Hewlett Packard Enterprise

HPE Security ArcSight Logger

ソフトウェアバージョン: 6.4

インストールおよび構成ガイド

2017年4月14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。

著作権情報

著作権と承認の完全な表明については、以下のリンク先をご覧ください。
https://www.protect724.hpe.com/docs/DOC-13026

サポート

連絡窓口

電話	電話番号のリストは、HPE SecurityArcSightテクニカルサポートページに記載されています: 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://www.protect724.hpe.com

目次

本書の概要

このガイドでは、ArcSight Data Platform (ADP) LoggerおよびスタンドアロンLogger のバージョン6.4のインストールと初期化の方法について説明します。Loggerアプライアンスを初期する方法およびソフトウェアLoggerをLinuxおよびVMware VMにインストールする方法についても説明します。

注: このドキュメントでは、具体的な相違がない場合は、すべてのタイプのLoggerを*Logger*と称します。違いがある場合は、Loggerの具体的なタイプが示されています。

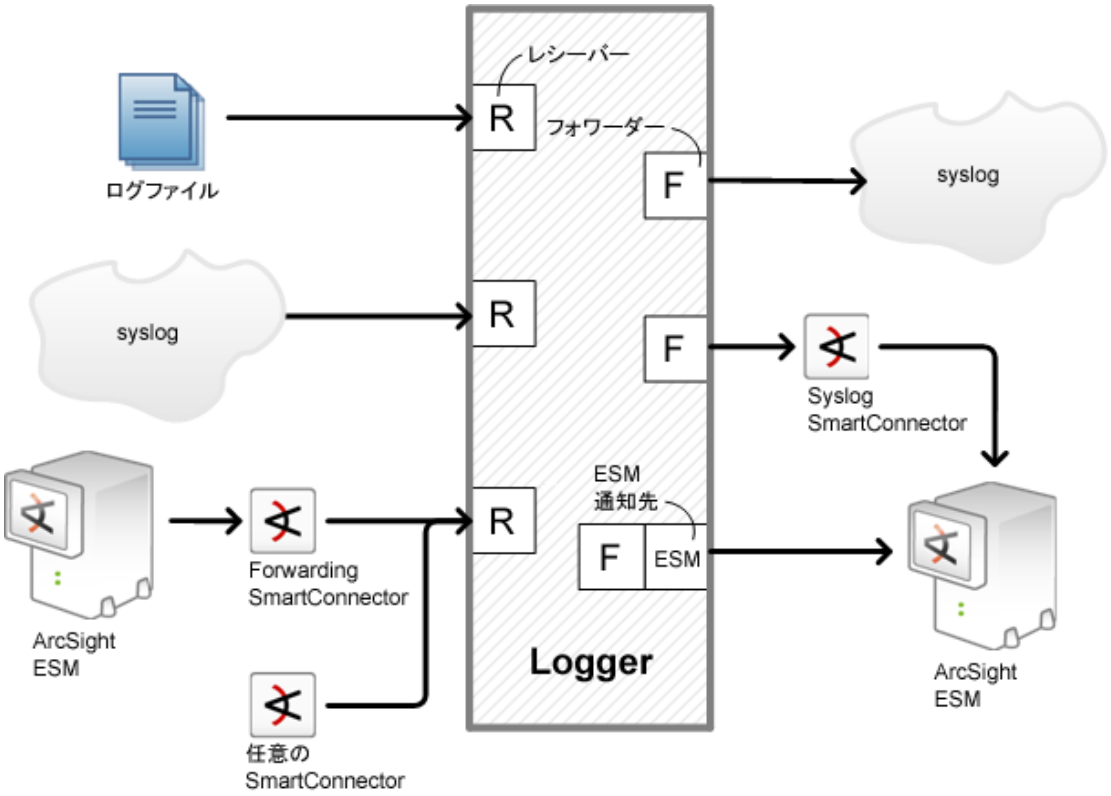
第1章: 概要

ArcSight Loggerは、きわめて高いイベントスループット、効率的な長期保存、高速なデータ分析のために最適化されたログ管理ソリューションです。イベントとは、ホストによって送信されたsyslogメッセージなどのタイムスタンプの付いたログエントリ、またはログファイルに追加された行です。Loggerはイベントを受信して格納し、検索、取得およびレポートをサポートします。また、関連付けと分析のために選択されたイベントをSyslogサーバーなどの送信先に転送することができます。

