合、両方に入力する必要はありません。これらの情報は、Active Directoryドメインと資格情報から取得されます。
- GUID変換が有効になっている場合は、Active Directoryドメインと資格情報が使用されます。すべての修飾子 (.comなど) を含む完全なドメイン名を指定する必要があります。

パラメーター	説明
Active Directory Domain	ホストが属しているActive Directoryドメインの名前を入力します。
Active Directory User Name	ターゲットホストからWindowsイベントを収集するための適切な特権を持つユーザーアカウントの名前を入力します。ADサーバーがドメインサーバー上に存在し、このドメインユーザー名とパスワードを使用してアクセスできることを想定しています。
Active Directory User Password	[**Active Directory User Name**] フィールドで指定したユーザーのパスワードを入力します。
Active Directory Server	ホスト参照機能でMicrosoft Active Directoryに対する認証に必要となるActive Directoryホスト名またはIPアドレスを入力します。

パラメーター	説明
Active Directory Filter	自動ホスト参照で、ホストを名前、オペレーティングシステム、作成日でフィルター処理するのに必要なActive Directoryフィルターを入力します。 クエリには、共通名 (cn)、オペレーティングシステム (operatingsystem)、'YYMMDDHHmmSS' 形式の作成日時 (whencreated) の属性を含めることができます。ここで、YY=年の下2桁、MM=月、DD=日、HH=時、mm=分、SS=秒 (24時間形式) です。 また、クエリ内でワイルドカード文字 (*) を使用して、属性を異なる複数の値と照合することもできます。 **Active Directory Filterの例** 特定日時以降のホストを作成するには、フィルターを次のように設定します: (&(cn=*)(operatingsystem=*)(whencreated>=YYMMDDHHmmSSZ)) 特定日時以降かつ特定日時以前のホストを作成するには、フィルターを次のように設定します: (&(cn=*)(operatingsystem=*)(whencreated>=YYMMDDHHmmSS)(whencreated<=YYMMDDHHmmSS))
Active Directory Protocol	使用するプロトコルが [**non_ssl**] (デフォルト値) かSSLかを選択します。SSLプロトコルの場合は、コネクターを起動する前に、Active Directoryのセキュリティ証明書をコネクターにインポートする必要があります。
Use Active Directory host results for	For WEF Only: 初期設定ウィンドウで [**Use Active Directory for OS Version**] を選択した場合、WEFソースホストのWindows OSバージョンを特定するのに、Active Directoryから取得したホストのリストが使用されます。[**For WEF Only**] を選択した場合、クエリの結果がテーブルパラメーター入力ウィンドウのホストのテーブルに読み込まれることはありません。 初期インストールでは、ローカルホストのみが存在して保持されているため、**[Merge Hosts] と [Replace Hosts]** の動作は同じになります。初期設定画面の [**Parameters to add hosts for event collection**] で [**Use Active Directory**] を選択した場合、またはホストを追加するためのパラメーターを変更する場合は、以下が適用されます。 [**Merge Hosts**] が選択されている場合、収集用のホストを取得するのにActive Directoryが使用されます (また、WECサーバーが存在し、初期設定画面で [**Use file for OS**] を選択していない場合は、Windowsイベント転送にもActive Directoryを使用できます)。元のホストは置き換えられません。その他の設定済みのホストもすべて保持されます。ホストはActive Directoryから取得したリストから追加され、デフォルトでセキュリティイベントが選択されます。重複が見つかった場合、既存のホストエントリは上書きされません。 [**Replace Hosts**] が選択されている場合、収集用のホストを取得するのにActive Directoryが使用されます (また、WECサーバーが存在し、初期設定画面で [Use file for OS] を選択していない場合は、Windowsイベント転送にもActive Directoryを使用できます)。ローカルホストは置き換えられませんが、その他の設定済みのホストはすべて、Active Directoryから取得したホストに置き換えられ、デフォルトでセキュリティイベントが選択されます。

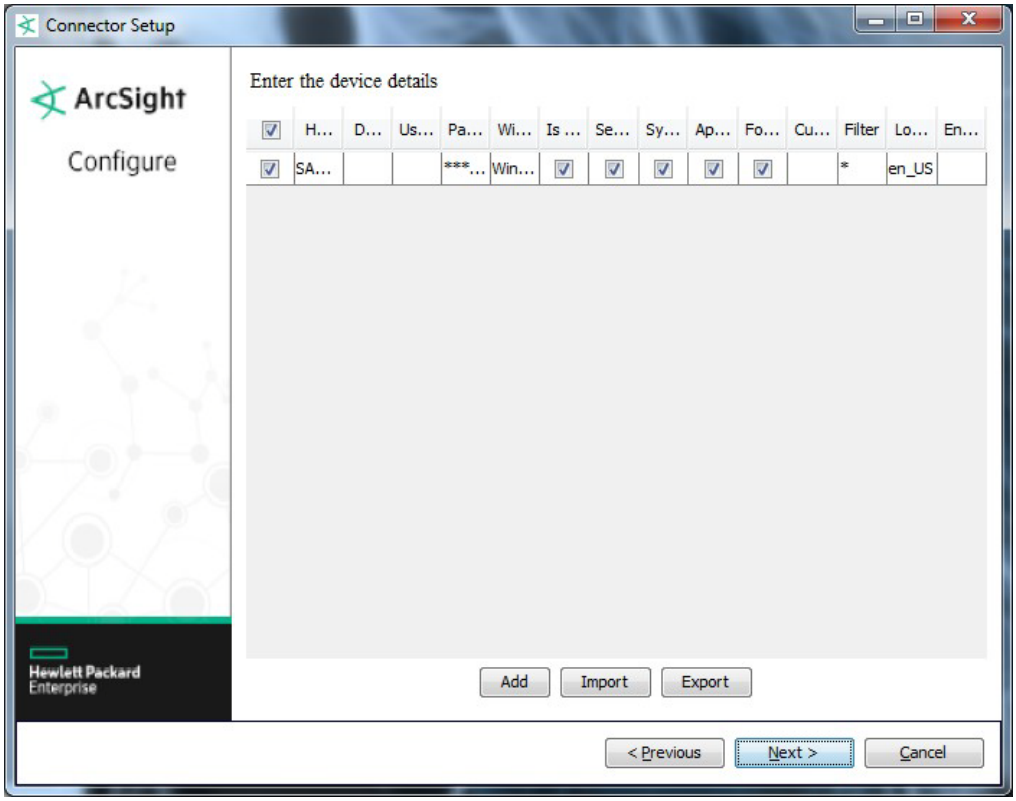
複数のホストパラメーターの設定

初期設定ウィンドウの [**Select logs for event collection**] セクションで [**Custom logs**] を選択した場合、またはホストの追加を行う場合は、テーブルパラメーター入力ウィンドウが表示されます (次のページの例を参照)。ローカルホストに対してフィルタリングを追加する場合は、[**Select logs for event collection**] セクションの [**Custom Logs**] をチェックして、フィルターパラメーターを入力するためにこのウィンドウが表示されるようにします。

ローカルホストに対して最初のパラメーター入力ウィンドウで選択した内容は、テーブルの最初の行に反映されています。[**Add**] をクリックし、ホストを手動で追加するか、[**Import**] をクリックし、.csvファイルを選択してホスト情報をインポートします。.csvファイルの最後のエントリにはキャリッジリターン (CR) を1つだけ配置します。このようにしないと、インポートは正しく実行されません。

追加ホストでは、ドメイン資格情報とWindowsバージョン情報はファイルまたはActive Directoryによって提供され、**セキュリティ**ログのみが選択された状態になります。別のオプションを選択して、追加ホストごとにカスタムログとフィルター情報を手動で提供することもできます。

追加したホストの中にイベント収集を行わないものがある場合、左端のカラムのチェックボックスを使用し、テーブル内の行を選択解除することができます。



以下の表に、各ホストのすべてのパラメーターと説明を示します。ローカルホストに対して最初のパラメーター入力ウィンドウで選択した内容は、テーブルの最初の行に反映されています。オプションを選択し、追加ホストごとにカスタムログとフィルター情報を手動で指定できます。

パラメーター	説明
Host Name	ターゲットWindowsホストのホスト名またはIPアドレス。
Domain Name	ホストが属しているドメインの名前。ターゲットホストでドメインユーザーアカウントを使用している場合や、Active Directoryを使用している場合は、[Domain Name] フィールドに入力します。OSバージョンを解決するため、これはIPアドレスではなく、名前である必要があります。

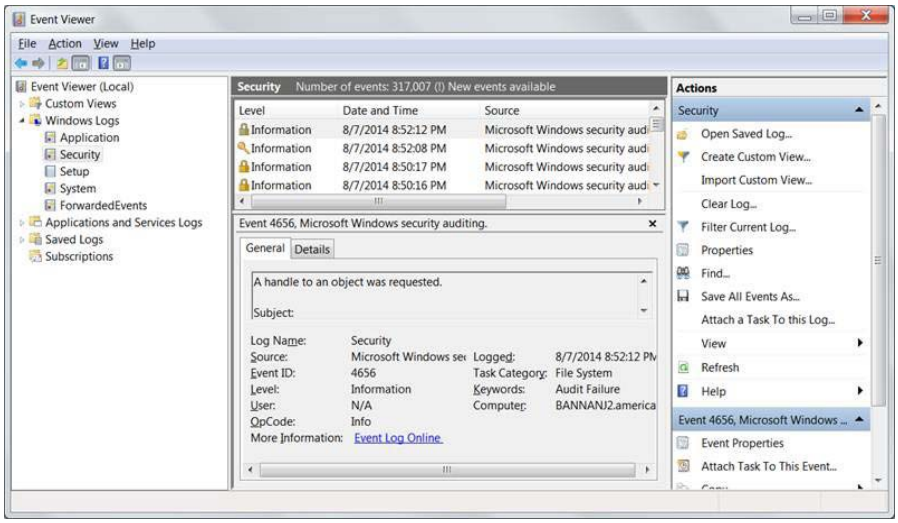
パラメーター	説明
User Name	ターゲットホストからWindowsイベントを収集するための適切な特権を持つユーザーアカウントの名前。これはユーザー名のみ (ドメインなし) になります。
Password	[**User Name**] で指定したユーザーのパスワード。
Windows Version	このホストで実行されているMicrosoftオペレーティングシステムのバージョンを選択します。
Is WEC	初期設定ページで [**Indicates that this is a WEC server**] を選択した場合、ローカルホストではこの選択項目にすでにチェックが入っています。
Security	このホストからセキュリティイベントを収集する場合に選択します。このログはすべてのホストで自動的に選択されます。
System	このホストからシステムイベントを収集する場合に選択します。
Application	このホストの**共通のアプリケーションイベントログ**からアプリケーションイベントを収集する場合に選択します。
ForwardedEvents	このホストの**ForwardedEvents**ログからイベントを収集する場合に選択します。
Custom Event Logs	カスタムアプリケーションログ名をコンマ区切りで指定します (例: “`Exchange Auditing, Directory Service`”)。Windowsイベントコレクターサーバーの場合は、**HardwareEvents**を使用します。詳細については、「カスタムログ名の指定」(33ページ) を参照してください。
Filter	これは特定のイベントを収集する場合に、Microsoftイベントビューアーから取得できるフィルターです。このフィールドにフィルターテキストをコピーできます。詳細については、「フィルターの設定」を参照してください。
Locale	お使いのロケールの値を入力するか、デフォルトの**en_US** (英語 (米国)) をそのまま使用します。ローカルホストのコネクターで正しいロケール値を自動判定する場合は、このフィールドを空白のままにします。 ロケール値は次のとおりです。 ■ フランス語 (カナダ): `fr_CA` ■ 日本語: `ja_JP` ■ 簡体字中国語: `zh_CN` ■ 繁体字中国語: `zh_TW` ■ 英語 (米国) (デフォルト): `en_US` その他の言語のローカリゼーションについては、「Nativeコネクターでのローカリゼーションサポートのカスタマイズ」(39ページ) を参照してください。
Encoding	ローカライズされたログイベントを送信するのに使用する言語のエンコーディング値を入力するか、デフォルトのen_US (英語 (米国)) をそのまま使用します。この値を自動判定することはできません。次の値から選択します。 ■ フランス語 (カナダ): `fr_CA` ■ 日本語: `Shift_JIS` ■ 簡体字中国語: `GB2312` ■ 繁体字中国語: `zh_TW` ■ 英語 (米国) (デフォルト): `UTF-8` その他の言語のローカリゼーションについては、「Nativeコネクターでのローカリゼーションサポートのカスタマイズ」(39ページ) を参照してください。

