



Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnectorユーザーガイド

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

© Copyright 2017 Hewlett Packard Enterprise Development, LP

著作権と謝辞の完全な記述については、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>

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-contact-list
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

ドキュメントの改訂履歴

日付	説明
2017/08/15	<ul style="list-style-type: none"> Windowsプラットフォームでのインストールとサービスとしての実行に必要な管理者権限を追加しました。
2017/05/15	<ul style="list-style-type: none"> カスタマイズされたイベントフィルタリングのセクションを新たに追加しました。 CEF Syslog通知先の切断および再接続機能を追加しました。 クラウドおよびWebサービスコネクタがFIPS準拠と認定されていないことが追加されました。 Event BrokerとESMクライアント認証ステップに関するFIPSドキュメントの参照に関する注記を追加しました。 通知先パラメーターの説明を訂正しました。 FIPS準拠のSmartConnectorの付録に記載されている手順を更新しました。
2017/02/15	<ul style="list-style-type: none"> 通知先の設定のセクションを新たに追加しました。 Event Brokerの情報を更新し、新たに [コンテンツの種類] オプションを追加しました。 CEF通知先の情報を更新し、CEF 1.0オプションを追加しました。 FIPS情報を更新し、設定とインストールに関する付録を新たに追加しました。 必要なライブラリにLinuxを追加しました。
2016/11/30	<ul style="list-style-type: none"> Event Broker (CEF Kafka) レシーバーの情報を追加しました。 Kafkaキーの情報を追加しました。 IPv6のサポートを更新しました。 コネクタフィルタリング情報を追加しました。 FIPS Suite Bモードの有効化の情報を追加しました。 NSPデバイスプールリスナーの通知先を削除しました。
2016/06/30	構成と目次を更新しました。
2016/05/16	<ul style="list-style-type: none"> Logfuコマンドをコネクタ機能表に追加しました。 ベンダーイベントのマッピングに関する手順を更新しました。 コネクタのアンインストール手順を改善しました。 コネクタ設定の変更について、『ArcSight FlexConnector Developer's Guide』への参照を追加しました。 ArcSight Management Centerでのソフトウェアベースのコネクタリモート管理について、ユーザー名とパスワード管理を追加しました。 Kafkaをコネクタ通知先タイプに追加しました。
2015/11/17	<ul style="list-style-type: none"> SmartConnectorの名前が同じ場合に通知されるエラーメッセージを記載しました。
2015/09/30	<ul style="list-style-type: none"> 「FIPS準拠モードの有効化」と「コネクタのリモート管理の有効化」の手順を追加しました。
2015/08/14	<ul style="list-style-type: none"> Loggerプールの通知先に必要な証明書をインポートする方法と、Loggerプールのリモート管理がサポート対象外である情報を追加しました。 ArcSight Logger SmartMessage Pool (暗号化) 通知タイプの提供に関する一般的な情報。

日付	説明
2015/06/30	<ul style="list-style-type: none">• コネクターのインストールで使用するユーザー特権情報を追加しました。• ArcSight マネージャーと ArcSight Logger プールの通知先の章を追加しました。• CEF フォワードモードの説明を更新しました。
2015/03/31	<ul style="list-style-type: none">• 必要なライブラリリストの更新、サイレントモードでのコネクタインストールの手順の改善、.csv 通知先のフィールドを追加する手順の追加を行いました。
2015/02/16	<ul style="list-style-type: none">• 必要なライブラリと通知先フィルターテーブルを更新しました。• リモート管理の資格情報をデフォルト以外に変更する方法を追加しました。• ESM から Logger へのイベント転送に関する手順を更新しました。• AUP 更新パックの情報を更新および訂正しました。

目次

ドキュメントの改訂履歴	3
第1章: コネクタについて	10
コネクタによるデータ収集	12
ベンダーイベントへのマッピング	12
イベントのフィルタリングとアグリゲーション	13
コネクタタイプ	14
ファイルコネクタ	14
データベースコネクタ	15
APIコネクタ	16
SNMPコネクタ	16
Microsoft Windows イベントログコネクタ	17
syslogコネクタ	17
スキャナーコネクタ	19
FlexConnector	19
モデルインポートコネクタ	20
その他のコネクタ	20
複数のメカニズムを使用するコネクタ	20
特殊な形式のTCPを使用するコネクタ	20
ArcSight Management Center/コネクタアプライアンス	20
ArcSight Logger	21
第2章: 展開計画	22
展開の概要	22
サポート対象プラットフォーム	22
展開シナリオ	23
展開シナリオ1	23
展開シナリオ2	24
展開シナリオ3	25
展開シナリオ4	25
ストレージ要件の見積もり	25
ArcSightのターボモード	26

第3章: コネクターのインストール	28
実行ファイルを使ったコネクターのインストール	28
コマンドラインを使ったコネクターのインストール	29
サイレントモードでのコネクターインストール	29
ESMからのコネクターのアップグレード	32
アップグレードの注意事項	33
ローカルアップグレード	34
ESMからのリモートアップグレード	34
コネクターの実行	35
スタンドアロンモードでのコネクターの実行	35
Windowsサービスとしてのコネクターの実行	35
UNIXデーモンとしてのコネクターの実行	36
インストール時のユーザー権限 (UNIXのみ)	36
サービスとして実行	37
スタンドアロンモードでの実行	38
ESMでのコネクターの動作状態を確認	39
コネクターのアンインストール	39
Windowsホストテーブルの使用	40
テーブルパラメーター値の手動入力	40
CSVファイルのインポートとエクスポート	41
第4章: コネクターの設定	43
コネクターの変更	43
コネクターの変更	43
コネクターパラメーターの変更	44
通知先の追加、変更、削除	44
通知先パラメーターの変更	45
通知先設定の変更	46
通知先の再登録	46
フェイルオーバー通知先の追加	47
サービスとしてのインストール	47
グローバルパラメーターの設定	48
その他の設定	50
FIPS Suite Bモードの有効化	50
ESMへのイベント送信時のネットワーク帯域幅の低減	50
ArcSightコンソールを使ったデフォルト設定と代替設定の定義	51
イベントフィルタリングのカスタマイズ	52

機能の使用	52
Java正規表現	54
ステータスの取得	54
パターンの例	55
agent.log内のログメッセージ	57
第5章: ArcSight Management Center/コネクタアプライアンスとコネクタ	58
ArcSight Management Center/コネクタアプライアンスでのコネクタ管理	58
ローカル (オンボード) コネクタ	59
リモートArcSight Management Center/コネクタアプライアンスの コネクタ	59
ソフトウェアベースコネクタ	59
ソフトウェアベースコネクタのリモート管理で使用するログイン資格情報	60
展開シナリオの選択	60
ArcSight Logger	61
ArcSight ESM	61
ESMとLogger	61
第6章: コネクタの通知先の概要	62
コネクタの通知先	62
ArcSight Manager (encrypted)	62
ArcSight Logger SmartMessage (encrypted)	63
ArcSight Logger SmartMessage Pool (encrypted)	63
CEF File	63
Event Broker	63
CEF Syslog	63
CEF Encrypted Syslog (UDP)	64
CSV File	64
Raw Syslog	64
通知先の追加	64
フェイルオーバー通知先	65
第7章: 通知先の設定	66
SmartConnectorのフィルター条件の管理	77
第8章: ArcSightマネージャー通知先	79
ArcSightマネージャー (暗号化)	79

第9章: ArcSight Logger SmartMessage (暗号化) 通知先	82
Loggerからマネージャーへのイベント送信	82
Loggerへのイベント送信	83
Loggerとマネージャー両方へのイベント送信	85
ESMからLoggerへのイベント転送	87
Loggerでのコネクター設定	88
第10章: ArcSight Logger SmartMessageプール (暗号化) 通知先	89
Loggerプール通知先の設定	89
SmartMessage転送のpersistent設定	92
第11章: CEF通知先	93
CEFファイル.....	93
ファイルローテーション	94
Event Broker	94
CEF Syslog.....	97
再接続による負荷分散.....	99
CEF Encrypted Syslog (UDP).....	100
第12章: CSVファイル通知先.....	102
CSVファイルのインストール	102
イベントデータのローテーション	104
第13章: Raw Syslog通知先	105
Raw Syslogの概要	105
付録A: ArcSight Update Pack (AUP).....	106
ArcSightコンテンツAUP.....	106
ESM.....	106
ESM/Logger	107
コネクター	107
Logger	107
コネクターアプライアンス	107
ArcSight Management Center	108
ESMによって生成されたAUP	108
ユーザー分類更新	108

システムゾーン更新	109
ユーザーゾーン更新.....	109
付録B: FIPS準拠のSmartConnector.....	110
FIPSとは.....	110
サポート対象のコネクタ	110
FIPS準拠のコネクタ	110
FIPS非準拠のコネクタ.....	111
FIPS準拠と認定されていないコネクタ	111
コネクタに関する注意事項.....	111
CEF Syslogを通知先として選択した場合	111
Microsoft SQL JDBCドライバー.....	112
FIPSサポートの有効化.....	112
手動でのFIPSモード有効化	112
手動でのFIPS Suite Bサポート有効化	112
パスワード管理	113
ストアの値	113
agent.propertiesファイルのエントリ	113
付録C: コネクタのFAQ	115
ドキュメントのフィードバックを送信	121

第1章: コネクタについて

この章では、ArcSightコネクタの概要を示し、イベント（ベンダーデバイスが生成）を収集してArcSight ESMマネージャーやLoggerなどの通知先に送信する方法を説明します。

コネクタとは、セキュリティデバイスからRAWイベントを収集し、そこからArcSightセキュリティイベントを生成して、通知先デバイスに転送するアプリケーションです。コネクタは、マネージャーと、ESM関連データを生成するネットワークデバイスとの間にあるインターフェイスとして機能します。

コネクタは、ネットワークデバイスから収集したイベントデータを正規化します。まず値（緊急度、優先順位、タイムゾーンなど）を共通の形式に正規化し、さらにデータ構造を共通のスキーマに正規化します。コネクタは、イベントのフィルタリングとアグリゲーションにより、マネージャーやArcSight Loggerなどの通知先への送信データ量を低減します。その結果、ArcSightの効率化とイベント処理時間の短縮が可能になります。

注: 各SmartConnectorの構成ガイドには、ArcSight Quality Assuranceによるテストが完了したデバイスのバージョンが記載されています。これは、一般的に認定デバイスとみなされます。各認定バージョンの間に提供されているマイナーバージョンについては、これまでの経験から、イベント生成メカニズムに大きな変更点はないと考えることができます。したがって、マイナーバージョンのデバイスもサポート対象です。必要に応じて、パーサーオーバーライドによる若干の調整が可能です。たとえば、Extreme Networks Dragon Export Toolバージョン7.4および8.0は認定済みなので、Dragon Export Toolバージョン7.5もサポート対象とみなされます。

コネクタの特徴をまとめます。

- 必要なデータをすべてソースデバイスから収集するため、調査や監査のためにデバイスを確認し直す必要がなくなります。
- 個々のイベントを解析し、イベントデータをESMマネージャーで使用できるように、イベントの値（緊急度、重要度、タイムゾーンなど）を共通のスキーマ（形式）に正規化します。
- 分析不要なデータをフィルターで除外することで、ネットワーク帯域幅とストレージ容量を節約します（オプション）。
- イベントアグリゲーションを使って、ESMマネージャーに送信するイベント件数を低減します。これにより、ArcSightの効率化とイベント処理時間の短縮を図ります（オプション）。
- 人間が判読可能な共通のフォーマットを使用してイベント进行分类します。これらのイベントカテゴリを活用することで、フィルター、ルール、レポート、データ監視を簡単に作成できるようになります。
- 処理されたイベントをESMマネージャーに渡します。

一部のネットワークデバイスでは、コネクタがデバイスに対してコマンドを発行することがあります。このようなアクションは、手動実行のほか、ルールや一部のデータ監視による自動実行が可能です。

コネクタが正規化してESMマネージャーに送信されたイベントは、中央のESMデータベースに格納されます。ESMは、イベントをフィルター処理し、ルールと相互相関させることでメタイベントを生成します。メタイベントは、対応するナレッジベース記事と一緒に管理者に自動送信されます。ナレッジベース記事には、社内ポリシーおよび手続きに沿った情報が記載されています。

コネクタは、エンタープライズ環境内にある各種ベンダーデバイスが生成したRAWデータを処理します。デバイスには、ルーター、メールサーバー、アンチウイルス製品、ファイアウォール、侵入検知システム (IDS)、アクセス制御サーバー、VPNシステム、アンチDoSアプライアンス、オペレーティングシステムログなど、セキュリティの検知や監査情報の報告を行うデバイスが含まれます。

コネクタは、異種混在の多様な情報を大量に収集します。コネクタは、このように多岐にわたるイベント情報を、共通のArcSightメッセージ形式に正規化します。これにより、すべてのイベントを対象に、同じイベントフィールドを使った検索、ソート、比較、分析を実行できるようになります。

各コネクタの構成ガイドには、個々のベンダーデバイスに関するデバイスとESMイベントのマッピング情報、インストールパラメーター、設定情報が記載されています。

次の表は、変更可能な通知先設定の一覧です。コネクタがイベントに対して実行する機能です。詳細については、「[通知先の設定](#)」を参照してください。

機能	説明
フィルタリングとデータの削減	AND/ORを使ったブール演算によって、デバイスから収集するデータと除外するデータ、通知先に送信するタイミングを指定します。
アグリゲーション	所定の値に一致するイベントを1つのイベントに集約することで、評価対象となるイベント件数を減らします。
一括転送処理	イベントをまとめて (都度送信ではなく) 一括送信することで、通知先のパフォーマンスを向上します。
時刻エラー補正	デバイスとコネクタ間、コネクタと通知先間で時刻を同期します。
タイムゾーン補正	必要に応じてローカルタイムゾーンを補正し、デバイス時刻のクエリ、関連付け、フィルター処理をサポートします。
カテゴリャー	通知先のカテゴリをイベントに割り当てます。
リゾルバー	デバイスが報告したホスト名とアドレスの解決と逆解決を行います。
データ正規化	デバイスが生成したイベントを、通知先で共通のイベント形式のメッセージ (ArcSightメッセージ) に変換します。
Logfuコマンド	HTMLレポート (logfu.html) を生成してログデータを時系列にグラフィカル表示することで、問題のトラブルシューティングのためにログファイルを分析します。Logfuは、問題が発生した時間をピンポイントで特定し、多くの場合は原因を特定します。 PuTTYを使用する場合は、Linuxマシンへの接続に使用するマシン上でX11クライアントを稼働する必要があります。

ヒント: コネクターは、デバイス、別のホストマシン、通知先システムがインストールされているホストマシンに展開できます。

コネクターは、ネットワークデバイスから情報を受信する操作と、情報を取得する操作の両方を実行できます。デバイスが情報を送信する場合、コネクターは情報を受信します。デバイスが情報を送信しない場合、コネクターはデバイスから情報を取得します。

コネクターは、受信したイベントにデバイス情報とイベント情報を付加し、メッセージを完成します。このメッセージは、設定されている通知先に送信されます。

コネクターによるデータ収集

コネクターとは、ネットワーク製品やセキュリティ製品との連携を目的に開発された製品であり、シンプルなログの転送と解析、ネイティブデバイスへの直接インストール、SNMP、syslogなど、さまざまな方法をサポートします。

次のように、幅広いデータ収集とイベントレポート形式をサポートしています。

- ログファイルリーダー (テキストファイルやログファイルなど)
- Syslog
- SNMP
- データベース
- XML
- 独自仕様のプロトコル (OPSECなど)

ArcSight ESMコンソール、ESMマネージャー、コネクターは、HTTP (HyperText Transfer Protocol) over SSL (Secure Sockets Layer: HTTPS) を介して通信します。

コネクターは、次のタイプのベンダーデバイスで使用できます。

- ネットワークおよびホストベースのIDSおよびIPS
- VPN、ファイアウォール、スイッチデバイス
- 脆弱性管理およびレポートシステム
- アクセスおよびID管理
- オペレーティングシステム、Webサーバー、コンテンツ配信、ログコンソリデーター、アグリゲーター

ベンダーイベントへのマッピング

コネクターは、ネットワークデバイスがログに記録したベンダー固有のイベントフィールドを収集します。このフィールドは、ArcSight ESMスキーマに基づいて、コネクター内にあるArcSightデータフィールドにマッピングされてから、設定された通知先に転送されます。

コネクタのデータフィールドと、ベンダー固有のイベント定義間のマッピングについては、各デバイス用コネクタの構成ガイドを参照してください。たとえば、SmartConnector for Cisco PIX/ASA Syslogのマッピングは、SmartConnector for Cisco PIX/ASA Syslogの構成ガイドに記載されています。

ArcSight共通イベントフォーマットのコネクタに一般的に適用されるマッピングは、『ArcSight Common Event Format (CEF) Guide』(『Implementing ArcSight Common Event Format (CEF)』)を参照してください。このドキュメントには、<https://www.protect724.hpe.com/docs/DOC-1072>からアクセスできます。

認定CEFベンダーのコネクタに適用されるマッピングについては、製品ドキュメントを参照してください。Protect 724のHPE Enterprise Security Technology Alliancesサイト (<https://www.protect724.hpe.com/community/technology-alliances>) からアクセスできます。

イベントのフィルタリングとアグリゲーション

フィルター条件とは、通知先に送信するイベントを選別するための条件であり、SmartConnectorのインストールと設定で追加できます。たとえば、フィルターを使用することによって、ネットワークデバイスや脆弱性スキャナーが生成したイベントを、その特性に基づいて取捨選択できます。コネクタのフィルタリング条件を満たしていないイベントは、転送されません。

コネクタは、回数または時間制限を指定することで、特定のフィールドセット内の値が同じイベントをアグリゲート (集計とマージ) する設定が可能です。

コネクタのアグリゲーションでは、一致する値を持つ複数のイベントが1つのイベントにマージされます。アグリゲートされたイベントには、イベントに共通する値と、最も早い開始時刻と最も遅い最終時刻のみが含まれます。これにより、評価が必要なイベント数を減らすことができます。

たとえば、特定のソースIP/ポート、通知先IP/ポート、イベント、デバイスアクションについて、イベントが30秒間に10回発生するという条件で、イベントアグリゲーションを設定した場合を考えてみましょう。コネクタが、この時間内に値が一致するイベントを10件受信した場合、この10件が1つのイベントに集約されます (アグリゲートされたイベント数は10)。

30秒が経過した時点で条件に一致したイベントが2件しかない場合、この2件が1つのイベントに集約されます (アグリゲートされたイベント数は2)。30秒間に900件の一致イベントを受信した場合、アグリゲーションイベントが90件生成されます (それぞれアグリゲートされたイベント数は10)。

ファイアウォールは複数のデバイスから類似するデータを含むイベントを大量に受信する点で、アグリゲーションの対象として適していると言えます。

イベントのフィルタリングについては、「[イベントフィルタリングのカスタマイズ](#)」を参照してください。

コネクタタイプ

コネクタはネットワーク上で、ESMマネージャーと、ESM関連データを生成するネットワークデバイスとの間にあるインターフェイスとして機能します。

一般的に、コネクタには次のような種類があります。

- APIコネクタ
- データベースコネクタ
- FlexConnector
- ファイルコネクタ
- Microsoft Windowsイベントログコネクタ
- モデルインポートコネクタ
- スキャナーコネクタ
- SNMPコネクタ
- Syslogコネクタ

コネクタは、ネットワークデバイスから収集したイベントデータを正規化します。まず値（緊急度、優先順位、タイムゾーンなど）を共通の形式に正規化し、さらにデータ構造を共通のスキーマに正規化します。コネクタでイベントのフィルタリングとアグリゲーションを行うことにより、通知先への送信データ量を削減できます。その結果、イベント処理の効率化と時間短縮が可能になります。

インストールに関する情報、各デバイスでの設定とマッピングについては、各デバイスのコネクタ構成ガイドを参照してください。

ファイルコネクタ

ログファイルコネクタには、**リアルタイム**と**フォルダーフォロワー**という2つのタイプが存在します。

リアルタイム

名前が変更されないログファイル、または現在の日付などに基づいて名前が変更されるログファイルをフォローします。リアルタイムファイルコネクタは、コネクタが監視するファイルの数によって分類され、1つのログファイルを監視するものと、複数のログファイルを監視するものがあります。

リアルタイムログファイルコネクタで読み取り可能なログファイルは、改行文字で行が分割されている通常のログファイルと、複数の固定長レコードが含まれる1行だけで構成されるログファイルです。

フォルダーフォロワー

フォルダーにコピーされたファイルを監視します。フォルダー内にある1つのログファイルを監視するものと、複数のログファイルを再帰的に監視するものがあります。

このコネクタでサポートされるファイルタイプは .txt と .xml であり、どちらのタイプかはデバイスに依存します。Nessus や NeXpose といったスキャナーファイルコネクタは、ほとんどが XML 形式です。

1つのデバイスに両方のコネクタが存在する場合を除き、ログファイルコネクタのタイプはコネクタ名に含まれていないのが一般的です。

ファイルコネクタはデバイスマシン上にインストールされるのが一般的ですが、監視対象ファイルへのアクセスがネットワーク共有や NFS マウント経由で発生する場合、リモートマシンにインストールされることもあります。

コネクタによっては、ファイルが処理可能な状態であることをコネクタに通知するために、トリガーファイルが必要になることがあります。一般的に、トリガーファイルには、拡張子だけが異なる同じ名前が割り当てられます。ファイルはデフォルトで、.processed、.processed.1 などのように増分値が付いた名前に変更されます。

通常、インストール時に必要になるパラメータは、ログファイルが格納されている場所 (絶対パス) のみです。デフォルトのファイルパスがわかっている場合、インストールウィザードに表示されます。

注: ログファイルの名前変更や削除には、ファイルフォルダに対する権限が必要です。

データベースコネクタ

データベースコネクタは、SQL クエリを使用して定期的にイベントのポーリングを行います。このコネクタは、MS SQL、MS Access、MySQL、Oracle、DB2、Postgres、Sybase など、一般的なデータベースタイプをサポートします。

インストール時に起動するウィザードでは、少なくとも次のパラメータ値の入力が必要です。

- JDBC ドライバー
- JDBC データベース URL
- データベースユーザー
- データベースパスワード

データベースユーザーには、データベースへのアクセス権限と読み取り権限が必要です。SQL Server Audit DB や Oracle Audit DB をはじめとする監査データベースコネクタには、システム管理者の権限が必要です。

単一データベースのイベント収集を行うコネクタだけでなく、Microsoft SQL Server Multiple Instance DB コネクタなど、複数のデータベースイベントをサポートするコネクタもあります。また、McAfee Vulnerability Manager DB など、スキャナーデータベースからイベントを収集するコネクタもあります。

データベースコネクタには、次の3つのタイプがあります。

時間ベース

時刻フィールドに基づいて、最後にクエリを実行した時刻から現在時刻までの範囲でイベントを取得します。

IDベース

増分されるIDフィールドに基づいて、最後にチェックしたIDから最大のIDまでの範囲でイベントを取得します。

ジョブIDベース

ジョブID (増分値である必要はありません) に基づいてイベントを取得します。処理対象となるのは追加された新しいジョブIDのみです。上記の2つのタイプとは異なり、ジョブIDベースのデータベースコネクタは、インタラクティブモードと自動モードのいずれかで実行できます。

APIコネクタ

APIコネクタは、標準または独自仕様のAPIを使用して、デバイスからイベントを収集します。ほとんどの場合、デバイスにアクセスするコネクタの認証に必要な証明書をデバイスからインポートする必要があります。また、デバイス側でも設定ステップをいくつか実行する必要があります。

インストール中、次のパラメーターが必要です。ただし、各デバイスのパラメーターのタイプはAPIによって異なります。

- デバイスIP
- サービスポート
- 取得するイベントタイプ
- 証明書情報
- API固有の情報

SNMPコネクタ

SNMPトラップには可変のバインディング情報が含まれ、それぞれにさまざまなイベント情報が格納されています。この情報はUDP経由でポート162に送信されます。ただし、ポートは変更可能です。

SNMPコネクタはポート162 (または設定された他のポート) をリッスンし、取得したトラップを処理します。処理対象は、一意のエントプライズOIDを持つ単一デバイスから取得したトラップのみですが、複数のトラップタイプを取得することが可能です。

SNMPはUDPを使用するので、ネットワーク転送中にイベントが損失する可能性がないとは言えません。

専用のSNMPコネクタもありますが、SmartConnector for SNMP UnifiedがほとんどのSNMPをサポートします。パーサーは、MIB情報をもとにイベントフィールドのマッピングを行いますが、他のSNMPベースアプリケーションとは異なり、コネクタ自体はMIBのロードは不要です。

Microsoft Windows イベントログコネクタ

Windows イベントログは、システム管理者がトラブルシューティングに使用するログです。イベントログ内のエントリには、**エラー**、**警告**、**情報**に加えて、**監査の成功**、**監査の失敗**という重要度が割り当てられています。

デフォルトのWindows イベントログは、次の3つです。

- アプリケーションログ (登録アプリケーションで発生したログを追跡)
- セキュリティログ (セキュリティの変更とセキュリティ違反の可能性を追跡)
- システムログ (システムイベントを追跡)

Microsoft Windows イベントログには、次の2つのコネクタが提供されています。

- **SmartConnector for Microsoft Windows Event Log - Native** および **SmartConnector for Microsoft Windows Event Log - Unified**: この2つのコネクタは、単一ドメインまたは複数ドメインのローカルマシンまたはリモートマシン (Windows または Windows 以外) に接続し、セキュリティおよびシステムイベントを取得して処理します。

Unified コネクタの詳細は、SmartConnector for Microsoft Windows Event Log - Unified の構成ガイドを参照してください。マッピングについては、『SmartConnector for Microsoft Windows Event Log - Unified Windows 2008/2012 Security Event Mappings』を参照してください。Native

コネクタの詳細については、SmartConnector for Microsoft Windows Event Log -- Native の構成ガイドを参照してください。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。

上記のコネクタは、すべてのシステムおよびアプリケーションイベントを対象に、Windows イベントヘッダーに基づく部分的なイベント解析をサポートしています。また、FlexConnector に類似したフレームワークをサポートし、すべてのシステムおよびアプリケーションログでイベントの説明を解析する独自パーサーの作成と展開も可能です。

一部のWindows イベントログアプリケーションは、Windows イベントログアプリケーションまたはシステムサポートが開発された Microsoft Windows Event Log - Unified コネクタと Microsoft Windows Event Log - Native コネクタによってサポートされます。コネクタがサポートするアプリケーション/システムイベントのリストは、構成ガイドを参照してください。

syslog コネクタ

syslog メッセージは自由形式のログメッセージで、数値コード (ファシリティと重要度)、タイムスタンプ、ホスト名で構成される syslog ヘッダーがプレフィックスとして付加されています。syslog デモン、パイプ、ファイルのコネクタとしてインストール可能です。syslog コネクタは他のコネクタとは異なり、複数のデバイスからイベントを取得し、処理することができます。デバイスの識別には、一意の正規表現が使用されます。

- **Syslog Daemon** コネクタは、設定可能なポートで syslog メッセージをリスンします。デフォルトポートは514です。デフォルトプロトコルはUDPですが、Raw TCPなどのプロトコルもサポート対象です。Windows プラットフォームで syslog に使用できるのはこのコネクタのみです。

- **Syslog Pipe**コネクタは、syslogのファシリティと重要度が記載されたメッセージを送信する設定が必要です。
SolarisプラットフォームでSyslog Pipeコネクタを使用すると、パフォーマンスが低下する傾向があります。オペレーティングシステムは、コネクタ (リーダー) でパイプファイルへの接続を開いてから、syslogデーモン (ライター) でメッセージを書き込む必要があります。Solaris環境でroot以外のユーザーとしてコネクタを実行する場合、Syslog Pipeコネクタはお勧めしません。syslogデーモンにHUP信号を送信する権限がないからです。
- **Syslog File**コネクタは、syslogのファシリティと重要度が記載されたメッセージを送信する設定が必要です。Syslog Fileコネクタはスループットが高く、Syslog Pipeコネクタよりも優れたパフォーマンスを発揮します。パイプ転送ではオペレーティングシステムのバッファ制限が適用されたためです。
- **Raw Syslog**コネクタは、一般的には解析を行わず、syslog文字列を取得してそのままrawEventフィールドに格納します。Raw Syslogの通知先はrawEventフィールドを取得し、選択したプロトコル (UDP、Raw TCP、TLSのいずれか) を使ってそのまま送信します。Raw Syslog通知先には、必ずRaw Syslogコネクタを使用します。イベントフローを合理化するために、付加価値のないコンポーネントは除外されます (たとえば、Raw Syslog転送の場合、イベントのカテゴリフィールドは無視されるので、分類コンポーネントは転送されません)。ArcSight Loggerへのデータ転送では、設定パラメータを使用することにより、syslogデータ (ソースとタイムスタンプ) の正規化を最小限に抑えることができます。
- **Syslog NG Daemon**コネクタは、BSD syslog形式向けにSyslog NGバージョン3.0をサポートします。これにより、IETF標準イベントの収集がサポートされます。このコネクタでは、セキュアな (暗号化された) TLSチャネルを介して他のコネクタ (通知先をCEF Syslog over TLSと設定) からイベントを受信する操作と、デバイスからイベントを受信する操作が可能です。
- **CEF Encrypted Syslog (UDP)** コネクタは、CEF Encrypted Syslog (UDP) 通知先によって暗号化されたイベントを復号化することで、暗号化チャネルを介したコネクタ間通信を可能にします。ESMIはCEFコネクタにより、CEF標準のログを提供するアプリケーションとデバイスのイベントを対象に、syslog転送プロトコルを使った接続、集計、フィルター処理、関連付け、分析を実行できます。

UNIXは、すべてのsyslogコネクタをサポートします。syslogプロセスがすでに実行中の場合、プロセスを終了するか、別のポートでコネクタを実行することができます。

UDPは信頼性の高いプロトコルではないので、ネットワーク転送中にsyslogメッセージが失われる可能性が若干あります。一般的に、syslogコネクタのプロトコルとしてTCPがサポートされています。

基本的なsyslogコネクタであるUNIX OS Syslog向けのコネクタは、すべてのsyslogサブコネクタで使用できるベースパーサーを提供します。

syslogコネクタの展開に関する情報は、UNIX OS Syslog向けのコネクタ構成ガイドを参照してください。各デバイスでの設定情報とフィールドマッピングについては、各デバイスのコネクタ構成ガイドを参照してください。syslogサブコネクタには、それぞれ専用の構成ガイドが提供されています。

コネクタのインストール中、すべてのsyslogコネクタで、**Syslog Daemon**、**Syslog Pipe**、**Syslog File**のいずれかを選択してください。syslogサブコネクタの名前は表示されません。

スキャナーコネクタ

スキャナーコネクタには、結果をファイル内に保持するタイプとデータベースから取得するタイプの2つがあります。XMLスキャナーコネクタの結果はファイルに保持されるので、ログファイルコネクタとみなされます。

また、スキャンしたイベントをデータベースに格納するコネクタはデータベースコネクタと見なされます。したがって、データベースコネクタと同じインストールパラメーターが必要になります。

スキャンレポートはベースイベントに変換されます。ESM通知先の場合、ベースイベントはコンソールに表示されます。また、集約されたメタイベントはコンソールには表示されません。メタイベントは、コンソール上でアセット、アセットカテゴリ、オープンポート、脆弱性を生成します。

スキャナーコネクタは、2種類のモード (自動またはインタラクティブ) のどちらかで実行されます。

インタラクティブモード

設定されたログディレクトリからインポート可能なレポートやログファイルを、グラフィカルユーザーインターフェイスで表示します。ログファイルの **[Send]** チェックボックスをオンにし、**[Send to ArcSight]** をクリックして、コネクタに送信するレポートを選択します。

自動モード

自動プロシージャを使用して定期的にスキャンを実行するためのモードです。プロシージャであるシェルスクリプトは、スキャナーを定期的に実行し、レポートを .cef 形式で保存します。スキャンが完了してレポートが保存されると、`<レポート名>.cef_ready` という名前の空のファイルが作成されます。コネクタではこのファイルを検出することで、.cef レポートがインポート可能であることを認識します。次にコネクタは、.cef_ready ファイルを検索し、それに対応する .cef レポートを処理します。処理されたレポートは `<元のレポート名>.cef_processed` という名前に変更されます。

動作モード以外の、スキャナーのインストールに必要なパラメーター値は、ファイル/データベースコネクタの有無によって異なります。ファイルコネクタでは、ログファイルの絶対パスと名前が必要です。データベースコネクタについては、「[データベースコネクタ](#)」(15ページ) を参照してください。

FlexConnector

FlexConnectorは、サードパーティデバイスからの情報を読み込んで解析し、その情報をArcSightイベントスキーマにマッピングするカスタムコネクタです。カスタムコネクタの作成では、ESMマネージャーまたはLoggerにインポートするログファイルなどのソースの形式を識別するプロパティセット (構成ファイル) を定義します。

ソフトウェア開発キット (SDK) であるFlexConnectorフレームワークを使用することで、ネットワーク上のデバイスとそのイベントデータの専用コネクタを作成できます。FlexConnectorの詳細と使用方法については、『FlexConnector Developer's Guide』を参照してください。