Loggerの仕組み

Loggerは、イベントと呼ばれるタイムスタンプの付いたログエントリを持続的な高い入力レートで保存します。rawデータは圧縮されますが、フォレンジック品質の訴訟データ用に、必要に応じていつでも圧縮前のデータを取得できます。Loggerは、ArcSight SmartConnectorで正規化されたCEFイベント形式のデータ、syslogメッセージを受信できるほか、デバイスからログファイルを直接受信できます。その後、Loggerは、受信したイベントをsyslogサーバーまたはArcSight ESMに転送できます。

SmartConnectorは、Loggerとネットワーク上のデバイス(Loggerに保存するイベントを生成するデバイス)との間のインターフェイスです。SmartConnectorは、イベントデータを収集し、そのデータを共通イベントフォーマット (CEF) に正規化します。CEFの詳細については、Protect 724のArcSight製品ドキュメントコミュニティで『ArcSight Common Event Format (CEF) Guide』を探し、「Implementing ArcSight」を参照してください。



イベントが一度Loggerに保存されると、次の操作を実行できます。

- 特定のクエリと一致するイベントを検索する。
- 関心のあるイベントのレポートを生成する。
- 所定の時間内にクエリとの一致が指定した回数だけ発生した場合にアラートを生成する。アラートは、電子メール、SNMPトラップ、またはSyslogメッセージの形式で通知できます。
- 特定のクエリに一致するイベントを表示するダッシュボードを設定する。
- 選択したイベントをArcSight ESMに転送して、関連付け、分析する。
- イベントをsyslogサーバーに転送する。

セキュリティ、コンプライアンス、およびIT運用のためのLogger

Loggerはさまざまな業界で利用することができますが、Loggerの検索、レポート、アラート機能は、セキュリティとコンプライアンスに関するレポート、およびIT運用の検索に直接適用できます。

Loggerには、一般的に検索されることが多いセキュリティ、IT運用、およびアプリケーション開発のイベント用のクエリを定義した定義済みのコンテンツフィルターが最初から含まれています。このコンテンツフィルターには、失敗したログイン試行、ソース別のイベント数、UNIXサー

バー上のSSH認証などが含まれます。したがって、一般的に検索されるイベントの多くについて検索用のクエリを定義する必要はありません。また、定義済みのコンテンツフィルターをコピーしてニーズに合わせて編集することができるので、クエリを最初から作成するために必要な時間と労力を節約できます。さらに、Loggerには、一般的なセキュリティおよびデバイス監視のユースケースのために定義済みのレポートも含まれています。

定義済みのコンテンツフィルターと定義済みレポートの完全なリストについては、『ArcSight Logger管理者ガイド』を参照してください。定義済みフィルターの使用方法に関する情報は、「システムフィルター(定義済みフィルター)」(82ページ)に記載されています。

第1章: 展開の計画

Loggerをインストールする前に、イベントを保存する方法と、保存する期間について計画する必要があります。展開を計画するときには以下の項の情報を考慮してください。

最新のドキュメントの入手

このリリースのドキュメントの最新版は、Protect 724のArcSight製品ドキュメントコミュニティからダウンロードできます (PDF形式)。

ヘルプは、Loggerのユーザーインターフェイス (UI) から利用できます。いずれかのユーザーインターフェイスページからオンラインヘルプにアクセスするには、ユーザー名の横の下矢印をクリックし、[ヘルプ] を選択します。

試用版のライセンス

どちらのArcSight Loggerにも90日間の評価期間に使用できる試用版ライセンスが付属しています。評価期間が終了した後は、有効なライセンスを適用するまでLoggerのどの機能にもアクセスできなくなります。

試用版ライセンスでは、以下の機能にアクセスできます。

- レポートを除くLoggerのすべての機能。
- 1日あたり5 GBのデータ収集量 (ソフトウェアLoggerのみ)。
- 90 GBのストレージ。

できるだけ早く、完全なライセンスをアップロードしてください。新しいライセンスをアップロードするには、メニューバーの **[システム管理]** を開き、**[システム]** セクションの **[ライセンスおよび更新]** をクリックします。手順については、『Logger管理者ガイド』の「システム管理」の章を参照してください。

使用するライセンスでArcMCによる管理が許可されているかどうかによって、試用版ライセンスをスタンドアロンライセンスまたはADPライセンスのいずれかで更新できます。(ADP LoggerはArcMCによって管理されます)。いずれかのライセンスをアップロードすると、レポート機能が有効になり、使用可能な1日のデータ量とストレージ量がライセンスで許可された容量に増加します。

Loggerが収集する1日のデータ量は、[データボリューム] ページの **[設定] > [詳細] > [データボリューム]** の下に表示されます。1日のデータの制限やその他のライセンス情報は、Loggerの **[設定] > [詳細] > [ライセンス情報]** および **[システム管理] > [システム] > [ライセンスおよび更新]** の下で確認できます。