パラメーター情報の入力が終わったら、[**Next**] をクリックします。

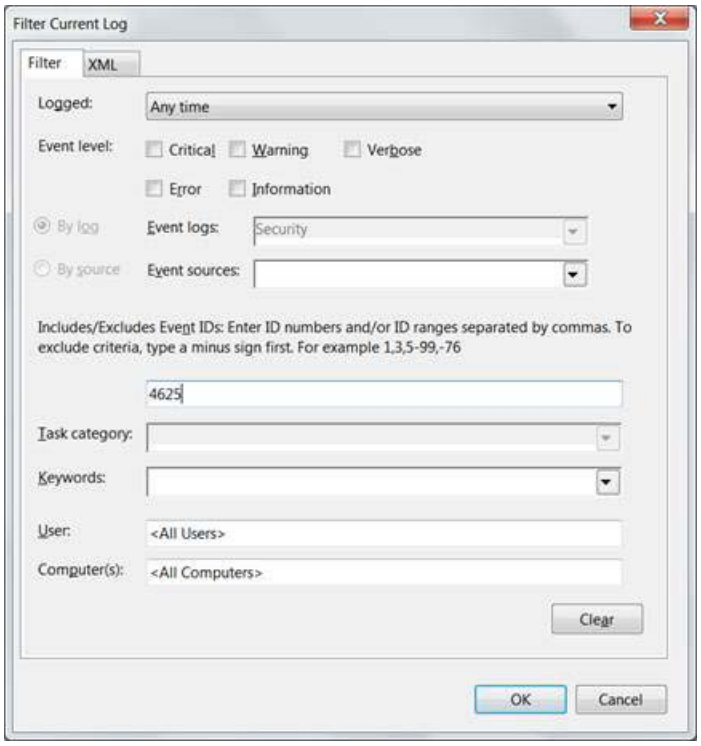
フィルターの設定

フィルターを設定するには、イベントビューアーを起動してから、フィルターの設定を使用するイベントログを選択します。

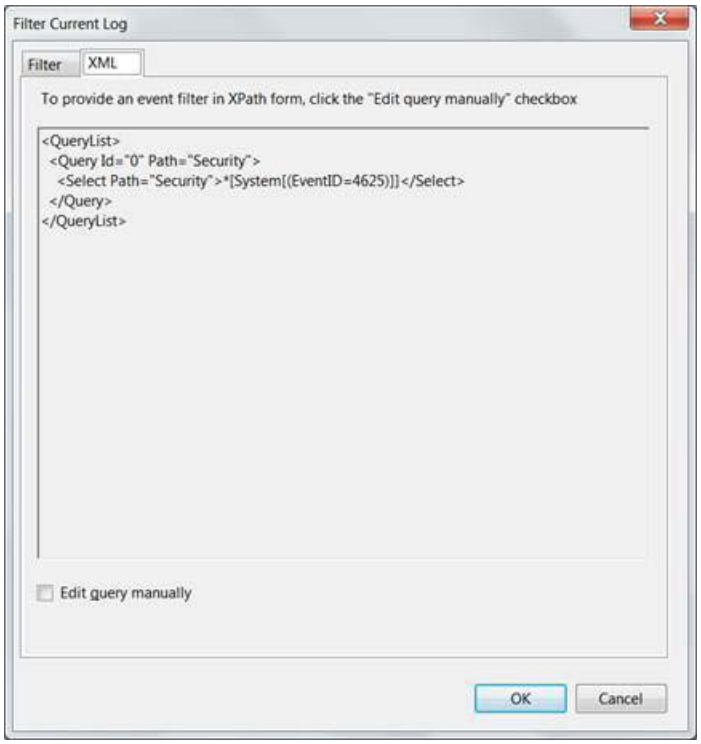
1. [**現在のログをフィルター (Filter current log)**] をクリックしてフィルターを設定します。



たとえば、イベントIDが4625のログオン失敗イベントを収集するには、以下の図のように、イベントID番号を入力します。



2. [**XML**] タブをクリックします。クエリがXMLで表示されます。



`<Select>`と`</Select>`の間に表示される式が、フィルターに入力できる値です。ここでは、`*[System[(EventID=4625)]]`となっています。これを、目的のイベントログのホストテーブルパラメーターの [**Filter**] カラムにコピーできます。

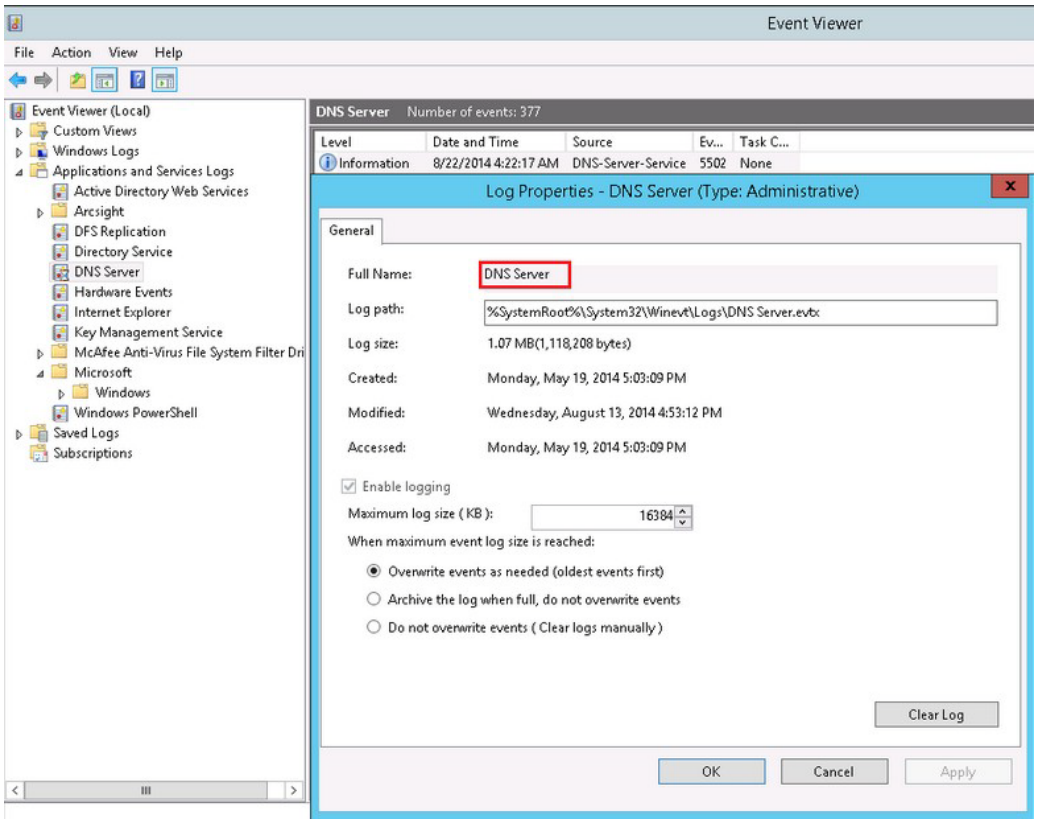
注: 場合によっては、テキストをUIウィザードの [Filter] カラムに直接コピーできないことがあります。フィルターテキストに “gt;”、“lt;”、“gt;=”、“lt;=” が含まれる場合は、これらを “>”、“<”、“>=”、“<=” にそれぞれ置き換える必要があります。

カスタムログ名の指定

Windowsホストのパラメーターウィンドウの、**カスタムログ名**パラメーター用カラムでは、カスタムイベントログの名前を指定できます。また、アプリケーションでは、DNS Server、Directory Service、Exchange Auditingなど、カスタムアプリケーションイベントログ用のイベントを生成できます(アプリケーションイベントでは、イベントヘッダーのみの解析サポートがサポートされます)。

たとえば、Active Directoryの場合は`Directory Service`を指定し、Microsoft Exchange監査の場合は`Exchange Auditing`を指定します。Microsoft Windowsプリントサービス管理ログの場合は、`Microsoft-Windows-PrintService/Admin`を使用します。