モデルインポートコネクタ

モデルインポートコネクタは、デバイスからイベントを収集して転送するのではなく、ID管理システムのユーザーデータをArcSight ESMにインポートするコネクタです。モデルインポートコネクタの使用方法については、Protect724に掲載されている各コネクタの構成ガイドを参照してください。

モデルインポートコネクタは、データベースからユーザーID情報を抽出し、ESM内の次のリストにデータを入力します。

- IDロールセッションリスト
- ID情報セッションリスト
- アカウント/IDマップアクティブリスト

上記のリストは、動的に入力されます。つまり、Identity ManagerのIDデータが変更されると、セッションリストの更新時にリスト内のデータが更新されます。

その他のコネクタ

複数のメカニズムを使用するコネクタ

一部のコネクタは、複数のメカニズムを使用します。たとえば、Oracle Audit Database向けのコネクタは、データベーステーブルと監査ファイルの両方を監視します。

特殊な形式のTCPを使用するコネクタ

次のコネクタは、特殊な形式のTCPを使用します。

IP NetFlow (NetFlow/J-Flow)

Ciscoが定義したバイナリ形式で、TCPを介してデータを取得します。

ArcSight Streaming Connector

ArcSight独自形式で、TCPを介してLoggerからデータを取得します。

ArcSight Management Center/コネクタアプライアンス

ArcSight Management Center (ArcSight Management Center) は、コネクタアプライアンスの全機能に加えて、他のArcSight製品 (コネクタアプライアンス、Logger、他のArcSight Management Center) の管理と監視を行う機能も備えています。本ガイドでは、これらの製品をArcSight Management Center/コネクタアプライアンスと呼びます。

ArcSight Management Center/コネクタアプライアンスには、コネクタを一元管理する機能があり、ローカルとリモートのArcSight Management Center/コネクタアプライアンス上のコネクタと、リモートホストにインストールされているソフトウェアベースのコネクタの管理を統合します。

ArcSight Management Center/コネクタアプライアンスはオンボードコネクタを搭載し、イベントソースをLoggerやESMなどの通知先に接続します。

ArcSight Management Center/コネクタアプライアンスには次のような特徴とメリットがあります。

- すべてのコネクタの一括処理が可能です。マネージドセキュリティサービスプロバイダー (MSSP) など、大量のコネクタを実装しているESM環境に最適です。
- Loggerのみの環境で、ESMIに類似したコネクタ管理機能を提供します。
- 1つのインターフェイスで、コネクタの設定、監視、調整、更新を行います。ArcSight Management Center/コネクタアプライアンスは、管理対象のコネクタからイベントを取得する操作は実行しません。これにより、多数のコネクタを一度に管理できます。ArcSight Management Center/コネクタアプライアンスが、動作中のコネクタに影響を与えることはありません。ただし、設定の変更は可能で、コネクタを再起動することもあります。

ArcSight Management Center/コネクタアプライアンスがサポートする全コネクタのリストについては、『Connector Appliance Release Notes』を参照してください。Protect 724コミュニティサイト (<https://protect724.hpe.com>) にもアクセスできます。ArcSightには、新しいコネクタが定期的に追加されます。

詳細については、「[ArcSight Management Center/コネクタアプライアンスとコネクタ](#)」(58ページ) を参照してください。

ArcSight Logger

Loggerとは、極めて高いイベントスループットに最適化されたイベントデータストレージアプライアンスです。Loggerはセキュリティイベントを圧縮形式で保存しますが、訴訟対応のフォレンジックデータの要求に応じて、変更前のイベントをいつでも取得できます。

Loggerをスタンドアロン展開することで、syslogメッセージやログファイルからイベントを受信したり、コネクタから共通イベント形式 (CEF) のイベントを受信したりできます。Loggerは、ESMIにイベントを転送できます。複数のLoggerが連携することで、高いスループットを維持します。イベントクエリは、Loggerのピアネットワーク全体に分散されます。コネクタとLoggerの関係については、「[ArcSight Logger SmartMessage \(暗号化\) の通知先](#)」(82ページ) を参照してください。

第2章: 展開計画

コネクターは、ネットワークセキュリティエンタープライズ環境の要件に応じて展開する必要があります。ここでは、ArcSightの展開におけるさまざまなシナリオをご紹介します。

以下では、ESMをエンタープライズ環境に展開するシナリオをご紹介します。ただしこれはあくまでも例であり、他のシナリオや方法でもESMを展開することが可能です。

展開の概要

ArcSightコンポーネントのインストール方法は、UNIX、Windows、Macintoshの各プラットフォームで共通です。ESMソフトウェアは、ArcSightデータベース、マネージャー、コンソールなどのコンポーネントの専用ホスト上で、単一のルートディレクトリ配下のディレクトリツリーにインストールされます (ただし、DBMSなどのサードパーティ製ソフトウェアはこのディレクトリの配下にインストールする必要はありません)。このルートディレクトリのパスは、\$ARCSIGHT_HOMEで参照します。

コネクターのドキュメントでは、'current' ディレクトリは\$ARCSIGHT_HOMEの場所にあるとは見なされず、明確に記載されています。また、パスの区切り文字にはバックスラッシュ (\) が使用されています (たとえば、\$ARCSIGHT_HOME\current)。この表記はコネクターの構成ガイドと同じです。またこれは、コネクターが他のESMコンポーネントと同じマシンにはインストールされず、一般的にアクティビティの監視対象デバイスと同じマシンにインストールされることも表しています。

\$ARCSIGHT_HOME配下のディレクトリ構造は、コンポーネントとプラットフォーム間で標準化されています。通常、ArcSightソフトウェアは\$ARCSIGHT_HOME\current\binディレクトリに格納されています。ArcSight設定を管理するプロパティファイルは\$ARCSIGHT_HOME\configに格納され、ログファイルは\$ARCSIGHT_HOME\logsに出力されます。

コネクターは、エンタープライズ環境内のさまざまなベンダーデバイスが生成したデータを収集して処理します。デバイスには、ルーター、メールサーバー、アンチウイルス製品、ファイアウォール、侵入防御システム (IPS)、アクセス制御サーバー、VPNシステム、DoS対策アプライアンス、オペレーティングシステムログなど、セキュリティ脅威の検知や報告を行うデバイスが含まれます。

コネクターは、異種混在の多様な情報を大量に収集します。コネクターはイベントを受信すると、デバイス情報を付加したメッセージを生成し、各種ArcSightコンポーネントに転送します。

サポート対象プラットフォーム

サポート対象プラットフォームについては、各コネクターに付属の『ArcSight SmartConnector Platform Support』ドキュメントを参照してください。このドキュメントのサポート対象とは異なる点がある場合のみ、デバイスのコネクター構成ガイドに記載されています。

展開シナリオ

コネクタは、ESMマネージャーマシン、ArcSight Management Centerをホストするマシン、コネクタアプライアンス、ホストマシン、デバイスにインストールできます。また設定により、SNMP、HTTP、syslog、独自仕様のプロトコル (OPSECなど)、デバイスのリポジトリへの直接データベース接続 (ODBCまたは独自仕様のデータベース接続など) を使用して、ネットワーク経由でイベントを取得することができます。

最適な展開シナリオは、コネクタのタイプ、ネットワークアーキテクチャー、オペレーティングシステムによって決まります。

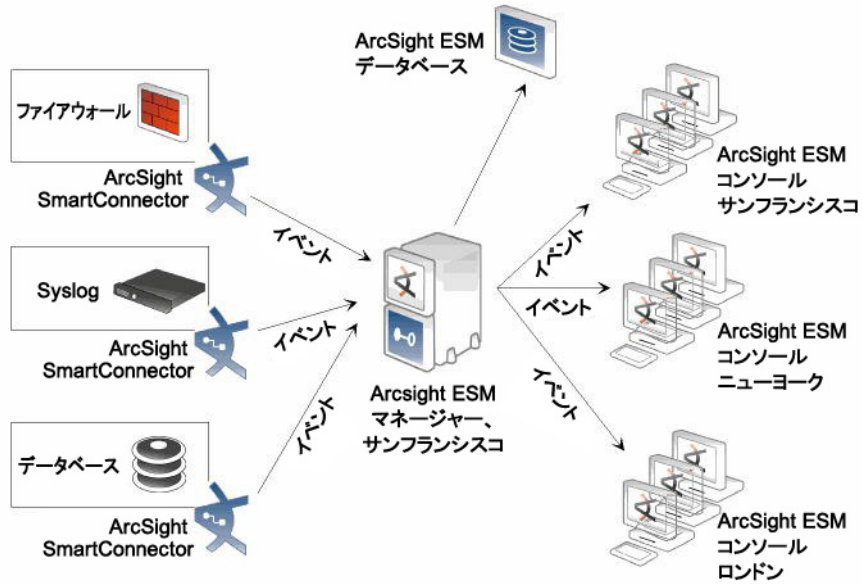
- syslogの展開シナリオは、『Connector for UNIX OS Syslog Configuration Guide』を参照してください。
- Windows Event Logコネクタの展開シナリオは、SmartConnector for Microsoft Windows Event Log UnifiedおよびNativeの構成ガイドを参照してください。

展開シナリオ1

このシナリオでは、ファイアウォール、IPS、UNIXオペレーティングシステムという異なる3つのデバイスで3つのコネクタが稼働しています。コネクタはデバイスまたはログから情報を取得し、キャプチャーしたイベントをコネクタ設定に基づいてマネージャーに送信します。

イベントを受信したマネージャーは、ルールに基づいてイベントを相互関連させ、データベースと、データベースにアクセスする全コンソールにメタイベントを送信します。

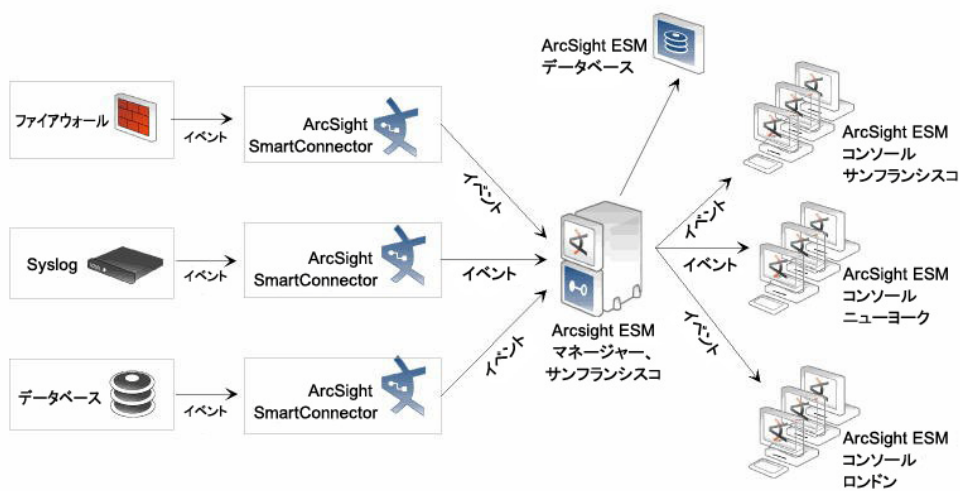
ESMマネージャーも、設定済みのアクションを実行できます。データベースに格納されているイベントとメタイベントを、[Replay] チャンネルを使って再生することで、イベント履歴の調査、分析、レポート作成が可能です。



3つのデバイスで3つのコネクタが稼働

展開シナリオ2

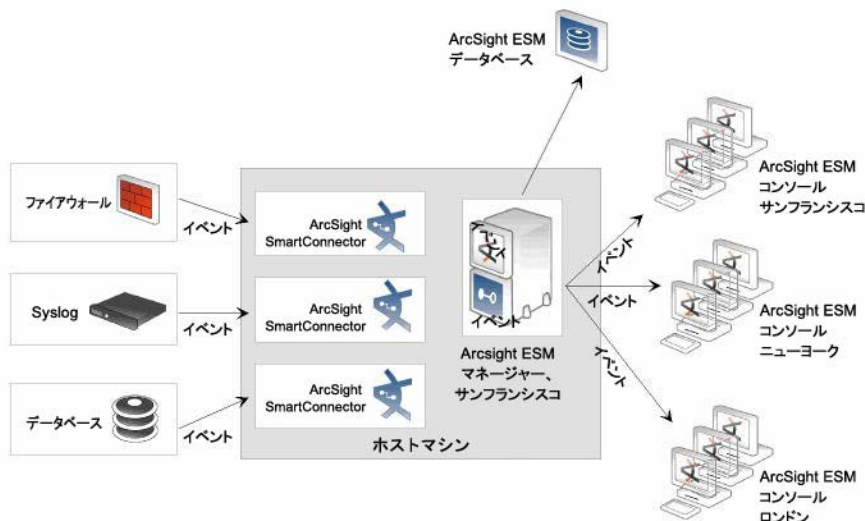
このシナリオはシナリオ1と同じですが、3つのコネクタがデバイスではなくホストマシンで稼働する点が異なります。コネクタはデバイス以外で稼働していても、デバイスから情報を取得することができます。コネクタはシナリオ1と同じように動作し、ArcSight ESMマネージャーとデータベースが同じ機能を実行します。



ホストマシンで3つのコネクタが稼働

展開シナリオ3

このシナリオでは、コネクタはホストマシンではなくESMマネージャーで稼働しますが、ネットワーク上のデバイスからイベントを取得します。ArcSightコネクタ、マネージャー、コンソールが実行する処理内容は、上記2つのシナリオと同じです。



ESMマネージャーで3つのコネクタが稼働

展開シナリオ4

このシナリオでは、上記のいずれかのシナリオに加えて、イベントをLoggerに送信するようにコネクタを設定します。LoggerからイベントをESMIに転送できます。

ストレージ要件の見積もり

日々発生するイベントのサイズを見積もるには、展開するデバイスとコネクタの範囲を明確にする必要があります。ログファイルのサイズは正確とは言えないので、平均的な1日に発生するイベントの件数を把握します。この件数はデバイスのタイプによって異なります。イベントのサイズだけでなく、各種アグリゲーションポリシーへの対応もデバイスタイプによって異なります。

イベント1件あたりの平均データサイズは、コネクタで**ターボモード** ([Fastest]、[Faster]、[Complete]) を指定しているかどうかによって変わります。ターボモードの詳細については、[次のページの「ArcSightのターボモード」](#)を参照してください。

トラフィックを低減する方法として、コネクタはイベントアグリゲーションを使用します。たとえば、あるイベントが500ミリ秒ごとに繰り返される場合、10秒ごとに発生する1つのイベントに集約すれば、20分の1に圧縮できます。イベントアグリゲーションを個々のコネクタで設定すれば、ESMマネージャーに転送されるイベントトラフィックを減らし、ESMデータベースのストレージ要求量を抑えることができます。

複数のESMマネージャーが動作する分散環境では、コネクタがESMマネージャーに送信するイベントと他のESMマネージャーから転送されるイベントの両方を考慮する必要があります。

ArcSightのターボモード

3種類のターボモードのいずれか ([**最速**]、[**より速く**]、[**完全**]) を選択すると、コネクタを介したセンサー情報の転送を加速できます。

[**最速**] モードでは、転送バイト数は最小になります。ファイアウォールなど、比較的イベントデータ量が少ないデバイスに最適です。[**より速く**] モードは、ESMマネージャーのデフォルトモードであり、ストレージ容量を節約できます。ネットワークオペレーティングシステムなどイベントが大量に発生するデータソースでは、[**完全**] モードをお勧めします。これは、コネクタのデフォルトモードです。[**完全**] モードでは、デバイスから取得したデータをすべて送信します。これには、カスタムデータやベンダー固有のデータ (追加データなど) が含まれます。

送信するイベントデータの量は、コネクタごとに設定できます。また、ESMマネージャーでは、コネクタ設定とは別に、読み取りおよび保存するイベントデータの量を設定できます。

一部のイベントは、他のイベントよりも多くのデータを必要とします。たとえば、オペレーティングシステムのログには、大量の環境データがキャプチャーされますが、セキュリティイベントに関連しないものも含まれています。これに対してファイアウォールは、通常は基本的な情報のみを報告します。

ArcSightでは、次のターボモードを指定できます。

モード	説明
最速 (モード1)	ファイアウォールなど、データ量が比較的少ないデバイスにお勧めします。
より速く (モード2)	ESMマネージャーのデフォルトモードです。スループットを最適化するために、コアのイベント属性以外のデータをすべて破棄します。イベントデータが小さいため、必要とされるストレージ容量が少なく、最高のパフォーマンスを実現できます。
完全 (モード3)	コネクタのデフォルトモードです。コネクタが取得したすべてのイベントデータ (追加データを含む) を保持します。

ターボモードが指定されていない場合は、モード3の完全モードがデフォルトモードとなります。バージョン3.0以前のESMは、**完全**モードで稼働します。

ESMマネージャーは、イベントデータの処理に特殊なターボモード設定を適用します。コネクタのターボモードがESMマネージャーよりも高い場合、コネクタはESMマネージャーの要求より多くのイベントデータを送信しますが、ESMマネージャー側ではこの余分なフィールドは無視されます。

これに対して、ESMマネージャーのターボモードがコネクタよりも高い場合、コネクタがESMマネージャーに送信するイベントデータが少なくなるため、ESMマネージャーにはイベントデータが空のフィールドが発生することになります。

ESMマネージャーの設定では幅広いコネクタ要件に対応する必要があるため、上記いずれのケースも実際によく発生します。

第3章: コネクターのインストール

コネクターのインストール準備が完了したら、監視対象となるデバイスに関する情報を各コネクターの構成ガイドで確認します。たとえば、Microsoft Windows イベントログ向けのコネクターをインストールする場合には、Microsoft Windows Event Log - Unified または Native のコネクター構成ガイドを参照してください。

構成ガイドには、インストールパラメーターの値、コネクターのイベント収集を有効化するためのデバイス設定、ESM フィールドへのイベントマッピングをカスタマイズする方法が記載されています。

注: Linux Red Hat 6.x 以降のプラットフォームを使用する場合には、次のライブラリをインストールしてから、コネクターをインストールしてください。

- Xライブラリ
- glibc
- libXext
- libXrender
- libXtst

32ビット版 SmartConnector の実行ファイルを64ビットマシンにインストールする場合には、64ビット版だけでなく、32ビット版の glibc、libXext、libXrender、libXtst もインストールする必要があります。

実行ファイルを使ったコネクターのインストール

インストールを実行すると、対象コネクターを指定する画面が表示されます。実行ファイルとドキュメントの zip ファイルをダウンロードしてください。コネクターごとに構成ガイドが提供されています。このガイドには、コネクターのインストール手順と関連デバイスの設定方法、ベンダーデバイスと ESM イベントのマッピング情報、インストールパラメーター、デバイス構成情報が記載されています。

また、『ArcSight SmartConnector Release Notes』も参照してください。リリースノートには、製品の new 機能、最新の更新、既知の問題と回避方法が記載されています。サポートされるオペレーティングシステムとプラットフォームの詳細については、『SmartConnector Platform Support』ドキュメントを参照してください。

注: 64ビット版の実行ファイルには、使用可能な SmartConnector の一部しか含まれていません。使用可能なコネクターについては、使用中のプラットフォーム向けの64ビット SmartConnector インストーラーで確認するか、『SmartConnector 64-Bit Support』ドキュメントを参照してください。このドキュメントは、Protect 724 から入手するか、HPE SSO サイトからダウンロード可能な『SmartConnector Configuration Guide』の zip ファイルに格納されています。

実行中の32ビット版SmartConnectorを64ビット版にアップグレードすることはできません。64ビット版SmartConnectorを実装するには、新規インストールが必要です。

インストールでは、通知先を指定する必要があります。デフォルトの通知先は、ArcSightマネージャー (暗号化) です。通知先の詳細については、「[コネクターの通知先の概要](#)」(62ページ) を参照してください。FIPS準拠のソリューションに関する情報は、各コネクターの構成ガイドを参照してください。[Parameters] ウィンドウに、選択したコネクターのパラメーターを入力します。パラメーターはデバイスによって異なります。詳しい説明は、各コネクターの構成ガイドに記載されています。

インストールするコネクターのディレクトリの場所、ファイル名、メニューオプション名を指定する際には、標準的な命名規則を使用することをお勧めします。1つのマシンに複数のコネクターをインストールする場合、コネクターはそれぞれ別のディレクトリにインストールするのが一般的です。

コネクターのインストールには、コマンドラインを使用する方法 (下記の「[コマンドラインを使ったコネクターのインストール](#)」) と、プロパティファイルの内容に基づいてウィザードに対応するサイレントモードを使用する方法 (下記の「[サイレントモードでのコネクターインストール](#)」) があります。

コマンドラインを使ったコネクターのインストール

グラフィカルユーザーインターフェイスウィザードを使用しないでコネクターをインストールするには、自己解凍アーカイブの起動時に、コマンドラインに「-i console」と入力します。コマンドウィンドウに表示される指示に従ってください。

インストールが正常に完了したら、runagentsetupを実行して、設定プログラムを手動で実行します。

サイレントモードでのコネクターインストール

コネクターは、サイレントモードでもインストールできます。このモードでは、ウィザードで必要な情報はプロパティファイルから提供されます。同一のコネクターを大量に展開する場合に便利です。

このモードを使用するには、最初にグラフィカルユーザーインターフェイスまたはコマンドラインを使用して、コネクターを1つインストールして設定しておく必要があります。最初のコネクターの設定時に、設定パラメーターをプロパティファイルに記録します。作成したプロパティファイルの設定情報を使用することで、他のコネクターをすべてサイレントモードでインストールできます。

ヒント: ArcSightでは、プロパティファイルを運用環境以外のシステムで作成してテストすることをお勧めします。

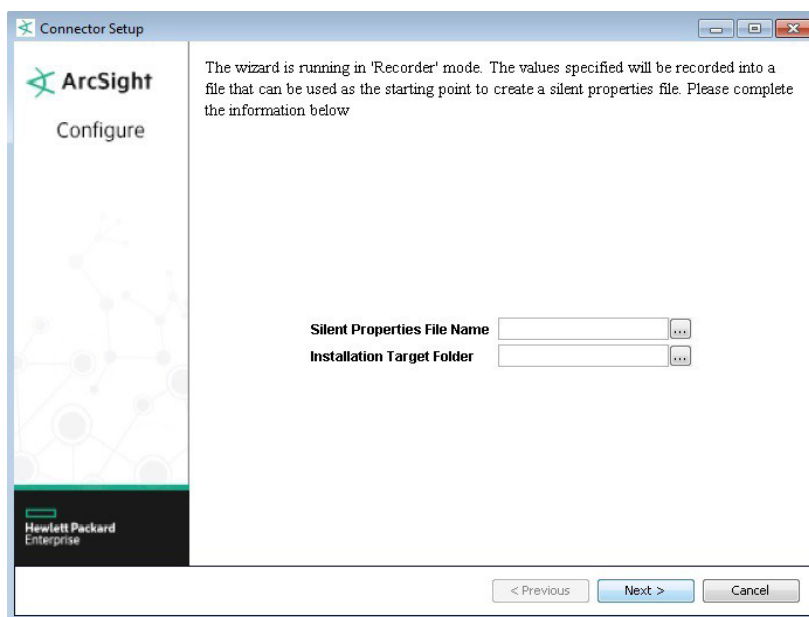
SmartConnectorの設定をプロパティファイルに記録するには、次の手順を実行します。

1. コネクターの設定ウィザードを実行し、コネクターのコアファイルを展開してインストールします。ウィザードで [Add a Connector] または [Set Global Parameters] が表示されたら、[Cancel] をクリックします。
2. コマンドプロンプトウィンドウから (ARCSIGHT_HOME\current\binディレクトリ)、次のコマンドを入力し、コネクターの設定ウィザードを記録モードで開きます。

UnixおよびLinuxの場合: `./runagentsetup.sh -i recorderui`

Windowsの場合: `runagentsetup.bat -i recorderui`

3. ウィンドウが開いたら、[Silent Properties File Name] にファイル名を入力します。[Installation Target Folder] でフォルダ一名を入力します。



4. コネクターの設定ウィザードの残りの画面もすべて同じように入力します。指定した場所に指定した名前のプロパティファイルが作成されます。

注: 作成されたプロパティファイルには、可読形式でパスワードが保存されています。

5. セットアッププロセスが完了したら、[Exit] を選択してから [Next] をクリックし、プロパティファイルが作成されたことを確認します。

SmartConnectorをサイレントモードでインストールしたいシステム上で、残りのステップを実行します。

1. サイレントモードでコネクターをインストールするシステムの設定と、プロパティファイルを作成したマシンの設定が同一であることを確認してください。設定が異なる場合、インストールは失敗します。
2. プロパティファイルを現在のシステムにコピーします。コピー先としては、インストールファイルをダウンロードしたディレクトリをお勧めします。
3. エディターでプロパティファイルを開きます。

4. ファイル内のUSER_INSTALL_DIRプロパティで、パスの値がコネクターのインストール先の絶対パスであることを確認します。

```
USER_INSTALL_DIR=C:\Program Files\ArcSightSmartConnectors
```

注: コロン (:) とバックスラッシュ (\) の前には、(\\) を置いてください。

5. ファイル内のARCSIGHT_AGENTSETUP_PROPERTIESプロパティで、パスの値がプロパティファイルのコピー先の絶対パスであることを確認します。

たとえば、プロパティファイルをC:\properties_files\silent.propertiesにコピーしている場合、パスの値は次のようになります。

```
ARCSIGHT_AGENTSETUP_PROPERTIES=C:\\properties_files\\silent.properties
```

6. 必要に応じてプロパティを変更します。たとえば、connectordetails.nameプロパティにはサイレントモードでインストールするコネクターの名前を指定します。次に、プロパティファイルの例を示します。

```
#=====
# Panel 'connectordetails'
#=====
# Enter the connector details.
#
# Name
connectordetails.name=The Name
# Location
connectordetails.location=The Location
# DeviceLocation
connectordetails.devicelocation=The Device Location
# Comment
connectordetails.comment=The Comment
#=====
```

プロパティファイル内のプロパティ (マネージャー情報、ユーザーの資格情報) は、すべて必要に応じて編集できます。

プロパティの定義:

- **connectordetails.name:** ESMでのコネクターの名前。
- **connectordetails.location:** ESM内でコネクターが格納されているフォルダーの名前。
- **connectordetails.devicelocation:** ESMがインストールされているマシンの場所。
- **connectordetails.comment:** コネクターに関する追加コメント。

7. プロパティファイルを保存します。
8. お使いのプラットフォーム向けに用意されているコネクターのインストールファイルをダウンロードします。
9. 次のコマンドを実行して、新しいコネクターをサイレントモードでインストールします。

```
ArcSight_Agent_install_file -i silent -f <プロパティファイルのパス>\
properties_filename
```

InstallShieldプログラムが起動し、コネクターがサイレントモードでインストールされます。

例: silent_propertiesという名前のプロパティファイルを使用して、Windowsプラットフォーム上にコネクターをインストールする場合、次のように入力します。

```
ArcSight-3.5.x.nnnn.y-Agent-Win.exe -i silent -f silent_properties
```

注: サイレントインストールで回答ファイルを指定すると、サイレントインストール後にrunagentsetup.batファイル内の元のコマンドが変更されてしまいます。

この問題を修正するには、二重引用符で囲まれたエントリを手動で編集および削除し、デフォルト設定に戻す必要があります。2番目の二重引用符で囲まれた部分は削除してください。たとえば、変更後のスクリプトは次のようになっています。

```
call arcsight.bat agentsetup -c -i "SILENT" -f "C:\ArcSight\silent_
properties_AD" %*
```

これを、次のように編集します。

```
call arcsight.bat agentsetup -c -i "SWING" -f "" %*
```

この問題を回避するには、次の手順を実行します。

先に展開を行い、silent_propertiesファイルを使用して設定を行います。次のようなコマンドを実行します。

```
<コネクターのインストールパス>\current\bin\arcsight.bat agentsetup -c -i silent -
f 2_addwinc
```

これにより、runagentsetup.batファイルにはsilent_propertiesが含まれないため、正しいパスが維持されます。

注意: 以下に重要なポイントをまとめます。

- コネクターをインストールしたら、システムでデフォルトのファイル権限を設定して、ArcSightによって作成されたファイル (イベント、ログファイルなど) をセキュリティ保護してください。
- UNIXシステムでは、シェルプロファイルにumaskコマンドを追加することで、ファイル権限を設定するのが一般的です。たとえば、umask設定を077にすると、現在のユーザー以外の読み取り/書き込みアクセスが禁止されます。umask設定を000にすると、不要なセキュリティホールが生じます。

ESMからのコネクターのアップグレード

コネクターはアップグレードが必要になる場合があります。このプロセスはローカルまたはリモートでの実行が可能です。コンソールからのリモートアップグレードは、Windows、Linux、Solarisプラットフォームでのみサポートされます。

注: Windowsプラットフォームで動作しているコネクターの場合、ESM通知先からのコネクターのアップグレードには既知の制限事項があります。

コネクターのアップグレードでは、一部のフォルダーやファイルが、旧バージョンから新バージョンへと移行されます。Microsoft Windowsでは、これらのフォルダーやファイルは読み取り用に開いている場合でもロックされてしまいます。コネクターのインストールに必要なフォルダーやファイルがロックされていると、アップグレード中にそれらにアクセスしたときにアップグレードが失敗する可能性があります。この問題を回避するには、**[スタート] > [すべてのプログラム]** でコネクターを起動します。これにより、ウィンドウを開かずにコネクターを実行できるため、フォルダーやファイルがロックされる可能性が低くなります。

アップグレードを行うには、次の手順を実行します。

1. HP SSOサイトから、最新のコネクターアップグレードをマネージャーにダウンロードします。アップグレードバージョンは、.aupファイル (圧縮ファイル群) で提供されます。
2. .aupファイルを、動作中のマネージャーのARCSIGHT_HOME\updates\にコピーします。マネージャーは.aupファイルを自動解凍し、ARCSIGHT_HOME\Repository\にコピーします。
3. コンソールから、アップグレードするコネクターを (一度に1つ) 選択して**upgrade**コマンドを実行します。全コネクターに対してこれを繰り返します。

注意: 以下に重要なポイントをまとめます。

- 1つのJVMに複数のコネクターをインストールしている場合、JVMに最初にインストールしたコネクターを選択して (これ以外のコネクターを選択するとアップグレードは失敗します)、**upgrade**コマンドを実行します。これにより、JVM内のすべてのコネクターがアップグレードされます。
- 1つのコネクターに複数のマネージャー通知先がある場合、アップグレード作業はプライマリコンソールから実行する必要があります。セカンダリなど、プライマリ以外のコンソールで実行すると、アップグレードは失敗します。

4. 選択したコネクターが**upgrade**コマンドを受信すると、アップグレードと再起動が実行され、アップグレード結果 (成功または失敗) がマネージャーを介してコンソールに通知されます。

アップグレードの注意事項

- アップグレードが成功すると、新しいコネクターが起動し、成功を示すアップグレードステータスが報告されます。
- アップグレード後のコネクターが起動に失敗すると、フェイルオーバーにより、元のコネクターが自動的に再起動します

ヒント: 役立つヒントをまとめます。

- この問題が発生した場合、関連ログを参照できます。コンソールメニューで、**[Send Command] > [Tech Support] > [Get Upgrade Logs]** を選択します。

- ログの送信ウィザードを使用して、アップグレードログなどのログを収集してサポート担当に送信することもできます。

- コネクターは、起動時に自身のアップグレードステータスを自動的に判断します。
- コネクターのアップグレードでは、構成ガイドの最新版をサポートWebサイトからダウンロードしてください。このサイトには最新版の構成ガイドが用意されており、コネクターデバイス固有の情報が記載されています。
- コネクターのアップグレードには、管理者権限が必要です。
- アップグレードできるのは、接続先のマネージャー上にあるバージョンのコネクターのみです。リモートアップグレードに対応しているのはESM 4.0以降のみであり、4.0.2以降のコネクターに対してのみ実行できます。
- コネクターをアップグレードする前に、マネージャーと対象コネクターの両方を実行状態にしてください。
- 32ビット版のSmartConnectorを64ビット版にアップグレードすることはできません。64ビット版のSmartConnectorを新規インストールする必要があります。

ローカルアップグレード

コネクターをローカルでアップグレードするには、次の手順を実行します。

1. 実行中のコネクターを停止し、コネクターのインストーラーを起動します。コネクターのインストール先を指定するプロンプトが表示されます。
2. アップグレード対象コネクターがインストールされている場所を選択します。「Previous Version Found. Do you want to upgrade?」というメッセージが表示されます。
3. 続行してコネクターをアップグレードするオプションを選択します。元のコネクターのインストール場所は、元のフォルダー名の前に文字が追加された名前に変更されます。アップグレードされたコネクターは `$ARCSIGHT_HOME\current` にインストールされます。

ESMからのリモートアップグレード

注: コンソールからのリモートアップグレードに対応しているのは、Windows、Linux、Solarisプラットフォームのみです。

ESMは、コネクターの一元管理/設定だけでなく、リモートアップグレードも可能です。コンソールから **[Upgrade]** コマンドを使用することで、管理対象デバイス向けのコネクターソフトウェアを新しいバージョンにアップグレードできます。