初期設定

インストールと初期化のプロセスにより、Loggerは、以下の項で説明する初期設定値にセットアップされます。保有ポリシーの実装のために、Loggerに追加の設定をすることができます。「Loggerの設定」(60ページ)を参照してください。詳細については、『Logger管理者ガイド』の「設定」の章を参照してください。

Loggerの初期設定については、以下の各項で説明しています。

ストレージボリューム

Loggerのストレージボリュームはバージョンによって異なり、最大容量は12 TBです。初期化処理でストレージボリュームをセットします。Loggerアプライアンスの場合は、ストレージボリュームは、該当モデルの最大容量または12 TBのどちらか小さい方に設定されます。ソフトウェアLoggerの場合は、ストレージボリュームは、ライセンスで指定された最大容量または使用可能なディスクスペースのどちらか小さい方に設定されます。

注意: Loggerの最大容量を超えたイベントは保存されません。これらのイベントを保存する方法については、『Logger管理者ガイド』の「設定」の章を参照してください。

Loggerのインストール後、**[設定] > [詳細] > [ライセンス情報]** ページで、現在の制限値を確認できます。手順については、『Logger管理者ガイド』の「設定」の章を参照してください。新しいライセンスのアップロード方法を含む、ライセンスの詳細については、『Logger管理者ガイド』の「システム管理」の章を参照してください。

ストレージボリュームはインストール後に拡張できますが、縮小はできません。ストレージボリュームの拡張については、『Logger管理者ガイド』の「設定」の章を参照してください。

ストレージグループ

デフォルトストレージグループと内部イベントストレージグループの2つのストレージグループが、Loggerのインストール中に自動的に作成されます。

これらのストレージグループには、以下の項目があらかじめ設定されています。

デフォルトストレージグループの設定済み項目

属性	アプライアンスLogger	ソフトウェアLogger
サイズ	ストレージボリューム容量の1/2	ストレージボリューム容量の1/2
保存期間	180日間	180日間

内部ストレージグループの設定済み項目

属性	アプライアンスLogger	ソフトウェアLogger
サイズ	5 GB	3 GB
保存期間	365日間	365日間

Loggerは、最大で6つのストレージグループを持つことができます。したがって、Loggerの初期化後に追加で4つのストレージグループを作成できます。各ストレージグループは、異なる設定が可能です。すべてのストレージグループについて、保有ポリシーとサイズを変更できます。ただし、名前の変更はユーザー定義のストレージグループのみ可能です。ストレージグループの追加、サイズ変更、および保有ポリシーの変更については、『Logger管理者ガイド』の「設定」の章を参照してください。

検索インデックス

Loggerは、フルテキスト検索に対応しているほか、よく使用されるフィールドは初期化中にインデックスが作成されます。インデックスにフィールドを追加できますが、一度追加すると、インデックスからフィールドを削除することはできません。詳細は、『Logger管理者ガイド』の「検索」の章を参照してください。

レシーバー

デフォルトのインストールにはいくつかのレシーバーが含まれています。イベントの受信を開始するには、デフォルトレシーバーに送信するようにイベントソースに指示します。初期化後に、イベントをリッスンする追加のレシーバーを作成できます。レシーバーがデータを受信できるようにするには、リッスンポートをファイアウォールで開く必要があります。詳細については、「ファイアウォールルール」(15ページ)を参照してください。

また、必要に応じて、レシーバーの変更や削除、有効化および無効化を実行できます。

ヒント: レシーバーを追加または削除するときは、必ずファイアウォールの設定を更新してください。

以下のレシーバーは、デフォルトのインストール処理でセットアップされ、有効になります。

- UDPレシーバー: デフォルトで有効にされます。

  Loggerアプライアンス用のUDPレシーバーは、ポート514/udpを使用します。ソフトウェアLoggerをrootでインストールしている場合、UDPレシーバーのポートは514/udpです。root以外でのインストールでは、ポート8514/udpです。このポートがすでに使用されている場合、次に番号の大きい未使用のポートがインストールプロセスで選択されます。
- TCPレシーバー: デフォルトで有効にされます。

  Loggerアプライアンス用のTCPレシーバーは、ポート515/tcpを使用します。ソフトウェアLoggerをrootでインストールしている場合、TCPレシーバーのポートは515/tcpです。root以外でのインストールでは、ポート8515/tcpです。このポートがすでに使用されている場合、次に番号の大きい未使用のポートがインストールプロセスで選択されます。
- SmartMessageレシーバー: デフォルトで有効にされます。