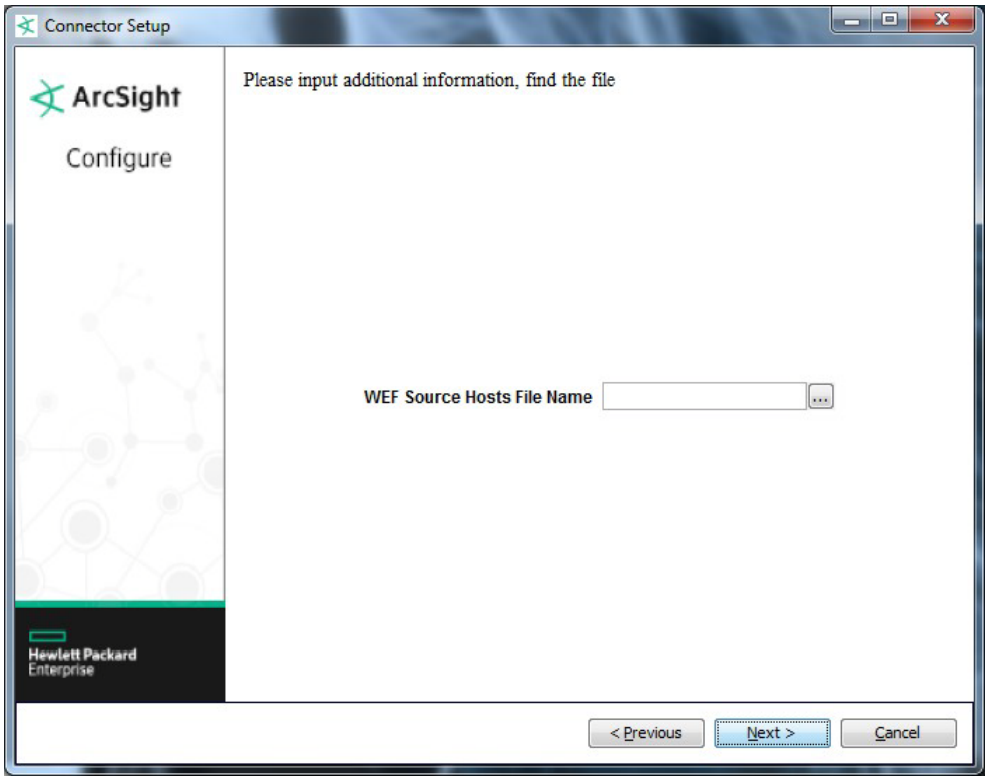
カスタムイベントログ名を識別するには、Microsoft Windowsの [**イベント ビューアー**] で**カスタムアプリケーションイベントログ**を選択します。ログ名は、以下の図に示すように、イベントログのプロパティの [**フル ネーム (Full Name)**] フィールドで確認できます。



このパラメーターの設定の詳細については、「ホストごとの詳細設定パラメーター」を参照してください。

WEFソースホストファイル名

[**Select logs for event collection from local host**] セクションで [**ForwardedEvents log**] を選択した場合、または [**Source hosts for all forwarded events**] セクションで [**Use file for OS version**] を選択した場合 (かつ [Use Active Directory] を選択していない場合)、ソースホスト情報を含むファイルの名前を入力するための以下のウィンドウが表示されます。このウィンドウは、テーブルパラメーターウィンドウで任意のホストに対して [**Is WEC**] を選択した場合にも表示されます。

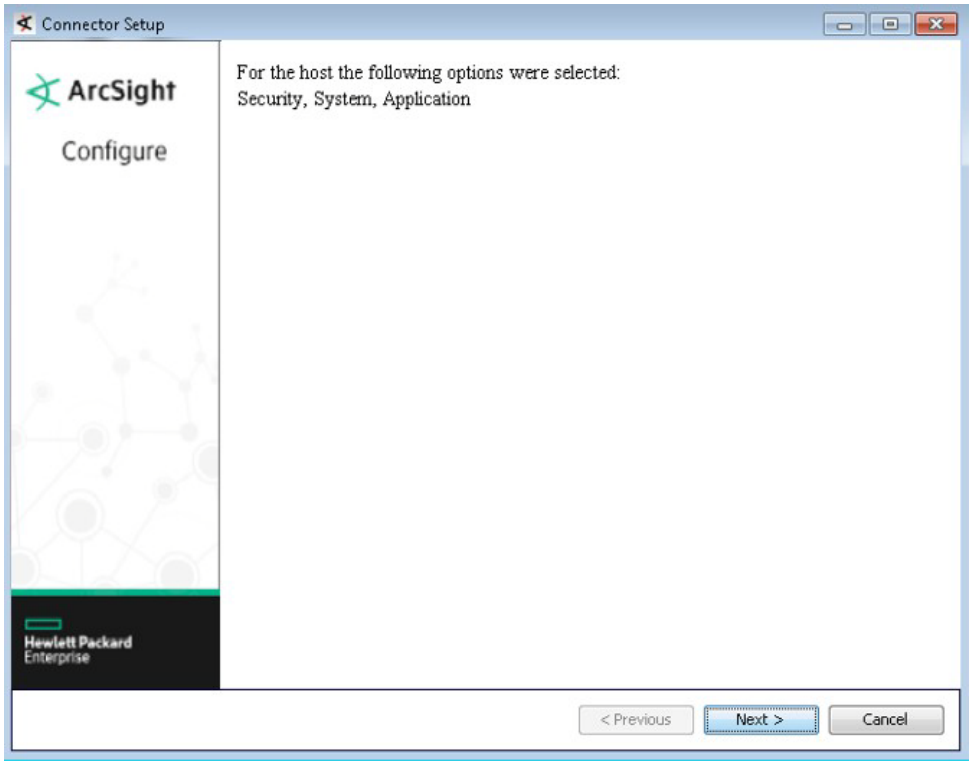


ソースホストファイル名を入力して、[**Next**] をクリックします。

設定のサマリー

設定が完了して [**Next**] をクリックすると、選択した内容をまとめたウィンドウが表示されます。次のウィンドウからは、通知先の設定になります。「通知先の選択」を参照してください。

たとえば、セキュリティログ、システムログ、およびアプリケーションログを選択してローカルホスト用にコネクターをインストールした場合、サマリー画面は次のようになります。



通知先の選択

ここでは、イベントをArcSight ESMに転送する場合について説明します。

1. **ArcSight Manager** (encrypted) が選択されていることを確認し、[**Next**] をクリックします。その他の内容については、『ArcSight SmartConnectorユーザーガイド』およびお使いのArcSight製品の『管理者ガイド』を参照してください。
2. [**Manager Host Name**]、[**Manager Port**]、およびArcSightの有効な [**User Name**] と [**Password**] を入力します。これは、ArcSight Managerのインストール時に作成したのと同じユーザー名とパスワードです。

   通知先のパラメーターの詳細については、『ArcSight SmartConnectorユーザーガイド』を参照してください。[**Next**] をクリックします。
3. 環境内でのコネクターの使用を識別するため、SmartConnectorの [**Name**] と、オプションで [**Location**]、[**Device Location**]、[**Comment**] を入力します。[**Next**] をクリックします。コネクターで登録プロセスが開始されます。
4. ESM Managerの証明書インポートウィンドウが表示されます。[**Import the certificate to the connector from destination**] を選択し、[**Next**] をクリックします。[**Do not import the certificate to connector from destination**] を選択した場合、コネクターのインストールは終了します。
5. 証明書がインポートされ、[**Add Connector Summary**] ウィンドウが表示されます。

インストールおよび設定の完了

SmartConnectorのインストールと設定を完了するには、次の手順に従います。

1. [**Add Connector Summary**] の内容を確認し、[**Next**] をクリックします。サマリーの内容が正しくない場合は、[**Previous**] をクリックして変更を行います。
2. ウィザードで、SmartConnectorをスタンドアロンプロセスとして実行するか、サービスとして実行するかを選択する画面が表示されます。コネクターをサービスとして実行する場合は、[**Install as a service**] を選択して、[**Next**] をクリックします。ウィザードで、サービスのパラメーターを定義する画面が表示されます。[**Service Internal Name**] と [**Service Display Name**] の値を入力し、[**Start the service automatically**] で [**Yes**] または [**No**] を選択します。[**Next**] をクリックすると、[**Install Service Summary**] ウィンドウが表示されます。コネクターをスタンドアロンプロセスとして実行する場合は、サービスのパラメーターを指定する画面は表示されないため、次のステップは省略できます。コネクターのサービスまたはデーモンとしての実行の詳細については、『SmartConnectorユーザーガイド』を参照してください。

   注: ArcSightでは、このコネクターをサービスとしてインストールすることを推奨しています。コネクターをスタンドアロンアプリケーションとして起動し、CTRL+Cを使ってコネクターをシャットダウンした場合、コネクターの「WINCエージェント」プロセスがSIDキャッシュ内に保持されず、途中で終了してしまう可能性があります。
3. サービスのパラメーターを入力して、[**Next**] をクリックします。[**Install Service Summary**] ウィンドウが表示されます。
4. [**Next**] をクリックします。
5. インストールを完了するには、[**Exit**] を選択して [**Next**] をクリックします。

   一部のSmartConnectorでは、設定内容を反映するのにシステムの再起動が必要になります。[**システムの再起動**] ウィンドウが表示されたら、内容を確認してシステムを再起動してください。

   注: お使いのコンピューターまたはデスクトップで作業中のものがある場合は保存し、実行中の他のすべてのアプリケーション (ArcSightコンソールが実行中の場合はこれも含む) をシャットダウンしてから、システムをシャットダウンしてください。

   続いて、「SmartConnectorの実行」に進みます。コネクターのアップグレードまたはアンインストールの手順については、『SmartConnectorユーザーガイド』を参照してください。

SmartConnectorの実行

SmartConnectorは、スタンドアロンモードでインストールして実行するか、WindowsプラットフォームでWindowsサービスとしてインストールして実行できます。また、SmartConnectorは、ショートカットやオプションの [**スタート**] メニューエントリを使用して実行することもできます。

スタンドアロンでインストールした場合、コネクターは手動で起動する必要があります。ホストを再起動したときも自動ではアクティブになりません。サービスとしてインストールした場合、コネクターはホストを再起動したときに自動的に実行されます。コネクターのサービスとしての実行については、『ArcSightSmartConnectorユーザーガイド』を参照してください。

スタンドアロンでインストールしたコネクターで、特定のホストにインストールされたすべてのコネクターを実行するには、コマンドウィンドウを開き、$ARCSIGHT_HOME\current\binに移動して、arcsight connectorsを実行します。

SmartConnectorのログを参照するには、$ARCSIGHT_HOME\current\logs\にあるagent.logファイルとwincagent.logファイルを確認します。すべてのSmartConnectorを停止するには、コマンドウィンドウでCTRL+Cを入力します。