[Upgrade] コマンドでは、全コネクターのアップグレードの開始、管理、ステータス表示を実行できます。アップグレードに失敗すると、フェイルオーバーによって旧バージョンのコネクターが起動します。コンポーネント(コンソール、マネージャー、コネクター) 間の通信プロセスとアップグレードプロセスはすべて、セキュアな接続を介して行われます。

コンソールには、全コネクターの最新バージョン情報が反映されます。

コネクターの実行

コネクターのインストールと実行には、**スタンドアロンモード**で行う方法と、Windows**サービス**またはUNIX**デーモン**として行う方法があります。スタンドアロンでインストールしたコネクターは、手動で起動する必要があります。ホストの再起動時も自動的に実行されません。WindowsサービスまたはUNIXデーモンとしてインストールしたコネクターは、ホストの再起動時に自動的に実行されます。Windowsプラットフォームでサービスとしてインストールおよび実行するには、管理者権限が必要です。Linux/Unixデーモンとして実行する場合に、rootユーザー権限またはroot以外のユーザー権限を使用する方法については、[次のページの「インストール時のユーザー権限 \(UNIXのみ\)」](#)を参照してください。

注意: 一部のSmartConnectorでは、設定の変更を反映するために再起動が必要になることがあります。

スキャナー向けのコネクターには注意が必要です。スキャナーコネクターをインタラクティブモードで実行するには、WindowsサービスまたはUNIXデーモンとしてではなく、スタンドアロンモードで実行してください。

スタンドアロンモードでのコネクターの実行

ホストにインストールされているコネクターをすべて実行するには、コマンドウィンドウを開き、ARCSIGHT_HOME/current/binに移動して次のコマンドを実行します。

```
arcsight connectors
```

コネクターのログを表示するには、次のファイルを開きます。

```
$ARCSIGHT_HOME/current/logs/agent.log
```

コネクターをすべて停止するには、コマンドウィンドウでCtrl+Cキーを押します。

ヒント: Windowsプラットフォームでは、コネクターはショートカットおよびオプションの [スタート] メニュー項目を使用して実行することも可能です。

Windowsサービスとしてのコネクターの実行

サービスとしてインストールしたコネクターは、プラットフォーム固有の手順に沿って、手動で起動および停止できます。

Windowsプラットフォームにサービスとしてインストールされたコネクターを起動または停止するには、次の手順を実行します。

1. [マイコンピュータ] を右クリックし、コンテキストメニューから [管理] を選択します。
2. [サービスとアプリケーション] フォルダーを展開し、[サービス] を選択します。

3. コネクターサービス名を右クリックし、**[開始]** をクリックするとコネクターのサービスが開始し、**[停止]** をクリックするとサービスが停止します。

コネクターサービスが開始したかどうかは、次のファイルで確認してください。

```
$ARCSIGHT_HOME/logs/agent.out.wrapper.log
```

コネクターをサービスとして再設定するには、コネクターの設定ウィザードを再度実行します。コマンドウィンドウを開き、\$ARCSIGHT_HOME/current/binに移動して次のコマンドを実行します。

```
runagentsetup
```

詳細については、「[サービスとしてのインストール](#)」(47ページ) を参照してください。

UNIXデーモンとしてのコネクターの実行

デーモンとしてインストールしたコネクターは、プラットフォーム固有の手順に沿って、手動で起動および停止できます。

UNIXシステムでは、コネクターを自動実行するように設定すると、ArcSightによって/etc/init.d ディレクトリにコントロールスクリプトが生成されます。コネクターを開始または停止するには、コントロールスクリプトを**start**または**stop**コマンドパラメーターで実行します。

例:

```
/etc/init.d/arc_serviceName {start|stop}
```

コネクターサービスが開始したかどうかは、次のファイルで確認してください。

```
$ARCSIGHT_HOME/logs/agent.out.wrapper.log
```

コネクターをデーモンとして再設定するには、コネクターの設定ウィザードを再度実行します。コマンドウィンドウを開き、\$ARCSIGHT_HOME/current/binに移動して次のコマンドを実行します。

```
runagentsetup
```

詳細については、「[サービスとしてのインストール](#)」(47ページ) を参照してください。

インストール時のユーザー権限 (UNIXのみ)

SmartConnectorは、サービスとして、またはスタンドアロンで実行できます。詳細については、[前のページの「コネクターの実行」](#)を参照してください。

SmartConnectorsは、arcsightなど、root以外のユーザーでも実行できます。SmartConnectorで1024未満の番号のポートをリッスンする場合、このポートは制限されているのでroot権限が必要です。たとえば、syslogデーモンコネクターでは、ポート514などの制限ポートにバインドする際にroot権限が必要になります。

以下のセクションでは、1) 小さい番号のポートをリッスンするためにコネクターの設定が必要なケースと、2) コネクターをサービスとして実行するケースについて、推奨オプションをご紹介します。インストールと設定に応じて、該当するケースを参考にしてください。

サービスとして実行

オプション1: 推奨オプション。arcsightユーザーでインストール、arcsightユーザーで実行

次の手順のarcsightユーザーとは、root以外の権限を持つユーザーの総称です。

arcsightユーザーでログインしてインストールを行う場合、ArcSightコネクタファイルの所有者はarcsightユーザーになります。

インストールを完了したら、arcsightユーザーでコネクタウィザードを実行します。以下の点に注意してください。

- Syslog Daemonコネクタを選択する場合、1024番以上のポートを使用してください (以下の「[オプション2: arcsightユーザーでインストール、ポート転送を使ってarcsightユーザーで実行](#)」を参照してください)。
- サービスとして実行する場合、セットアップウィザードでダイアログボックスが開き、次のメッセージが表示されます。

```
The Connector Setup Wizard is not able to modify the service configuration because the Wizard is not running as root. Please run this Wizard as root. Or to manually install, logged on as root, execute the following script:
```

```
$ARCSIGHT_HOME/current/bin/arcsight agentsvc -i -u user
```

```
To manually remove the service, logged on as root, execute the following script:
```

```
$ARCSIGHT_HOME/current/bin/arcsight agentsvc -r
```

ウィザードをrootで実行することはお勧めしません。arcsightユーザーでウィザードを実行し、サービスを手動でインストールしてください。rootでログインし、次のスクリプトを実行してコネクタをサービスとしてインストールします。

```
$ARCSIGHT_HOME/current/bin/arcsight agentsvc -i -u arcsight -u arcsightオプションを指定しているので、サービスはarcsightユーザーで実行されます。
```

オプション2: arcsightユーザーでインストール、ポート転送を使ってarcsightユーザーで実行

このオプションはオプション1と同じですが、1024未満のポートに送信されたイベントをSyslog Daemonで受信できます。このオプションを選択する場合は、まずオプション1の手順を実行します。さらに別のプログラムを実行し、小さい番号のポートのトラフィックを、コネクタ用に設定したポートに転送します。たとえば、syslogイベントがポート514に転送されており、コネクタの受信ポートが6000に設定されている場合、フォワーダーによってポート514からポート6000にトラフィックが転送されます。ポート転送を実行するプログラムには、**iptables**、**ncat**、**socat**などがあります。**iptables**プログラムは一部のLinux/Unixバージョンに同梱されているので、簡単に使用できます。

オプション3: rootユーザーでインストール、rootユーザーで実行

root権限は、コネクタのインストール、設定、メンテナンスに必要な権限のため、このオプションは他のオプションよりもセキュリティレベルが低下します。

rootでログインし、ArcSightコネクターをインストールします。これにより、ArcSightコネクターのファイルはすべてrootユーザーが所有者になります。コネクターのセットアップウィザードも、rootユーザーで実行します。コネクターをサービスとして実行する場合、コネクターのセットアップウィザードでサービスを設定するので、追加設定は必要ありません。

注意: 「arcsightユーザーでインストール、rootユーザーで実行」という方法は行わないでください。

セキュリティの脆弱性に関する問題が発生します。コネクターの設定ファイルの所有者はarcsightユーザーとなるため、悪意のあるユーザーによってファイルが改ざんされる危険性が高くなります。この状態でrootでコネクターを実行すると、改ざんによって権限のエスカレーションが発生する恐れがあります。

スタンドアロンモードでの実行

オプション1: 推奨オプション。arcsightユーザーでインストール、arcsightユーザーで実行

次の手順のarcsightユーザーとは、root以外の権限を持つユーザーの総称です。

arcsightユーザーでログインしてインストールを行う場合、ArcSightコネクターファイルの所有者はarcsightユーザーになります。

インストールを完了したら、arcsightユーザーでコネクターウィザードを実行します。

Syslog Daemonコネクターを選択する場合、1024番以上のポートを使用してください（[前のページの「オプション2: arcsightユーザーでインストール、ポート転送を使ってarcsightユーザーで実行」](#)を参照してください）。

オプション2: arcsightユーザーでインストール、ポート転送を使ってarcsightユーザーで実行

このオプションはオプション1と同じですが、1024未満のポートに送信されたイベントをSyslog Daemonで受信できます。このオプションを選択する場合は、まずオプション1の手順を実行します。さらに別のプログラムを実行し、小さい番号のポートのトラフィックを、コネクター用に設定したポートに転送します。たとえば、syslogイベントがポート514に転送されており、コネクターの受信ポートが6000に設定されている場合、フォワーダーによってポート514からポート6000にトラフィックが転送されます。ポート転送を実行するプログラムには、**iptables**、**ncat**、**socat**などがあります。**iptables**プログラムは一部のLinux/Unixバージョンに同梱されているので、簡単に使用できます。

注意: 次の2つの方法ではインストールしないでください。

- arcsightユーザーでインストール、rootユーザーで実行

セキュリティの脆弱性に関する問題が発生します。コネクターの設定ファイルの所有者はarcsightユーザーとなるため、悪意のあるユーザーによってファイルが改ざんされる危険性が高くなります。この状態でrootでコネクターを実行すると、改ざんによって権限のエスカレーションが発生する恐れがあります。

- rootユーザーでインストール、rootユーザーで実行

root権限は、コネクターのインストール、設定、メンテナンスに必要な権限のため、このオプションはセキュリティレベルが低下します。rootでログインし、ArcSightコネクターをインストールします。これにより、ArcSightコネクターのファイルはすべてrootユーザーが所有者になります。コネクターのセットアップウィザードも、rootユーザーで実行します。

ESMでのコネクターの動作状態を確認

コネクターが実行中かどうかを確認するには、ArcSightコンソールナビゲーターの [リソース] タブで、[コネクタ] を確認します。実行中のコネクターは、<コネクター名> (running) と表示されます。

コネクターのアンインストール

サービスまたはデーモンとして実行中のコネクターをアンインストールする場合、まずそのサービスまたはデーモンを停止する必要があります。また、\$ARCSIGHT_HOME/current/bin/arcsight agentsvc -rを実行してサービスファイルを削除してから、コネクターをアンインストールしてください。

アンインストーラーを実行しても、コネクターのホームフォルダーにあるファイルとディレクトリのいくつかは削除されません。アンインストールが完了した後で、手動で削除してください。

Windowsでのアンインストール:

1. [スタート] メニューを開きます。
2. [すべてのプログラム] > [ArcSight SmartConnectors] で [Uninstall SmartConnectors] (またはコネクターのインストール時に指定したフォルダー名) を選択します。
3. [スタート] メニューにコネクターが登録されていない場合は、
\$ARCSIGHT_HOME/current/UninstallerDataフォルダーで次のコマンドを実行します。
Uninstall_ArcSightAgents.exe

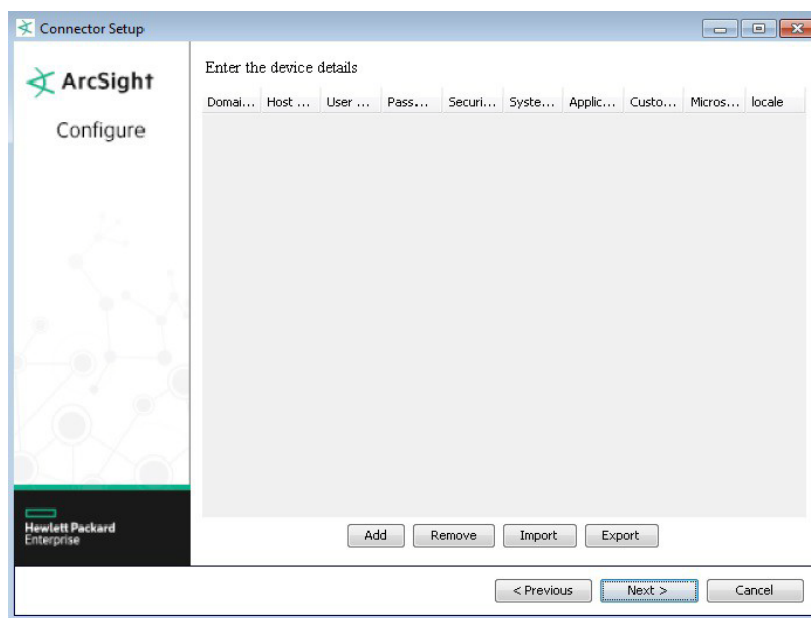
UNIXホストでのアンインストール:

1. \$ARCSIGHT_HOME/UninstallerDataディレクトリでコマンドウィンドウを開きます。
2. ./Uninstall_ArcSightAgentsコマンドを実行します。

注: UninstallerDataディレクトリの.com.zerog.registry.xmlファイルは、すべてのユーザーに読み取り、書き込み、実行権限が割り当てられています。Windowsプラットフォームでアンインストーラーを実行するには、この3つの権限が必要です。一方、UNIXプラットフォームの場合、すべてのユーザーに読み取りと書き込みを許可する (つまり666) 権限に変更することができます。

Windowsホストテーブルの使用

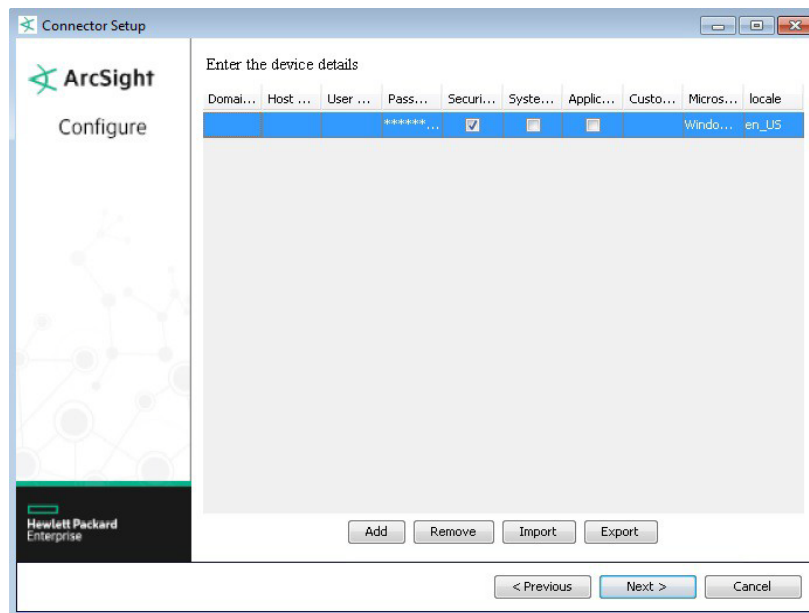
コネクターのインストールでは、コネクターがテーブルパラメーターを使用する場合、次のウィンドウが開き、パラメーターデータを入力できます。パラメーターテーブルを使用するコネクターには、複数のファイル、複数のサイトやサーバー、複数のデータベースインスタンスコネクターなどがあります。



このタイプのコネクターのパラメーターには、データ件数が少ない場合に手動で入力する方法と、データ件数が多い場合に、.csvファイルでインポートする方法があります。また、すでに入力したデータをエクスポートして、.csvファイルを作成することも可能です。具体的な手順については、[次のページの「CSVファイルのインポートとエクスポート」](#)を参照してください。

テーブルパラメーター値の手動入力

パラメーターを手動で入力するには、[Add] ボタンをクリックしてフィールドを作成し、下の図のようにデータを入力します。



[Export] ボタンを使用すれば、パラメーターテーブルデータを外部の .csvファイルにエクスポートし、後で使用できるように保存することができます。

この機能を使用する場合は、次の点に注意してください。

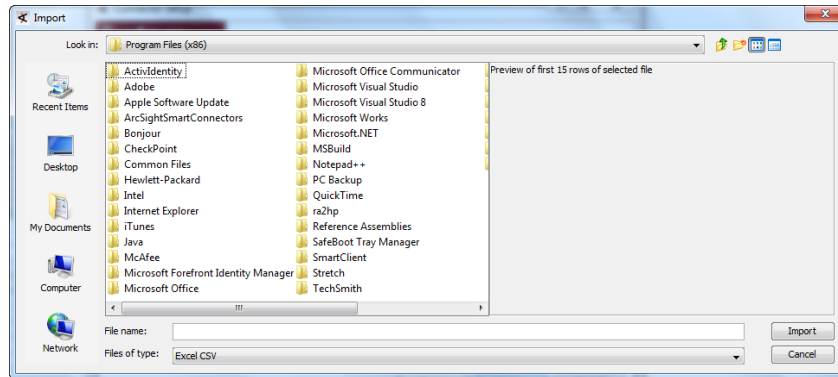
- パスワードなどの個人データ (アスタリスク表示) が含まれるカラムは、[Export] ボタンでデータをエクスポートしても、エクスポート後のファイルには含まれません。
- .csvファイルをインポート ([Import] ボタンを使用) しても、個人データのカラムは非表示時 (アスタリスク表示) のままです。
- 個人情報のカラムには手動でデータを入力できますが (スプレッドシートプログラムでCSVにカラムを追加するか、設定ウィザードで入力)、エクスポート後のファイルには含まれません。これはセキュリティ対策のためです。
- .csvファイルからデータをインポート ([Import] ボタンを使用) すると、テーブル内の既存データは、すべて削除または置換されます。

CSVファイルのインポートとエクスポート

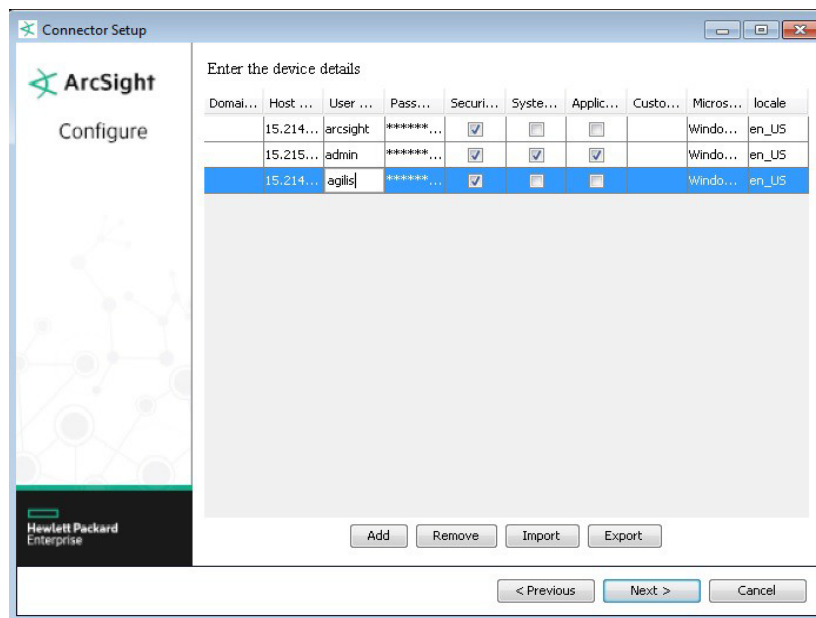
大量のパラメーターデータを入力する場合、.csvファイルを作成しておけば、[Import] ボタンを使用することで、設定ウィザードのパラメーター入力テーブルに入力することができます。

インポート機能を使用するには、次の手順を実行します。

1. スプレッドシートプログラム (Microsoft Excelなど) を開き、テーブルにパラメーターデータを入力し、.csvファイルとして保存します。
2. コネクターのインストール中に、[Import] ボタンをクリックし、作成した.csvファイルの場所を指定します。ウィンドウが開き、CSVファイルの内容がプレビュー表示されます。



3. [Import] ウィンドウで [Import] ボタンをクリックします。これにより、コネクターのパラメーターフィールドにデータが入力されます。



4. さらに手動で行を追加し (通常は [Add] ボタンを使用)、完成したテーブルを後で使用できるように、外部の .csv ファイルにエクスポートすることができます (通常は [Export] ボタンを使用)。

注: 上記の画面例では、設定ウィザードに [Password] カラムが表示されていますが、これは元の .csv ファイルには存在しません。この個人情報のカラムには、実際のパスワードデータは格納されておらず、エクスポート後のファイルにも含まれません。

5. データの入力が完了したら、[Next] をクリックします。

第4章: コネクタの設定

この章のほとんどのセクションでは、マネージャーにアクセスしなくても実行できる設定タスクについて説明します。ただし、「ArcSightコンソールを使ったデフォルト設定と代替設定の定義」(51ページ) は例外です。

コネクタの変更

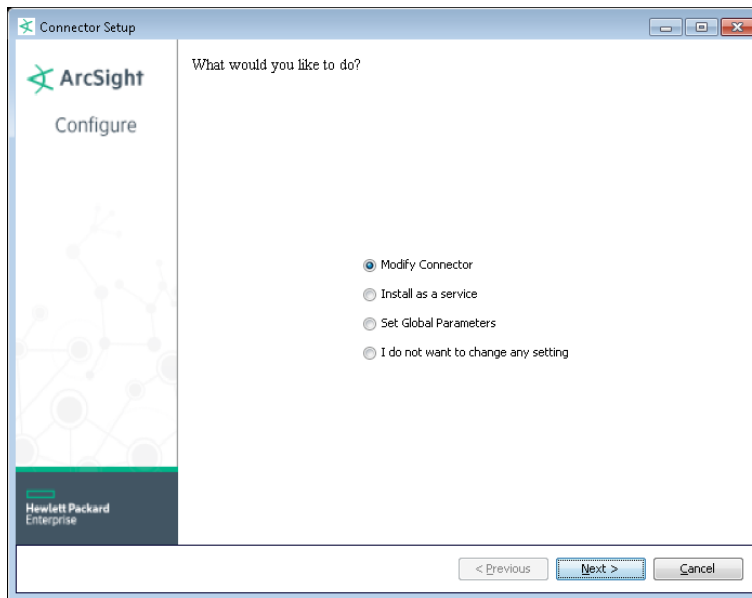
ここでは、ウィザードで最初に設定したコネクタパラメータを変更する方法を説明します。これには、通知先パラメータ、サービス設定、グローバルパラメータなどがあります。

設定した値を変更するには、次の手順を実行します。

コネクタを最初にインストールした後に設定を変更するには、ウィザードを再度実行します。
\$ARCSIGHT_HOME/current/binで、次のコマンドを実行します。

```
runagentsetup
```

次のウィンドウが開きます。



コネクタの変更

コネクタのインストール中に設定した初期値を変更するには、**[Modify Connector]** を選択します。

コネクターパラメーターの変更

この後の手順ではウィンドウに情報が表示されていますが、これはサンプルデータです。実際のウィンドウに表示される内容は、インストールされているコネクターとその設定によって異なります。

パラメーター値を変更するには、次の手順を実行します。

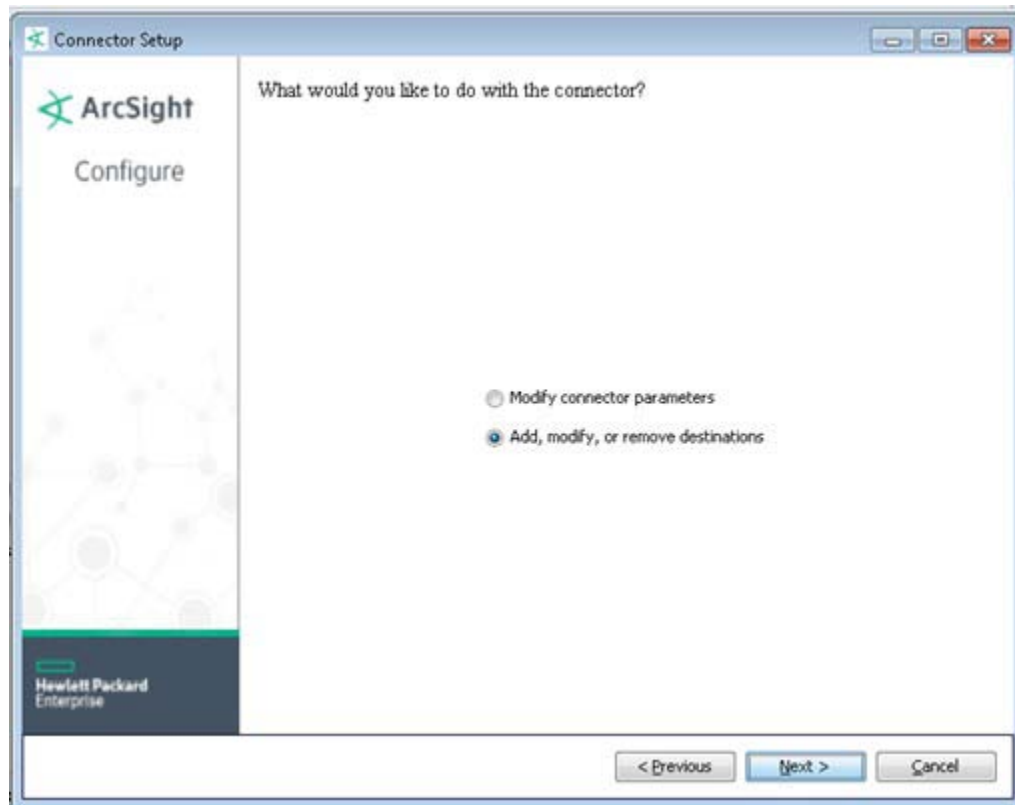
1. ウィザードを開始したら、**[Modify Connector]** を選択して **[Next]** をクリックします。**[Modify connector parameters]** または **[Add, modify, or remove destinations]** を選択できます。**[Modify connector parameters]** を選択します。
2. パラメーターウィンドウが表示されたら、パラメーターを変更します。表示されるパラメーターは、インストールしたコネクターごとに異なります。
3. **[Next]** をクリックします。コネクターパラメーターの変更が処理され、コネクター設定が変更されます。変更が完了すると、「**Successfully updated parameters**」というメッセージが表示されます。
4. **[Next]** をクリックします。**[Exit]** をクリックしてコネクターの変更を終了するか、**[Continue]** をクリックしてコネクターの変更作業を続けます。**[Next]** をクリックして、終了または続行します。

通知先の追加、変更、削除

既存の通知先を変更するか、新しい通知先を追加します。コネクターのインストールおよび設定時に指定した通知先が表示されます。

通知先を追加するには、次の手順を実行します。

1. ウィザードを実行すると、デフォルトで **[Modify Connector]** が選択されます。これは変更しないでください。
2. **[Next]** をクリックします。表示されるウィンドウで、**[Add, modify, or remove destinations]** を選択します。
3. **[Next]** をクリックします。表示される選択肢は、設定済みの通知先によって異なります。通知先のパラメーターと設定を変更するか、**[Add destination]** をクリックして別の通知先を追加します。
4. **[Next]** をクリックすると、通知先を追加、変更、削除するウィンドウが開きます。



通知先を削除するには、次の手順を実行します。

1. ウィザードを実行すると、デフォルトで **[Modify Connector]** が選択されます。これは変更しないでください。
2. **[Next]** をクリックします。**[Add, modify, or remove destinations]** を選択します。
3. **[Next]** をクリックします。通知先リストから、削除する通知先を選択します。
4. **[Next]** をクリックします。**[Remove destination]** を選択します。
5. **[Next]** をクリックします。通知先の削除が開始されます。
6. **[Next]** をクリックします。通知先の削除が完了します。
7. **[Next]** をクリックします。**[Exit]** をクリックしてコネクタの変更を終了するか、**[Continue]** をクリックしてコネクタの変更作業を続けます。**[Next]** をクリックして、終了または続行します。

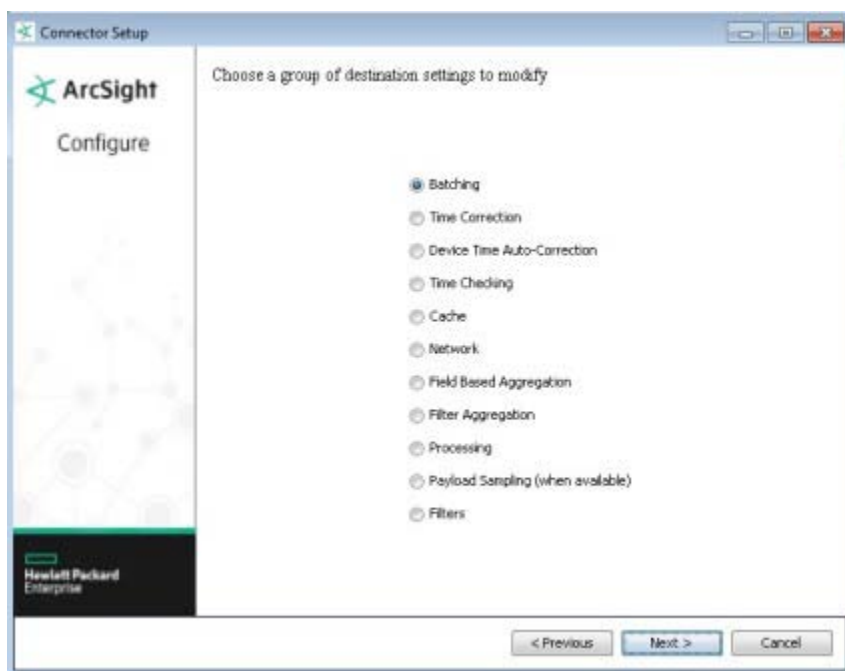
通知先パラメーターの変更

[Modify destination parameters] を選択し、通知先を最初に設定したときに指定したパラメーター値を変更します。表示されるパラメーターは、設定済みのコネクタによって異なります。

通知先設定の変更

ArcSight SmartConnectorでは、パフォーマンスを最適化し、機能性を向上する設定が可能です。設定では、アグリゲーション、一括転送処理、時刻補正、ペイロードのサンプリングの有効化や、フィルター条件の指定が可能です。SmartConnectorは、指定した条件に基づいて、通知先に送信するイベントをフィルタリングします。

1. ウィザードを実行すると、デフォルトで **[Modify Connector]** が選択されます。これは変更しないでください。
2. **[Next]** をクリックします。表示されるウィンドウで、**[Add, modify, or remove destinations]** を選択します。
3. 通知先が選択されていることを確認し、**[Next]** をクリックします。
4. **[Modify destination settings]** を選択し、次のパラメーターを設定します。



パラメーターの詳細については、「[通知先の設定](#)」を参照してください。

通知先の再登録

マネージャーはコネクタを認識すると、IDトークンを生成します。コネクタはこのトークンを使用して、セキュリティイベントを識別します。マネージャーが何らかの理由でコネクタからのイベント受信を停止した場合や、アップグレードしたコネクタのリソースがデータベースから削除されていた場合には、コネクタの再登録が必要になります。

通知先を再登録するには、次の手順を実行します。

1. ウィザードを実行すると、デフォルトで **[Modify Connector]** が選択されます。これは変更しないでください。
2. **[Next]** をクリックします。**[Add, modify, or remove destinations]** を選択します。

3. **[Next]** をクリックします。表示されたリストから現在の通知先を選択します。表示内容は、最初のコネクタ設定によって異なります。
4. **[Next]** をクリックします。**[Reregister destination]** を選択します。
5. **[Next]** をクリックします。コネクタの通知先に応じて、必要な資格情報を入力します。資格情報が不要な場合は、ウィンドウは表示されません。
6. **[Next]** をクリックします。再登録が開始されます。
7. **[Next]** をクリックします。再登録が完了します。
8. **[Next]** をクリックします。**[Exit]** をクリックし、**[Next]** をクリックします。
9. コネクタを再起動し、新しいIDトークンを適用します。

フェイルオーバー通知先の追加

フェイルオーバー通知先を追加するには、次の手順を実行します。

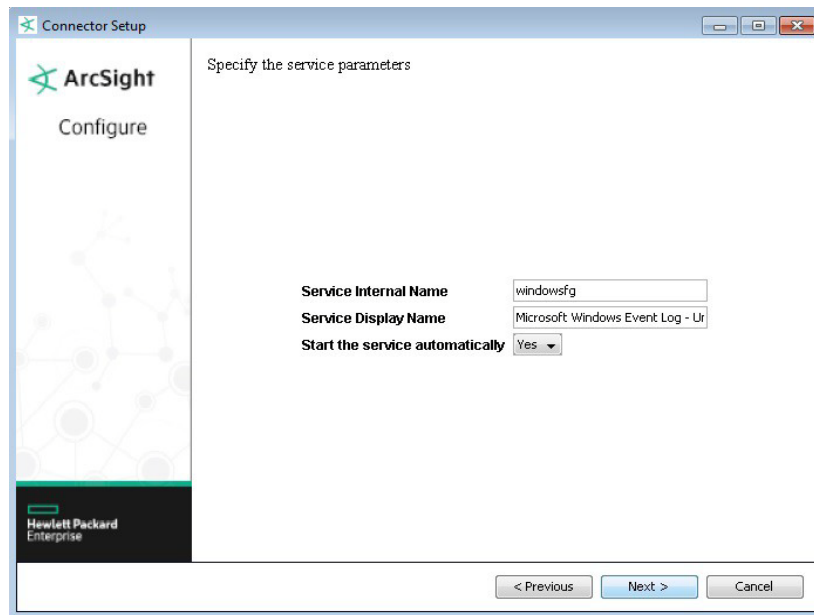
1. ウィザードを開始すると、デフォルトで **[Modify Connector]** が選択されます。これは変更しないでください。
2. **[Next]** をクリックします。次のウィンドウで、**[Add, modify, or remove destinations]** を選択します。
3. **[Next]** をクリックします。表示されたリストから現在の通知先を選択します。表示内容は、最初のコネクタ設定によって異なります。
4. **[Next]** をクリックします。**[Add fail a over destination]** を選択します。
5. **[Next]** をクリックします。通知先タイプを選択します。
6. **[Next]** をクリックします。フェイルオーバー通知先のパラメータを入力します。
7. **[Next]** をクリックします。通知先のパラメータの更新が開始されます。
8. **[Next]** をクリックします。通知先のパラメータ更新が完了します。
9. **[Next]** をクリックします。**[Exit]** をクリックし、**[Next]** をクリックします。
10. コネクタを再起動すると、変更内容が有効になります。