  SmartConnectorからイベントを受信するには、SmartConnectorをダウンロードし、通知先の設定で **[Receiver Name]** を「SmartMessage Receiver」に設定します。SmartMessageレシーバーは、ユーザーインターフェイスと同じポートをリッスンします。Loggerアプライアンスについては443/tcp、rootでインストールされたソフトウェアLoggerについては通常443/tcp、root以外でインストールされたソフトウェアLoggerについては9000/tcpです。ソフトウェアLoggerのポートは異なる可能性があります。

Loggerにはさらに、LoggerのApache URLアクセスエラーログ、システムメッセージログ、およびシステム監査ログ (ご使用のLinux OSで監査が有効になっている場合) 用にフォルダーフォロワーレシーバーがあらかじめ設定されています。これらのレシーバーを使用するには、有効化する必要があります。

注: LoggerのApache URLアクセスエラーログ、http_error_logは、フォーマットがApache access_logに類似しています。Apache URLアクセスエラーログには、アクセスの失敗のみが記録されます。

ソフトウェアLoggerの場合、設定済みのフォルダーフォロワーレシーバーには以下のものが含まれます。

- Varログメッセージ: `/var/log/messages`
- 監査ログ: `/var/log/audit/audit.log`
- Apache URLアクセスエラーログ: `<install_dir>/userdata/logs/apache/http_error_log`

  注: `/var/log/audit/audit.log`用のフォルダーフォロワーレシーバーは、システムのインストール時にすでに`/var/log/audit/`フォルダーが存在している場合にのみ作成されます。

Loggerアプライアンスモデルには、監査が無効になっているものがあります。監査が有効になっているLoggerアプライアンスは、ソフトウェアLoggerと同じ設定済みレシーバーを持ちます。

Loggerがインストールされたシステムで監査が無効である場合、設定済みフォルダーフォロワーレシーバーは、以下のものを含みます。

- Varログメッセージ: `/var/log/messages`
- Apache URLアクセスエラーログ: `/opt/arcsight/userdata/logs/apache/http_error_log`

設定済みレシーバーを有効にする方法については、「レシーバー」(61ページ)を参照してください。すべてのLoggerレシーバーの詳細については、『Logger管理者ガイド』の「設定」の章を参照してください。

ファイアウォールルール

Loggerがデータを受信できるようにするには、一部のポートをファイアウォールで開く必要があります。

- ソフトウェアLoggerの場合、ファイアウォールの設定はユーザーが行います。Logger 6.4を最初にインストールした後で、現在の設定に必要なポートだけを開くようにファイアウォールを設定する必要があります。

  注意: HPE ArcSightは、必要なポートだけを開くようにファイアウォールを設定することを強くお勧めします。

- Logger アプライアンスの場合、ファイアウォールは設定済みです。HPE ArcSightには、ファイアウォールの更新に使用できるスクリプトが用意されています。

ヒント: レシーバーやSNMPポーリングなど、受信トラフィックにオープンポートが必要なサービスを追加または削除するときは、必ずファイアウォールの設定を更新してください。

デフォルトポートのリストとその他の情報については、『Logger管理者ガイド』の「システム管理」の章を参照してください。

第2章: Loggerアプライアンスのセットアップ

この章では、Loggerアプライアンスをラックにマウントし、IPアドレスと初期設定を設定する方法について説明します。アプライアンスのセットアップのためにインストーラーを実行する必要はありません。Loggerソフトウェアはアプライアンスにプリインストールされています。以下の基本的な手順で、Loggerアプライアンスの使用を開始できます。

ソフトウェアLoggerをLinuxにインストールする方法の詳細は、「Linuxへのソフトウェアloggerのインストール」(26ページ)を参照してください。ソフトウェアLoggerをVMware VMにインストールする方法の詳細は、「VMwareへのソフトウェアLoggerのインストール」(46ページ)を参照してください。

暗号化されたアプライアンスでのLoggerの実行

Loggerは暗号化されたハードウェア上で実行できるため、保存されている機密データをセキュリティで保護し、コンプライアンス規制やプライバシーの課題に対応することができます。

Server Management Software > HPE Secure Encryption Webページから入手可能なHPE Secure Encryptionを使用して、L7600Loggerアプライアンスを暗号化できます。手順については、そのページのTechnical Support> ManualsリンクからPDFおよびCHM形式の『HPE Secure Encryption Installation and User Guide』を参照してください。