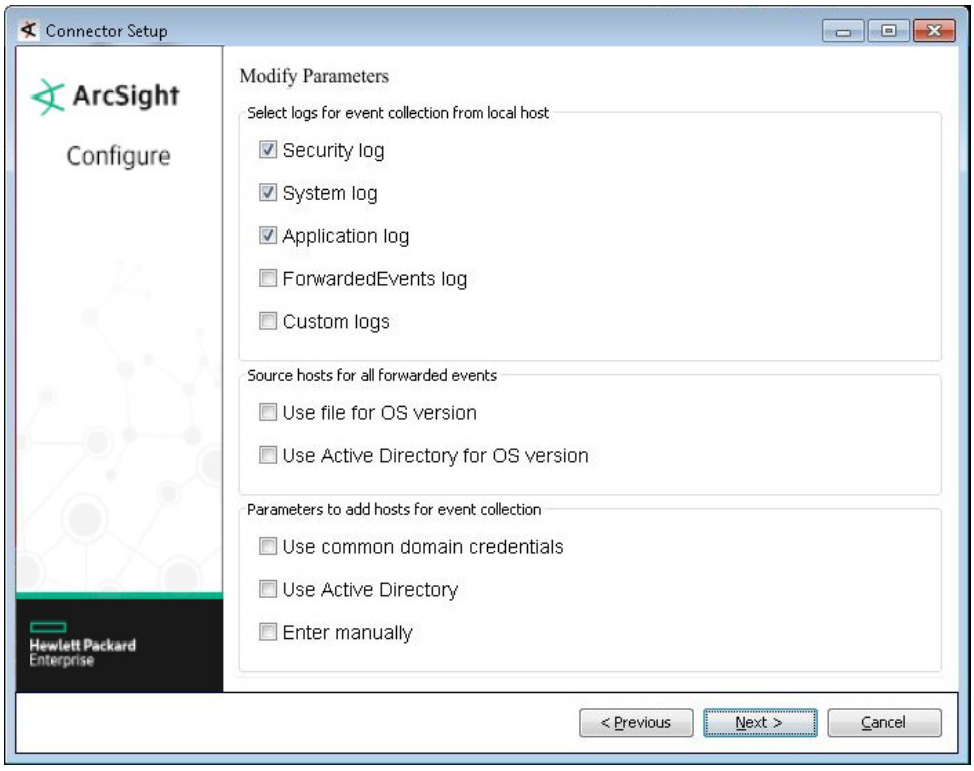
設定パラメーターの変更

設定パラメーターを変更するには、$ARCSIGHT_HOME\current\binに移動して、runagentsetup.batをダブルクリックします。

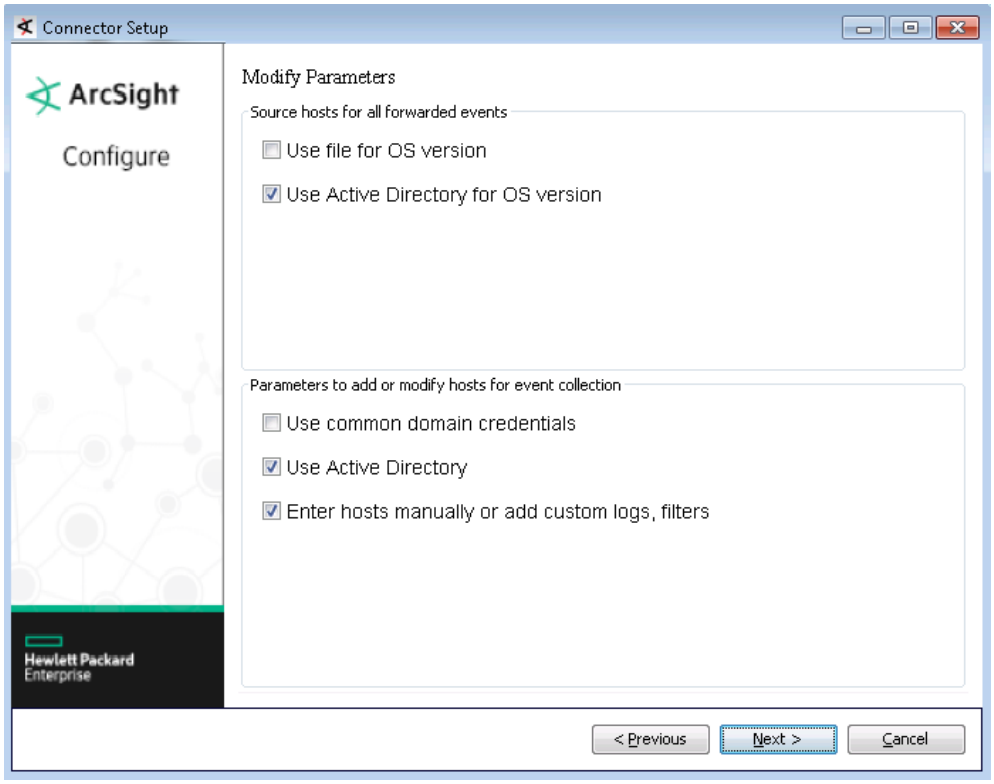
1. [**Modify Connector**] を選択します。[**Next**] をクリックします。
2. [**Modify connector parameters**] を選択し、[**Next**] をクリックします。

必要な変更を行い、コネクターの初期設定のときと同じようにウィザードを続行します。パラメーターの説明については、「コネクターの設定」を参照してください。

設定内容がローカルホストに関するもののみの場合は、次のようなウィンドウが表示されます。



[**Select logs for event collection from local host**] セクションはローカルホストのみに関するものであるため、設定内容が複数のホストに関するものである場合は、表示されるウィンドウに [**Source hosts for all forwarded events**] と [**Parameters to add hosts for event collection**] のセクションのみが含まれます。



システムイベントとアプリケーションイベントに対するカスタムパーサーの作成

このガイドで示しているように、SmartConnectorでは、すべてのセキュリティイベントと一部のシステムイベントで、Windowsのイベントヘッダーとイベントの説明の両方の詳細な解析を行うことができます。

コネクターでは、すべてのシステムイベントとアプリケーションイベントで、Windowsのイベントヘッダーの詳細な解析を行うことができます。また、コネクターには、イベントの説明を解析するために独自のパーサーの作成と展開を行うためのフレームワークも用意されています。このようなパーサーでは、ChannelやProviderNameごとにイベントを解析できます。

- システムイベントログ (NTServicePack、サービスコントロールマネージャー、WINSなど) からイベントを収集する場合は、[**Windows Log type**] で [**System**] を選択します。
- アプリケーションイベントログ (Microsoft Forefront Protection 2010 for Exchange、Microsoft SQL Server Auditなど) からイベントを収集する場合は、[**Windows Log type**] で [**Application**] を選択します。

パーサーを作成する前に

パーサーを作成する前に、以下の手順を実行します。

1. 必要なシステムイベントまたはアプリケーションイベントを生成します。
2. システムイベントまたはアプリケーションイベントを収集し、RAWイベントを保存するようにコネクターを設定します。

3. コネクターを実行して、システムイベントまたはアプリケーションイベントを収集し、ArcSightのRAWイベントを生成します。RAWイベントには、JSON形式でキーと値のペアが格納されます。これらの生成したRAWイベントを使用し、「独自のパーサーの作成と展開」を参照して、パーサーファイルを作成することで、これらのキーの値をArcSightイベントスキーマのフィールドにマッピングします。

   注: 必ずしもすべてのRAWイベントのイベント本体にキーと値のペアが含まれる訳ではありません。このようなイベントでは、ArcSightイベントスキーマのフィールドに何かをマッピングするパーサーを作成する必要はありません。その場合でも、このようなイベントのイベント名またはイベントの説明をマッピングするパーサーを作成することはできます。

独自のパーサーの作成と展開

独自のパーサーを作成して展開するには、以下の手順に従います。

1. パーサーファイルを展開するため、次のディレクトリに移動します。

   `$ARCSIGHT_HOME\user\agent\fcp\winc`

2. 解析が必要なイベントのチャネルを識別します (たとえば、システム、アプリケーション、ディレクトリサービス、DNSサーバー、キー管理サービスなど)。
3. 解析が必要なイベントのプロバイダー名を識別します。これは、1つのチャネルから収集されるイベントが複数のプロバイダー名で生成される可能性があるためです。たとえば、`Channel: System`から収集されるイベントは、`ProviderName: Service Control Manager`や`WINS`などで生成される可能性があります。
4. 解析が必要なイベント本体の`SectionName`を識別します (`EventData`、`UserData`など)。
   a. イベント本体の`EventData`セクションを解析するには、**ステップ1**で確認したディレクトリに、次の命名規則を使用してキー/値パーサーファイルを作成します。

      `\{正規化されたChannel}\{正規化されたProviderName}.sdkkeyvaluefilereader.properties`

      たとえば次の場合、

      - Channel: `Security`
      - ProviderName: `Microsoft Windows Event Log`
      - SectionName: `EventData`

      キー/値パーサーファイル名は次のようになります。

      `\security\microsoft_windows_eventlog.sdkkeyvaluefilereader.properties`

   b. イベント本体のその他のセクション (`UserData`など) を解析するには、**ステップ1**で確認したディレクトリに、次の命名規則を使用してJSONパーサーファイルを作成します。

      `\{正規化されたChannel}\{正規化されたProviderName}.{正規化されたSectionName}.jsonparser.properties`

たとえば次の場合、

- Channel: `Security`
- ProviderName: `Microsoft Windows Event Log`
- SectionName: `UserData`

キー/値パーサーファイル名は次のようになります。

```
\security\microsoft_windows_eventlog.userdata.jsonparser.properties
```

注: `Channel`、`ProviderName`、`SectionName`の値を正規化するには、すべての英字を小文字に変更し、英数字以外の各文字 (特殊文字とスペースを含む) をアンダースコア (_) に置き換えます。ロケールおよびエンコーディングの値は正規化しないでください。

5. WindowsイベントIDにすでにマッピングされている、ArcSightの`externalId`フィールドに基づいた条件付きマッピングを使用し、それぞれの要件に従って、これらのパーサー内にマッピングを作成します。

   前述のように、コネクターはWindowsイベントヘッダーのフィールドをArcSightイベントのフィールドにすでにマッピングしているため、(マッピングの値をオーバーライドする必要がある場合を除き) これらのマッピングを再定義する必要はありません。マッピングが必要なのは、特定のイベントの説明をマッピングする場合のみです。

   a. 以下はイベントヘッダーのキー/値パーサーの使用例です。

      - Channel: `Security`
      - ProviderName: `Microsoft Windows Event Log`
      - SectionName: `EventData`

      次のようにイベント名フィールドをマッピングできます。

```
key.delimiter=&&
key.value.delimiter==
key.regexp=([^&=]+)

event.deviceVendor= getVendor("Microsoft")

conditionalmap.count=1
conditionalmap[0].field=event.externalId
conditionalmap[0].mappings.count=2

# The event logging service has shut down.
conditionalmap[0].mappings[0].values=1100
conditionalmap[0].mappings[0].event.flexString1=
conditionalmap[0].mappings[0].event.name= stringConstant("The event
logging service has shut down.")

# The security log is now full.
```

```
conditionalmap[0].mappings[1].values=1104
conditionalmap[0].mappings[1].event.flexString1=
conditionalmap[0].mappings[1].event.name= stringConstant("The security
log is now full.")
```

この例をコピーして貼り付ける場合は、ファイル内に末尾のスペースが残らないようにしてください。

b. 以下はサンプルJSONパーサーのUserDataセクションの例です。

- Channel: `Security`
- ProviderName: `Microsoft Windows Event Log`
- SectionName: `UserData UserData`