サービスとしてのインストール

ここでは、コネクタをサービスとして実行する方法と、コネクタサービスを削除する方法を説明します。

コネクタをサービスとして実行するように設定するには、次の手順を実行します。

1. ウィザードを実行し、**[Install as a service]** を選択します。
2. **[Next]** をクリックします。サービスパラメータを指定または変更します。



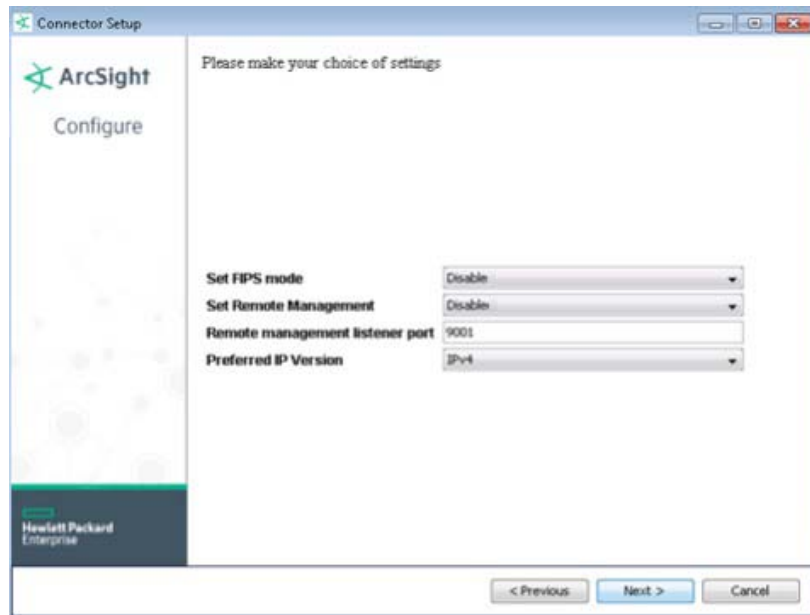
3. **[Next]** をクリックします。サービスサマリーが表示されます。
4. **[Next]** をクリックします。**[Exit]** をクリックしてコネクターの変更を終了するか、**[Continue]** をクリックしてコネクターの変更作業を続けます。**[Next]** をクリックして、終了または続行します。

SmartConnectorサービスを削除するには、次の手順を実行します。

1. **[Uninstall as a service]** を選択します。
2. **[Next]** をクリックします。コネクターサービスの削除を確認するメッセージが表示されます。
3. **[Next]** をクリックします。**[Exit]** をクリックしてコネクターの変更を終了するか、**[Continue]** をクリックしてコネクターの変更作業を続けます。**[Next]** をクリックして、終了または続行します。

グローバルパラメーターの設定

FIPSモード、リモート管理、優先するIPバージョンの設定値を変更する場合は、**[Set Global Parameters]** を選択します。



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手順は、「 FIPS Suite Bモードの有効化 」を参照してください。初期値は [Disable] です。
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からのクエリには、この有効/無効の設定値とポート番号が使用されます。初期値は [Disable] です。
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ているマシン) でIPv4とIPv6両方のアドレスが使用できる場合、優先的に使用するバージョンを選択できます。いずれか一方のみが使用可能な場合は、表示される選択肢は1つだけです。両方使用できる場合の初期設定は [IPv4] です。

選択が完了したら、[Next] をクリックします。サマリー画面が表示されます。選択した内容を確認し、[Next] をクリックして、終了または続行します。

その他の設定

ここでは、その他の設定について説明します。

FIPS Suite Bモードの有効化

FIPS Suite Bモードを有効にするには、次の手順を実行します。

1. インストールが完了したら、`$ARCSIGHT_HOME\current\bin`ディレクトリで`runagentsetup`を実行します。
2. ウィンドウが開いたら、**[Modify Connector]** を選択します。
3. **[Add, Modify, or remove destinations]** を選択し、**[Next]** をクリックします。
4. FIPS Suite Bモードを有効化する通知先を選択し、**[Next]** をクリックします。
5. **[Modify destination parameters]** を選択し、**[Next]** をクリックします。
6. パラメーターウィンドウが開いたら、FIPS Cipher Suites/パラメーターとして **[FIPS with Suite B 128-bits]** または **[FIPS with Suite B 192 bits]** を選択します。**[Next]** をクリックします。
7. ウィンドウが開き、変更内容が表示されます。内容を確認して **[Next]** をクリックします (内容を変更する場合は **[Previous]** をクリックします)。
8. 設定変更のサマリーが表示されます。**[Next]** をクリックして続行します。
9. **[Exit]** をクリックして設定ウィザードを終了します。

ESMへのイベント送信時のネットワーク帯域幅の低減

コネクタは、HTTP圧縮による圧縮形式で、イベント情報をマネージャーに送信できます。この圧縮形式を使用すると、入力データ (この場合はコネクタが送信するイベント) によっては10分の1以上の圧縮率が可能です。圧縮によってコネクタが使用するネットワーク帯域幅が大幅に低減され、全体的なパフォーマンスに対する影響もありません。

デフォルトでは、すべてのコネクタで圧縮が有効になっています。圧縮を無効にするには、`agent.properties`ファイル (`ARCSIGHT_HOME\current\user\agent\`) に次の行を追加してください。
`http.transport.compressed = false`

ArcSightコンソールを使ったデフォルト設定と代替設定の定義

SmartConnectorでは、デフォルト設定に加えて、さまざまな代替設定が可能です。

代替設定とは、毎日指定された時間にデフォルト設定の代わりに適用されるランタイムパラメーターのセットです。たとえば、時間帯ごとに異なるバッチ方式（緊急度またはサイズによる）を指定するとします。1つの送信先に対して複数の代替設定を定義し、1日の異なる時間範囲にそれぞれ適用します。たとえば、ある設定を午前8時～午後5時の時間範囲に定義し、別の設定を午後5時～午前8時の時間範囲に定義することが可能です。

デフォルト設定を定義するには、次の手順を実行します。

1. ナビゲーターパネルで、**[コネクタ]** リソースツリーを選択します。
2. **[コネクタ]** リソースツリーで管理対象のSmartConnectorを右クリックし、**[設定]** を選択します。
コネクタエディターの **[調査/編集]** パネルが開きます。**[コネクタ]** タブの **[名前]** フィールドには、SmartConnectorのインストール時に指定した名前が自動入力されます。
3. **[コネクタ]** タブで、**[コネクタロケーション]** と **[デバイスロケーション]** を入力します。SmartConnectorは、このフィールドを使ってすべてのイベントのタグ付けを行います。作成日などの情報は、自動入力されます。
4. **[デフォルト]** タブでは、一括転送処理や時刻補正などの追加パラメーターを変更できます。『ArcSightコンソールユーザーズガイド』の「SmartConnectorの管理」で、「コネクタエディタのオプションタブ」と「**[コネクタ]** タブの設定フィールド」の設定フィールドの説明を参照してください。
5. **[適用]** をクリックすると変更が追加されます。コネクタエディターは開いたままです。

設定に関連付けられた説明は、ツールチップ情報として表示されます。このパラメーターはコネクタから直接送信され、コネクタには新しいリソースが含まれている可能性がある（コネクタが新しいバージョンになっている可能性がある）ので、ローカライズされません。

コネクタコマンドのフレームワークも同様に動作します。コネクタコマンドメニューの設定は、登録時にコネクタでサポートされるコマンドリストを送信することにより行われます。

コネクタエディターには、調整可能なコントロールがいくつかあります。エディターの各タブまたはサブタブで使用できるオプションについて簡単に説明します。

代替設定を作成するには、次の手順を実行します。

1. SmartConnectorの [調査/編集] パネルを開きます。
2. [デフォルト] タブで、[代替設定追加] をクリックします。
新しいタブ [代替#1] が編集パネルに追加されます。このタブには、時間間隔を入力するためのフィールドがあります。
3. [時間間隔] で、[開始時刻] と [終了時刻] を入力します。必要に応じて追加の変更を行った後、[適用] をクリックします。
4. 追加の代替設定が必要な場合は、異なる時間間隔とパラメーターを使用して、上記のプロセスを繰り返します。たとえば、1日の特定の時間に緊急度やサイズに基づいて異なる一括処理を実行したい場合に、代替設定を作成します。

24時間の中で、代替設定で指定されていない時間範囲については、デフォルトのパラメーターが適用されます。

詳細については、『ArcSightコンソールユーザーズガイド』の「SmartConnectorの管理」を参照してください。コネクタアプライアンスの実装については、『Connector Appliance Administrator's Guide』の「Managing Alternate Configurations」を参照してください。

イベントフィルタリングのカスタマイズ

不要なイベントを除外したり、必要なイベントのみを含めたりする場合は、イベントフィルタリングをカスタマイズします。フィルタリングは、事前定義したパターンに基づいて実行されます。これにより、すべてのコネクタ通知先は、定義したフィルターに基づいて、関連イベントのみを受信できるようになります。

この機能は、デフォルトで無効になっています。有効にすると、rawEventフィールドに特定のパターンが含まれるイベントのみを含めたり、あるいは除外したりすることが可能です。コネクタの実行中に [ステータスの取得] コマンドを実行すると、次の内容を確認できます。

- 前回のコネクタ起動以降にフィルター処理されたイベント総数
- イベントフィルタリングの現在のステータス

機能の使用

フィルタリング機能は、ArcSightセキュリティイベントのrawEventフィールドに適用されます。セキュリティイベントがコネクタから送信されると、rawEventフィールドが抽出および評価され、フィルターが適用されます。

フィルタリング機能を使用するには、次の3つのプロパティのうち、2つをagent.propertiesファイルに追加する必要があります。最初のパラメーターは必須です。残りの2つはいずれか1つを追加してください。

```
customeventsfilter.regex.enabled=false
customeventsfilter.regex.pattern.include=
customeventsfilter.regex.pattern.exclude=
```

フィルタリングを適用するには、最初のプロパティを**true**に設定します。さらに、残りの2つのプロパティの**いずれか**で、有効な正規表現を指定します。デフォルト値をそのまま使用する場合は、上記のプロパティをagent.propertiesファイルに追加する必要はありません。詳細については、「[Java正規表現](#)」を参照してください。

注: この機能を有効化し、両方のパターンを定義した場合、除外パターンが優先され、包含パターンは無視されます。

この機能はデフォルトでは無効であり (customeventsfilter.regex.enabled=false)、フィルタリングはイベントに適用されません。

注: 包含パターンでフィルタリングを行うと、指定したパターンがrawEventフィールド内にはないイベントはすべて除外されます。包含パターンを使用する場合は、想定した結果が得られるかどうかを、事前に確認してください。

注: すべてのプロパティは一意とみなされるため、包含または除外パターンで同じプロパティを複数回定義しないでください。

コネクターに送られるすべてのデバイスイベントにrawEventフィールドが存在するため、この機能の影響を受けます。agent:017 (ステータスの取得) など一部の内部イベントにもrawEventフィールドが存在し、フィルタリング機能の影響を受けます。ほとんどの内部イベント (agent:030、agent:031、agent:050など) は、rawEventフィールドがないため影響を受けません。この機能が適用されるのは、rawEventフィールドが空でないイベントのみです。

この機能を有効化しても、包含パターンと除外パターンの両方が無効または空の場合、[\[ステータスの取得\]](#) コマンドを実行すると、フィルターステータスについて次のようなメッセージが表示されます。

```
Custom Filtering: Events Filtering State.....Events Filtering Disabled
Due to Syntax Error in User Defined Regex
```

次の表では、各ユーザー設定の組み合わせに対するフィルターステータスをまとめています。

customeventsfilter.regex.enabled	customeventsfilter.regex.pattern.exclude	customeventsfilter.pattern.include	結果
false	任意のパターン (有効、無効、空)	任意のパターン (有効、無効、空)	フィルターは無効になります。
true	空ではない有効なパターン	任意のパターン (有効、無効、空)	フィルターは有効になり、除外フィルターが適用されます。包含パターンによる影響はありません。
true	空または無効	有効なパターン	フィルターは有効になり、包含フィルターが適用されます。
true	空または無効	空または無効	フィルターは無効になります。

Java正規表現

次のリンクでは、JAVA正規表現の使用方法が解説されています。

Java 8のPatternクラス

正規表現に誤りがあると (JAVA Patternクラスでコンパイル不能)、agent.logファイルにエラーメッセージが記録されます。詳細については、「[ログメッセージ](#)」を参照してください。

ステータスの取得

ESMコンソール

ESMコンソールで [ステータスの取得] コマンドを実行すると、フィルタリングの現在のステータスと、前回のコネクタ一起動時以降にフィルター処理されたイベントの総数が表示されます。

ESMコンソールでコネクタを右クリックし、[コマンドの送信] > [ステータス] > [ステータスの取得] を選択します。

コネクタにコマンドが送信され、結果が表示されます。結果には、カスタムフィルタリング機能に関する2行の情報が表示されます。次の画面例の、青でハイライト表示された箇所です。

The screenshot displays the ESM console interface. On the left, the 'Navigator' pane shows a tree view of connectors under 'testLoc', with 'syslog-main(running)' selected. The right pane, titled 'Viewer', shows the output of the 'Connector Command - Get Status' for 'syslog-main'. The output includes a table of connector status and a detailed list of metrics. Two lines in the metrics list are highlighted in blue:

Connector Command	Time	Connector
Connector Command - Get Status	27 Mar 2017 11:31:16 PDT	syslog-main

```

From Connector:: syslog-main (3Rt5jAVsBABDHRiscS3ggDQ==)

Status Generated: Mon Mar 27 11:31:16 PDT 2017
Memory Usage: 32Mb out of 230Mb

Agent Type.....syslog
Agent Version.....7.5.0.32738.0
CommandResponses Processed.....3
Custom Filtering: Events Filtered Out.....5
Custom Filtering: Events Filtering State.....Events Filtering Enabled Through Exclude Filter
Event rate LTC.....Mon Mar 27 11:28:47 PDT 2017
Events Processed.....11
Events Processed(SLC).....6
Events/Sec.....0.09482758620689655
Events/Sec(SLC).....0.1
FCP Version.....0
FIPS Enabled.....false
First CommandResponse Processed.....Mon Mar 27 11:27:47 PDT 2017
First Event Processed.....Mon Mar 27 11:27:50 PDT 2017
Host Address.....10.12.90.80
Host Name.....10.12.90.80
Last CommandResponse Processed.....Mon Mar 27 11:28:47 PDT 2017
Last Event Processed.....Mon Mar 27 11:29:47 PDT 2017
Parser AUP Version.....7.5.0.32738.0
Queue Drop Count.....0.0
Queue Rate.....0.075
Queue Rate(SLC).....0.0

```

コマンドライン

コネクタのコマンドラインからステータスを取得するには、<ARCSIGHT_HOME>/current/binから次のコマンドを入力します。

```
arcsight agentcommand -c status
```

パターンの例

パターンは、`java.util.regex.Pattern`クラスでコンパイルされます。空白以外のパターンのうち、コンパイル可能なパターンが有効なパターンと見なされます。次の表に、有効なパターンと結果の例をいくつかまとめます。

有効なパターンの例	実行結果
<code>customeventsfilter.regex.pattern.exclude=IPSec\\s+tunnel</code>	rawEventにIPsec tunnelというパターンがあるイベントをすべて除外します。
<code>customeventsfilter.regex.pattern.exclude="Bad\\s+\\S+"</code>	rawEventに "Bad anyWord" というパターン (二重引用符を含む) があるイベントをすべて除外します。
<code>customeventsfilter.regex.pattern.exclude=111.112.113.114</code>	rawEventにIP 111.112.113.114が含まれるイベントをすべて除外します。
<code>customeventsfilter.regex.pattern.include=remote_peer-_ip\\s*=\\s*\\d+\\.\\d+\\.\\d+\\.\\d+</code>	包含フィルターが有効になり (ただし、除外パターンが空の場合)、指定のパターンを含むイベントのみが抽出されます。たとえば、rawEventに <code>remote_peer-_ip = 11.12.13.14</code> が含まれるイベントはフィルター条件を満たします。

次の10件のメッセージは、実際のrawEventです。この10件のrawEventにフィルターを適用した場合に、イベントがどのように除外または含まれるのかを、4つのケースを使って説明します。

1. Nov 28 22:03:21 10.0.111.2 Nov 28 2016 22:02:17: %PIX-6-106015: Deny TCP (no connection) from 101.102.103.104/3671 to 10.0.111.22/80 flags RST ACK on interface inside
2. Nov 28 22:03:21 10.0.111.2 Nov 28 2016 22:02:17: %PIX-2-106006: Deny inbound UDP from 10.0.65.116/2908 to 10.0.126.55/123 on interface outside
3. Nov 28 22:03:53 10.0.111.2 Nov 28 2016 22:02:49: %PIX-2-106020: Deny IP teardrop fragment (size = 32, offset = 0) from 101.102.103.104 to 10.0.126.55
4. Nov 28 22:04:09 10.0.111.2 Nov 28 2016 22:03:04: %PIX-2-106001: Inbound TCP connection denied from 10.0.65.116/3694 to 10.0.126.55/23 flags SYN on interface outside
5. Nov 28 22:04:10 10.0.111.2 Nov 28 2016 22:03:05: %PIX-3-305005: No translation group found for tcp src inside:10.0.112.9/37 dst outside:10.0.65.116/3562

6. Nov 28 22:04:44 10.0.111.2 Nov 28 2016 22:03:39: %PIX-2-106001: Inbound TCP connection denied from 10.11.12.13/3699 to 10.0.126.55/8080 flags SYN on interface outside
7. Nov 28 22:05:07 10.0.111.2 Nov 28 2016 22:04:02: %PIX-4-500004: Invalid transport field for protocol=17, from 10.0.142.116/1234 to 10.0.126.55/0
8. Nov 28 22:05:25 10.0.111.2 Nov 28 2016 22:04:20: %PIX-2-106020: Deny IP teardrop fragment (size = 36, offset = 0) from 10.11.12.13 to 10.0.126.55
9. Nov 28 22:06:01 10.0.111.2 Nov 28 2016 22:04:57: %PIX-2-106012: Deny IP from 10.0.142.116 to 10.0.126.55, IP options: "0x1f"
10. Nov 28 22:06:10 10.0.111.2 Nov 28 2016 22:05:05: %PIX-3-305005: No translation group found for tcp src inside:10.0.112.9/37 dst outside:101.102.103.104/3562

次に、上記のRAWイベントに4つの異なるフィルタリングを適用したケースの結果を示します。

ケース1:

```
customeventsfilter.regex.enabled=true
customeventsfilter.regex.pattern.exclude=Deny IP.*from \d+\.\d+\.\d+\.\d+
```

フローからイベント3、8、9が除外されます。このパターンは、1つのRAWイベントに<Deny IP>と<from IPaddress>の両方が存在するRAWイベントをすべて除外します。

ケース2:

```
customeventsfilter.regex.enabled=true
customeventsfilter.regex.pattern.exclude=(10.11.12.13)|(101.102.103.104)
```

フローからイベント1、3、6、8、10が除外されます。このパターンは、IPが10.11.12.13または101.102.103.104のRAWイベントをすべて除外します。

ケース3:

```
customeventsfilter.regex.enabled=true
customeventsfilter.regex.pattern.include=(10.11.12.13)|(101.102.103.104)
```

フローからイベント2、4、5、7、9が除外されます。このパターンは、IPが10.11.12.13または101.102.103.104 (両方のIPが同じパターンである必要はありません) のRAWイベントを含めます。どちらのIPも含まれていないイベントはすべて除外されます。

ケース4:

```
customeventsfilter.regex.enabled=false
customeventsfilter.regex.pattern.include=(10.11.12.13)|(101.102.103.104)
```

enabledプロパティがfalseに指定されているので、フィルタリングは実行されません。

agent.log内のログメッセージ

コネクターの初期化では、フィルタリングステータスとパターンに関する情報メッセージおよびエラーメッセージは、agent.logファイルに記録されます。以下は、agent.logファイルからの抜粋です。除外パターンで無効な正規表現が定義されている例です。

```
[2017-03-24 16:07:54,485][INFO ][default.com.arcsight.agent.loadable._CustomEventsRegexFilter]
[init] CustomEventsRegexFilter Initialized: Filtering Enabled =true, Exclude Regex =remote_peer_
ip\s+\is\s+\d+\d+\d+\d+, Include Regex =
```

```
[2017-03-24 16:07:54,485][ERROR][default.com.arcsight.agent.loadable._
CustomEventsRegexFilter][init] Unable to compile custom filter exclude regex=remote_peer_
ip\s+\is\s+\d+\d+\d+\d+
```

```
[2017-03-24 16:07:54,500][INFO ][default.com.arcsight.agent.loadable._CustomEventsRegexFilter]
[init] Events Filtering Disabled Due to Syntax Error in User Defined Regex
```

第5章: ArcSight Management Center/コネクタ アプライアンスとコネクタ

HP ArcSightでは、複数のコネクタを一元管理する方法として、コネクタアプライアンスとArcSight Management Centerという2つのソリューションが提供されています。コネクタアプライアンスはHP ArcSightレガシー製品であり、複数のコネクタを一元的に管理および監視する機能を備えています。この後継製品となるのがArcSight Management Center (ArcSight Management Center) です。コネクタアプライアンスが持つすべてのコネクタ管理機能に加えて、他のArcSight製品 (コネクタアプライアンス、Logger、他のArcSight Management Center) の管理機能と監視機能も備えています。ArcSight Management Center/コネクタアプライアンスは、Webベースのユーザーインターフェイスを使用して、ローカルおよびリモートのコネクタを管理します。

ArcSight Management Centerまたはコネクタアプライアンスの操作方法については、『HP ArcSight Management Center管理者ガイド』または『ArcSight Connector Appliance Administrator's Guide』を参照してください。

ESMにイベントを転送するコネクタは、コンソールで管理できます。したがって、コネクタの通知先がESMのみである場合、ArcSight Management Center/コネクタアプライアンスは必要ありません。ただし、複数の異種混在環境 (たとえば、LoggerとESMが混在する環境)、Loggerのみの環境、多数のコネクタが存在する環境 (MSSP環境など) では、ArcSight Management Center/コネクタアプライアンスは大きな威力を発揮します。

ArcSight Management Center/コネクタアプライアンスのコネクタは、コンテナでグループ化されます。各コンテナはJava仮想マシン (JVM) であり、複数のコネクタをグループ化できます。

ArcSight Management Center/コネクタアプライアンスでの コネクタ管理

ArcSight Management Center/コネクタアプライアンスは、次の3種類のコネクタを管理します。

- 「ローカル (オンボード) コネクタ」(次のページ)
- 「リモートArcSight Management Center/コネクタアプライアンスのコネクタ」(次のページ)
- 「ソフトウェアベースコネクタ」(次のページ)

ローカル (オンボード) コネクタ

ArcSight Management Center/コネクタアプライアンスには、複数のコンテナとオンボードコネクタが実装されています。ローカルコネクタとリモートコネクタの管理は、管理者向けインターフェイスで実行できます。

注: オンボードコネクタがビジー状態になると、ArcSight Management Center/コネクタアプライアンスのWebベースインターフェイスのパフォーマンスが低下することがあります。

リモートArcSight Management Center/コネクタアプライアンスのコネクタ

ArcSight Management Center/コネクタアプライアンスは、リモートArcSight Management Centers/コネクタアプライアンスのコネクタや、他のArcSightハードウェアソリューション (Loggerなど) のコネクタを管理できます。

ソフトウェアベースコネクタ

一部のArcSight Management Center/コネクタアプライアンスモデルは、インストール済みのソフトウェアベースコネクタのリモート管理に対応していますが、ソフトウェアコネクタのリモート管理機能はデフォルトで無効になっています。

注: ESMまたはExpressでは、以下の手順を実行する必要はありません。これらはSmartConnectorをサービスとして実行する場合の手順であり、自動で再起動できないスタンドアロンSmartConnectorは該当しません。

ソフトウェアベースのコネクタをArcSight Management Center/コネクタアプライアンスで管理するには、コネクタでリモート管理を有効にする必要があります。ArcSight Management Center/コネクタアプライアンスで管理するコネクタのインストールディレクトリにあるuser/agent/agent.propertiesファイルに、次のプロパティを追加します。

```
remote.management.enabled=true
```

コネクタを再起動すると、プロパティの変更が有効になります。

コネクタがリッスンするポートのカスタマイズも可能です。デフォルトポートは9001ですが、user/agent/agent.propertiesに次のプロパティを追加することで変更が可能です。

```
remote.management.listener.port=9002
```

上記の例では、コネクタはポート9002をリッスンします。

注意: リモート管理をサポートしているのは第5世代のコネクタのみです。

この機能を使用するには、ビルド4855 (4.0.5.4878.0) 以降のコネクタが必要です。AIXを実行するコネクタでは、リモート管理はサポートされていません。これは、AIXプラットフォーム内の要素の制限によるものです。

ヒント: 1つのホストに複数のソフトウェアベースコネクタをインストールするには、ポートを個別に割り当てる必要があります。コネクタのデフォルトポートは9001なので、同じホストにインストールする2番目以降のコネクタはそれ以外のポートを使用する必要があります。9002、9003、9004などのポートの使用をお勧めします。

ArcSight Management Center/コネクタアプライアンスがサポートするコネクタのリストは、『Connector Appliance Release Notes』を参照してください。Protect 724コミュニティサイト (<https://protect724.hpe.com>) にもアクセスできます。ArcSightには、新しいコネクタが定期的に追加されます。

ソフトウェアベースコネクタのリモート管理で使用するログイン資格情報

ソフトウェアベースコネクタのリモート管理では、ログイン資格情報が必要です。各コネクタには、以下に示すデフォルトの資格情報があらかじめ定義されています。ユーザー名は変更できません。デフォルトのパスワードを変更する方法については、『ArcSight Management Center管理者ガイド』の「コンテナ認証情報の変更」または『ArcSight Connector Appliance Administrator's Guide』の「Changing Container Credentials」を参照してください。

注: ロードバランサーが動作するためには、コネクタでデフォルトのリモート管理ユーザー名およびパスワードを使用する必要があります。

管理者に問い合わせ、ご使用の環境に適した資格情報を確認してください。リモート管理用のデフォルト資格情報は、以下の通りです。

- ユーザー名: connector_user
- パスワード: change_me

展開シナリオの選択

ArcSight Management Center/コネクタアプライアンスは、コネクタが必要となる任意の場所に展開できます。次のような利点があります。

- ESMを使用せずにコネクタを管理可能 (Loggerのみの環境)
- 実行時パラメーターをリモート管理可能 (帯域幅の管理など)
- コネクタのアップグレードを一元管理可能
- コネクタのトラブルシューティングを一元実行可能

ArcSight Logger

Loggerはコネクタとの間でイベントの送受信を行います。ESMのように高度なコネクタ管理機能はありません。

Loggerのみの環境では、ArcSight Management Center/コネクタアプライアンスを使用することに多くのメリットがあります。ESMの管理機能も、すべてではありませんがほとんど利用可能になります (たとえば、フィルター設計機能はありません)。また、ArcSight Management Center/コネクタアプライアンスは、一括処理などESMにはない機能も備えています (複数のコネクタを一括管理)。

さらにArcSight Management Center/コネクタアプライアンスは、フェイルオーバー通知先を使ったコネクタ設定にも対応しているので、Loggerの冗長展開によるフェイルオーバーの一元管理も可能です。プライマリ通知先に通信障害が発生した場合に別のLoggerやイベントファイルにイベントを送信する設定を、すべてまたは一部のコネクタで行うこともできます。

Loggerの詳細については、「[ArcSight Logger SmartMessage \(暗号化\) 通知先](#)」(82ページ) を参照してください。

ArcSight ESM

ArcSight Management Center/コネクタアプライアンスをESM環境に展開すると、コネクタのアップグレード、ログ管理、その他の設定の問題を一元管理できます。詳細については、「[ArcSight マネージャー \(暗号化\)](#)」(79ページ) を参照してください。

ESMとLogger

ArcSight Management Center/コネクタアプライアンスは、ESMとLoggerにイベントを同時送信する場合のタイミングを一元管理します。たとえば、Loggerにはすべてのイベントを送信し、ESMには (詳細な分析のために) 重要なイベントのみを送信する方法や、両方にすべてのイベントを送信するものの、Loggerではイベントの保持期間を長期間に設定する方法などがあります。

コネクタにはそれぞれ通知先パラメーターが設定されていますが、ArcSight Management Center/コネクタアプライアンスでは「一括」管理が可能です。これにより、個々のリモートコネクタホストに手動でアクセスして通知先を追加または変更する手間を省くことができます。

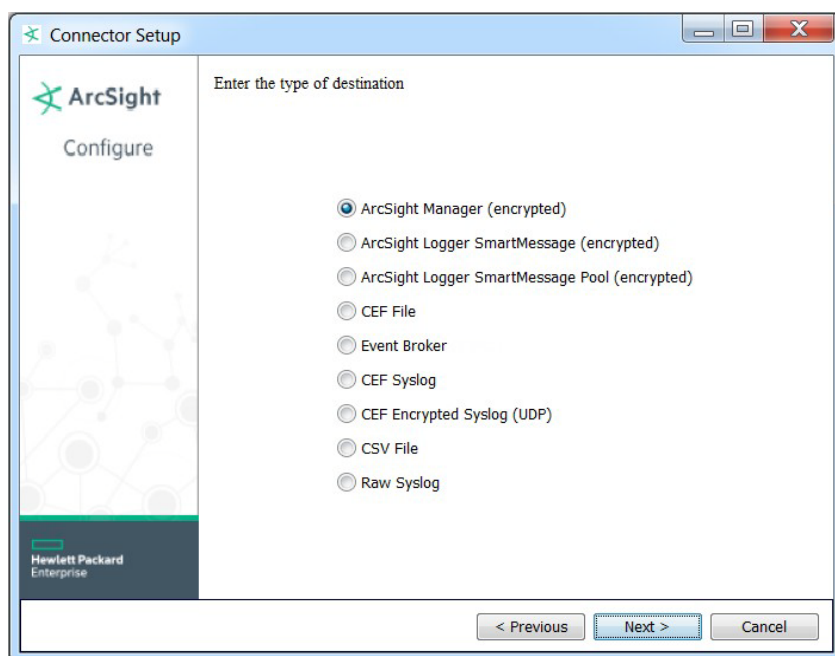
ArcSight Management Center/コネクタアプライアンスの詳細については、『HP ArcSight Management Center管理者ガイド』または『ArcSight Connector Appliance Administrator's Guide』を参照してください。

第6章: コネクターの通知先の概要

この章では、コネクターでイベントを1つまたは複数の通知先に送信する設定を行う方法について説明します。通知先には、マネージャーや、特定のコネクターからイベントを受信できるデバイスを指定します。以下の説明では、コネクター設定で選択できる通知先が表示されていますが、イベントは、これ以外にもフェイルオーバーなどの通知先に送信できます。

コネクターの通知先

コネクターのインストールでは、コネクターが収集したイベントを送信する通知先を指定します。通知先は、次のウィンドウに表示されるリストから選択します。



ArcSight Manager (encrypted)

最も多く使用される通知先です。コネクターがマネージャーにイベントを送信すると、マネージャーはイベントをリレーショナルデータベースに格納し、関連エンジンで処理してから、コンソールやWebインターフェイスに表示します。詳細については、「[ArcSightマネージャー \(暗号化\)](#)」(79ページ)とコンソールのオンラインヘルプを参照してください。

ESMとSmartConnectorでFIPSを設定する方法については、[Protect 724](#)の「Configuring FIPS for ESM and SmartConnectors」を参照してください。

ArcSight Logger SmartMessage (encrypted)

コネクターは、CEFイベントを暗号化してLoggerに送信することができ、オプションでSmartMessageと呼ばれる圧縮チャンネルの使用が可能です。また、LoggerはCEF syslogイベントをコネクターから受信できます。詳細については、「[ArcSight Logger SmartMessage \(暗号化\) 通知先](#)」(82ページ) を参照してください。

ArcSight Logger SmartMessage Pool (encrypted)