L7600 Loggerアプライアンスには暗号化の機能があります。HPE Secure Encryptionを使用した暗号化に必要なものがあらかじめインストールされています。暗号化に必要な時間は、暗号化されるサーバー上のデータ量によって異なります。弊社のテストでは、7.5TBのデータが格納されたL7600 Loggerアプライアンスの暗号化に約72時間かかりました。暗号化の実行中も、引き続きLoggerを使用できます。既存のLoggerアプライアンスを暗号化した後で、パフォーマンスが低下することがあります。

注意: Loggerを暗号化した後では、暗号化前の状態に復元することはできません。

Loggerアプライアンスのインストール

開始する前に

- 同梱の「License Entitlement Certificate」ドキュメントに記載された手順に従ってライセンスキーを取得してください。このキーを取得すると、Loggerの機能にアクセスするために必要なライセンスが得られます。詳細については、「Loggerアプライアンスのライセンスの取得」(20ページ)を参照してください。
- Protect 724 (https://www.protect724.hpe.com) のArcSightユーザーコミュニティでアカウントを申請してください。製品のドキュメントやその他のコミュニティベースのリソースにアクセスするには、このアカウントが必要です。

アプライアンスをインストールするには

1. アプライアンスと付属のアクセサリを箱から出します。

   注: アプライアンスに同梱されている指示、注意、警告を注意深く読んでください。これらの指示、注意、警告に従わない場合、けがやアプライアンスの故障の原因となります。

2. ラックの取り付け手順に従って、アプライアンスを確実にラックに取り付けます。
3. リアパネルにケーブルを接続します。
4. アプライアンスの電源を入れます。

アプライアンスのIPアドレスの設定

アプライアンスは、eno1にデフォルトのIPアドレス192.168.35.35 (サブネットマスク255.255.255.0) を設定して出荷されます。アプライアンスのセットアップを開始するには、次の手順に従って、Loggerアプライアンスのコマンドラインインターフェイス (CLI) に新しいIPアドレスを設定します。

Logger CLIでコマンドを実行するには、プロンプトでコマンドを入力し、Enterキーを押します。コマンドラインインターフェイスの詳細については、「Loggerアプライアンスのコマンドラインインターフェイスの使用」(23ページ)を参照するか、プロンプトで`help`と入力して、使用可能なコマンドのリストを確認してください。

注: アプライアンスは、IPv4アドレス、IPv6アドレス、またはその両方を使用して設定できます。

新しいIPアドレスを設定するには

1. 次のいずれかの方法を使用してLoggerのCLI (オペレーティングシステムのCLIではありません) に接続します。
   - HPE ProLiant Integrated Lights-Out (iLO) にログインし、リモートコンソール機能を起動します。詳細については、「アプライアンスのリモートアクセスのセットアップ」(19ページ)を参照してください。
   - キーボードとモニターをアプライアンスのリアパネルにあるポートに接続します。
   - DB-9コネクター付きヌルモデムケーブルを使用して、ターミナルをアプライアンスのシリアルポートに接続します。シリアルポートには、標準的なVT100互換のターミナルを接続し、9600 bps、8ビット、パリティなし、1ストップビット (8N1)、フロー制御なしに設定することを推奨します。

     CLIに接続すると、ログインプロンプトが表示されます。
2. 次のデフォルトの資格情報を入力して、管理者としてログインします。

   ログイン: admin
   パスワード: password
3. 固定IPv4アドレスを指定するか、自動 (SLAAC) 設定を選択してIPv6アドレスを設定します。
   - 固定IPv4設定では、次のコマンド形式を使用します。

     `set ipv4 eno1 <ip>/<prefix>`

     例: `set ipv4 eno1 192.0.2.5/24`
   - 自動IPv4設定では、次のコマンド形式を使用します。

     `set ipv4 eno1 <ip> <subnetmask>`

     例: `set ipv4 eno1 192.0.2.5 255.255.255.0`
4. オプションで、固定IPv6アドレスを指定するか、自動 (SLAAC) 設定を選択してIPv6アドレスを設定します。
   - 固定IPv6設定では、次のコマンド形式を使用します。

     `set ipv6 <interface-name> <ipv6-address>`

     例: Set ipv6 eno1 fd0c:f179:edc0:999f:c634:6bff:feb9:2d0
   - 自動IPv6設定では、次のコマンド形式を使用します。