セクションの例:

```
{
   "UserData":
      { "LogFileCleared":

         "@xmlns:auto-ns3":
"http://schemas.microsoft.com/win/2004/08/events",
         "@_xmlns_":
http://manifests.microsoft.com/win/2004/08/windows/eventlog",
          "SubjectUserSid":  "S-1-5-18",
         "SubjectUserName": "SYSTEM",
         "SubjectDomainName": "NT AUTHORITY",
         "SubjectLogonId": "0x3e7"
         }
      }
}
```

c. 以下はEventBody JSONパーサーの使用例です。

- Channel: `Security`
- ProviderName: `Microsoft Windows Event Log`
- SectionName: `UserData EventBody`

セクションの例:

```
trigger.node.location=/UserData
event.deviceVendor= getVendor("Microsoft")
token.count=7
token[0].name=SubjectUserSid
token[0].location=LogFileCleared/SubjectUserSid
token[0].type=String
```

```
token[1].name=SubjectUserName
token[1].location=LogFileCleared/SubjectUserName
token[1].type=String

token[2].name=SubjectDomainName
token[2].location=LogFileCleared/SubjectDomainName
token[2].type=String

token[3].name=SubjectLogonId
token[3].location=LogFileCleared/SubjectLogonId
token[3].type=String

token[4].name=Reason
token[4].location=AuditEventsDropped/Reason
token[4].type=String

token[5].name=Channel
token[5].location=AutoBackup/Channel
token[5].type=String

token[6].name=BackupPath
token[6].location=AutoBackup/BackupPath
token[6].type=String

conditionalmap.count=1
conditionalmap[0].field=event.externalId
conditionalmap[0].mappings.count=3

conditionalmap[0].mappings[0].values=1101
conditionalmap[0].mappings[0].event.name= stringConstant("Audit events
have been dropped by the transport.The real time backup file was
corrupt due to improper shutdown.")
conditionalmap[0].mappings[0].event.deviceCustomNumber3= safeToLong
(Reason)
conditionalmap[0].mappings[0].event.deviceCustomNumber3Label=____
stringConstant("Reason Code")

conditionalmap[0].mappings[1].values=1102
conditionalmap[0].mappings
[1].event.destinationNtDomain=SubjectDomainName
conditionalmap[0].mappings[1].event.destinationUserName=___extractNTUser
(___oneOf(SubjectUserName,SubjectUserSid))
```

```
conditionalmap[0].mappings[1].event.destinationUserId=SubjectLogonId
conditionalmap[0].mappings[1].event.name= stringConstant("The audit
log was cleared.")

conditionalmap[0].mappings[2].values=1105
conditionalmap[0].mappings[2].event.fileType=Channel
conditionalmap[0].mappings[2].event.fileName=BackupPath
conditionalmap[0].mappings[2].event.name=___stringConstant("Event log
automatic backup")
```

この例をコピーして貼り付ける場合は、ファイル内に末尾のスペースが残らないようにしてください。

6. コネクターを起動します。

新しいイベントのカテゴライズを確認してください。追加のカテゴライズが必要になる場合があります。カテゴライズについては、HPEソフトウェアサポートサイトで入手できるテクニカルノート『ArcSight Categorization: A Technical Perspective』を参照してください。パーサーの作成の詳細については、HPEソフトウェアサポートサイトおよびProtect 724サイトで入手できる『ArcSight FlexConnector Developer's Guide』を参照してください。

Nativeコネクターでのローカリゼーションサポートのカスタマイズ

ArcSight SmartConnectorは、ArcSight SIEM用のイベント収集レイヤーを提供します。このため、SmartConnectorのコンテキストでは、ローカリゼーションは、ローカライズされたイベントによって生成され、英語以外の言語で記述されたイベントメッセージの収集、解析、および正規化と関連しています。ローカリゼーション (L10N) は、特定のロケールまたは国で実行するためにプログラムを変更するプロセスです。これには、すべてのテキストの表示やユーザーインターフェイスのネイティブ言語への翻訳などが含まれます。

ArcSightで提供されているものの他にロケーションサポートを追加するには、次の手順に従います。

1. イベントデータをローカライズするイベントのChannel、ProviderName、ロケール、およびエンコーディングを識別します。
2. ステップ1で識別したロケールとエンコーディングのパラメーター値を使用して、ホストテーブルパラメーターを設定します。

   コネクターのホストテーブル設定の選択項目に現れないロケールとエンコーディングのサポートを追加するには、`agent.properties`ファイル (`$ARCSIGHT_HOME\current\user\agent`) の以下の行のロケールとエンコーディングの値を変更します。

   ```
   agents[x].windowshoststable[y].locale=<ロケール>
      agents[x].windowshoststable[y].encoding=<エンコーディング>
   ```

   ここで、xはコネクターのインデックスで、yはコネクター設定のホストのインデックスです。

例

```
agents[0].windowshoststable[0].locale=de_DE
   agents[0].windowshoststable[0].encoding=UTF-8
```

3. ログファイル内のイベントの文字セットのエンコーディングのタイプを入力します (例: event.name)。次の場所に対してコンテンツを作成します: $ARCSIGHT_HOME\user\agent\fcp\winc\
4. ローカリゼーションの追加プロセッサーマップファイルの呼び出し元のパーサーを識別します。

```
$ARCSIGHT_HOME\user\agent\winc\<正規化されたChannel>\
   <正規化されたProviderName>.sdkkeyvaluefilereader.properties
```

例

```
$ARCSIGHT_HOME\user\agent\winc\security\
   microsoft_windows_security_auditing.sdkkeyvaluefilereader.properties
```

注: Channel、ProviderName、SectionNameの値を正規化するには、すべての英字を小文字に変更し、英数字以外の各文字 (特殊文字とスペースを含む) をアンダースコア (_) に置き換えます。ロケールおよびエンコーディングの値は正規化しないでください。

5. ロケールとエンコーディングの組み合わせごとに、このパーサー内で追加プロセッサーマップファイルを1つずつ宣言します。

```
extraprocessor[4].type=map
extraprocessor
[4].filename=winc/<正規化されたChannel>/<正規化されたProviderName>.
   <ロケール>.<エンコーディング>.map.csv
extraprocessor[4].conditionfield=event.oldFileHash
extraprocessor[4].conditiontype=equals
extraprocessor[4].conditionvalues=<ロケール>|<エンコーディング>
extraprocessor[4].charencoding=<エンコーディング>
extraprocessor[4].allowoverwrite=true
extraprocessor[4].overrideeventmappings=true
extraprocessor[4].clearfieldafterparsing=false
extraprocessor[4].flexagent=false
```

例

```
extraprocessor[4].type=map
extraprocessor[4].filename=winc/security/
   microsoft_windows_security_auditing.fr_CA.UTF-8.l10n.map.csv
extraprocessor[4].conditionfield=event.oldFileHash
extraprocessor[4].conditiontype=equals
extraprocessor[4].conditionvalues=fr_CA|UTF-8
extraprocessor[4].charencoding=UTF-8
```

```
extraprocessor[4].allowoverwrite=true
extraprocessor[4].overrideeventmappings=true
extraprocessor[4].clearfieldafterparsing=false
extraprocessor[4].flexagent=false
```

6. 次のL10N追加プロセッサーマップファイルを作成します。

```
$ARCSIGHT_HOME\user\agent\winc\<正規化されたChannel>\
   <正規化されたProviderName>.<ロケール>.<エンコーディング>.l10n.map.csv
```

注: L10N追加プロセッサーマップファイルを作成、編集、または保存する際は、デフォルトの**ASCII**、**UTF-8**、またはその他の標準エンコーディングのアプリケーションを使用しないでください。ローカライズされたデバイスやローカライズされたエディターでファイルを作成し、保存時にエンコーディングが上書きされないようにしてください。

例

```
$ARCSIGHT_HOME\user\agent\winc\security\
   microsoft_windows_security_auditing.fr_CA.UTF-8.l10n.map.csv
```

注: Channel、**ProviderName**、**SectionName**の値を正規化するには、すべての英字を小文字に変更し、英数字以外の各文字 (特殊文字とスペースを含む) をアンダースコア (_) に置き換えます。**ロケール**および**エンコーディング**の値は正規化しないでください。

7. このファイル内で、getterおよびsetterを宣言し、すべてのローカリゼーションコンテンツを追加します。event.externalIdフィールドをgetterとして使用し、ローカライズするフィールドをsetterとして使用します。以下にフランス語の場合のサンプルファイルを示します。

```
event.externalId,set.event.name
"4886","Les services de certificats ont reçu une demande de certificat."
"4887","Les services de certificats ont approuvé une demande de
certificat et émis un certificat."
"4884","Les services de certificats ont importé un certificat dans sa base
de données."
"4885","Le filtre d'audit des services de certificats modifié."
"4882","Les autorisations de sécurité pour les services de certificats ont
été modifiées."
"4883","Les services de certificats ont récupéré une clé archivée."
"4880","Les services de certificats ont démarré."
"4881","Les services de certificats se sont arrêtés."
...
...
```

追加設定

複数のコネクターインスタンスの設定

ソースホストでコネクターの別のインスタンスをインストールして実行するには、次の手順に従います。

ウィザードで [**Add a connector**] ウィンドウが表示されたら、ウィザードを終了します。

1. インストールディレクトリに移動します。例:

   ```
   $ARCSIGHT_HOME\ArcSightSmartConnectors\current\
   ```

2. $ARCSIGHT_HOME\current\user\agentディレクトリで、agent.propertiesファイルを編集します。
3. mq.server.listener.portプロパティで、有効なTCPポート値を選択します。この値をコネクターの別のインスタンスで使用することはできません。指定可能な範囲は1～65535で、デフォルト値は61616です。
4. mq.server.listener.portプロパティで、パラメーターと値を追加します。
5. $ARCSIGHT_HOME\current\user\agent\wincディレクトリに、次の内容のconfig.iniファイルを作成します。

   ```
   mq.server.hostname=localhost
   mq.protocol=tcp
   mq.server.port=<有効なtcpポート>
   ```

   このファイルのmq.server.portの値は、agent.propertiesで設定したものと一致している必要があります。

6. $ARCSIGHT_HOME\current\binディレクトリから**runagentsetup**を実行して、セットアップウィザードを起動します。

注:

- 設定ウィザードを実行する場合、イベントリスナーがRemoteAgentIdに割り当てられる前にハートビートの送信を始めると、以下の警告メッセージがログ記録されることがあります。

  ```
  [updateHeartbeat]RemoteAgentId unspecified.Ignoring the heartbeat.
  ```

- 同じマシンにインストールされたNative Windows Event Logの各インスタンスのmq.server.portの値が一意でない場合、コネクターは実行されません。これは、そのポートがすでに使用中であることを示します。
- コネクターのインスタンス数が増えるにつれて、リソース消費量も増大します。このため、社内で使用するインスタンス数が制限される場合があります。