複数のLoggerデバイスで構成されたプールがあり、プール内のLogger間でイベントが分散されている場合、そのプールを1つの通知先として指定することが可能です。コネクターが処理するイベントの「バッチ」は、ラウンドロビン方式で、プール内の次のLoggerに送信されます。詳細については、「[Loggerプールの通知先設定](#)」(89ページ) を参照してください。

CEF File

セキュリティイベントをマネージャーに転送するのではなく、共通イベントフォーマット (CEF) ファイルにキャプチャーします。

詳細については、「[CEF通知先](#)」(93ページ) を参照してください。

Event Broker

イベントを共通イベントフォーマット (CEF) またはバイナリ形式でEvent Brokerにピックに送信します。Event Broker内のイベントは、任意の数のアプリケーションが取得できます。

ESMIに適用する [**AUP Master Destination**] と [**Filter Out All Events**] は、**True**に設定する必要があります。詳細については、「[ArcSightマネージャー \(暗号化\)](#)」を参照してください。

Event BrokerとSmartConnectorでFIPSを設定する方法については、[Protect 724](#)の「Configuring FIPS for Event Broker and SmartConnectors」を参照してください。

詳細については、「[Event Broker](#)」(94ページ) を参照してください。

CEF Syslog

共通イベントフォーマット (CEF) (UTF-8エンコーディングでバイトに変換) でイベントを送信します。UDP、TCP、TLSの3つのプロトコルを使用できます。

TCPと**UDP**は、Loggerへの送信に使用できます (TLSは使用できません)。このプロトコルを介するデータは、TCPレシーバーまたはUDPレシーバーで受信します。1つのレシーバーで複数のコネクターからの受信が可能です。TCPとUDPは、Syslog Daemonコネクターへの送信にも使用できます。

TLSプロトコルは、セキュアなチャネルを確立し、1方向または双方向の認証をサポートします。TLSプロトコルを選択すると、Syslog NG Connectorによるイベント受信が可能になります。

この通知先の詳細については、「[CEF通知先](#)」(93ページ) を参照してください。Syslog NG Connectorの詳細については、『SmartConnector for Syslog NG Daemon』を参照してください

CEF Encrypted Syslog (UDP)

この通知先は、UDPプロトコルを使用して共通イベントフォーマット (CEF) でイベントを送信し、対称鍵暗号化を行います。このオプションは、データ暗号化設定が必要になる「共有秘密」鍵に対応しています。このデータはレシーバー側で、CEF Encrypted Syslog (UDP) コネクターによって復号化されます。

この通知先の詳細については、「[CEF通知先](#)」(93ページ) を参照してください。データを復号化する方法については、『SmartConnector for ArcSight CEF Encrypted Syslog (UDP)』を参照してください。

CSV File

通常はコネクターがマネージャーに送信するイベントを、CSVファイルにキャプチャーします。これは高度な方法です。一般的なArcSight設定では、マネージャーとのイベントのやり取りに外部ファイルを使用する必要はありません。詳細については、「[CSVファイル通知先](#)」(102ページ) を参照してください。

Raw Syslog

未加工のsyslogイベントを、UDP、TCP、TLSプロトコルで送信します。Raw Syslog Daemon向けのコネクターを使用して、今後の処理のために未加工の解析前イベントを収集します。詳細については、「[Raw Syslog通知先](#)」(105ページ) を参照してください。ArcSight Loggerへのデータ転送では、設定パラメーターを使用することにより、syslogデータ (ソースとタイムスタンプ) の正規化を最小限に抑えることができます。

通知先の追加

コネクターは、追加で設定した通知先にイベントのコピーを送信します。ArcSightの開発環境と運用環境を並行して運用し、ルールやレポートをテストしたい場合などには、通知先を追加すると便利です。複数の通知先を設定したり、プライマリ通知先が使用不能になった場合に備えてフェイルオーバー通知先を設定したりすることも可能です。

運用環境マネージャーと開発環境マネージャーの両方にアラートを送信する設定をコネクターで行っておけば、両方のシステムでイベントフローをリアルタイムで確認できます。通知先はそれぞれ独立して動作するので、運用環境マネージャーに送信するイベントが影響を受けることはありません。追加方法については、「[通知先の追加、変更、削除](#)」(44ページ) を参照してください。

フェイルオーバー通知先

それぞれのコネクタ通知先には、コネクタからのセキュリティイベントを受信するフェイルオーバー通知先を設定できます。プライマリ通知先 (マネージャーなど) が使用不能 (ネットワーク障害など) になった場合や、受信イベントを処理しきれなくなった場合にフェイルオーバーが動作を開始し、フェイルオーバー通知先にイベントがバックアップされます。また、コネクタは、可能な限りイベントをキャッシュし、フローが復旧した時点でプライマリ通知先に再送します。

プライマリ通知先が動作している間は、フェイルオーバー通知先は動作しません。したがって、セカンダリマネージャーのレポートやリプレイ機能には、不完全な情報が含まれる可能性があります。フェイルオーバーとは、プライマリ通知先に重大な問題が発生した場合に、リアルタイムで処理を引き継ぐ機能です。詳細については、「[フェイルオーバーの追加](#)」を参照してください。

第7章: 通知先の設定

SmartConnectorでイベント送信の設定を行ったら、[Modify Destination Settings] セクションで詳細な動作を設定します。選択項目の詳細を以下の表にまとめます。

次の表では、設定可能な値について説明します。

設定

フィールド名	値
Batching	SmartConnectorでイベントを一括転送することで、ネットワークのパフォーマンス向上と帯域幅の最適化が可能です。一括処理をアクティブにすると、SmartConnectorはイベントブロックを作成し、(1) ブロックが特定のサイズに達した時点、または (2) 特定の時間が経過した時点でブロックを送信します。また、重要度に基づいてバッチに優先順位を付けることも可能です。これにより、重要度が高い順にブロックが送信されます。
Enable Batching (per event)	指定したサイズのイベントバッチを作成します (100、200、300、400、500、200、600件のイベント)。デフォルト値は100です。 注意: バッチサイズを500または600に設定すると、データ損失の恐れがあります。このサイズに設定する場合には、カスタマーサポートに事前にお問い合わせください。
Enable Batching (in seconds)	指定した時間 (1、5、10、15、30、60秒) が経過した時点でイベントを送信します。 デフォルト値は5です。
Batch By	到着した順序でバッチを送信する場合は [Time Based] (デフォルト)、重要度に基づいてバッチを送信する場合は [Severity Based] (緊急度が最も高いイベントのバッチを最初に送信) を指定します。
Time Correction	時刻の報告が正しくないデバイスの問題をいくつかの方法で修正します。
Use Connector Time as Device Time	(No Yes) デバイスが報告する時刻をオーバーライドし、コネクタがイベントを受信した時刻を使用します。コネクタが報告する時刻の方が正確である可能性が高い場合に、このオプションを使用します。 デフォルトは [No] です。
Enable Device Time Correction (in seconds)	deviceReceiptTimeフィールドで報告される時刻を、この設定に基づいて調整します。リモートデバイスのクロックがArcSightマネージャーと同期されていない場合に、この設定を行います。これは一時的な設定として使用してください。マネージャーとデバイスのクロック同期には、NTPプロトコルをお勧めします。このパラメーターは、startTimeフィールドとendTimeフィールドに影響します。 デフォルト値は0です。

設定 (続き)

フィールド名	値
Enable Connector Time Correction (in seconds)	この設定を使用することで、SmartConnectorは、SmartConnector自身が報告するコネクタ時刻も調整できます。これは情報提供のみを目的としており、SmartConnectorのローカル時刻を変更できます。これは一時的な設定として使用してください。マネージャーとSmartConnectorのクロック同期には、NTPプロトコルをお勧めします。 デフォルト値は0です。
Set Device Time Zone To	(Disabled <タイムゾーン>) (デフォルトは [Disabled]) 通常、オリジナルデバイスが時刻に加えてタイムゾーンも報告することが前提となります。また、オリジナルデバイスがタイムゾーンを報告しない場合は、SmartConnectorが報告することが前提となります。この方法でタイムゾーンが報告されていない場合や、デバイスが報告するタイムゾーンが正しくない場合、このオプションを [Disabled] からGMTなどのワールドタイムゾーンに切り替えることができます。ドロップダウンリストからオプションを選択してください。選択したタイムゾーンが、報告される時刻に適用されます。
Device Time Auto- correction	デバイスの時刻を自動補正する範囲を選択します。
Future Threshold	検出時刻がコネクタの時刻より、[Future Threshold] で設定されている秒数以上進んでいる場合に自動補正します。[Future Threshold] と [Past Threshold] の一方または両方が負の値である場合、自動補正は無効になります。 デフォルト値は-1です。
Past Threshold	検出時刻がコネクタの時刻より、[Past Threshold] で設定されている秒数以上遅れている場合に自動補正します。 デフォルト値は-1です。
Device List	閾値が適用されるデバイスのカンマ区切りのリストです。デフォルト ([ALL]) は、すべてのデバイスを意味します。
Time Checking	
Future Threshold	コネクタの時刻チェック用進み閾値を延長する秒数。 デフォルト値は5分 (300秒) です。
Past Threshold	コネクタの時刻チェック用遅れ閾値を延長する秒数。 デフォルト値は1時間 (3600秒) です。
Frequency	未来の閾値と過去の閾値を指定された秒間隔でチェックします。 デフォルト値は1分 (60秒) です。

設定 (続き)

フィールド名	値
Cache	キャッシュ設定を変更しても、キャッシュ済みのイベントに影響することはありません。新たにキャッシュに送信されるイベントのみが対象となります。
Cache Size	ArcSightマネージャーがダウンした場合やSmartConnectorが大量のイベントを受信した場合、SmartConnectorは圧縮ディスクキャッシュを使用して大量のイベントを保持します。このパラメーターでは、使用するディスク容量を指定します。デフォルト値は 1GB であり、コネクタによって異なりますが、およそ1,500万件のイベントを保持できます。設定可能な最小値は200MBです。このディスク容量が一杯になると、SmartConnectorは最も古いイベントを破棄してディスクキャッシュスペースを空けます。ドロップダウンリストからオプションを選択してください。 デフォルト値は1GBです。
Notification Threshold	通知をトリガーするキャッシュ内のイベント件数。デフォルト値は10,000件です。
Notification Frequency	通知閾値に達した後、通知を送信する頻度です。ドロップダウンリストからオプションを選択してください。 デフォルト値は10分です。
Network	
Heartbeat Frequency	コネクタがArcSightマネージャーにハートビートメッセージを送信する頻度を制御します。デフォルトは 5秒 ですが、 5秒~10分 の範囲で設定できます。ハートビートはSmartConnectorとの通信にも使用されるので、頻度を 10分 に設定すると、SmartConnectorへの設定情報やコマンドの送信にも同じように10分かかる可能性があります。ドロップダウンリストからオプションを選択してください。 デフォルト値は10秒です。
Enable Name Resolution	(No Source/Dest only Yes) イベントレート内で実行できて、名前解決が必要な場合、SmartConnectorはIPアドレスをホスト名に、ホスト名をIPアドレスに解決します。この設定により、名前解決機能が制御されます。ソース、ターゲット、デバイスのIPアドレスとホスト名も、この設定の影響を受ける場合があります。[Source/Dest Only] を選択すると、デバイスアドレスとデバイスホスト名のフィールドは名前解決で無視されます。 デフォルトは [Yes] です。
IPv6 Name Resolution Control	<ul style="list-style-type: none"> • IPv4 Only for Legacy Events (デフォルト) • IPv6 (Prefer IPv4 for reverse resolution) for Legacy Events • IPv6 (Prefer IPv6 for reverse resolution) for Legacy Events
Name Resolution TTL (secs)	名前解決を有効にする時間 (Time to Live) です。名前解決エントリは、この時間だけキャッシュされます (デフォルトは 3600秒 です)。
Wait For Name Resolution	(Yes No) [Yes] に設定すると、SmartConnectorは名前解決が完了するまで待機します。[Yes] を選択した場合、イベントの処理速度が大幅に低下し、イベントが失われる可能性もあります。 デフォルトは [No] です。

設定 (続き)

フィールド名	値
Name Resolution Host Name Options	<ul style="list-style-type: none"> • Set host name only (デフォルト) • Set host name only (lowercase) • Set host and domain names • Set host and domain names (lowercase) <p>逆解決 (IPアドレスからホスト名への解決) の場合、ホスト名フィールドのみが設定されます。[host name only] 以外の場合、ホスト名は分割され、DNSドメインフィールドとホスト名フィールドの両方に入力されます。この設定は、ソース、ターゲット、デバイス、エージェントのアドレスに影響します。[(lowercase)] オプションのいずれかを選択すると、名前は小文字に変換されてからホスト名 (およびDNSドメイン) フィールドに入力されます。</p>
Name Resolution Domain from Email	<p>(Yes No) [Yes] に設定すると、ホスト名とDNSドメインのフィールドが空で、対応するユーザー名フィールドにメールアドレスが表示される場合、メールアドレスのドメインがDNSドメインフィールドに入力されます。この設定は、ソースおよびターゲットのフィールドにのみ影響します。</p> <p>デフォルトは [Yes] です。</p>
Clear Host Names Same as IP Address	<p>(Yes No) [Yes] に設定した状態で、ホスト名フィールドが、対応するIPアドレスフィールドと一致するIPアドレスに設定されている場合、ホスト名フィールドはクリアされます。この設定は、ソース、ターゲット、デバイスの各フィールドに影響します。</p> <p>デフォルトは [Yes] です。</p>
Set Host Names to IP Addresses When Unknown	<p>(Yes No) [Yes] に設定すると、未解決のホスト名をIPアドレスに設定します。</p> <p>デフォルトは [No] です。</p>
Don't Resolve Host Names Matching	<p>デフォルトでは、ホスト名はIPアドレスに解決されます。ここでは、「システムがホスト名からIPアドレスへの解決を試行する必要のない」ホスト名の全部または一部に対応する正規表現を指定することができます。</p> <p>このオプションを設定すると、システムはこの表現と一致するホスト名を解決できません。</p>
Don't Reverse- Resolve IP Ranges	<p>デフォルトでは、IPアドレスはドメイン名に解決されます。ここでは、「システムがドメイン名への逆解決を試行する必要のない」IPアドレスの範囲を指定することができます。</p> <p>このフィールドをクリックして、IPアドレスの範囲を入力します。IPアドレスを1つだけ入力する場合は、[From] 列にアドレスを入力し、[To] 列は空白のままにして、[Apply] をクリックします。アドレスの範囲を指定する場合は、[From] 列に開始IPアドレスを入力し、[To] 列に終了アドレスを入力して、[Apply] をクリックします。このフィールドには、範囲のリストを入力できます。</p> <p>このオプションを設定すると、システムは指定範囲に含まれるIPアドレスの逆解決を実行できません。</p>
Remove Unresolvable Names/IPs from Cache	<p>(Yes Yes (w/ negative cache) No) [No] に設定すると、解決できないホスト名またはIPアドレスはキャッシュに残ったままになります。[Yes] に設定すると、解決できないホスト名またはIPアドレスはキャッシュから消去されます。[Yes (w/negative cache)] に設定すると、コネクタは、解決できなかった名前/IPを保存することで、同じ名前解決を繰り返さないようにします。</p> <p>デフォルトは [No] です。</p>

設定 (続き)

フィールド名	値
Limit Bandwidth To	ネットワーク上でのコネクタ出力を抑制する帯域幅オプションを選択します。ドロップダウンリストからオプションを選択してください。 デフォルトは [Disabled] です。
Transport Mode	(Normal Cache Cache but send Very High severity events) 。SmartConnectorが受信して処理した全イベントをディスクにキャッシュする設定が可能です。これは、SmartConnectorを一時停止するのと同等の設定です。ただし、この設定を使用すれば、特定の期間に発生するイベント送信を遅らせることができます。たとえば、日中のイベントをキャッシュしておき、夜間に送信することができます。また、業務時間内は重要度が非常に高いイベントを除いてすべてのイベントをキャッシュし、残りを夜間に送信する設定も可能です。 デフォルトは [Normal] です。
Cache Mode	(Normal Drop if Dest Down) プライマリ送信先がダウンし、コネクタがフェイルオーバー通知先へのイベント送信を開始したときに、プライマリ送信先のキャッシング動作を制御します。[Normal] モードでは、イベントはキャッシュされ、プライマリ通知先が復帰した時点で送信されます。[Drop if Dest Down] モードでは、イベントはキャッシュされず、ドロップされます。したがって、イベントはプライマリ通知先が復帰しても送信されません。 デフォルトは [Normal] です。
Address-Based Zone Population Defaults Enabled	(Yes No) [Yes] の場合、コネクタのデフォルトゾーンをゾーンの割り当てに使用します。このゾーンが使用されるのは、ESMまたはArcMCがネットワークモデルを送信しない場合、またはネットワークモデルでカバーできないアドレスがある場合のみです。[Address-Based Zone Population] (下記) を指定する場合は、[No] に変更してもかまいません。 デフォルトは [Yes] です。
Address-Based Zone Population	セットアップ時またはArcMCで指定する場合、3つの要素をカンマ区切りにしたリストを指定します。3つの要素のうち、1番目はゾーンの開始IPアドレス、2番目は終了IPアドレス、3番目はこのアドレス範囲に割り当てるゾーンのURIです。このゾーンが使用されるのは、ESMまたはArcMCがネットワークモデルを送信しない場合、またはネットワークモデルでカバーできないアドレスがある場合のみです。[Address-Based Zone Population Defaults Enabled] が [Yes] に設定されていても、ここで指定したゾーンが優先されます。 たとえば、2つのゾーンの例として、15.0.0.0,15.255.255.255,/All Zones/ArcSight System/Public Address Space Zones/Hewlett-Packard Company,17.0.0.0,17.255.255.255,/All Zones/ArcSight System/Public Address Space Zones/Apple Computer Inc.があります。
Zone Population Mode	(Normal Rezone (override) No Zoning (clear)) [Normal] に設定すると、ゾーンが未設定の場合、計算して割り当てを行います。[Rezone (override)] は、すでに読み込まれているゾーンを再計算および再割り当てします。[No Zoning (clear)] は、ゾーンがすでに読み込まれている場合、クリアします。 デフォルトは [Normal] です。
Customer URI	指定した顧客URIを、コネクタから受信するイベントに適用します。顧客リソースが存在する場合、ArcSightマネージャー上の全顧客フィールドが入力されます。このコネクタで報告されるデータが、複数の顧客に適用される可能性がある場合、このフィールドでVelocityテンプレートを使用することで、条件に基づいて顧客を識別することができます。

設定 (続き)

フィールド名	値
Field Based Aggregation	<p>フィールドベースのアグリゲーションは、柔軟性の高いアグリゲーションメカニズムを実装します。2つのイベントがあり、両方のイベントの「選択された」フィールドだけが同一である場合でも、イベントはアグリゲーションされます</p> <p>注: フィールドベースのアグリゲーションでは、[Preserve Common Fields] が [Yes] に設定されている場合を除いて、指定されたフィールドのみを含む新しいアラートが作成され、残りのフィールドは無視されます。</p> <p>SmartConnectorでアグリゲーションを使用すると、受信データ量が大幅に削減されます。ただし、イベントが提供するすべての情報は必要なく、一部のみを使用する場合にのみ適用してください。たとえば、フィールドベースのアグリゲーションを有効にし、ファイアウォールで「許可」と「拒否」の件数を集計できます。ただし、ファイアウォールで提供されるすべての情報ではなく、イベントの件数が必要である場合のみ使用する必要があります。</p>
Time Interval	<p>コネクタが収集するイベントの集約の基準となる時間間隔を選択します (該当する場合)。アグリゲーションを有効にするには、アグリゲーションの時間間隔と閾値を両方とも設定する必要があります。ドロップダウンリストからオプションを選択してください。</p> <p>デフォルトは [Disabled] です。</p>
Event Threshold	<p>コネクタが収集するイベントの集約の基準となるイベント数を選択します (該当する場合)。アグリゲーションを実行できるイベントの最大数を指定します。たとえば、選択した時間内に受信したイベントのうち、900件のイベントが同一である場合 (つまり、選択したフィールドが同一)、[Event Threshold] を500に設定すると、件数が500のイベントと400のイベントの2つのイベントを受信することになります。このオプションは、[Time Interval] と同時には使用できません。ドロップダウンリストからオプションを選択してください。</p> <p>デフォルトは [Disabled] です。</p>
Field Names	<p>コネクタが収集するイベントのアグリゲーションを行う場合の基準となるフィールドを1つ以上選択します。結果は、監視対象を示すカンマ区切りのフィールドリストになります。</p>
Fields to Sum	<p>コネクタが収集するイベントのアグリゲーションを行う場合の基準となるフィールドを1つ以上選択します。</p> <p>指定した場合、これらの数値フィールドは、アグリゲーション、保存、破棄されるのではなく、合計されます。合計されるフィールドの例には、bytesInやbytesOutがあります。ここで指定したフィールドが、アグリゲーションの対象となるフィールド名のリストにも含まれる場合、合計ではなくアグリゲーションが実行されます。</p>
Preserve Common Fields	<p>(Yes No) [Yes] を選択した場合、各イベントで値が同じフィールドは、アグリゲーション後のイベントに追加されます。[No] を選択すると (デフォルト)、アグリゲーション後のイベントで、集約対象外のフィールドは無視されます。</p>
Filter Aggregation	<p>フィルターアグリゲーションは、エージェントフィルターによって破棄されるイベントから、アグリゲーション後のイベントデータを取得するための手段です。フィルターアグリゲーションでは、フィルターで破棄されるイベントのみが考慮されます (すべてのイベントを参照するフィールドベースアグリゲーションとは異なります)。</p>
Time Interval	<p>コネクタが収集するイベントの集約の基準となる時間間隔を選択します (該当する場合)。これは、[Event Threshold] と同時には使用できません。ドロップダウンリストからオプションを選択してください。</p> <p>デフォルトは [Disabled] です。</p>

設定 (続き)

フィールド名	値
Event Threshold	<p>コネクターが収集するイベントの集約の基準となるイベント数を選択します (該当する場合)。アグリゲーションを実行できるイベントの最大数を指定します。たとえば、選択した時間内に受信したイベントのうち、900件のイベントが同一である場合 (つまり、選択したフィールドが同一)、[Event Threshold] を500に設定すると、件数が100のイベントと400のイベントの2つのイベントを受信することになります。このオプションは、[Time Interval] と同時には使用できません。ドロップダウンリストからオプションを選択してください。</p> <p>デフォルトは [Disabled] です。</p>
Fields to Sum	<p>(オプション) コネクターが収集するイベントのアグリゲーションを行う場合の基準となるフィールドを1つ以上選択します (該当する場合)。</p>
Processing	
Preserve Raw Event	<p>(Yes No) 一部のデバイスには、生成されるアラートの一部としてキャプチャーできるRAWイベントが含まれます。それ以外のデバイスでも、ほとんどのコネクターは、ArcSightイベント生成のために解析/処理されたシリアルデータストリームの生成も可能です。この機能によってコネクターは、シリアル化された「RAWイベント」をイベントインスペクター内のフィールドとして保存できます。この機能はデフォルトで無効化されています。RAWデータを使用するとイベントサイズが増え、必要なデータベース記憶領域も増大するからです。</p> <p>有効にするには、[Preserve Raw Event] 設定を変更します。[Yes] を選択すると、「RAWイベント」をシリアル化したデータが通知先に送信され、rawEventフィールドに保存されます。</p> <p>デフォルトは [No] です。</p>
Turbo Mode	<p>設定、レポート、分析での使用に影響しない場合、2つの「ターボ」(狭いデータ帯域幅) モードの1つを選択することで、SmartConnectorを介したセンサーのイベント情報送信を大幅に高速化できます。</p> <p>デフォルトの転送モードは [Complete] です。追加データ (カスタム、またはベンダー固有) を含め、デバイスから送信される全データを転送します。これは、マネージャーでのturbo.enabled=false設定に対応します。この値はデフォルトではないので、このプロパティをマネージャーの<ARCSIGHT_HOME>/config/server.propertiesファイルに追加してください。ファイルの変更後は、マネージャーを再起動する必要があります。</p> <p>最初のターボモードは [Faster] です。追加のデータのみを破棄し、他の情報はすべて保持します。もう1つの[Fastest] モードでは、最高のスループットを達成するために、コアイベント属性を除くすべてのデータを破棄します。このモードを選択する場合には、特定のデバイスからのデータセットを制限することによる影響 (たとえば、レポート、ルール、脅威の解決に及ぼす影響) を検討してください。</p> <p>このモードで適用されるイベント属性は、ArcSightマネージャーの<ARCSIGHT_HOME>/config/server.default.propertiesファイルで定義されています。これらのプロパティは、対応するserver.propertiesファイル内でお客様の環境に合わせて調整されている可能性があるため、このserver.propertiesファイルを最終的なリストとして参照してください。詳細については、『ESM管理者ガイド』の「プロパティファイル設定の管理と変更」を参照してください。</p> <p>スキャナーSmartConnectorだけは、追加データの取得のために [Complete] モードで実行する必要があります。</p> <p>注: SmartConnectorのターボモードよりも、イベントを処理するArcSightマネージャーが使用するターボモードの方が優先します。たとえば、マネージャーが [Faster] に設定されている場合、SmartConnectorがデフォルトの[Complete] に設定されていても、全データを転送することはできません。</p>

設定 (続き)

フィールド名	値
Enable Aggregation (in secs)	<p>注: 旧SmartConnectorのセットアップでこの機能をすでに使用している場合、引き続き使用できます。ただし、もっと柔軟な新しい「Field Based Aggregation」(71ページ)の使用をお勧めします。</p> <p>ここでは、引き続き従来の「Enable Aggregation」機能を使用する場合の説明を行います。</p> <p>[Enable Aggregation (in seconds)] を有効にすると、選択した時刻の値に基づいて2つ以上のイベントが集約されます。(Disabled、1、2、3、4、5、10、30、60)。</p> <p>デフォルトは [Disabled] です。</p> <p>集約されたイベントには、イベント数 (表示されたイベントに集約されたイベントの数) とイベントタイプが含まれます。残りのフィールドは、集約されたイベントセットの最初のイベントの値をとります。</p>
Limit Event Processing Rate	<p>SmartConnectorの処理速度を下げることで、CPU負荷を軽減することができます。これは、イベントバーストの影響に対処するための手段にもなります。</p> <p>選択できる範囲は、[Disabled] (CPU要求に対する制限なし) から [1eps] (渡すイベント数が1秒あたり1個だけになるため、CPUに対する要求が最小限) です。</p> <p>このオプションの効果は、使用するSmartConnectorのカテゴリ (SmartConnectorの処理カテゴリの表) によって異なります。</p>
Fields to Obfuscate	<p>セキュリティイベント内で、MD5ハッシュで難読化するフィールドを指定します。FIPSモードでは、SHA-256が使用されます。</p>
Store Original Time In	<p>(Disabled Flex Date 1) 時刻が補正機能によって変更されている場合、元のデバイスの受信時刻を指定したフィールドに移動できます。</p> <p>デフォルトは [Disabled] です。</p>
Enable Port-Service Mapping	<p>(No Yes) [Yes] を選択し、2つのフィールド (通知先ポートとアプリケーションプロトコル) のうち1つを設定してもう1つを設定していない場合、設定済みのフィールドを使用して他方のフィールドを設定します。たとえば、送信先ポートが22に設定され、アプリケーションプロトコルが設定されていない場合、アプリケーションプロトコルはsshに設定されます。</p> <p>デフォルトは [No] です。</p>

設定 (続き)

フィールド名	値
Uppercase User Names	<p>(Disabled Enabled (orig to ID) Enabled(orig to ID or Flex) Enabled(orig to Add.Data))</p> <p>[Enabled] に設定すると、2つのユーザー名フィールドは自動的に大文字に変更されます。</p> <p>元の値は次のように保存されます。</p> <ul style="list-style-type: none"> • Enabled (orig to ID): 元の値をそれぞれsourceUserIDフィールドとdestinationUserIDフィールドに保存し、フィールドに含まれていた値を上書きします。 • Enabled (orig to ID or Flex): 同sフィールドにまだ値が含まれていない場合は元の値を保存し、IDフィールドに値が含まれている場合は、flexString1 (ソース) フィールドとflexString2 (ターゲット) フィールドに元の値を保存します。 • Enabled (orig to Add. Data): 元の値をそれぞれ追加データフィールドOrigSrcUserNameおよびOrigDstUserNameに保存します。 <p>注: 通常、大文字変換は、選択されたプラットフォームでデフォルトのロケールを使用して行われます。agent.propertiesのconnector.uppercase.user.name.localeプロパティを、各ロケール (たとえば、米国英語の場合はen_USを使用) に設定してください。</p> <p>デフォルトは [Disabled] です。</p>
Enable User Name Splitting	<p>(Yes No) [Yes] を選択すると、イベントの送信先ユーザー名にカンマが含まれている場合、そのイベントを複製します。リスト内のユーザー名は、それぞれ1つのイベントに格納されます。</p> <p>たとえば、イベントの通知先ユーザー名が「User 123, User 456」の場合、イベントは2回送信され、最初のイベントの通知先ユーザー名は「User 123」、2番目のイベントの通知先ユーザー名は「User 456」に設定されます。</p> <p>デフォルトは [No] です。</p>
Split File Name into Path and Name	<p>(Yes No) [Yes] を選択し、イベントのファイル名フィールドは設定されているがファイルパスフィールドが設定されていない場合、ファイル名をパスと名前に分割し、それぞれの部分を該当するフィールドに格納します。</p> <p>たとえば、ファイル名フィールドがC:\dir\file.extに設定され、ファイルパスが設定されていない場合、ファイルパスはC:\dir、ファイル名はfile.extに設定されます。区切り文字は、SmartConnectorのプラットフォームに応じて、\または/のいずれかになります。</p> <p>デフォルトは [No] です。</p>
Event Integrity Algorithm	<p>(Disabled SHA-256 SHA-1 MD5 SHA-512)</p> <p>いずれかのアルゴリズム (SHA-256など) に設定し、なおかつ [Preserve Raw Event] パラメーターが [Enabled] の場合、約50件の通常イベントあたり1件の割合で、イベント整合性内部イベントが追加生成されます。</p> <p>また、暗号化した電子署名フィールドも、各イベントで「#seq(alg):digest」という形式で設定されます。seqは永続的なイベントシーケンス番号、algはメッセージダイジェストアルゴリズム、digestは16進メッセージダイジェストです。</p> <p>追加イベントと暗号化した電子署名フィールドの値は、生成後にイベントが改ざんされていないことを検証するために使用できます。</p> <p>サポートされているアルゴリズムは、SHA-256、SHA-1、MD5、SHA-512です。</p> <p>デフォルトは [Disabled] です (アルゴリズムは適用されません)。</p>

設定 (続き)

フィールド名	値
Generate Unparsed Events	<p>(Yes No) [Yes] を選択し、一部の受信イベントデータを解析できない場合 (理由としては、SmartConnectorパーサーの作成後にデバイスがアップグレードされたことが考えられます)、「Unparsed Event」という名前の特別なイベントが生成されます。イベントメッセージフィールドには、RAWイベントが表示されます。</p> <p>[No] に設定すると、SmartConnectorログファイルに解析されないイベントが記録されます。</p> <p>デフォルトは [No] です。</p>
Preserve System Health Events	<p>(Yes No) [Yes] に設定すると、内部システムヘルスイベントが保存されます。</p> <p>SmartConnectorは、インストールされているシステムに関する情報 (ディスク使用量、ネットワークメモリ、JVMメモリ、CPU使用率、メモリ使用量など) を提供するシステムヘルスイベントを生成します。デフォルトでは、これらのイベントは保持されず、ArcSight通知先にも送信されないため表示できません。このオプションを [Yes] に設定すると、内部システムヘルスイベントをコンソールや通知先 (Loggerなど) で使用できるようになります。</p> <p>デフォルトは [No] です。</p>
Enable Device Status Monitoring (in millisec)	<p>(<ミリ秒数> -1 (無効))</p> <p><ミリ秒数> に設定すると、選択したSmartConnectorは、コネクタが通常イベントを受信しているデバイスのステータスに基づいて、1分 (60,000ミリ秒) 以上の間隔で定期的に内部イベントを生成します。生成されるイベントの名前は、「Connector Device Status」です。</p> <p>定期的なデバイスステータス監視イベントを有効にすると、SmartConnectorとデバイスの稼働時間を監視できます。</p> <p>デバイスステータス監視イベントには、次の情報が含まれます (該当する場合)。</p> <ul style="list-style-type: none"> イベント名 (Connector Device Status) ベンダーおよび製品情報 ソースアドレスとホスト名 ゾーン 最終イベント受信日時 コネクタが開始してから受信したデバイスのイベント総数 最終コール以降のイベント数 <p>デバイスステータス監視イベントは、1分 (60,000ミリ秒) 以上の間隔で生成するように設定できます (最小値より大きなミリ秒数)。</p> <p>60,000ミリ秒より小さい値を指定すると、最小値は60,000ミリ秒 (1分) であることを示す警告がログに記録され、最小値が適用されます。</p> <p>このフィールドに数字以外の値を入力すると、値を解析できないことを通知するエラーがログに生成されます。この場合、この機能は無効になります (ログにも記録されます)。</p> <p>そのため、コネクタはエラーを通知できないので、異常が生じていることはコンソールに表示されません。</p>
Payload Sampling (使用可能な場合)	<p>一部のSmartConnectorは、ペイロードサンプリングによって、元のイベントと共に、(完全なペイロードではなく) パケットペイロードの一部を送信します。この部分を取得するのは、イベントインスペクターのオンデマンドペイロード取得機能です。</p>