     `set ipv6 <interface-name> auto`

     例: `set ipv6 eno1 auto`

   注: IPv6の設定には、サブネットマスクは必要ありません。
5. IPv4またはIPv6のデフォルトゲートウェイを設定できます。

- IPv4設定のデフォルトゲートウェイを構成するには、次のコマンド形式を使用します。

  `defaultgw <ip>`と入力します。`<ip>`は、使用するデフォルトゲートウェイのIPアドレスに置き換えます。

- IPv6設定のデフォルトゲートウェイを構成するには、次のコマンド形式を使用します。

  `set ipv6 defaultgw <gateway> [interface]`

  例：`set ipv6 defaultgw fe80::20c:29ff:fe93:4192 eno1`

6. `set hostname <domain>.<company.com>`と入力します。`<domain>.<company.com>`は、目的のホストの完全修飾ドメイン名 (FQDN) に置き換えます。
7. `set dns <search_domain1>,<search_domain2> <nameserver1> <nameserver2>`と入力します。`<search_domainN>`は検索ドメインに、`<search_domainN>`はネームサーバーのIPアドレスにそれぞれ置き換えます。

   例：`set dns domain1.company.com,domain2.company.com 192.0.2.1 192.0.2.2`

   ヒント：複数の検索ドメインを使用する場合は、スペースではなくカンマで区切ります。複数のネームサーバーを使用する場合は、カンマではなくスペースで区切ります。

8. `set ntp <ntp_server1> <ntp_server2> <ntp_server3>`と入力します。`<ntp_serverN>`は、時刻の設定に使用するNTPサーバーと置き換えます。

   例：`set ntp time.nist.gov`

9. `show config`と入力して、前の手順で入力した設定値を確認します。必要に応じて、設定を変更します。

アプライアンスのリモートアクセスのセットアップ

すべてのArcSightアプライアンスには、HPE ProLiant Integrated Lights-Out (iLO) 拡張リモート管理カードが装備されています。HPEは、アウトオブバンドリモートアクセスが可能になるようにアプライアンスを設定することを強くお勧めします。そうすることで、お客様 (およびカスタマーサポートがお客様の許可と支援を受けて) が、リモートからアプライアンスのコンソールにアクセスし、トラブルシューティング、保守、および電源制御を実行できます。

アプライアンスのリモートアクセスをセットアップするには、『HPE ProLiant Integrated Lights-Out User Guide』の指示に従います。このガイドは、hhttp://www8.hp.com/us/en/products/servers/ilo/index.htmlから入手できます。

注：L7600モデルでは、ライセンスキーの取得と入力が必要です。iLOライセンスはプリインストールされていますが、今後の使用に備えて、iLOライセンスキーとドキュメントを入手して保管しておく必要があります。このライセンスキーは、すべての交換用アプライアンスで使用できます。

ライセンスキーの取得方法は、License Entitlement Certificateに記載されています。ライセンスキーを取得したら、iLOにログインし、**[Administration] > [Licensing]** で入力します。

Loggerアプライアンスのライセンスの取得

Loggerの一部の機能は、アクセスするために、有効なライセンスファイルをLoggerアプライアンスに適用する必要があります。詳細と手順については、「試用版のライセンス」(11ページ)を参照してください。ライセンスを取得するには、Loggerアプライアンスに付属する『Entitlement Certificate』ドキュメントに記載された手順に従ってライセンスキーを取得してください。このドキュメントがない場合は、https://softwaresupport.hpe.comのカスタマーサポートに連絡してください。

注: 複数のLoggerがある場合、注文の内容によっては、それぞれのLoggerについてライセンスファイルが必要です。

Loggerの初期化後、[ライセンス情報] および [ライセンスおよび更新] ページで現在のライセンスの詳細を表示できます (**[設定] > [詳細] > [ライセンス情報]** および **[システム管理] > [システム] > [ライセンスおよび更新]**)。詳細については、『Logger管理者ガイド』の「設定」および「システム管理」の各章を参照してください。

Loggerアプライアンスへの接続

Loggerのユーザーインターフェイス (UI) は、暗号化されたHTTPS接続を使用し、パスワードで保護されたWebブラウザーアプリケーションです。Logger 6.4のブラウザーのサポートに関する詳細は、Protect 724サイトで提供されている『ADP Support Matrix』ドキュメントを参照してください。

パブリックにアクセス可能なLoggerのポートは、任意のファイアウォールルールで許可する必要があります。ソフトウェアLoggerの場合、ファイアウォールの設定はユーザーが行います。Loggerアプライアンスでは、ファイアウォールのルールはあらかじめ設定されています。詳細については、「ファイアウォールルール」(15ページ)を参照してください。