イベントソースマッピングのカスタマイズ

Windows Event Log – Nativeのアプリケーション/システムイベントパーサーロード機能は、各イベントのイベントソースに依存し、以下の命名規則を用いてパーサーのロードを試みます。

<Channel>\<ProviderName>.sdkkeyvaluefilereader.properties

この命名規則は、ほとんどの場合は問題なく機能しますが、パーサーによってはもっと柔軟な設定が必要になる場合もあります。このような場合には、変数ChannelおよびProviderNameをリダイレクトすることで、これらのパーサーの検索場所をカスタマイズできます。柔軟性をさらに向上させる場合は、入力のProviderNameを正規表現と照合して最小限の変更でエントリの重複を回避することができます。

オーバーライドマップファイルの作成

1. $ARCSIGHT_HOME/current/user/agent/fcp/winc/core_mapsに移動し、以下のカラムを含むcustomeventsource.map.csvという名前のオーバーライドマップファイルを作成します。

   SourceChannel
   SourceProviderNamePattern
   TargetProviderName
   TargetChannel

   SourceProviderNamePatternの値には、文字列または正規表現を使用できます。
2. $ARCSIGHT_HOME/current/user/agent/fcpにサブディレクトリwinc/coremapsが存在しない場合は、このサブディレクトリを作成します。
3. 最後のフィールドTargetChannelはオプションで、空の場合は、SourceChannelと同じであるとみなされます。

クラスター環境でのイベント解析の例

クラスター環境では、デフォルトのパーサーファイル名規則が原因で問題が発生する可能性があります。これは、異なるクラスターからの同じイベントが、カスタマイズされた異なるプロバイダー名を持つ可能性があるためです。たとえば、SQL Server のアプリケーションイベントの ProviderName は MSSQLSERVER であるため、パーサー名は application\mssqlserver.sdkkeyvaluefilereasder.propertiesになります。

SQL Serverのクラスター環境では、各クラスターのプロバイダー名をSQLSERVER01やSQLSERVER02などにカスタマイズして設定できます。しかし、コネクターはMSSQLSERVERというプロバイダー名を期待しているため、変更を行わないと、カスタマイズしたプロバイダー名を持つイベントでの解析が失敗します。

このような結果を回避するには、マップファイル $ARCSIGHT_HOME/user/agent/fcp/winc/core_maps/customeventsource.map.csvを使用して、これらの異なるすべてのプロバイダー名を1つのプロバイダー名の値にマッピングします。

以下は、上記のクラスター環境に基づいたエントリの例です。

```
Application, MSSQLSERVER01, MSSQLSERVER, Application
Application, MSSQLSERVER\d*, MSSQLSERVER, Application
Application, MSSQLSERVER.*, MSSQLSERVER, Application
```

2つのエントリを含むcustomeventsource.map.csvのサンプルファイルの内容全体は、次のようになります。

```
#SourceChannel,  SourceProviderNamePattern,  TargetProviderName,
 System,         Service.*,                  service_control_manager,
 Application,    MSSQLSERVER.*,              MSSQLSERVER,
```

詳細オプションの設定

ここでは、このコネクターで使用できる詳細設定パラメーターの一部について説明します。詳細設定パラメーターへのアクセス方法に続く表は、社内のニーズに応じて調整できるパラメーターについて説明したものです。

詳細パラメーターへのアクセス

SmartConnectorのインストール後に、agent.propertiesファイルを編集してパラメーターを変更できます。このファイルは、$ARCSIGHT_HOME\current\user\agentにあります。

詳細なコンテナー設定プロパティ

指定内容	パラメーター	デフォルト
コネクターとコレクターの間で使用するプロトコル。現在は、TCPプロトコルをサポートしています。	mq.protocol	tcp
コネクターとコレクターの間で使用するポート。コネクターのインストール時に指定したポートにバインドされます。同じホストに複数のコネクターをインストールする場合は、未使用のポート番号を使ってこれを設定します。	mq.server.listener.port	61616
MQコンポーネントでメッセージパーシステンスに使用する最大ディスクサイズ (KB)。	mq.persistent.storage.limit	409600

指定内容	パラメーター	デフォルト
MQコンポーネントで使用する最大メモリサイズ (KB)。	mq.memory.limit	65536
永続的なストアから処理済みメッセージをクリーンアップする頻度 (ミリ秒)。winc-agentからより多くのメッセージを受け取るには、ストレージをクリーンアップする必要があります。	mq.persistent.storage.cleanup.interval	10000
メモリ内に事前にロードするメッセージやイベントバッチの数。winc-agentから受け取ったメッセージはメモリストアに保存されますが、処理するためにはメモリにロードする必要があります。事前にロードすることで、データロードの待機時間が短縮され、パフォーマンスの改善に役立ちます。	mq.consumer.prefetch.size	80

詳細な共通設定パラメーター

指定内容	パラメーター	デフォルト
1つのコレクターの専用のイベント処理スレッドの数。	eventprocessthreadcount	10
パフォーマンスを向上させるため、実行準備完了のイベント処理タスクを保持するのに使用するキューのサイズ。キューを大きくするほど、メモリ使用量は増えますが、処理に使用できるスレッド数に制限があるため、パフォーマンスの向上に役立つとは限りません。	Executequeuelength	100
デフォルトで、統計情報は10分ごとに計算され、user/agent/agentdataのagent.logとEventStatsレポートファイルにダンプされます。この間隔設定は、統計の計算頻度を調整します。統計には、1秒あたりのイベント数の最後の間隔の平均が含まれます。	pdastatsinterval	600000ms
コネクターが終了するか、デバイスがダウンする直前に処理されたIDを保存するかどうかを示します。	preservestate	true
preservestateを書き込むまでのイベント数。	preservedstatecount	100
preservestateを書き込むまでの時間間隔 (ミリ秒)。	preservedstateinterval	10000

ホストごとの詳細設定パラメーター

指定内容	パラメーター	デフォルト
リアルタイムイベントを取得するか、イベントログの先頭から読み込むかを示します。	startatend	true
カスタムアプリケーションイベントログからアプリケーションイベントを収集するには、カスタムアプリケーションイベントログのコンマ区切りのリストを提供します。ワークグループのホストには、それぞれ別の共有SIDキャッシュがあります。	eventlogtypes	null

SIDおよびGUID変換に関する詳細設定パラメーター

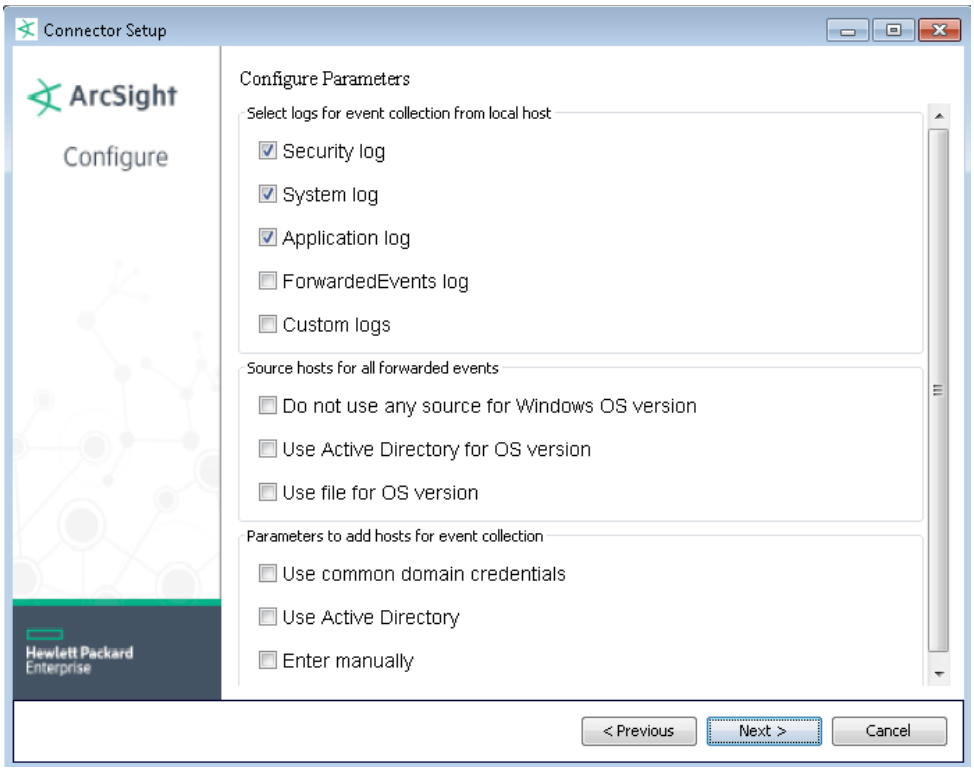
指定内容	パラメーター	デフォルト
GUID変換を有効にします。	enableguidtranslation	false
GUIDとそれぞれの変換後の値を格納するキャッシュのサイズ	guidcachesize	50000
キャッシュ内のGUIDエントリのTime-to-Live (ミリ秒)	guidcachetimetolive	600000
SIDおよびGUIDエントリがキャッシュで期限切れになる間隔 (ミリ秒)	sidguidcacheexpirationthreadsleeptime	600000
SIDおよびGUIDキャッシュがディスクファイルに保存される間隔 (ミリ秒)。各ドメインのSIDキャッシュは、個別のディスクファイルに保存されます。ワークグループホストのSIDキャッシュは、個別の共有ディスクファイルに保存されます。	sidguidcachepersistencethreadsleeptime	600000