設定 (続き)

フィールド名	値
Maximum Length	<p>次の値を使用してペイロードサンプルの最大長を設定できます。</p> <ul style="list-style-type: none"> • Discard • 128 bytes • 256 bytes • 512 bytes • 1 Kbyte <p>[Discard] オプションを選択すると、送信される元のイベント内部にペイロードサンプルは含まれません。</p> <p>デフォルトは [256 bytes] です。</p>
Mask Non-printable Characters	(False True) ペイロードサンプル内の印刷不可能な文字をマスクします。デフォルトは [False] です。
Filters	エージェントの緊急度とは、デバイスの緊急度を正規化した値です。たとえば、コネクタによっては、デバイスの緊急度を1~10のスケールで示すものや、高/中/低のスケールで示すものがあります。この値は正規化され、エージェントの緊急度の単一スケールに変換されます。デフォルトのスケールは、[Low]、[Medium]、[High]、[Very High] です。データソースによって緊急度が評価されなかった場合、イベントのエージェントの緊急度が不明になることがあります。
Filter Out	SmartConnectorのフィルターは排他的 (フィルターアウト) に機能します。コネクタのフィルタリング基準を満たすイベントは、通知先に転送されません。SmartConnectorのセットアップ時に、通知先にイベントを渡さないフィルター条件をコネクタで設定できます。たとえば、フィルターを使用して、任意の特性を持つイベントや特定のネットワークデバイスからのイベントを除外することが可能です。
Very High Severity Event Definition	緊急度が最高のイベントをソートするフィルター条件を入力します。
High Severity Event Definition	緊急度が高いイベントをソートするフィルター条件を入力します。
Medium Severity Event Definition	緊急度が中のイベントをソートするフィルター条件を入力します。
Low Severity Event Definition	緊急度が低いイベントをソートするフィルター条件を入力します。
Unknown Severity Event Definition	緊急度が不明のイベントをソートするフィルター条件を入力します。

SmartConnectorのフィルター条件の管理

フィルター条件とは、通知先に送信するイベントを選別するための条件であり、SmartConnectorのインストールと設定で追加できます。たとえば、フィルターを使用することによって、ネットワークデバイスや脆弱性スキャナーが生成したイベントを、その特性に基づいて取捨選択できます。コネクターのフィルタリング条件を満たしていないイベントは、転送されません。

ESMコンソールで適用可能なフィルターについては、『ArcSight ESMコンソールユーザーズガイド』にある「SmartConnectorの管理」の章の「SmartConnectorのフィルタ条件の管理」を参照してください。このガイドは、[Protect 724](#)のArcSight Product Documentation (ArcSight ESM and ESM Express) から入手できます。ESMコンソールでフィルターを適用する場合、そのESMに送信されたイベントのみが対象になります。

他のタイプの通知先については、次のようにフィルターをテキストで記述する必要があります。多くのコネクターでは、対象となるイベントを絞り込むフィルター条件を指定できます。次に、フィルター文字列の例を示します。

Name EQ “Agent”

(name Contains “Super”) Or (name EQ “Agent”)

attackerAddress Between (“10.0.0.1”, “10.0.0.10”)

destinationAddress Is “NOT NULL”

次の表では、使用可能な演算子をまとめます。データフィールド、イベントマッピング、CEFフィールドの詳細については、『ArcSight ESM User’s Reference』の「Data Fields」、「Audit Events」、「Cases」、「Events」を参照してください。

演算子	説明
EQ	等しい
NE	等しくない
LT	より小さい
LE	以下
GE	以上
GT	より大きい
Between	指定した範囲を比較
ContainsBits	等しい (ビットマップフィールドの場合)
In	メンバーシップテストのための標準CCE演算子
Contains	指定した文字列を含む
StartsWith	指定した文字列で始まる

演算子	説明
EndsWith	指定した文字列で終わる
Like	文字列型に対して単純なパターンマッチングを実行する標準CCE演算子 (1文字のマッチングはワイルドカード「_」、任意の文字数のマッチングはワイルドカード「%」)
InSubnet	指定したサブネット以外のIPアドレス
InGroup	指定したアセットカテゴリ内のアセット、または指定したゾングループ内のゾーン
Is	状態 (「NULL」または「NOT NULL」) に対する真偽をテスト。「Is」の記述は、すべて大文字にはしない

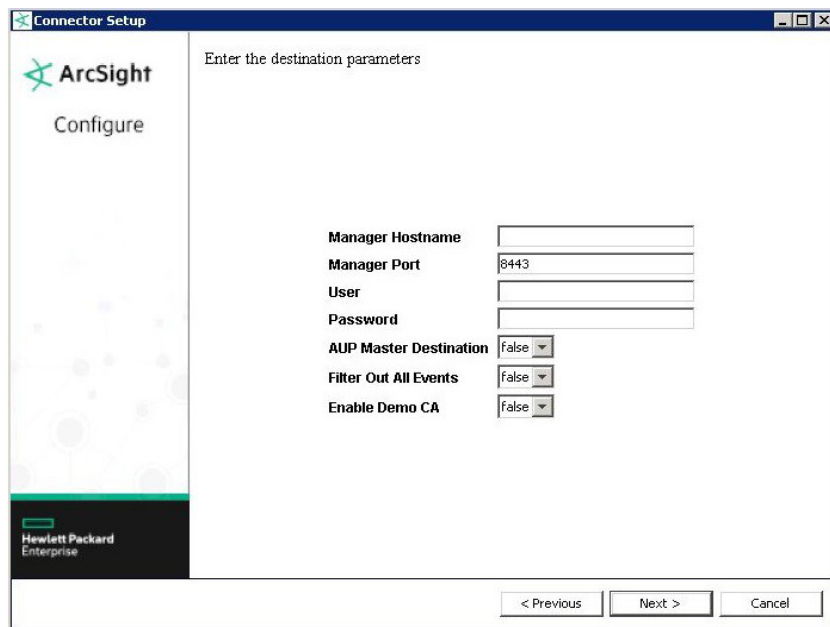
第8章: ArcSightマネージャー通知先

この章では、ArcSightマネージャー (暗号化) 通知先について説明します。

ArcSightマネージャー (暗号化)

コネクタがESMマネージャーにイベントを送信すると、マネージャーはイベントをリレーショナルデータベースに格納し、
関連エンジンで処理してから、コンソールやWebインターフェイスに表示します。

1. 追加する通知先を選択します。オプションについては、「[コネクタの通知先](#)」(62ページ) を参照してください。
2. **[Next]** をクリックして通知先のパラメーターを入力します。



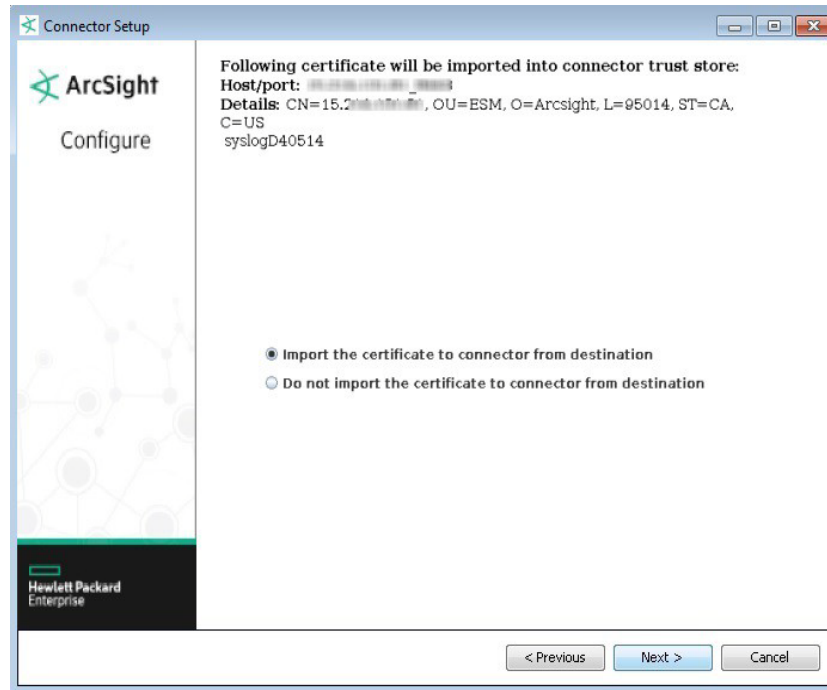
The screenshot shows a window titled "Connector Setup" with the ArcSight logo and "Configure" text. The main area is titled "Enter the destination parameters" and contains the following fields:

Manager Hostname	<input type="text"/>
Manager Port	<input type="text" value="8443"/>
User	<input type="text"/>
Password	<input type="password"/>
AUP Master Destination	<input type="button" value="False"/>
Filter Out All Events	<input type="button" value="False"/>
Enable Demo CA	<input type="button" value="False"/>

At the bottom of the window, there are three buttons: "< Previous", "Next >", and "Cancel". The Hewlett Packard Enterprise logo is visible in the bottom left corner.

パラメーター	説明
Manager Hostname	<p>ArcSightマネージャーがインストールされているマシンのローカルホスト名、IPアドレス、または完全修飾ドメイン名です。すべてのクライアント (ArcSightコンソールなど) は、ここで指定した名前をマネージャーとの通信に使用します。柔軟性を確保するために、IPアドレスではなくホスト名、特に完全修飾ドメイン名を使用することを推奨します。</p> <p>マネージャーのホスト名は、自己署名証明書の生成に使用されます。証明書のCN (共通名) は、この画面で指定するマネージャーのホスト名です。マネージャーはデフォルトで自己署名証明書を使用しますが、必要に応じてCA署名証明書に切り替えることができます。詳細については、『ESM管理者ガイド』を参照してください。</p>
Manager Port	8443
User	有効なESMユーザー名を入力します。
Password	ESMユーザーのパスワードを入力します。
AUP Master Destination	<p>デフォルト値: false。コネクタは、ESM通知先とESM以外の通知先に同時にイベントを送信することが可能です。この設定では、AUP Master Destination機能を使用すると便利です。詳細については、「ArcSightコンテンツ/AUP」を参照してください。</p> <p>注: ESMが、マネージャーのゾーン情報を、SmartMessage (Logger) やEvent Brokerなどマネージャー以外の通知先に使用する場合、[True] に設定してください。</p>
Filter Out All Events	<p>デフォルト値: false。[AUP Master Destination] が [true] に設定されている場合に、このコネクタのイベントをマネージャーに送信する (または送信しない) 設定が可能です。マネージャーでイベントを受信しない場合は、[true] に設定します。この場合、マネージャーは単にゾーン情報のソースとして機能します。たとえば、コネクタがEvent Brokerに送信したイベントをESMで読み取るような場合、この設定が便利です。</p>
Enable Demo CA	<p>デフォルト値: false</p> <p>ArcSightマネージャーのホスト名は、ArcSight ESMのインストール時に自己署名証明書を生成する際に使用されます。証明書のCN (共通名) は、ESMのインストール時に指定するマネージャーのホスト名です。</p> <p>運用環境では、デモ版のSSL証明書を使用しないでください。切り替え時には、すべてのSmartConnectorおよびArcSightコンソール上のcacertsからデモ版CAを削除してください。</p>

3. **[Next]** をクリックします。通知先の詳細を追加する画面が表示されます。
4. **[Next]** をクリックして続行します。
5. ArcSightマネージャーの証明書をインポートするウィンドウが開きます。**[Import the certificate to connector from destination]** を選択し、**[Next]** をクリックします ([Do not import the certificate to the connector from the destination] を選択すると、コネクタのインストールは終了します)。



6. ダイアログボックスが開き、更新されたコネクタとプライマリ通知先に関する情報が表示されます。[Next] をクリックして続行します。
7. [Exit] をクリックしてインストールを終了します。

第9章: ArcSight Logger SmartMessage (暗号化) 通知先

ArcSight Loggerは、非常に高いイベントスループットに最適化されたログ管理ソリューションです。Loggerは、イベントと呼ばれるタイムスタンプ付きテキストメッセージを、高い入力速度を維持しながらログに記録 (保存) します。イベントは、受信時刻、ソース (ホスト名またはIPアドレス)、未解析のメッセージ部分で構成されます。LoggerはRAWデータを圧縮しますが、訴訟対応のフォレンジックデータとして未加工の状態でも取得することも可能です。ESMとは異なり、Loggerはイベントを正規化しません。

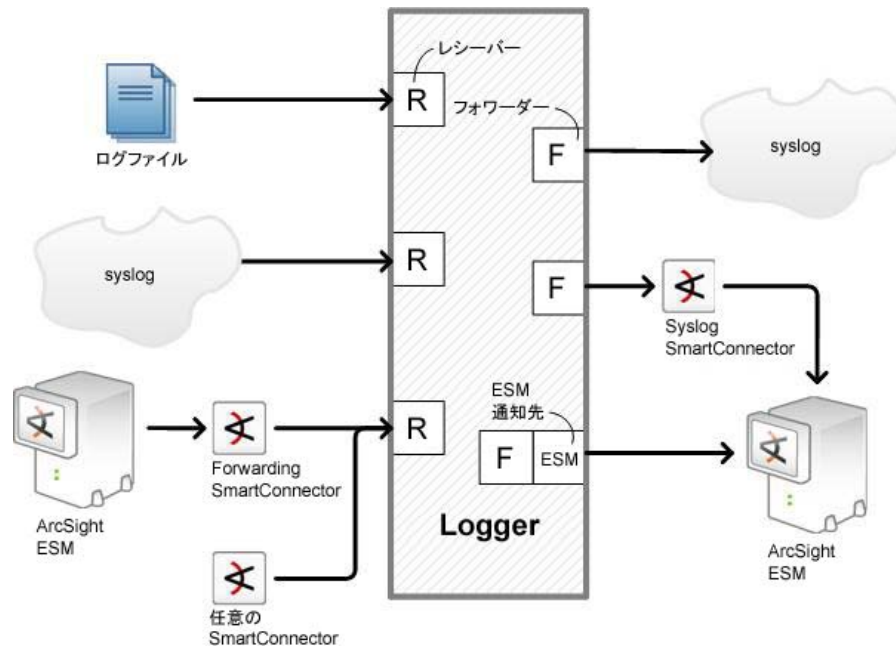
複数のLoggerが連携することで、膨大な量のイベントを処理できます。Loggerをピアネットワークとして設定し、クエリをすべてのピアLoggerに分散することが可能です。

Loggerからマネージャーへのイベント送信

Loggerの基本機能は、大量のセキュリティイベントの保存です。Loggerは、保存したイベントのサブセットをマネージャーに送信することができます。ESM通知先と呼ばれる付属のコネクタを使用することで、syslogイベントやArcSight共通イベントフォーマット (CEF) のイベントをESMに直接送信します。ESM通知先は、コンソール上でコネクタとして表示されます。ESM通知先についての詳細は、『ArcSight Logger管理者ガイド』を参照してください。

SmartMessageは、コネクタとLogger間でセキュアなチャネルを確立するためにLoggerが使用するArcSightテクノロジーです。SmartMessageは、暗号化されたセキュアなエンドツーエンドのチャネルを提供します。チャネルの一端はコネクタで、サポートする多くのデバイスから送信されたイベントを受信します。もう一端は、Logger上のSmartMessageレシーバーです。

Loggerレシーバー (R) とフォワーダー (F)

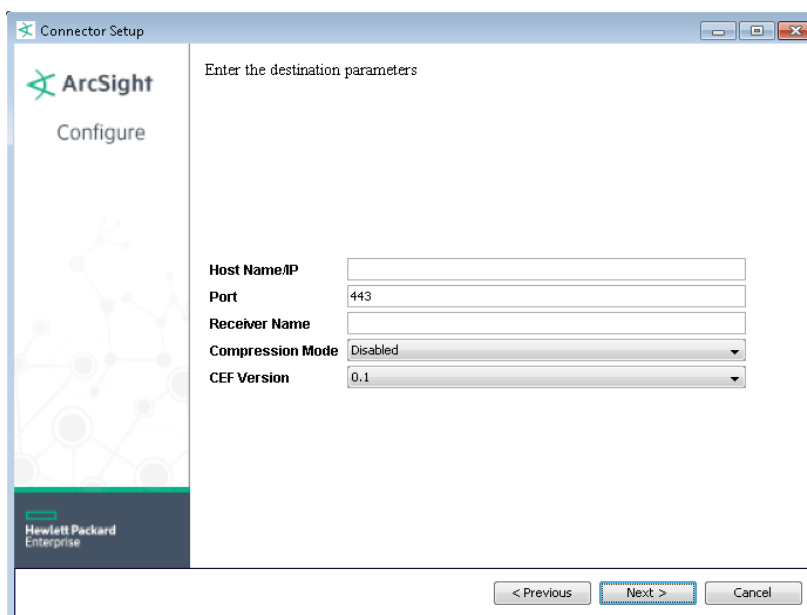


注: SmartMessageのセキュアチャンネルは、HTTPS (セキュアなソケットレイヤープロトコル) を使用して暗号化されたイベントをLoggerに送信します。これは、コネクタとESMマネージャー間で使用される暗号化バイナリプロトコルと似ていますが、異なるものです。

セキュアチャンネルではHTTPSを使用するので、ポート443を使用してください (これまでArcSightではポート8443を使用)。

Loggerへのイベント送信

1. LoggerでSmartMessageレシーバーを設定します (詳細については、『ArcSight Logger管理者ガイド』を参照してください)。
2. コネクタコンポーネントをインストールします。詳細については、各コネクタの構成ガイドを参照してください。
3. ウィンドウの指示に従って設定を続け、[ArcSight Logger SmartMessage (encrypted)] を選択します。オプションについては、「コネクタの通知先」(62ページ) を参照してください。
4. [Next] をクリックします。[Logger Host Name/IP] に入力します。ポート番号はデフォルト (443) のままにするか、通知先がソフトウェアLoggerの場合は9000に変更します。[Receiver Name] も入力します。ここには、ステップ1で作成したレシーバーの名前を入力してください。これにより、Loggerはコネクタからイベントをリッスンできるようになります。

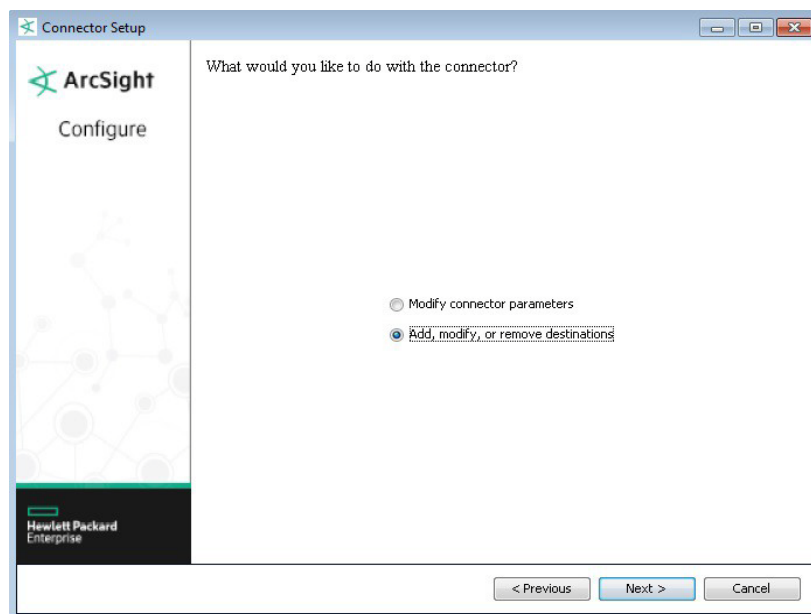


パラメーター	説明
Host Name/IP	通知先のホスト名またはIPアドレス。
Port	Loggerアプライアンスの場合は443、ソフトウェアLoggerの場合は9000。
Receiver Name	通知先のレシーバー名。
Compression Mode	データ圧縮モードのチェックボックス。オンにすると有効、オフにすると無効になります。デフォルトはオフです。
CEF Version	<p>ドロップダウンメニューから [0.1] または [1.0] を選択します。選択した通知先がCEF 1.0に対応しているかどうか不明な場合は [0.1] を選択してください。CEF 1.0は、IPv4とIPv6の両方に対応しています。</p> <p>0.1 - [デバイスアドレス]、[ソースアドレス]、[通知先アドレス]、[エージェントアドレス] の各フィールドは常に [IPv4] に設定されるか、あるいは省略されます。IPv6アドレスがある場合は、[デバイスカスタムIPv6アドレス] フィールドに入力されます。[受信バイト数] と [送信バイト数] の両フィールドは整数型に制限されます (最大値は$2^{31}-1$)。</p> <p>1.0 - アドレスフィールドは [IPv4] と [IPv6] のいずれかであり、[受信バイト数] と [送信バイト数] の両フィールドは長整数型となります (最大値は$2^{63}-1$)。</p>

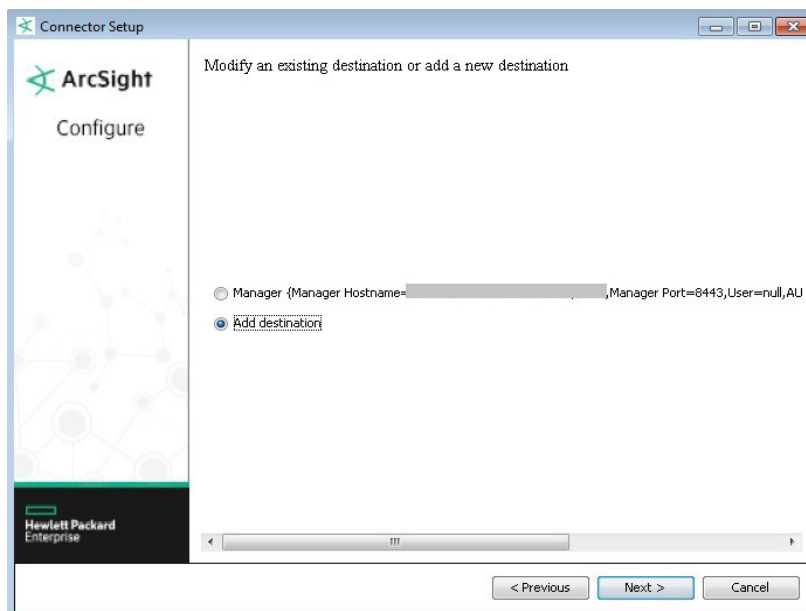
1. **[Next]** をクリックします。まだ証明書をインポートしていない場合は、証明書をコネクターにインポートするように促すLogger証明書メッセージが表示されます。
2. **[Import the certificate to connector from destination]** を選択し、**[Next]** をクリックします。
3. ウィンドウの指示に従って設定を続けると、設定の完了を通知するメッセージが表示されます。**[Exit]**、**[Next]** の順にクリックし、ウィザードを終了します。

Loggerとマネージャー両方へのイベント送信

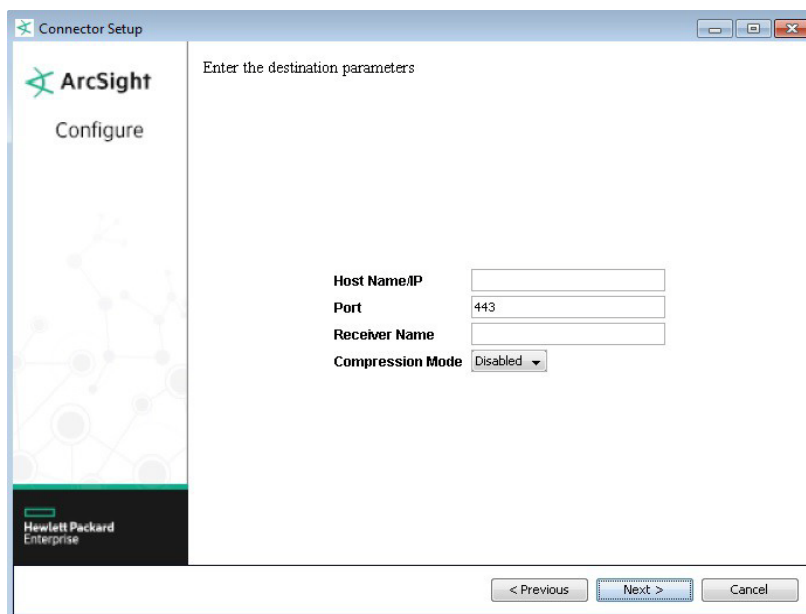
1. LoggerでSmartMessageレシーバーを設定します (詳細については、コネクターの構成ガイドを参照してください)。
2. コネクタコンポーネントをインストールします (詳細については、使用するデバイスのコネクタ構成ガイドを参照してください)。
3. 実行中のESMマネージャーでコネクタを登録し、コネクタが正常に動作することをテストします。
4. `$ARCSIGHT_HOME\current\bin\runagentsetup`スクリプトを使用して、コネクタ設定プログラムをもう一度起動します。
5. **[Add, modify, or remove destinations]** を選択します。



6. **[Next]** をクリックします。**[Add destination]** を選択します。



7. **[Next]** をクリックします。**[ArcSight Logger SmartMessage (encrypted)]** を選択します。オプションについては、「[コネクターの通知先](#)」(62ページ) を参照してください。
8. **[Next]** をクリックします。**[Logger Host Name/IP]** に入力します。ポート番号はデフォルト (443) のままにするか、通知先がソフトウェアLoggerの場合は9000に変更します。**[Receiver Name]** も入力します。



9. **[Next]** をクリックします。まだ証明書をインポートしていない場合は、証明書をコネクターにインポートするように促すLogger証明書メッセージが表示されます。
10. **[Import the certificate to connector from destination]** を選択し、**[Next]** をクリックします。
11. **[Next]** をクリックします。設定の完了を通知するメッセージが表示されます。**[Exit]**、**[Next]** の順にクリックし、ウィザードを終了します。

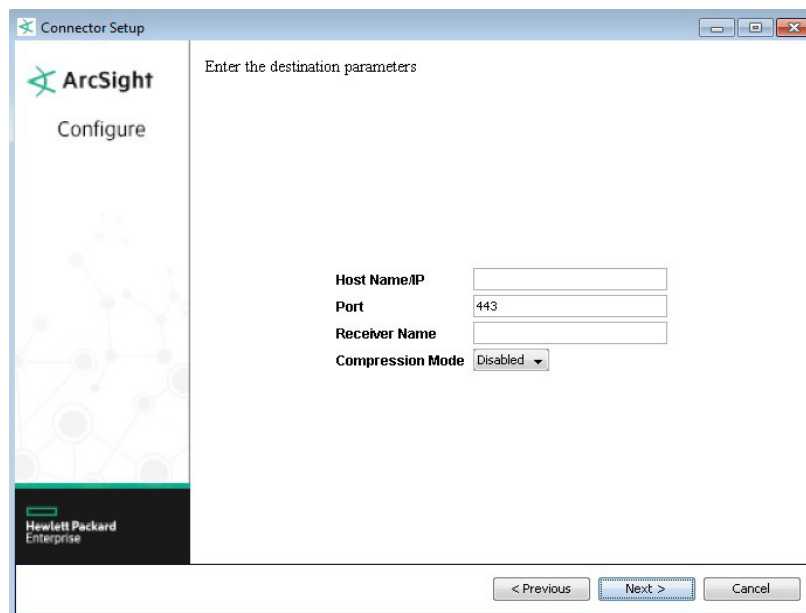
12. コネクタを再起動すると、変更内容が有効になります。

ESMからLoggerへのイベント転送

ArcSight Forwarding Connectorは、ESMマネージャーからイベントを読み取り、ArcSight共通イベントフォーマット(CEF)でLoggerに転送します。

注: Forwarding Connectorは個別のインストールファイルであり、ArcSight-6.x.x.<build>.x-SuperConnector-<platform>.exeのような名前提供されます。Forwarding Connectorは、Logger 1.5以降との互換性を持つビルド4810以降を使用してください。

1. デバイス用のコネクタの構成ガイドに従って、コネクタをインストールします。
2. 通知先のタイプを指定するウィンドウが開いたら、[ArcSight Logger SmartMessage (encrypted)] を選択します。オプションについては、「コネクタの通知先」(62ページ) を参照してください。
3. [Next] をクリックします。[Logger Host Name/IP] に入力します。ポート番号はデフォルト (443) のままにするか、通知先がソフトウェアLoggerの場合は9000に変更します。[Receiver Name] も入力します。



The screenshot shows the 'Connector Setup' window with the 'Configure' section active. The title bar reads 'Connector Setup'. The main area is titled 'Enter the destination parameters'. On the left, there is an ArcSight logo and the word 'Configure'. The right side contains the following fields and controls:

- Host Name/IP: [Empty text box]
- Port: [443]
- Receiver Name: [Empty text box]
- Compression Mode: [Disabled] (dropdown menu)

At the bottom of the window, there are three buttons: '< Previous', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

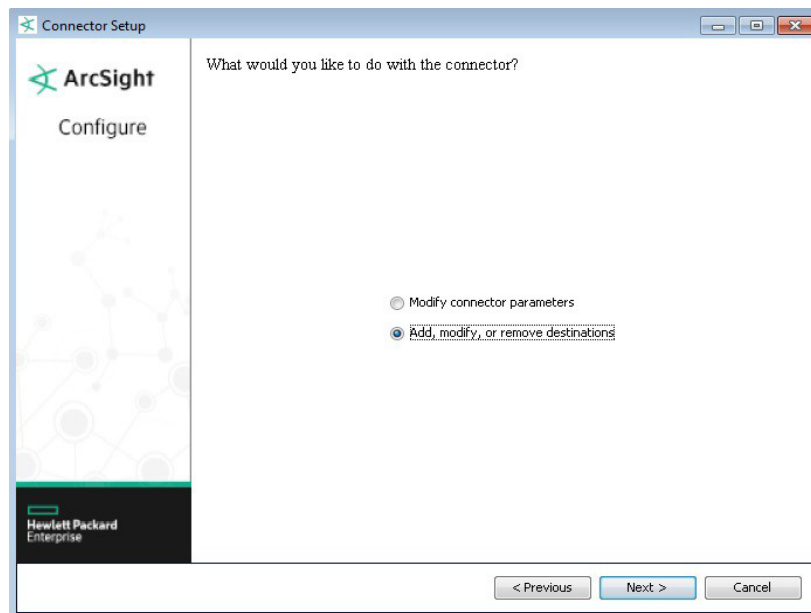
4. [Next] をクリックします。コネクタに証明書をインポートするように促すLogger証明書メッセージが表示されます。
5. [Import the certificate to connector from destination] を選択し、[Next] をクリックします。
6. [Next] をクリックします。設定の完了を通知するメッセージが表示されます。[Exit]、[Next] の順にクリックし、ウィザードを終了します。
7. コネクタを再起動すると、変更内容が有効になります。

Forwarding Connectorで、CEF出力をLoggerに送信し、イベントを別のマネージャーに送信する設定については、「[Loggerとマネージャー両方へのイベント送信](#)」(85ページ)を参照してください。

Loggerでのコネクタ設定

Loggerと通信するコネクタのインストールが完了したら、コネクタの設定ウィザードでプロパティを指定します。前述の手順でコネクタコンポーネントがインストールされていれば (詳細については「[コネクタのインストール](#)」(28ページ)を参照)、次の手順を実行します。

1. `$ARCSIGHT_HOME\current\bin\runagentsetup`スクリプトを使用して、コネクタ設定プログラムをもう一度起動します。
2. **[Add, modify, or remove destinations]** を選択します。



3. **[Next]** をクリックします。詳細については、「[コネクタの設定](#)」(43ページ)を参照してください。
4. **[Next]** をクリックして設定を続けます。

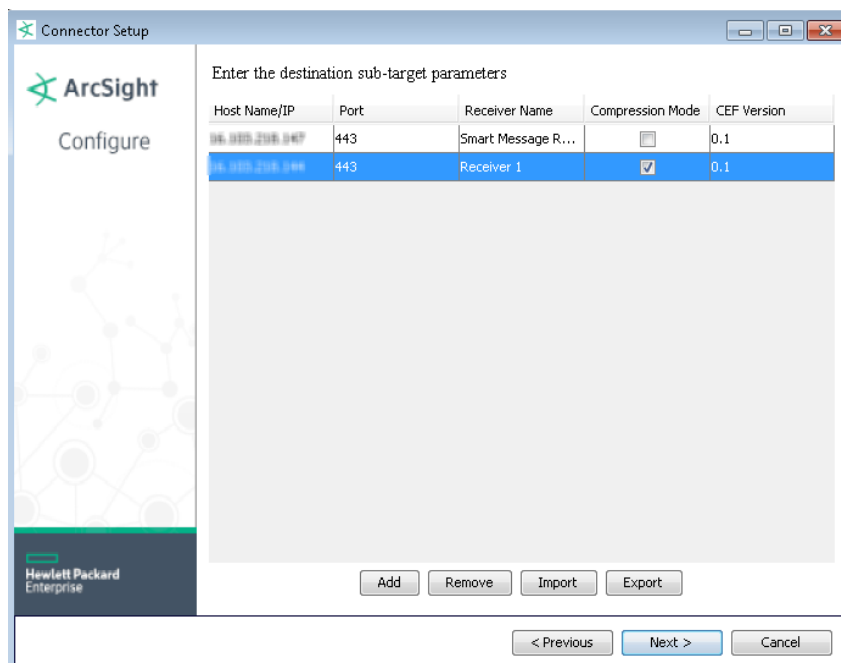
第10章: ArcSight Logger SmartMessageプール (暗号化) 通知先