- rootユーザーによるインストールの場合は、UDPレシーバー用のポート`514/udp`やTCPレシーバー用のポート`515/tcp`などのLoggerレシーバーが必要とするすべてのプロトコル用のポートに加え、ポート`443/tcp`へのアクセスも許可します。
- root以外のユーザーによるインストールの場合は、UDPレシーバー用のポート`8514/udp`やTCPレシーバー用のポート`8515/tcp`などのLoggerレシーバーが必要とするすべてのプロトコル用のポートに加え、ポート`9000/tcp`へのアクセスも許可します。

  注: ここで挙げたポートはデフォルトポートです。ご使用のLoggerでは、異なるポートを使用する場合があります。

JavaScriptとCookieは有効にしておく必要があります。

初めて接続してログインするには

1. Loggerに接続します。

   Loggerのインストール時に設定したURLを使用し、サポートされているブラウザーからLoggerに接続します。

   ソフトウェアLoggerの場合：`https://<hostname or IP address>:<configured_port>`

   Loggerアプライアンスの場合：`https://<hostname or IP address>`

   hostname or IP addressはLoggerソフトウェアがインストールされているシステムのホスト名またはIPアドレスであり、configured_portは、Loggerのインストール時に設定したポートです (該当する場合)。

   注： IPv6アドレスは、ブラウザーが認識できるように、角カッコで囲む必要があります。

2. **エンドユーザーライセンス契約 (EULA)**が表示されます。画面の一番下までスクロールしてEULAを確認し、承認します。承認後、[ログイン] 画面が表示されます。
3. ログインします。

   [ログイン] ダイアログが表示されたら、ユーザー名とパスワードを入力して [**ログイン**] をクリックします。

   初めて接続する場合は、次のデフォルトの資格情報を使用します。

   ユーザー名： admin
   パスワード： password

   注： デフォルトのユーザー名とパスワードで初めてログインすると、パスワードの変更を求めるプロンプトが表示されます。プロンプトに従って、新しいパスワードを入力して確認します。

   ログイン画面とLoggerへの接続方法の詳細については、『Logger管理者ガイド』の「ユーザーインターフェイスとダッシュボード」の章を参照してください。

正常にログインできたら、「Loggerアプライアンスの初期化」(21ページ)に進みます。

Loggerアプライアンスの初期化

EULAを承認して、最初にログインすると、[**Logger設定**] 画面が表示されます。この画面で、ライセンスファイルをアップロードし、ご使用のLoggerアプライアンスを初期設定できます。設定が完了すると、Loggerアプライアンスを使用できます。

注： Loggerアプライアンスを初期化するには、Loggerを工場出荷時の初期設定に戻すしか方法がありません。詳細については、『Logger管理者ガイド』を参照してください。

Loggerには、90日間有効な試用版ライセンスが付属しています。試用版ライセンスでは、機能が限定されています。すべての機能にアクセスするには、ArcSight Data Platform LoggerまたはスタンドアロンArcSight Loggerの完全なライセンスをアップロードする必要があります。詳細については、「試用版のライセンス」(11ページ)を参照してください。

ライセンスがない場合は、「Loggerアプライアンスのライセンスの取得」(20ページ)を参照してください。

Loggerアプライアンスを初期化するには

1. 初めて接続するときに完全なライセンスをアップロードするか、今は試用版ライセンス使用しておいて、後でライセンスをアップロードすることができます。
   - ライセンスがある場合は、すぐに適用することができます。

     ライセンスを適用するには、[**Logger設定**]画面の[**アップロードするライセンスファイルを選択**]の下で、Loggerアプライアンスのライセンスファイルの位置まで移動するか、パスとファイル名を指定して[**ライセンスのアップロード**]をクリックします。

     アップロード後、更新されたライセンス情報が[ライセンス]ペインに表示されます。
   - 今はライセンスを適用しない場合は、試用版の有効期限が切れる前に必ず適用してください。
2. [**システムロケール設定**]の下で、ドロップダウンリストから、このLoggerアプライアンス用の[**ロケール**]を選択します。

   ロケールの設定により、ユーザーインターフェイスの情報(たとえば日付、時刻、数字、メッセージ)が選択された国で適切な形式と言語で表示されます。この設定は一度設定すると変更できません。
3. [**日付/時刻設定**]の下で、[現在のタイムゾーン]および[現在の時刻]の設定が、ご使用の環境に適切かどうかを確認してください。

   時刻の設定を更新するには、それぞれ[**タイムゾーンの変更**]および[**日付/時刻の変更**]をクリックします。詳細については、『Logger管理者ガイド』の「システム管理」の章を参照してください。
4. [**保存**]をクリックします。