付録A セットアップシナリオ

以下の例では、一般的なセットアップシナリオについて説明します。設定の詳細については、「コネクターの設定」を参照してください。

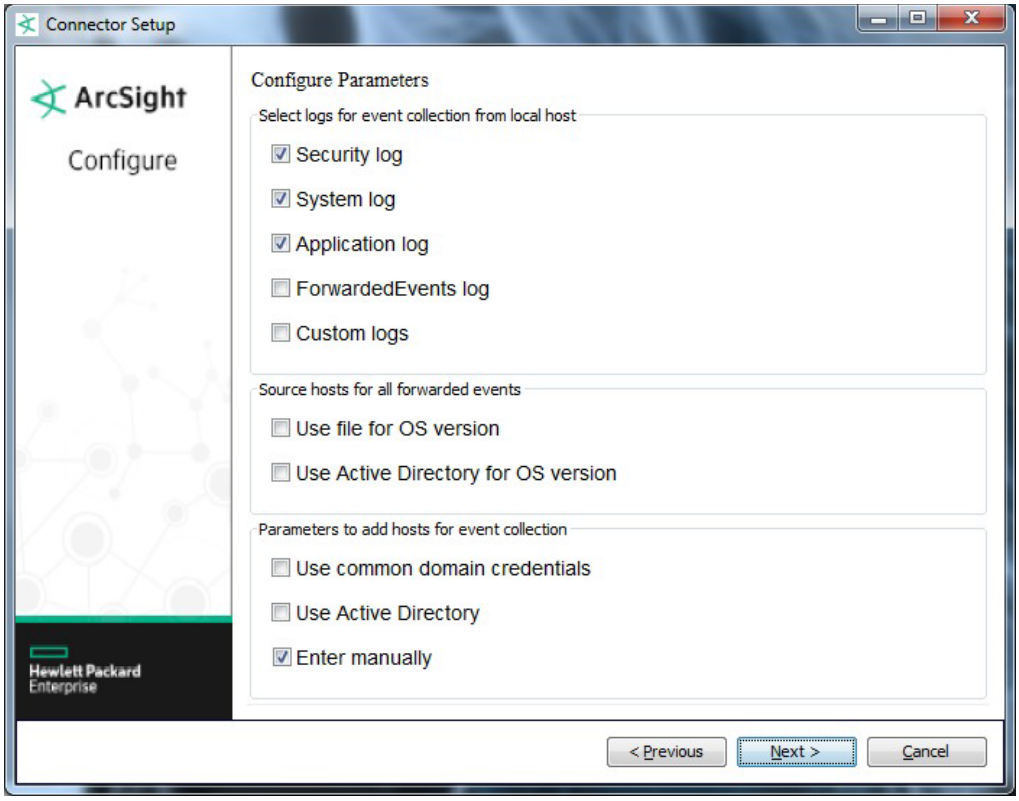
- ローカルホストでアプリケーション、セキュリティ、およびシステムログを収集する
- 1つのドメインで、複数のリモートホストからアプリケーション、セキュリティ、およびシステムログを収集し、ホストを手動で入力する
- Active Directoryに記録されたホストからアプリケーション、セキュリティ、およびシステムログを収集する
- ローカルまたはリモートホストから転送されたイベントまたは他のWECログを収集する

ローカルホストでアプリケーション、セキュリティ、およびシステムログを収集する



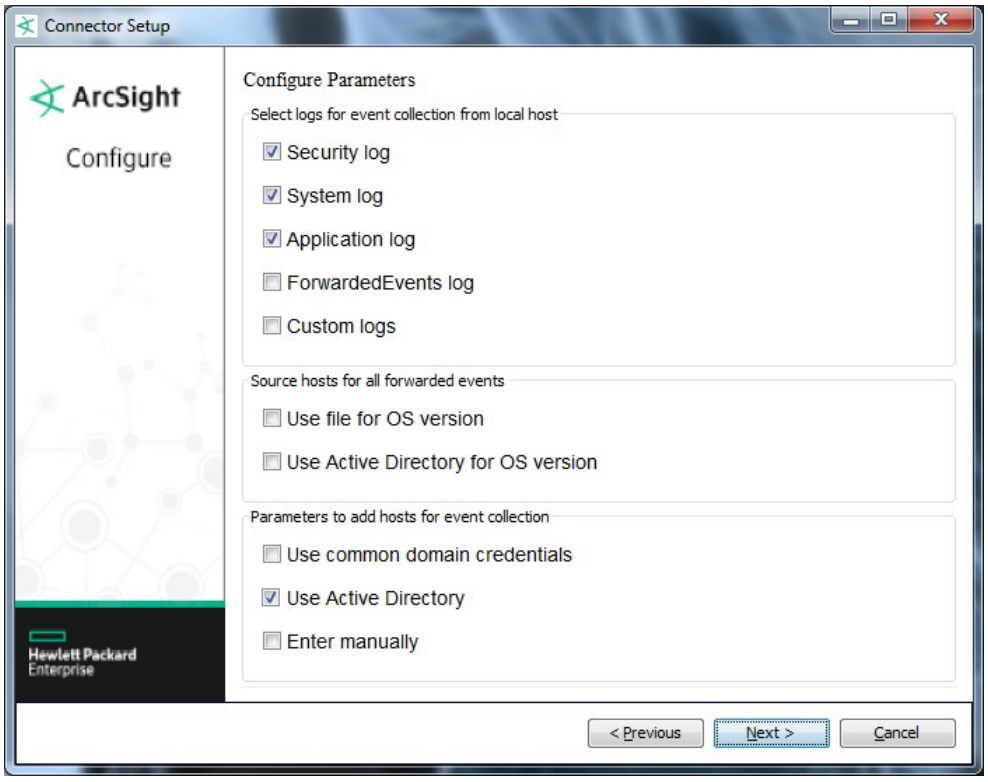
コネクター用の追加のパラメーター入力画面は表示されません。通知先の選択に進む前に、選択内容のサマリーを示す画面が表示されます。これは、「ワンクリック」で実行できるシナリオです。最初の設定ウィンドウでローカルホストのログを選択し、リモートホスト、カスタムログやイベントフィルター、WEFの設定は行いません。

1つのドメインで、複数のリモートホストからアプリケーション、セキュリティ、およびシステムログを収集し、ホストを手動で入力する



このシナリオでは、テーブルパラメーター入力ウィンドウが表示されます。[**Add**] をクリックしてテーブルに行を追加し、ホスト情報を入力します。または、[**Import**] をクリックして、ホスト情報を含むCSVファイルをインポートします。ただし、インポートする際には、インポートしたファイルの内容で既存のホスト情報が置き換えられるため、ローカルホストからイベント収集を行う場合は、CSVファイルにローカルホストを含める必要があります。

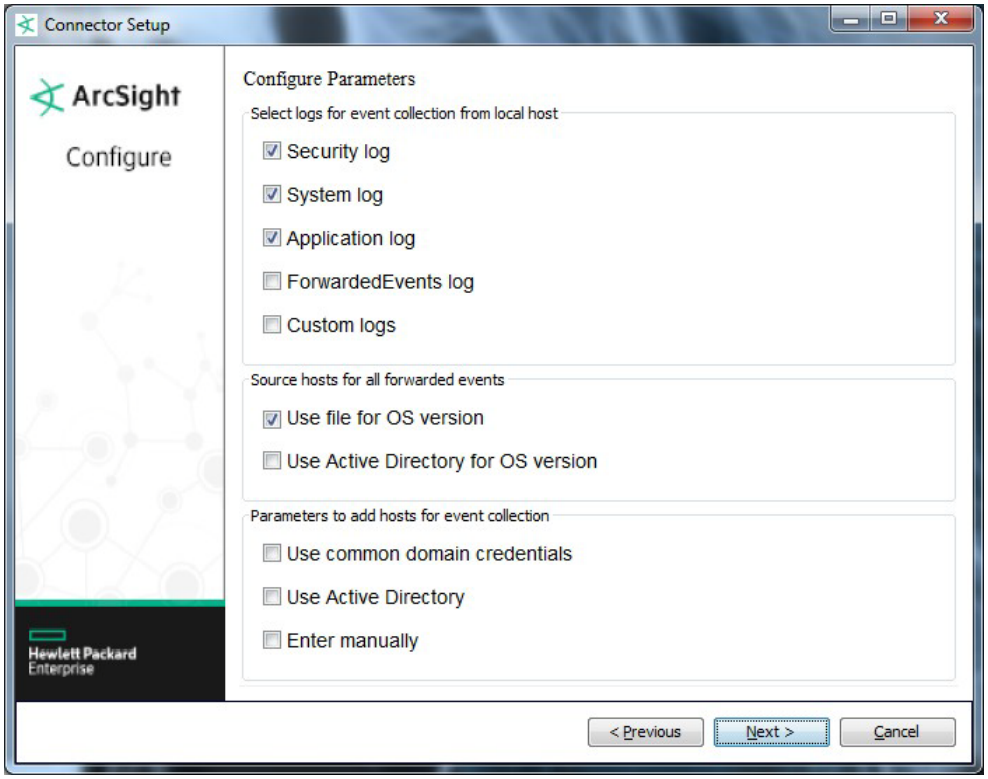
Active Directoryに記録されたホストからアプリケーション、セキュリティ、およびシステムログを収集する



ドメインおよびActive Directoryの資格情報を指定するウィンドウが表示されます。セットアップ時には、必ず [**Use Active Directory host results for**] パラメーターで [**Replace**] を選択します。コネクターのパラメーターを変更する場合は、[**Merge**] または [**Replace**] を選択します。次にテーブルパラメーター入力ウィンドウが表示されます。このウィンドウでは、各ホストの設定を選択できます。

ローカルまたはリモートホストから転送されたイベントまたは他のWECログを収集する

上記のいずれかのシナリオで、ローカルホスト (またはリモートホスト) から転送されたイベントまたは他のWECログを収集します。テーブルパラメーター入力ウィンドウでホストの設定を選択した後に表示されるウィンドウで、ソースホストの名前とホストのWindows OSバージョンが保存されたCSVファイルの名前を指定します。



付録B 内部イベントのタイプ

Windows Event Log – Nativeコネクターは、以下のタイプの内部イベントを記録します。

コレクター接続

フィールド	説明
Event Name	'Collector'
Device Event Category	'/Informational'
Agent Severity	'2'
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<コレクターホスト名>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<コレクタードメイン名>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<コレクターオペレーティングシステムバージョン>

コレクター接続解除

フィールド	説明
Event Name	'Collector Disconnected'
Device Event Category	'/Informational/Warning'
Agent Severity	'3'
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<コレクターホスト名>

フィールド	説明
Device Custom String 2 Label	‘Collector Domain Name’
Device Custom String 2	<コレクタードメイン名>
Device Custom String 5 Label	‘Collector Operating System Version’
Device Custom String 5	<コレクターオペレーティングシステムバージョン>

コレクターアップ

フィールド	説明
Event Name	‘Collector Up’
Device Event Category	‘/Informational’
Agent Severity	‘2’
Device Custom String 1 Label	‘Collector Host Name’
Device Custom String 1	<コレクターホスト名>
Device Custom String 2 Label	‘Collector Domain Name’
Device Custom String 2	<コレクタードメイン名>
Device Custom String 5 Label	‘Collector Operating System Version’
Device Custom String 5	<コレクターオペレーティングシステムバージョン>

コレクターダウン

フィールド	説明
Event Name	‘Collector Down’
Device Event Category	‘/Informational/Warning’
Agent Severity	‘3’
Device Custom String 1 Label	‘Collector Host Name’
Device Custom String 1	<コレクターホスト名>
Device Custom String 2 Label	‘Collector Domain Name’
Device Custom String 2	<コレクタードメイン名>
Device Custom String 5 Label	‘Collector Operating System Version’
Device Custom String 5	<コレクターオペレーティングシステムバージョン>