ArcSight SmartMessage Loggerプール (暗号化) の通知先タイプを使用して、Loggerデバイスのプールを指定します。プールとは、1つまたは複数のLoggerを1つにまとめた通知先です。コネクターが処理するイベントの「バッチ」は、ラウンドロビン方式で、プール内の次のLoggerに送信されます。バッチサイズは設定可能ですが、100件のイベントで1つのバッチを構成するのが一般的です。プール内のメンバーが使用不可能になると、イベントは残りのメンバーに送信されます。プールメンバーが使用可能な状態に復帰すると、そのメンバーへのイベント送信が再開されます。プール内に使用可能なメンバーが存在しない場合、イベントはフェイルオーバー通知先に送信されます。

注: Logger SmartMessage Pool通知先を使用する場合、ArcSight Management Center 2.0以前またはコネクターアプライアンスではコネクターを管理できません。

Loggerプール通知先の設定

1. LoggerSecure Poolに追加するすべてのLoggerでSmartMessageレシーバーを設定します (詳細については、『ArcSight Logger管理者ガイド』を参照してください)。
2. コネクターコンポーネントをインストールします。詳細については、各コネクターの構成ガイドを参照してください。
3. ウィンドウの指示に従って設定を続けると、通知先タイプを指定するウィンドウが開きます。[ArcSight Logger SmartMessage Pool (encrypted)] を選択します。オプションについては、「コネクターの通知先」(62ページ) を参照してください。
4. [Next] をクリックし、プールメンバーの追加作業を続行します。



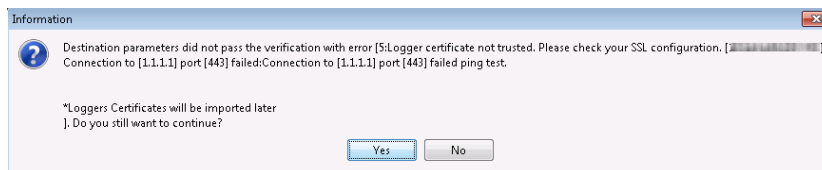
5. [Add] をクリックし、プールメンバーを追加します。ホスト名、ポート番号、レシーバー名のフィールドに入力します。次の表にパラメーターとボタンをまとめます。

パラメーター	説明
Host Name/IP	通知先のホスト名またはIPアドレス。
Port	Loggerアプライアンスの場合は443、ソフトウェアLoggerの場合は9000。
Receiver Name	通知先のレシーバー名。
Compression Mode	データ圧縮モードのチェックボックス。オンにすると有効、オフにすると無効になります。デフォルトはオフです。
CEF Version	<p>ドロップダウンメニューから [0.1] または [1.0] を選択します。選択した通知先がCEF 1.0に対応しているかどうか不明な場合は [0.1] を選択してください。CEF 1.0は、IPv4とIPv6の両方に対応しています。</p> <p>0.1 - [デバイスアドレス]、[ソースアドレス]、[通知先アドレス]、[エージェントアドレス] の各フィールドは常に [IPv4] に設定されるか、あるいは省略されます。IPv6アドレスがある場合は、[デバイスカスタムIPv6アドレス] フィールドに入力されます。[受信バイト数] と [送信バイト数] の両フィールドは整数型に制限されます (最大値は $2^{31}-1$)。</p> <p>1.0 - アドレスフィールドは [IPv4] と [IPv6] のいずれかであり、[受信バイト数] と [送信バイト数] の両フィールドは長整数型となります (最大値は $2^{63}-1$)。</p>

ボタン	説明
Add	テーブルに行を追加し、Loggerをプールに追加します。情報を手入力してください。有効化と無効化は、 [Compression Mode] チェックボックスで行います。デフォルトはオフであり、無効になっています。Loggerのデフォルトのポート番号は443です。
Remove	loggersecureプールからLoggerを削除します。
Import	loggersecureプールの情報が保存されている.csvファイルをインポートします。
Export	パネルに入力したデータをエクスポートして保存します。エクスポートファイルの拡張子は.csvにします。ファイルには、 [Compression Mode] がデフォルトのままの場合は「Disabled」と入力され、有効になっている場合は「TRUE」と入力されます。

6. プールメンバーをすべて追加したら、**[Next]** をクリックします。

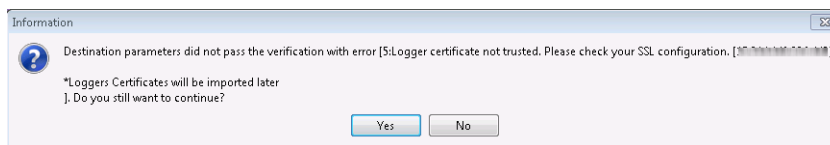
a. 検証が成功しないパラメーターがあると、SSL設定を確認するよう促すエラーメッセージが表示されます。



b. **[No]** をクリックして接続エラーを確認します。パラメーターウィンドウに戻り、エラーが報告されたLoggerのパラメーターを編集します。

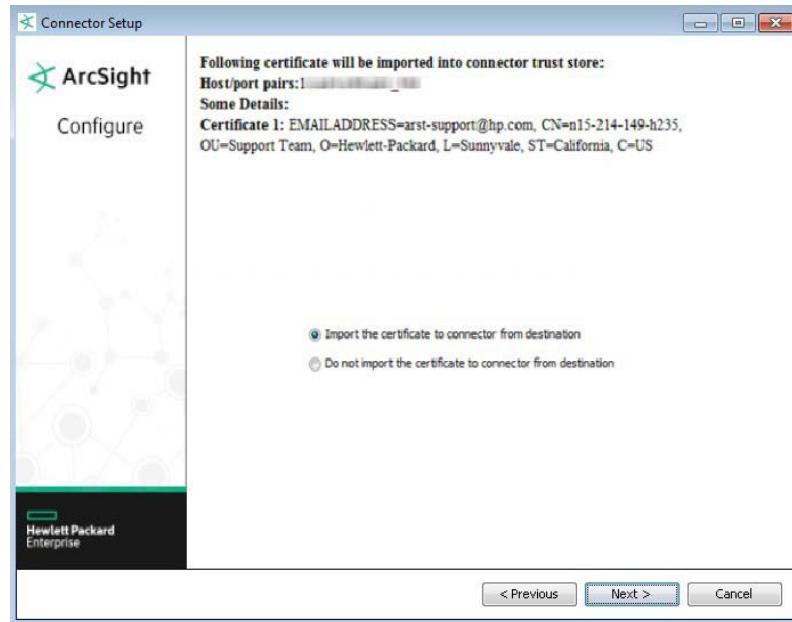
c. 設定を続ける場合はもう一度 **[Next]** をクリックします。

d. 作業の継続を確認するメッセージが表示されます。**[Yes]** をクリックします。



e. コネクターの場所の名前を入力し、**[Next]** をクリックします。

7. コネクターに証明書をインポートするよう促すLogger証明書メッセージが表示されます。**[Import the certificate to connector from destination]** を選択し、**[Next]** をクリックします。



SmartMessage転送のpersistent設定

ネットワーク環境によっては、コネクタがバッチイベントをLoggerに送信する際に問題が発生することがあります。このような場合、Logger pingテストが頻繁に失敗する、EPSがダウンする、ハートビート転送リンクとイベント転送リンクがアップ/ダウンを繰り返す、といった現象がログに記録されます。統計データによると、「event sent」確認応答のラウンドトリップ時間が長くなり、イベント送信が失敗しやすくなり、キャッシングが発生します。

SmartMessage転送をpersistent設定すると、Logger通知先のスループットを向上できます。agent.propertiesファイル (\$ARCSIGHT_HOME\current\user\agent) で、次のプロパティの値をtrueに変更します。

```
transport.loggersecure.connection.persistent=true
```

Logger接続数が250を超える場合には、persistentの値をtrueすることはお勧めしません。

第11章: CEF通知先

この章では、共通イベントフォーマット (CEF) でのイベント送信で使用できる選択肢を説明します。Event Broker通知先は、CEF形式またはバイナリ形式でイベントを送信できます。

- [CEFファイル](#)
- [Event Broker](#)
- [CEF Syslog](#)
- [CEF Encrypted Syslog \(UDP\)](#)

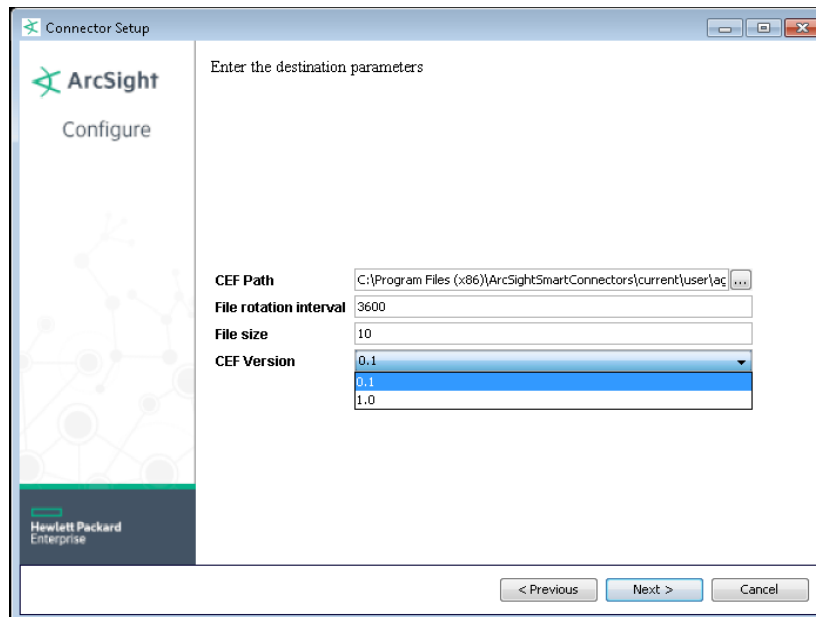
CEFファイル

ここでは、コネクタが通常であればESMマネージャーに送信するイベントをキャプチャーし、ファイルに保存する方法を説明します。共通イベントフォーマット (CEF) は、セキュリティデバイスベンダーとセキュリティ以外のデバイスベンダーの両方が容易に採用できる形式です。最も関連性の高いイベント情報が含まれるため、イベントの解析と利用が簡単に行えます。

フィールドの詳細については、『Cloud CEF Implementation Standard.』を参照してください。

1. インストールウィザードを実行し、**[CEF File]** を選択します。オプションについては、「[コネクタの通知先](#)」(62ページ) を参照してください。
2. 次のパラメーターの値を入力します。

パラメーター	入力または選択する値
CEF Folder	CEFファイルが格納されているパス。
File Rotation Interval	ファイルローテーションの間隔 (秒)。デフォルトは 3,600 (1時間) です。
File Size	ファイルサイズ (MB)。デフォルトは10MBです。
CEF Version	<p>ドロップダウンメニューから [0.1] または [1.0] を選択します。選択した通知先がCEF 1.0に対応しているかどうか不明な場合は [0.1] を選択してください。CEF 1.0は、IPv4とIPv6の両方に対応しています。通知先は、Logger、別のSmartConnector、ArcSight以外の製品です。</p> <p>0.1 - [デバイスアドレス]、[ソースアドレス]、[通知先アドレス]、[エージェントアドレス] の各フィールドは常に [IPv4] に設定されるか、あるいは省略されます。IPv6アドレスがある場合は、[デバイスカスタムIPv6アドレス] フィールドに入力されます。[受信バイト数] と [送信バイト数] の両フィールドは整数型に制限されます (最大値は $2^{31}-1$)。</p> <p>1.0 - アドレスフィールドは [IPv4] と [IPv6] のいずれかであり、[受信バイト数] と [送信バイト数] の両フィールドは長整数型となります (最大値は $2^{63}-1$)。</p>



3. [Next] をクリックしてインストールを続行します。

ファイルローテーション

ローテーション間隔が経過するか、ファイルサイズが最大値に達するまで、イベントはカレントファイルに追記されていきます。どちらかの条件に到達すると、新たにカレントファイルが作成され、古いカレントファイルは名前が変更されます(以下を参照)。

イベントファイルの名前には作成時のタイムスタンプが使用され、カレントファイル以外のすべてのファイルに「done.cef」というテキストが付加されます。1時間ごとにローテーションを行う場合、CEFファイルセットのそれぞれのファイル名は次のようになります。

2010-01-28-10-55-33.cef

2010-01-28-09-55-33.done.cef

2010-01-28-08-55-33.done.cef

Event Broker

Event Broker通知先は、Event Brokerクラスターへのイベント送信に使用されます。受信したイベントは、リアルタイム分析やデータウェアハウスシステムに配信することが可能です。Event Brokerからデータを取得できるアプリケーション(ESM、ArcSight Investigate、Hadoop、Loggerなど)は、すべてこれらのイベントを取得できます。

注: ESMの設定は、ESMコンソールではなくコネクタ側で行う必要があります。

イベントのトピック名を指定します。同じLoggerプールを使用するコネクターは、すべて同じイベントトピック名を使用するように設定する必要があります。これにより、これらのコネクターのイベントは同じイベントトピックにパブリッシュされます。

CEF 0.1およびCEF 1.0のコンテンツタイプでは、イベントの送信時に、コネクターのIPアドレスとフラグを含むキーが送信されます。フラグは1バイトの値です。ESMの場合、キーはエージェントIDです。

キーは、1バイトのフラグに、(4バイトまたは16バイトの) IP (v4またはv6) アドレスを付加した形式です。IPバージョンビットの値に基づいて、4バイトまたは16バイトの追加バイトをチェックします。これは将来、キーが破られないように長くなった場合に備えたものです。

ビット位置	説明
0	IPバージョン: 0 = IPv4 1 = IPv6
1	キーバージョン: 0を指定します。 将来的に、この定義と下位互換性のないキーバージョンが登場したら1に変更されます。
2-7	キーバージョン: 0を指定します。 将来的なニーズに備えたものです。

CEF 0.1および1.0では、イベントは独自のメッセージ形式でEvent Brokerに送信されます。これは、Event Brokerで定義されたトピックのパーティションにラウンドロビン形式で配信されます。ESMでは、イベントはバイナリ形式のバッチで送信されます。クライアント証明書の認証方法としては、TLS暗号化がサポートされています。

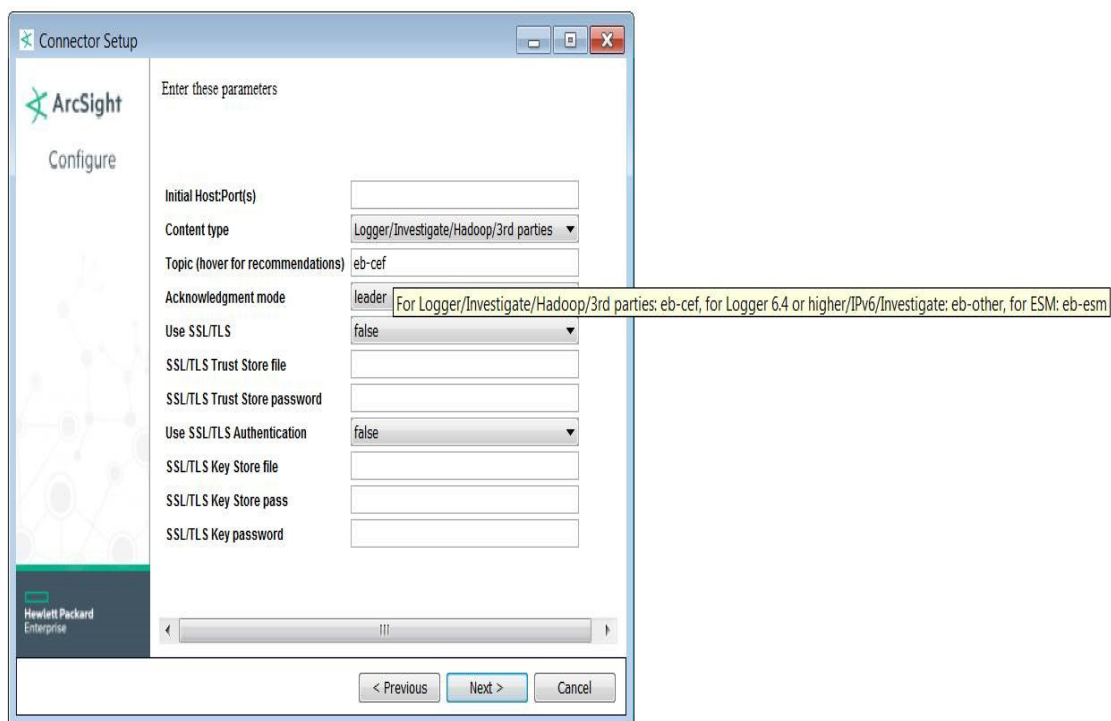
通知先の設定で、**[Use SSL/TLS]** パラメーターを **[true]** に設定してTLSを有効化する場合、Event BrokerのKafkaクラスターの証明書または署名済みの証明書が格納されたJava KeyStore形式のファイル (.jks) が必要になります。通知先の設定中に、このトラストストアファイルの場所が必要になります。詳細については、Kafkaのドキュメント (https://kafka.apache.org/documentation.html#security_ssl) を参照してください。

また、**[Use SSL/TLS Authentication]** パラメーターを **[true]** に設定して、クライアント証明書の認証を有効にする場合、プライベートキーと証明書が格納された.jksファイルも必要になります。Event Brokerクラスターはトラストストア内に証明書 (または署名済み野証明書) が必要です。キーストアファイルと認証情報の場所は、**[SSL/TLS Key Store file]**、**[SSL/TLS Key Store pass]**、**[SSL/TLS Key password]** の各パラメーターで指定されます。キーおよびキーストアのパスワードは、Event Brokerの設定時に生成されます。

1. インストールウィザードを実行し、通知先として **[Event Broker]** を選択します。
2. 次のパラメーターの値を指定します。

パラメーター	入力または選択する値								
Initial Host:Port(s)	<p>このフィールドは必須フィールドです。Event Brokerクラスターとの通信を確立するためのホスト名とポートを、カンマ区切りのリストで指定します。クラスター内のサーバーをすべてリストする必要はありませんが、リスト内のサーバーのどれにもアクセスできない場合、コネクタはEvent Brokerにイベントを送信できません。少なくとも1つのサーバーを指定してください。以下に例を示します。</p> <p>kafka1.example.com:9093,kafka2.example.com:9093</p>								
Content Type	[Content Type] に応じて [Topic] を選択します。								
Topic (カーソルを上にとくと推奨値が表示)	<table border="1"> <thead> <tr> <th>Content Type</th> <th>Topic</th> </tr> </thead> <tbody> <tr> <td>Logger/Investigate/Hadoop/3rd parties</td> <td> eb-cef IPv4をサポートします。Logger 6.3.0以前のバージョンで使用します。 </td> </tr> <tr> <td>Logger 6.4 or higher/IPv6/Investigate</td> <td> eb-other IPv4とIPv6をサポートします。Logger 6.4.0以降のバージョンで使用します。IPv6のサポートに加えて、[Bytes In] と [Bytes Out] フィールドに長整数型の値を入力できるようになります。 </td> </tr> <tr> <td>ESM</td> <td> eb-esm Protect 724で、「ArcSight ESM Support Matrix」の「ESM Support of Other ArcSight Products/Components」を参照してください。 </td> </tr> </tbody> </table>	Content Type	Topic	Logger/Investigate/Hadoop/3rd parties	eb-cef IPv4をサポートします。Logger 6.3.0以前のバージョンで使用します。	Logger 6.4 or higher/IPv6/Investigate	eb-other IPv4とIPv6をサポートします。Logger 6.4.0以降のバージョンで使用します。IPv6のサポートに加えて、[Bytes In] と [Bytes Out] フィールドに長整数型の値を入力できるようになります。	ESM	eb-esm Protect 724で、「 ArcSight ESM Support Matrix 」の「ESM Support of Other ArcSight Products/Components」を参照してください。
Content Type	Topic								
Logger/Investigate/Hadoop/3rd parties	eb-cef IPv4をサポートします。Logger 6.3.0以前のバージョンで使用します。								
Logger 6.4 or higher/IPv6/Investigate	eb-other IPv4とIPv6をサポートします。Logger 6.4.0以降のバージョンで使用します。IPv6のサポートに加えて、[Bytes In] と [Bytes Out] フィールドに長整数型の値を入力できるようになります。								
ESM	eb-esm Protect 724で、「 ArcSight ESM Support Matrix 」の「ESM Support of Other ArcSight Products/Components」を参照してください。								
Acknowledgment mode	<p>このフィールドは必須フィールドです。コネクタが、Event Brokerからイベント受信の確認応答が送信されるまで待機するかどうかを決定します。次のオプションを指定できます。</p> <p>Leader: デフォルト値。コネクタは、イベントのパーティションに関する確認応答が、プライマリ Event Brokerサーバーから送信されるまで待機します。このオプションを選択すると、ほとんどの状況でデータ損失を防ぐことができます。適切なパフォーマンスが維持されますが、スループットは低下する可能性があります。</p> <p>None: コネクタは、確認応答を待機しません。Kafkaサーバーがダウンした場合にイベントが失われる可能性があります、スループットは大幅に向上します。</p> <p>All: コネクタは、イベントのパーティションに関する確認応答が、バックアップを含むすべての Event Brokerサーバーから送信されるまで待機します。ほぼすべての状況でデータ損失を防ぐことができますが、スループットは大幅に低下します。</p>								
Use SSL/TLS	<p>イベント送信にTLS暗号化を使用するかどうかを指定します。次のオプションを指定できます。</p> <ul style="list-style-type: none"> • True • False (デフォルト) <p>[true] を選択した場合、[SSL/TLS Trust Store Password] と [SSL/TLS Trust Store file] (場所) も入力する必要があります。</p>								
SSL/TLS Trust Store file	トラストストアファイルの場所を入力します。								

パラメーター	入力または選択する値
SSL/TLS Trust Store password	SSL/TLSトラストストアのパスワードを入力します。
Use SSL/TLS Authentication	<p>TLSによるコネクターの識別にクライアント証明書を使用するかどうかを指定します。次のオプションを指定できます。</p> <ul style="list-style-type: none"> • True • False (デフォルト) <p>[true] を選択した場合、[Use SSL/TLS] も有効にする必要があります。また、[SSL/TLS Key Store File]、[SSL/TLS Key Store Pass]、[SSL/TLS Key password] の各パラメーターも指定してください。</p>
SSL/TLS Key Store file	SSL/TLSキーストアファイルの場所を入力します。
SSL/TLS Key Store pass	SSL/TLSキーストアのパスワードを入力します。
SSL/TLS Key password	SSL/TLSキーのパスワードを入力します。



3. [Next] をクリックしてインストールを続行します。

CEF Syslog

Loggerへのイベント送信には、TCPおよびUDP通知先が使用できます。データはTCPまたはUDPレシーバーによって受信されます。1つのレシーバーで複数のコネクタからの受信が可能です。また、Syslog Daemonコネクタや、ArcSight syslog以外のレシーバーへの送信にも使用できます。

Loggerへの送信の詳細については、「[ArcSight Logger SmartMessage \(暗号化\) 通知先](#)」(82ページ) を参照してください。

TLSプロトコルは、セキュアなチャネルを介したイベント送信を可能にします (Loggerでは使用できません)。TLS syslogの受信に対応していれば、どのアプリケーションでもこのデータを受信できます。これには、ArcSight's Syslog NG Daemonコネクタなどが含まれます。

1. 使用するデバイスの構成ガイドの指示に従って、コネクタをインストールします。通知先を追加した後に、次のウィンドウが表示されることがあります。詳細については、「[通知先の追加、変更、削除](#)」(44ページ) を参照してください。
2. 通知先のタイプを指定するウィンドウが開いたら、[CEF Syslog] を選択します。オプションについては、「[コネクタの通知先](#)」(62ページ) を参照してください。
3. [Next] をクリックします。
4. 次のパラメーターの値を入力します。

パラメーター	入力または選択する値
IP/Host	IP/ホスト情報を入力します。
Port	ポート情報を入力します。

パラメーター	入力または選択する値
Protocol	ドロップダウンメニューからプロトコルを選択します。
Forwarder	<p>CEF Forwarderモードパラメーターは、デフォルトで [false] に設定されています。通知先がSyslog Daemonコネクタのときに、元のコネクタに関する情報を保持したい場合、この通知先と受信側のコネクタの両方でCEFのForwarderモードをtrueに設定します。つまり、syslog、syslog NG、CEF Encrypted Syslog (UDP) のいずれかで複数のコネクタを接続している状態で、元のコネクタの情報を保持するには、すべての通知先でCEFのForwarderモードをtrueに設定し (CEF Encrypted Syslog (UDP) では暗黙的にtrueとなります)、そこから情報を受信するコネクタでもCEFのForwarderモードをtrueに設定します。</p> <p>たとえば、多くのMicrosoft Windows Event Log Unifiedコネクタがある場合、すべてCEF Syslog通知先タイプを使ってイベントを単一のSyslog Daemonコネクタに送信し、そこからESMIに送信するように設定することが可能です。ESMIに到着したイベントで、イベントを収集したUnifiedコネクタの情報を保持するには、コネクタのCEF Syslog通知先でForwarderモードを [true] に設定し、Syslog DaemonコネクタでもForwarderモードを [true] に設定します。情報は、イベントの元のエージェントのフィールドに表示されます。</p>
CEF Version	<p>ドロップダウンメニューから [0.1] または [1.0] を選択します。選択した通知先がCEF 1.0に対応しているかどうか不明な場合は [0.1] を選択してください。CEF 1.0は、IPv4とIPv6の両方に対応しています。通知先は、Logger、別のSmartConnector、ArcSight以外の製品です。</p> <p>0.1 - [デバイスアドレス]、[ソースアドレス]、[通知先アドレス]、[エージェントアドレス] の各フィールドは常に [IPv4] に設定されるか、あるいは省略されます。IPv6アドレスがある場合は、[デバイスカスタムIPv6アドレス] フィールドに入力されます。[受信バイト数] と [送信バイト数] の両フィールドは整数型に制限されます (最大値は2³¹-1)。</p> <p>1.0 - アドレスフィールドは [IPv4] と [IPv6] のいずれかであり、[受信バイト数] と [送信バイト数] の両フィールドは長整数型となります (最大値は2⁶³-1)。</p>

5. [Next] をクリックしてインストールを続行します。

再接続による負荷分散

複数階層にコネクタをインストールし、各階層間にロードバランサーを配置している場合、再接続機能を利用することで負荷分散動作を効率化できます。たとえば再接続機能を使用しない場合、階層1コネクタが起動すると、CEF Syslog通知先 (階層1) に接続します。ロードバランサーは初期接続時に負荷分散方法を決定し、階層1コネクタは常に同じ階層2コネクタに接続します。

reconnectパラメーターを使用すると、階層1コネクタはこれまでと同じように階層2コネクタに初期接続し、ロードバランサーが負荷分散方法を決定して階層2コネクタを選択します。ただし、再接続タイムアウト後、階層1コネクタは新しい接続を確立します。ロードバランサーは負荷分散方法を決定し直し、階層2コネクタを選択しますが、これは前回接続した階層2コネクタとは異なる可能性があります。その結果、階層2コネクタ全体に負荷が均一に分散されることとなります。

reconnectパラメーターを使用するには、次の手順を実行します。

1. \$ARCSIGHT_HOME/current/user/agentのagent.propertiesファイルを開きます。
2. 次のパラメーターを探します。
`agents[0].destination[0].params`
3. reconnectの値を、「-1」からタイムアウトの秒数に変更します。CEF Syslog通知先は、この時間が経過すると切断と再接続を実行します。

たとえば、

```
<Parameter Name=\"reconnect\" Value=\"-1\"/>\n
```

を次のように変更します。

```
<Parameter Name=\"reconnect\" Value=\"60\"/>\n
```

この場合、1分ごとに切断と再接続が繰り返されます。

4. agent.propertiesを保存して閉じます。

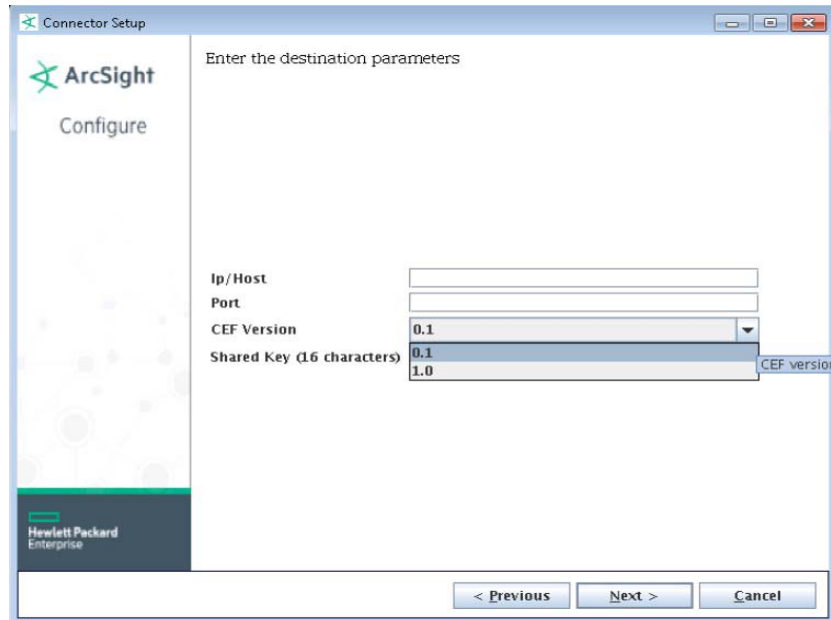
CEF Encrypted Syslog (UDP)

CEF Encrypted Syslog (UDP) 通知先は、「共有シークレット」を使って暗号化したイベントをUDPを介して送信できます。

注意: LoggerはCEF Encrypted Syslogに対応していません。

受信側でデータを復号化するには、ArcSight CEF Encrypted Syslog (UDP) コネクターのインストールと設定が必要です。コネクターがインストールされていない場合は、『SmartConnector for ArcSight CEF Encrypted Syslog (UDP)』を参照してください。

1. コネクターコンポーネントをインストールします (詳細については、使用するデバイスのコネクター構成ガイドを参照してください)。通知先を追加した後に、次のウィンドウが表示されることがあります。詳細については、「[通知先の追加、変更、削除](#)」(44ページ)を参照してください。
2. 通知先のタイプを指定するウィンドウが開いたら、[CEF Encrypted Syslog (UDP)] を選択します。オプションについては、「[コネクターの通知先](#)」(62ページ)を参照してください。
3. [Next] をクリックします。
4. 次のパラメーターの値を入力します。



パラメーター	入力または選択する値
IP/Host	IP/ホスト情報を入力します。
Port	ポート情報を入力します。
CEF Version	<p>ドロップダウンメニューから [0.1] または [1.0] を選択します。選択した通知先がCEF 1.0に対応しているかどうか不明な場合は [0.1] を選択してください。CEF 1.0は、IPv4とIPv6の両方に対応しています。通知先は、対応するSmartConnectorのみです。</p> <p>0.1 - [デバイスアドレス]、[ソースアドレス]、[通知先アドレス]、[エージェントアドレス] の各フィールドは常に [IPv4] に設定されるか、あるいは省略されます。IPv6アドレスがある場合は、[デバイスカスタムIPv6アドレス] フィールドに入力されます。[受信バイト数] と [送信バイト数] の両フィールドは整数型に制限されます (最大値は $2^{31}-1$)。</p> <p>1.0 - アドレスフィールドは [IPv4] と [IPv6] のいずれかであり、[受信バイト数] と [送信バイト数] の両フィールドは長整数型となります (最大値は $2^{63}-1$)。</p>
Shared Key (16 characters)	暗号化に使用する16文字の共有キー (共有シークレット) を入力します。受信側でCEF Encrypted Syslog (UDP) コネクターを設定する際は、同じ共有キーを使用してください。

5. [Next] をクリックしてインストールを続行します。

第12章: CSVファイル通知先

この章では、コネクタが通常であればESMマネージャーに送信するイベントをキャプチャーし、ファイルに保存する方法を説明します。一般的なArcSight設定では、ESMマネージャーとのイベントのやり取りに外部ファイルを使用する必要はありません。

イベントデータは、Excel互換のカンマ区切り (CSV) 形式のファイルに記述され、コメントの先頭には「#」が付加されません。コネクタを設定することで、データの先頭にコメント行を置き、それ以降の行のフィールドに関する説明を記述することができます。次に、イベントファイルの例を示します。

```
#event.eventName,event.attackerAddress,event.targetAddress
```

```
"Port scan detected","1.1.1.1","2.2.2.2"
```

```
"Worm ""Code red"" detected","1.1.1.1","2.2.2.2"
```