コレクター設定許可

「コレクター設定許可」のコレクターステータス

フィールド	説明
Event Name	‘Collector Configuration Accepted’
Reason	<成功ステータス/失敗理由>
Device Event Category	理由に応じて‘/Informational’または‘/Informational/Warning’
Agent Severity	理由に応じて‘2’または‘3’
Device Custom String 1 Label	‘Collector Host Name’
Device Custom String 1	<コレクターホスト名>
Device Custom String 2 Label	‘Collector Domain Name’
Device Custom String 2	<コレクタードメイン名>
Device Custom String 5 Label	‘Collector Operating System Version’
Device Custom String 5	<コレクターオペレーティングシステムバージョン>

「コレクター設定許可」のホストステータス

フィールド	説明
Event Name	‘Collector Configuration Accepted’
Device Host Name	<デバイスホスト名>
Reason	<成功ステータス/失敗理由>
Device Event Category	理由に応じて‘/Informational’または‘/Informational/Warning’
Agent Severity	理由に応じて‘2’または‘3’
Device Custom String 1 Label	‘Collector Host Name’
Device Custom String 1	<コレクターホスト名>
Device Custom String 2 Label	‘Collector Domain Name’
Device Custom String 2	<コレクタードメイン名>
Device Custom String 5 Label	‘Collector Operating System Version’
Device Custom String 5	<コレクターオペレーティングシステムバージョン>

「コレクター設定許可」のイベントログステータス

フィールド	説明
Event Name	‘Collector Configuration Accepted’
Device Host Name	<デバイスホスト名>
Device Custom String 3 Label	‘Event Log’
Device Custom String 3	<設定されたイベントログ名>
Reason	<成功ステータス/失敗理由>
Device Event Category	理由に応じて‘/Informational’または‘/Informational/Warning’
Agent Severity	理由に応じて‘2’または‘3’
Device Custom String 1 Label	‘Collector Host Name’
Device Custom String 1	<コレクターホスト名>
Device Custom String 2 Label	‘Collector Domain Name’
Device Custom String 2	<コレクタードメイン名>
Device Custom String 5 Label	‘Collector Operating System Version’
Device Custom String 5	<コレクターオペレーティングシステムバージョン>

コレクターステータス更新

「コレクターステータス更新」のコレクターステータス

フィールド	説明
Event Name	‘Collector Status Updated’
Reason	<成功ステータス/失敗理由>
Device Event Category	理由に応じて‘/Informational’または‘/Informational/Warning’
Agent Severity	理由に応じて‘2’または‘3’
Device Custom String 1 Label	‘Collector Host Name’
Device Custom String 1	<コレクターホスト名>
Device Custom String 2 Label	‘Collector Domain Name’
Device Custom String 2	<コレクタードメイン名>
Device Custom String 5 Label	‘Collector Operating System Version’
Device Custom String 5	<コレクターオペレーティングシステムバージョン>

「コレクターステータス更新」のホストステータス

フィールド	説明
Event Name	‘Collector Status Updated’
Device Host Name	<デバイスホスト名>
Reason	<成功ステータス/失敗理由>
Device Event Category	理由に応じて‘/Informational’または‘/Informational/Warning’
Agent Severity	理由に応じて‘2’または‘3’
Device Custom String 1 Label	‘Collector Host Name’
Device Custom String 1	<コレクターホスト名>
Device Custom String 2 Label	‘Collector Domain Name’
Device Custom String 2	<コレクタードメイン名>
Device Custom String 5 Label	‘Collector Operating System Version’
Device Custom String 5	<コレクターオペレーティングシステムバージョン>

「コレクターステータス更新」のイベントログステータス

フィールド	説明
Event Name	‘Collector Status Updated’
Device Host Name	<デバイスホスト名>
Device Custom String 3 Label	‘Event Log’
Device Custom String 3	<設定されたイベントログ名>
Reason	<成功ステータス/失敗理由>
Device Event Category	理由に応じて‘/Informational’または‘/Informational/Warning’
Agent Severity	理由に応じて‘2’または‘3’
Device Custom String 1 Label	‘Collector Host Name’
Device Custom String 1	<コレクターホスト名>
Device Custom String 2 Label	‘Collector Domain Name’
Device Custom String 2	<コレクタードメイン名>
Device Custom String 5 Label	‘Collector Operating System Version’
Device Custom String 5	<コレクターオペレーティングシステムバージョン>

コレクターイベント収集開始

「コレクター収集開始」のコレクターステータス

フィールド	説明
Event Name	‘Collector Collection Started’
Reason	<成功ステータス/失敗理由>
Device Event Category	理由に応じて‘/Informational’または‘/Informational/Warning’
Agent Severity	理由に応じて‘2’または‘3’
Device Custom String 1 Label	‘Collector Host Name’
Device Custom String 1	<コレクターホスト名>
Device Custom String 2 Label	‘Collector Domain Name’
Device Custom String 2	<コレクタードメイン名>
Device Custom String 5 Label	‘Collector Operating System Version’
Device Custom String 5	<コレクターオペレーティングシステムバージョン>

「コレクター収集開始」のホストステータス

フィールド	説明
Event Name	‘Collector Collection Started’
Device Host Name	<デバイスホスト名>
Reason	<成功ステータス/失敗理由>
Device Event Category	理由に応じて‘/Informational’または‘/Informational/Warning’
Agent Severity	理由に応じて‘2’または‘3’
Device Custom String 1 Label	‘Collector Host Name’
Device Custom String 1	<コレクターホスト名>
Device Custom String 2 Label	‘Collector Domain Name’
Device Custom String 2	<コレクタードメイン名>
Device Custom String 5 Label	‘Collector Operating System Version’
Device Custom String 5	<コレクターオペレーティングシステムバージョン>

「コレクター収集開始」のイベントログステータス

フィールド	説明
Event Name	‘Collector Collection Started’
Device Host Name	<デバイスホスト名>
Device Custom String 3 Label	‘Event Log’
Device Custom String 3	<設定されたイベントログ名>
Reason	<イベント収集成功ステータス/失敗理由>
Device Event Category	理由に応じて‘/Informational’または‘/Informational/Warning’
Agent Severity	理由に応じて‘2’または‘3’
Device Custom String 1 Label	‘Collector Host Name’
Device Custom String 1	<コレクターホスト名>
Device Custom String 2 Label	‘Collector Domain Name’
Device Custom String 2	<コレクタードメイン名>
Device Custom String 5 Label	‘Collector Operating System Version’
Device Custom String 5	<コレクターオペレーティングシステムバージョン>

付録C Microsoft Windows Event Log Nativeコネクターと Unifiedコネクターの機能比較

ここでは、SmartConnector for Microsoft Windows Event Log - NativeとSmartConnector for Microsoft Windows Event Log - Unifiedの機能の比較を行います。

Nativeコネクターは、ArcSightのWindowsイベントログ収集用SmartConnectorです。このコネクターは、Microsoftのネイティブテクノロジーを利用し、幅広い機能を備えていますが、インストールできるのはWindowsシステムのみです。

Unifiedコネクターは、ArcSightの従来のWindowsイベントログ収集用SmartConnectorです。このコネクターは、WindowsシステムとUnixシステムの両方にインストールできるポータブルコネクターです。これは、Javaで実装したWindowsロギングテクノロジー (JCIFS) を用いて実現されています。このため、コネクターはJCIFSの機能の制約を受けます。

Windows Event Log - NativeおよびUnifiedコネクターの機能比較

機能	Nativeコネクター	Unifiedコネクター
スケーラビリティ	スケーラビリティが向上しています。「プル」ではなく「プッシュ」を使用します。ラウンドロビンを使用せず、遅いデバイスや応答のないデバイスで「ハング」しません。イベントソースのバランシングが必要ありません。	ラウンドロビンシーケンスでイベントをプルします (ラウンドロビンはイベントのバッチの収集元のホストに適用されます)。 遅いソースや応答のないソースをポーリングする際に遅延が発生します。
事前フィルタリング	送信サーバーで事前フィルタリングを行います。これにより、帯域幅が節約され、コネクターのパフォーマンスが向上します。たとえば、ログオン失敗 (イベントID 4625など) のみを把握したい場合、その他のイベントをコネクターに収集する必要はありません。	事前フィルタリングを行いません。
IPv6スタック	IPv6スタックで完全に実行できます。	IPv6スタックはサポートされていません。
SMBv2およびSMBv3	SMBv2およびSMBv3をサポートしており、セキュリティとパフォーマンスが強化されています。	SMBv1のみに制限されます。
設定の容易さ	Windowsオプションや設定オプションの数が少なく、設定が容易です。1つの画面に、Windowsイベント転送 (WEF) の使用を含む、一般的な実装に必要なすべての設定が含まれます。	設定でより多くのWindowsオプションや設定オプションが必要です。

機能	Nativeコネクター	Unifiedコネクター
転送されたイベント	ForwardedEventsログから収集します。これはWEFサブスクリプションを設定する場合のデフォルト設定です。	セキュリティ/アプリケーション/システムの他は、HardwareEventsイベントログからのみリモートログを収集します。
カスタムイベントログ	AppLockerおよびWindows Defenderイベントを含む、任意のWindowsイベントログ内のイベントを読み込むことができます。 フレックスフレームワークにより、カスタムパーサーを容易に作成できます。	Windowsイベントログの読み込みに制限がありますが、WEFを使用するAppLockerイベントには回避策が存在します。
コネクターのインストールでサポートされるオペレーティングシステム	Windows	Windows、Linux
イベントログタイプ	[Windows ログ] の下の [セキュリティ]、[システム]、[アプリケーション] のイベントログ、および [アプリケーションとサービス ログ] の下のすべてのイベントログ	[Windows ログ] の下の [セキュリティ]、[システム]、[アプリケーション] のイベントログ
パーサーのサポート	Windows OSに依存しません。Nativeでは正しい解析を行うのにOS情報が必要ではないため、ソースホストOSバージョンの設定はオプションです。	Windows OS非依存ではありません。

SmartConnector for Windows Event Log - Nativeの制限事項

- Windowsのみで動作します。ArcMC、コネクターアプライアンス、またはLinux/Unix OSでは実行できませんが、ArcMCからリモートで管理できます。
- 64ビット版OSのみで動作します。

ドキュメントのフィードバックを送信

本ドキュメントについてのご意見、ご感想については、電子メールでドキュメント制作チームまでご連絡ください。このシステムで電子メールクライアントが設定されていれば、このリンクをクリックすることで、以下の情報が件名に記入された電子メールウィンドウが開きます。

構成ガイドに関するフィードバック (SmartConnectors)

本文にご意見、ご感想を記入の上、[送信] をクリックしてください。

電子メールクライアントが利用できない場合は、上記の情報をコピーしてWebメールクライアントの新規メッセージに貼り付け、arc-doc@hpe.com.宛にお送りください。

お客様からのご意見、ご感想をお待ちしています。