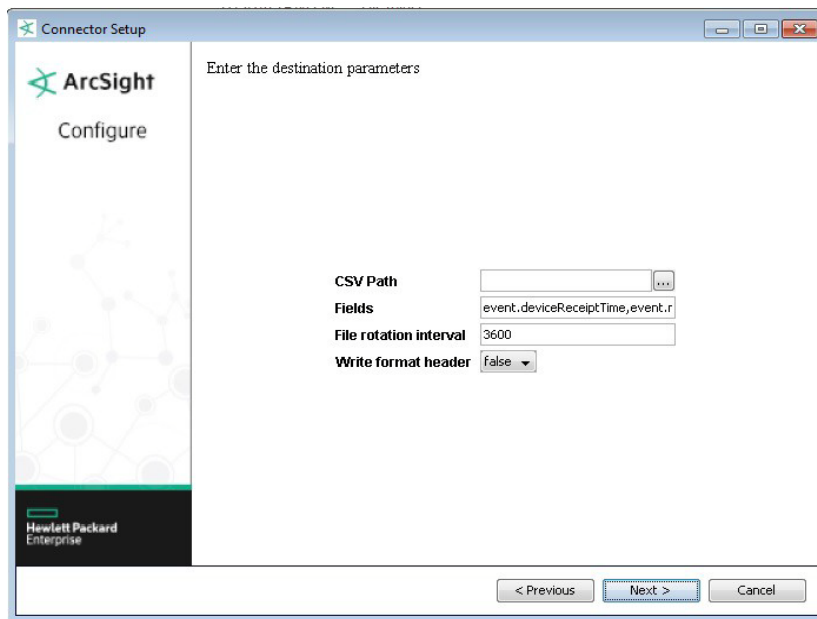
```
"SQL Slammer detected","1.1.1.1","2.2.2.2"
```

```
"Email virus detected","1.1.1.1","2.2.2.2"
```

イベントデータは指定したフォルダーに保存され、定期的にローテーションを行う設定が可能です。

CSVファイルのインストール

1. セキュリティイベントをESMマネージャーに転送するのではなく、CSVファイルに記録するコネクタをインストールするには、コネクタのインストールウィザードを実行し、通知先の選択ウィンドウで **[CSV File]** を選択します。オプションについては、[「コネクタの通知先」\(62ページ\)](#) を参照してください。
2. 次のパラメーターの値を入力または選択します。



パラメーター	入力または選択する値
CSV Path	出力ファイルのパス。存在しない場合、フォルダーが作成されます。
Fields	<p>CSVファイルに送信するフィールド名をカンマ区切りで指定します。デフォルト値は次の通りです。</p> <p>event.deviceReceiptTime,event.name,event.deviceAddress, event.deviceHostName,event.sourceAddress, event.sourceHostName,event.sourcePort, event.destinationAddress,event.destinationHostName, event.destinationPort</p> <p>リストを変更する場合、先頭に次のいずれかの文字列を置きます。</p> <ul style="list-style-type: none"> 「event.」。この後に、事前定義された通常のイベントフィールド名を続けます。 「additionaldata.」。この後に、このコネクタに適用する追加データフィールド名を続けます。ここで指定する名前は、すべてのコネクタで共通の名前ではありません。 <p>フィールド名の間にあるカンマの前後には、スペースを挿入しないでください。 例: 「event.deviceReceiptTime,event.name」は正しい記述です。「event.deviceReceiptTime, event.name」は間違った記述です。</p>
File rotation interval	ファイルローテーションの間隔 (秒) を入力します。デフォルトは 3,600 (1時間) です。
Write format header	[true] を選択すると、上記で説明したように、各列のラベルが付いたヘッダー行が送信されます。

3. [Next] をクリックしてインストールを続行します。

イベントデータのローテーション

イベントはカレントファイルに追記されます。ローテーション間隔が経過すると、新しいカレントファイルが作成され、古いカレントファイルの名前が変更されます。ローテーション間隔として一般的な設定は1時間です。

イベントファイルの名前には作成時のタイムスタンプが使用され、カレントファイル以外のすべてのファイルに「.done.csv」というテキストが付加されます。1時間ごとにローテーションを行う場合、CSVファイルセットのそれぞれのファイル名は次のようになります。

2007-01-28-10-55-33.csv

2007-01-28-09-55-33.csv.done

2007-01-28-08-55-33.csv.done

プロパティファイルを使ったCSVコネクタ設定のカスタマイズにより、イベントのフィルタリングやアグリゲーションを実行できます。

また、CSVファイルとESMマネージャーに同時にイベントを送信する設定も可能です。

第13章: Raw Syslog通知先

この章では、Raw Syslogイベントをキャプチャーする方法について説明します。コネクタとRaw Syslog通知先の詳細については、『Connector Configuration Guide for Raw Syslog Daemon』を参照してください

Raw Syslogの概要

データは、正規化した方が解析やアクセスを高速かつ簡単に行えるのですが、IT専門家の間では、レビュー、フォレンジック、訴訟対策用のRAWデータが好まれる場合があります。Raw Syslogコネクタ通知先とRaw Syslog Daemon向けコネクタを組み合わせることにより、TLS、Raw TCP、UDPの各プロトコルを介して、syslogサーバーからRaw Syslogイベントを収集できます。

注: ArcSight Loggerへのデータ転送では、設定パラメーターを使用することにより、syslogデータ (ソースとタイムスタンプ) の正規化を最小限に抑えることができます。詳細については、『SmartConnector for Raw Syslog Daemon Configuration Guide』を参照してください。

この通知先はRaw Syslogコネクタと連携し、Raw Syslogにセキュリティイベントをキャプチャーします。Raw Syslogコネクタをインストールするには、コネクタのインストールウィザードを実行し、通知先として **[Raw Syslog]** を選択します。オプションについては、「[コネクタの通知先](#)」(62ページ) を参照してください。

Raw Syslog通知先パラメーターを入力して、**[Next]** をクリックすると、コネクタ設定ウィザードが起動し、設定プロセスが開始されます。

付録A: ArcSight Update Pack (AUP)

この付録では、ArcSight Update Pack (AUP) を使用して、ESMマネージャーとコネクタ間のコンテンツを更新する方法を説明します。AUPファイルには、コネクタやESMに関連する更新についての情報が記録されています。

ArcSightコンテンツAUP

AUPファイルは、ファイルの一括収集に使用します。ArcSightリソースを更新する機能と、コネクタ間でパーサーを分散する機能があります。ArcSightでは、新しいコネクタイベント分類マッピングが継続的に作成されています。これを「コンテンツ」と呼びます。コンテンツは、ArcSight Update Pack (AUP) ファイルにパッケージ化されます。既存のコンテンツはすべてメジャー製品リリースに含まれていますが、HP Subscribers Choiceから定期的に提供される最新のコンテンツ更新を取得することで、完全に最新の状態に保つことができます。詳細については、HP SSOにお問い合わせください。

コンテンツ更新 (ArcSight-xxxx-ConnectorContent.aup) はサポートによって提供され、その中のデータは登録済みのコネクタに転送されます。AUPは、次の要素の更新を提供します。

1. イベント分類 (カテゴリ動作、カテゴリオブジェクトなど)
2. デフォルトのゾーンマッピング (IPとゾーンのデフォルトマッピング)
3. OSマッピング (ネットワークスキャン時のアセットの作成先)

フィルター、ルール、ダッシュボードなどのコンテンツは、AUPでは提供されません。

注: ArcSight Management Center/コネクタアプライアンスは、AUPの自動展開をサポートしていません。詳細については、カスタマーサポートにお問い合わせください。

以下で示すように、AUPのアップロード方法はArcSight製品ごとに異なります。

ESM

コンテンツ更新はサポートから入手できます。更新作業は、次の手順で実行します。

1. 最新のAUPリリースをダウンロードします。
2. 実行中のESMマネージャーのARCSIGHT_HOME\updates\に、.aupファイルを、コピーします。このESMに登録されているコネクタによって、.aupが自動的にダウンロードされます。完了すると、監査イベントが生成されます。

ESM/Logger

コネクターは、ESMとLoggerに同時にイベントを送信することが可能です。この設定では、AUP Master Destination機能を使用すると便利です。AUP Master Destinationを使用することで、ESMは、Logger通知先で使用するコネクターに対してAUPコンテンツをプッシュできます。Loggerには、AUPコンテンツを保存したりプッシュしたりする機能はありません。

1. コネクターの設定ウィザードを実行し、ESM通知先を追加して、AUP Master Destinationパラメーターを**true**に設定します (デフォルトはfalse)。
2. Logger通知先が追加されていない場合は、追加します。
3. ステップ1で追加したESMマネージャーのARCSIGHT_HOME\updates\に、.aupファイルを追加します。

コネクター

AUPコンテンツは、ESMからコネクターにプッシュされ、そこから確認のための内部イベントが送信されます。ESM通知先でAUP Master Destinationパラメーターが設定されている場合、そのAUPコンテンツは、Loggerなど、ESM以外の通知先のコネクターによって使用されます。

注意: AUP Master Destinationパラメーターを**true**に設定できるのは、同時に1つのESM通知先に限定されます。複数のESM通知先が設定され、複数の通知先でこのパラメーターがtrueに設定されている場合、最初の通知先のみがマスターとして認識されます。

フェイルオーバーESM通知先では、AUP Master Destinationパラメーターをtrueに設定できません。

Logger

Loggerには、AUPを保存してコネクターに転送する機能はありません。

コネクターアプライアンス

コネクターアプライアンスでのAUPのアップロードには、Webベースのユーザーインターフェイスを使用します。[Advanced Operations] タブの [Connector Upgrade Repository] に、Connector Upgradeコマンドを使ってアップロードされたアップグレードが表示されます。

新しいコンテンツAUPを適用するには、次の手順を実行します。

1. 新しいコンテンツAUPバージョンを、サポートサイト (<http://support.openview.hp.com/>) から、ブラウザーベースインターフェイスを使用するコンピューターにダウンロードします。
2. AUPファイルをダウンロードしたコンピューターから、ブラウザーベースのインターフェイスにログインします。

3. 上部のメニューバーで **[Setup] > [Repositories]** をクリックします。
4. 左側のパネルで **[Content AUP]** をクリックします。
5. 右側のパネルで **[Upload]** をクリックします。
6. **[Browse]** をクリックし、ダウンロードしたファイルを選択します。
7. **[Submit]** をクリックすると、指定したファイルがリポジトリに追加され、該当するすべてのコネクターに自動的にプッシュされます。または、**[Cancel]** をクリックして終了します。

コネクター上の現在のコンテンツAUPバージョンを確認するには、以下のいずれかの手順を実行します。

- コネクター通知先でGetStatusコマンドを実行し、aup[acp].versionの値が、適用したAUPバージョンと同じであることを確認します。コネクター通知先でコマンドを実行する方法については、『Connector Appliance Administrator's Guide』を参照してください。
- マウスカーソルをコネクター名の上に置くと、コネクターのすべての通知先に適用されているAUPバージョンが表示されます。

コネクターアプライアンスの詳細については、『Connector Appliance Administrator's Guide』を参照してください。

ArcSight Management Center

ArcSight Management CenterでAUPコンテンツを使用するには、AUP/ENCリポジトリを使用します。このツールにより、複数のコネクターAUP (アップグレード) ファイルを保持できます。これらのAUPアップグレードファイルをコンテナに適用することで、特定のバージョンにアップグレードできます。その結果、コンテナ内のすべてのコネクターが、コンテナに適用したバージョンにアップグレードされます。

アップグレードの方法については、『HP ArcSight Management Center Administrator's Guide』の「Upgrade AUP/ENC Repository」を参照してください。

ESMによって生成されたAUP

一部のAUPは、ESM自身によって、内部メンテナンスおよび操作の用途に生成されます。

ユーザー分類更新

ユーザー分類更新 (user-categorizations_user_supplied_ 0000000001300014581.aupなど) は、ユーザーがイベントの分類方法をコンソールで変更した場合に、ESMによって生成されます。この更新は登録済みコネクターに転送され、新たに送信されるイベントの分類方法が更新されます。これは一般的に、ArcSightには分類が用意されていないカスタムシグネチャーの分類に使用されます。

システムゾーン更新

システムゾーン更新 (system-zone-mappings_00000000000000000001.aupなど) は、ArcSight Systemゾーンの変更が検出されるとESMIによって生成され、必要なコネクターに転送されます。この更新には新しいシステムゾーンマッピングが含まれます。これにより、受信イベントはESM内の正しいゾーンまたはアセットにアタッチされます。

システムゾーンは常に存在するため、ESMIに接続されたすべてのコネクターは、システムゾーンをAUPとして定期的に受信します。

ユーザーゾーン更新

ユーザーゾーン更新 (user-zone-mappings_3Rxkk0xYBABDRZlZyr6nrWg==_00000000001700001895.aupなど) は、ユーザーが作成したゾーン設定の変更が検知されるとESMIによって生成され、必要なコネクターに転送されます。この更新には新しいゾーンマッピングが含まれます。これにより、受信イベントはESM内の正しいゾーンまたはアセットにアタッチされます。

付録B: FIPS準拠のSmartConnector

この付録では、FIPSの設定とインストールについて説明します。

FIPSとは

Information Technology Management Reform Act (情報技術マネジメント改革法、Public Law 104-106) に従って、National Institute of Standards and Technology (NIST: 米国国立標準技術研究所) が策定した連邦政府のコンピューターシステム向けの標準規格およびガイドラインです。商務長官の承認を受けた後、NISTによってFederal Information Processing Standards (FIPS: 連邦情報処理規格) として公布され、政府規模で施行されています。NISTがFIPSを策定した背景には、セキュリティや相互運用性といった政府機関の厳しい要件を満たすことのできる業界標準規格やソリューションが存在しなかったという点があります。

FIPS Suite B規格では、ハッシュ化を行う暗号化アルゴリズム、デジタル署名、鍵交換が規定されています。暗号化アルゴリズムは、機密/非機密の国家安全システムおよび情報の保護を目的としています。

注: FIPS準拠のコネクターが非準拠の通知先に接続するソリューションは、FIPS準拠とはみなされません。また、FIPS Suite B準拠モードで通知先をインストールする場合、SmartConnectorもFIPS Suite B準拠モードでインストールする必要があります。

サポート対象のコネクター

FIPS準拠のコネクター

- すべてのsyslogコネクター
- すべてのファイルリーダーコネクター
- すべてのSNMPコネクター
- ほとんどのデータベースコネクター (ただし、Oracle Audit DBと、SQL Serverドライバー (暗号化) を使用する場合を除く)
- Cisco Secure IPS SDEEコネクター
- Sourcefire Defense Center eStreamerコネクター
- Check Point OPSEC NGコネクター

FIPS非準拠のコネクター

- Microsoft Windows Event Log – Unified
- SQL Serverドライバー (暗号化) を使用するデータベースコネクター
- Oracleドライバーを使用するコネクター
- AIXまたはHPE UXプラットフォームのみで動作するコネクター

FIPS準拠と認定されていないコネクター

- 独自仕様の各種APIコネクター
- Webサービスおよびクラウドコネクター

コネクターに関する注意事項

一部のコネクタータイプには、次のような制限事項があります。

CEF Syslogを通知先として選択した場合

コネクターの通知先として**CEF Syslog** (TLSプロトコルを使用) を選択すると、ウィザードは通知先からセキュリティ証明書を取得し、入力値に従ってインポートしようとしています。CEF Syslog通知先はFIPS準拠モードでも正しく動作しますが、**agent.properties**を編集してFIPS準拠モードを有効化すると (**「FIPSサポートの有効化」**を参照)、通知先から取得された証明書がトラストストアに正しくインポートされません。

SmartConnectorウィザードで通知先の証明書を取得およびインポートできない場合には、証明書を手動でインポートできます。

1. 証明書を通知先から一時ディレクトリにコピーします。
2. `$ARCSIGHT_HOME/current/bin`ディレクトリで次のコマンドを実行し、証明書をインポートします。
`arcsight keytoolgui`
3. `$ARCSIGHT_HOME/jre/lib/security/cacerts`のキーストアを開きます (パスワードはchangeit)。
4. メニューバーで **[Tools] > [Import Certificate]** を選択します。証明書ファイルをアップロードします。
5. 信頼された証明書として指定します。
6. コネクターとデバイスを起動します。

Microsoft SQL JDBCドライバー

実行しているデータベースコネクタが、暗号化が有効になっているSQL JDBCドライバーを使用している場合、FIPS準拠モードではコネクタをインストールできません。

Microsoft SQL Server JDBCドライバーのダウンロードとインストールの手順については、インストールするデータベースコネクタの構成ガイドを参照してください。

FIPSサポートの有効化

ソフトウェアコネクタをインストールする場合、インストール中にFIPSサポートの有効化を行います。コネクタのインストールと設定で、[Set Global Parameters] ウィンドウが開いたら、[Enable] を選択してFIPS準拠モードを有効にします。ウィザードでFIPS Suite Bモードを有効にする手順は、「[FIPS Suite Bモードの有効化](#)」を参照してください。

SmartConnectorをアプライアンスにインストールする場合、ユーザーインターフェイスを使ってFIPSサポートを有効化できます。手順としては、FIPSサポートを有効化したいコネクタが格納されているコンテナで、サポートを有効化します。

手動でのFIPSモード有効化

1. `$ARCSIGHT_HOME/current/user/agent`にある`agent.properties`ファイルを開きます。
2. 次のプロパティを入力します。
`fips.enabled=true`
3. `agent.properties`を保存して閉じます。

手動でのFIPS Suite Bサポート有効化

SmartConnectorをFIPS準拠モードでインストールした場合、`agent.properties`ファイルでESM通知先パラメータを次のように変更すると、FIPS Suite Bサポートを手動で有効化できます。

注: 通知先もFIPS Suite Bモードでインストールする必要があります。

1. `$ARCSIGHT_HOME\current\user\agent`にある`agent.properties`ファイルを開きます。
2. 通知先パラメータの次のプロパティを探します (ファイルの10行目前後にあります)。

```
agents[0].destination[0].params=<?xml version="1.0" encoding="UTF-8"?>\n<ParameterValues>\n <Parameter Name="port" Value="8443"/>\n <Parameter Name="filterevents" Value="false"/>\n <Parameter Name="host" Value="samplehost.sv.arcsight.com"/>\n <Parameter Name="aupmaster"
```



```
Value\="false"/>\n <Parameter Name\="fipsciphers"  
Value\="fipsDefault"/>\n</ParameterValues>\n
```

3. 通知先パラメーターはXML文字列で指定されており、各要素がそれぞれ1つのパラメーターに相当します。通知先のSuite Bモードに応じて、fipsDefaultをsuiteb128 (128ビットセキュリティ) またはsuiteb192 (192ビットセキュリティ) に変更します。
4. agent.propertiesを保存して閉じます。

コネクタを再起動すると、変更内容が有効になります。

パスワード管理

次のコマンドを実行し、キーストアとトラストストアのパスワードを変更します。次に、agent.propertiesファイルを新しい値で更新します。

キートラストストアのパスワードを変更するには、次の手順を実行します。

1. 次のコマンドを実行します (ストアの値は下の図を参照してください)。

```
bin/arcsight agent keytool -store <ストアの値> -storepasswd
```

2. プロンプトが表示されたら、新しいパスワードを入力します。
3. 次の表に基づいてagent.propertiesを更新します。

注: クライアント認証の設定を行っていないと、キーストアファイルは存在しません。

キーストア内のキーのパスワードを変更するには、次の手順を実行します。

キーではキーストアと同じパスワードを使用するので、キーストアのパスワードを変更すると、キーのパスワードも変更されます。

```
bin/arcsight agent keytool -store agentkeys -keypasswd -alias <キーのエイリアス>
```

ストアの値

キーストア (クライアント認証)	トラストストア
agentkeys	agentcerts

agent.propertiesファイルのエントリ

パスワードの変更では、agent.propertiesで対応するプロパティ値を追加または更新してください。

	キーストア (クライアント認証)	トラストストア
FIPS	ssl.fips.keystore.password=<新しいパスワード>	ssl.fips.truststore.password=<新しいパスワード>
非FIPS	ssl.keystore.password=<新しいパスワード>	ssl.truststore.password=<新しいパスワード>

付録C: コネクターのFAQ

以下に、よくある質問をまとめます。内容は定期的に更新されます。

- 「en_US」以外のロケールのマシンを使用しています。タイムスタンプフィールドの解析中に、コネクターでパーサーエラーが発生します。
- 使用中のデバイスがサポート対象コネクターリストに含まれていません。
- サポート対象デバイスを使用していますが、コネクター設定ウィザードで表示されません。
- SmartConnectorで報告されないイベントがあります。
- コンソールに表示されないイベントフィールドがあります。
- SmartConnectorがイベントを報告しません。
- データベースSmartConnectorでイベントを先頭から読み取る方法を教えてください。
- イベントをキャッシュしている状態で、マネージャーとの接続が再確立された場合、どのようなイベントが送信されますか。
- ステータスレポートで、キャッシュサイズに実際より小さい値が表示されます。たとえば、マネージャーがダウンした後、SmartConnectorでいくつかのイベントを受信しているはずですが、レポートではイベント数がゼロと表示されます。
- キャッシュサイズの概算が変更されないコネクターや、負の値になるコネクターがあります。
- SmartConnectorのキャッシュは、user/agent/agentdata以外の場所に配置できますか。
- 終了日時を設定しても、必ずさらに後の日時に設定されてしまいます。
- Syslogコネクターは、KIWIやAIXから転送されたメッセージをサポートしますか。
- SmartConnectorステータスに繰り返し表示される「T」とは何を意味しますか。
- EvtSとEpsは何を意味しますか。
- ファイルリーダーSmartConnectorがネットワーク共有を介してファイルを読み取る場合、ネットワーク共有を切断するとエラーが表示されますか。agent.logとagent.out.wrapper.logに表示されるエラーメッセージが、それぞれどのファイルのエラーなのかを識別することは可能ですか。
- ログファイルのアクセスは、シーケンシャルとパラレルのどちらですか。
- SmartConnectorでログファイルを読み取った後、NFSを使用して移動できますか。
- SmartConnectorで、リモートマシンからネットワーク共有を使ってログファイルを読み取るにはどうすればいいですか。
- EPSを使用する場合、パフォーマンスに制限はありますか。
- SmartConnectorで一度にアクセスできるログファイルの数を教えてください。

- マネージャー1つあたりのコネクターの数として、推奨されている最大数を教えてください。
- サービス (Windows) やデーモン (Unix) としてコネクターを実行する設定を行う場合、「An issue has been encountered configuring the connector to run as a service. Check agent.log (Service Installation) for details.」というメッセージが表示されます。

「en_US」以外のロケールのマシンを使用しています。タイムスタンプフィールドの解析中に、コネクターでパーサーエラーが発生します。

コネクターは、デフォルトのロケール「en_US」での使用を前提としています。別のロケールで動作しているマシンでは、タイムスタンプフィールドの解析中にコネクターでパーサーエラーが発生することがあります。

user/agent/agent.propertiesに「agent.parser.locale.name=<マシンのロケール>」プロパティを追加してパーサーのロケールを変更し、コネクターを再起動します。

たとえば、中国とフランスの場合、ロケールは次のようになります。

```
agent.parser.locale.name=zh_CN
```

```
agent.parser.locale.name=fr_FR
```

コネクターマシンでデフォルトロケールを使用する場合は、ロケールを空白のままにしてください。例:

```
agent.parser.locale.name=
```

使用中のデバイスがサポート対象コネクターリストに含まれていません。

- ArcSightではFlexConnector開発キット (SDK) がオプションで提供されています。これを使用すれば、お使いのデバイス用にカスタムコネクターを作成できます。
- ArcSightではカスタムコネクターの作成が可能です。詳細については、カスタマーサポートにお問い合わせください。

サポート対象デバイスを使用していますが、コネクター設定ウィザードで表示されません。

コネクターがインストール可能かどうかは、使用するオペレーティングシステムによって異なります。デバイスが表示されていない理由として考えられるのは、オペレーティングシステムがサポートしていない場合、またはSyslogサーバーが提供するsyslogサブコネクターである場合があります。Syslogコネクターをインストールするには、インストール中に[Syslog Daemon]、[Syslog Pipe]、[Syslog File] のいずれかを選択してください。

SmartConnectorで報告されないイベントがあります。

イベントのフィルタリングとアグリゲーションが適切にセットアップされていることを確認してください。

コンソールに表示されないイベントフィールドがあります。

コネクターとマネージャーのターボモードがそれぞれ、コネクターリソースと互換性があることを確認してください。マネージャーのターボモードがコネクターよりも速いモードに設定されている場合、イベントの詳細の一部が失われます。詳細については、「ArcSightのターボモード」(26ページ)を参照してください。

SmartConnectorがイベントを報告しません。

コネクターのログでエラーを確認します。また、コネクターがマネージャーと通信できない場合、イベントはコネクターのキャッシュに保存されますが、キャッシュが一杯になると、イベントは完全に失われます。

データベースSmartConnectorでイベントを先頭から読み取る方法を教えてください。

タイムベースDB用のFlexConnectorの場合、agent.propertiesで次のパラメーターを指定します。

```
agents[0].startatdate=01/01/1970 00:00:00
```

IDベースDB用のFlexConnectorの場合、agent.propertiesで次のパラメーターを指定します。

```
agents[0].startatid=0
```

イベントをキャッシュしている状態で、マネージャーとの接続が再確立された場合、どのようなイベントが送信されますか。

送信イベントの70%はライブイベントであり、30%はキャッシュイベントです。ライブイベントの到着に時間がかかる場合、キャッシュイベントの割合が高くなっている可能性があります。ライブイベントがない場合、キャッシュイベントは100%まで達します。

また、接続の回復時に特定の重要度のイベントを送信しない設定を行っている場合、そのイベントは送信されません。イベントが最初に生成（およびキャッシュ）された時点では送信する設定になっていたとしても、上記の場合には送信されなくなります。

ステータスレポートで、キャッシュサイズに実際より小さい値が表示されます。たとえば、マネージャーがダウンした後、SmartConnectorでいくつかのイベントを受信しているはずですが、レポートではイベント数がゼロと表示されます。

HTTP転送キューなど、システムの他の場所に存在するイベントも存在します。コネクターをシャットダウンし、.size.dfltファイルでキャッシュサイズをチェックすることにより、イベントの実際の有無を確認できます。

キャッシュサイズの概算が変更されないコネクターや、負の値になるコネクターがあります。

概算のキャッシュサイズを取得するためのサイズファイルは、起動時に読み取り、シャットダウン時に書き込みが行われます。コネクターがシャットダウン時にサイズを書き込めなかった場合（強制終了やディスク障害などの問題により発生）、誤った数値が報告されることがあります。新しいバージョンでは、キャッシュサイズの誤りが検知されると再構築されますが、古いバージョンでは対応していません。

この問題の解決方法の1つを示します。

1. コネクターを停止します。
2. current\user\agent\agentdataにあるサイズファイル（ファイル拡張子は.size.dflt）を削除します。
3. コネクターを再起動します。

コネクターは、サイズファイルが存在しないことを検出し、すべてのキャッシュファイルを読み取ってキャッシュサイズを再構築します。

SmartConnectorのキャッシュは、user/agent/agentdata以外の場所に配置できますか。

コネクターキャッシュを格納するフォルダーを変更します。agent.propertiesに次のプロパティを追加します。

`agentcache.base.folder=<フォルダーの相対パス>`

<フォルダーの相対パス> には\$ARCSIGHT_HOMEの相対パスを指定します。

終了日時を設定しても、必ずさらに後の日時に設定されてしまいます。

マネージャーは、古いイベントに対して時刻補正を自動的に実行します。終了時刻が保有期間よりも前の場合、保有期間の終わりに自動的に設定されます。警告が表示され、同じメッセージを含む内部イベントが送信されます。

Syslogコネクターは、KIWIやAIXから転送されたメッセージをサポートしますか。

はい、サポートします。

KIWIに関連するプロパティ:

`syslog.kiwi.forwarded.prefix=KiwiSyslog Original Address`

Kiwiは、オリジナルアドレスをプレフィックスとして追加します。たとえば、メッセージ

```
Jan 01 10:00:00 myhostname SSH connection open to 1.1.1.1
```

は次のように変換されます。

```
Jan 01 10:00:00 myhostname KiwiSyslog Original Address myoriginalhost: SSH connection open to 1.1.1.1
```

コネクターはプレフィックスを削除し、`myoriginalhost`をデバイスのホスト名として使用します。

AIXに関連するプロパティ:

`syslog.aix.forwarded.prefixes=Message forwarded from,Forwarded from`

AIXを使用して転送されたメッセージにも、同じような処理が行われます。

SmartConnectorステータスに繰り返し表示される「T」とは何を意味しますか。

「T」は、「throughput(SLC)」の略です。`agent.defaults.properties`には、次の行が含まれています。

```
status.watermark.stdoutkeys=AgentName,Events  
Processed,Events/Sec(SLC),Estimated Cache  
Size,status,throughput(SLC),hbstatus,sent  
status.watermark.stdoutkeys.alias=N,Evts,Eps,C,ET,T,HT,S
```

SLCは「Since Last Check」の略です。`status.watermark.sleepTime=60`がオーバーライドされていない場合、「過去1分間」を意味します。

EvtsとEpsは何を意味しますか。

Evtsは「Events Processed (処理済みのイベント数)」、**Eps**は「Events/Sec(SLC) (1秒あたりのイベント数)」を示します。

ファイルリーダーSmartConnectorがネットワーク共有を介してファイルを読み取る場合、ネットワーク共有を切断するとエラーが表示されますか。agent.logとagent.out.wrapper.logに表示されるエラーメッセージが、それぞれのファイルのエラーなのかを識別することは可能ですか。

ネットワーク共有が、Linux/UNIXのNFSマウントか、またはWindowsのネットワークにマッピングされたドライブの場合、ファイルリーダーコネクターのagent.logにエラーが記録されます。

ネットワークマッピングが不要なWindows UNCパスを使用してファイルが読み込まれている場合、ファイルリーダーコネクターはネットワークの切断を検出できません。

ファイルアクセスに関連するエラーメッセージではファイル名が報告されますが、ログ解析に関連するエラーメッセージではファイル名は報告されません。

ログファイルのアクセスは、シーケンシャルとパラレルのどちらですか。

使用するコネクターによって異なります。ログファイルをシーケンシャルに処理するコネクターと、ログファイルをパラレルに処理するコネクターがあります。

SmartConnectorでログファイルを読み取った後、NFSを使用して移動できますか。

はい、できます。Folder Followerコネクターは、NFSを使用してファイルの名前変更と移動を行います。ただし、ログファイルが格納されているフォルダーに対する適切な権限がコネクターに必要です。

SmartConnectorで、リモートマシンからネットワーク共有を使ってログファイルを読み取るにはどうすればいいですか。

リモートマシンに対するネットワーク共有を確立するには、Windowsプラットフォームではネットワークマッピングを使用し、Linux/UNIXプラットフォームではNFSまたはSambaマウントを使用します。

コネクターをWindowsサービスとして実行している場合、ネットワーク共有に対するアクセス権限が必要です。ユーザー名とパスワードのパネルにアクセスするには、次の操作を実行します。

1. [スタート] > [コントロールパネル] を選択します。
2. [管理ツール] をダブルクリックします。
3. [サービス] をダブルクリックします。
4. コネクターの名前を右クリックして、[プロパティ] を選択します。
5. [ログオン] タブで、ファイル共有へのアクセス権限を持つユーザーのユーザー名とパスワードを入力します。ネットワークにマッピングされたドライブではなく、UNC表記法を使ってファイルパスを指定します。

EPSを使用する場合、パフォーマンスに制限はありますか。

システムリソース、デバイス数、イベント数などによって変動します。

SmartConnectorで一度にアクセスできるログファイルの数を教えてください。

コネクターは、設定された数のログファイルにアクセスできます。フォルダーはパラレル処理されます。

マネージャー1つあたりのコネクターの数として、推奨されている最大数を教えてください。

絶対的な最大値はありません。マネージャーには、同時コネクタースレッド数として、64という制限値がデフォルトで適用されます。スレッドの数が増えるほど、スレッドのコンテキストスイッチのオーバーヘッドが増大するので、パフォーマンスは低下します。一般的に、スレッド数は常に2桁以内に抑えることをお勧めします。

サービス (Windows) やデーモン (Unix) としてコネクターを実行する設定を行う場合、「An issue has been encountered configuring the connector to run as a service. Check agent.log (Service Installation) for details.」というメッセージが表示されます。

このメッセージは、さまざまな理由から、コネクターをサービスまたはデーモンとして実行する設定が不可能な場合に表示されます。たとえば、WindowsやUnixに、まったく同じ名前やタイプの別のコネクターをインストールしている場合があります (デフォルトオプションを使用した場合など)。具体的なサービスのインストール場所を含め、詳細はagent.logに記録されています。たとえば、「<サービスのインストール場所> - SE:wrapperm | Unable to install the ArcSight Syslog NG Daemon service -」は、指定したサービスがインストール済みであることを示します (0x431)。

この問題を解決するには、追加のコネクターからagent.wrapper.confファイルを手動で削除します。このファイルは、\$ARCSIGHT_HOME/current/user/agentフォルダーに格納されています。

複数のコネクターを設定する場合は、重複を避けるため、異なる名前とタイプを使用してください。

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。

Feedback on SmartConnector User Guide (Connectors)

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。