   Loggerの初期化プロセスが開始します。初期化が完了すると、システムは再起動します。これで、Loggerのインストールと初期化が完了しました。Loggerをセットアップしてイベントの受信を開始する方法については、『Loggerインストールガイド』の「Loggerの設定」の章を参照してください。

Loggerのインストールと初期化が完了したら、設定済みレシーバーを有効にし、設定デバイス、デバイスグループ、および保有ポリシーの実装に必要なストレージグループを設定できます。Loggerをセットアップしてイベントの受信を開始する方法については、「Loggerの設定」(60ページ)および『Logger管理者ガイド』の「設定」の章を参照してください。

ログイン画面とLoggerへの接続方法の詳細については、『Logger管理者ガイド』の「ユーザーインターフェイスとダッシュボード」の章を参照してください。

Loggerアプライアンスのコマンドラインインターフェイスの使用

LoggerアプライアンスのCLIを使用すると、Loggerアプリケーションのコマンドを発行するだけでなく、アプライアンスを起動したり停止したりすることが可能になります。

アプライアンスのCLIに接続するには、以下のいずれかの方法を使用します。

- HPE ProLiant Integrated Lights-Out (iLO) にログインし、リモートコンソール機能を起動します。詳細については、「アプライアンスのリモートアクセスのセットアップ」(19ページ)を参照してください。
- キーボードとモニターをアプライアンスのリアパネルにあるポートに接続します。
- DB-9コネクター付きヌルモデムケーブルを使用して、ターミナルをアプライアンスのシリアルポートに接続します。

  シリアルポートには、標準的なVT100互換のターミナルを接続し、**9600 bps**、**8ビット**、**パリティなし**、**1ストップビット** (**8N1**)、**フロー制御なし**に設定することを推奨します。
- CLIに接続すると、ログインプロンプトが表示されます。

CLIプロンプトでは以下のコマンドを使用できます。

カテゴリ	コマンド	説明
システムコマンド		
	exit	ログアウトします。
	halt	Loggerアプライアンスを停止し、電源をオフにします。
	help	コマンドラインインターフェイスのヘルプを開きます。
	reboot	Loggerアプライアンスを再起動します。
管理コマンド		
	show admin	デフォルト管理者ユーザーの名前を表示します。
認証コマンド		
	reset authentication	認証メカニズムをデフォルトのローカル認証に戻します。これは、CAC、LDAP、Radiusなどの異なる認証メカニズムが設定されていて、何らかの理由で機能しなくなった場合に役に立ちます。
設定コマンド		
	show config	Loggerのホスト名、IPアドレス、DNS、およびデフォルトゲートウェイを表示します。

カテゴリ	コマンド	説明
日付コマンド		
	show date	現在Loggerに設定されている日付と時刻を表示します。
	set date	Loggerに日付と時刻を設定します。 日付と時刻の形式はyyyyMMddhhmmssです。 日付の例：20101219081533
デフォルトゲートウェイコマンド		
	set defaultgw <IP> [nic]	1つまたはすべてのネットワークインターフェイスのデフォルトゲートウェイを設定します。
	show defaultgw [nic]	すべてまたは指定したネットワークインターフェイスのデフォルトゲートウェイを表示します。
DNSコマンド		
	show dns	現在LoggerにDNSサーバーを表示します。
	set dns <sd> <ns> set dns <sd1>,<sd2> <ns1> <ns2>	DNSネームサーバーを設定します。 sd=検索ドメイン、ns = ネームサーバー 3台までのネームサーバーと6個までの検索ドメインを追加できます。 **注：**複数の検索ドメインを使用する場合は、スペースではなくカンマで区切ります。複数のネームサーバーを使用する場合は、カンマではなくスペースで区切ります。
ホスト名コマンド		
	show hostname	現在Loggerに設定されているホスト名を表示します。
	set hostname <host>	Loggerのホスト名を設定します。
IPコマンド		
	show ip [nic]	すべてのネットワークインターフェイスまたは指定したネットワークインターフェイスのIPアドレスを表示します。
	set ip <nic> <IP> [/prefix] [netmask]	特定のネットワークインターフェイスについて、LoggerのIPアドレスを設定します。
NTPコマンド		
	set ntp <ntp server> <ntp server> <ntp server> ...	NTPサーバーのアドレスを設定します。このエントリは、現在のNTPサーバー設定を上書きします。 NTPサーバーは必要に応じていくつでも指定できます。複数

カテゴリ	コマンド	説明
		のNTPサーバーを指定した場合、サーバーは順番に確認されます。最初に応答したサーバーから取得した時刻が使用されます。 例 `logger> set ntp ntp.arcsight.com time.nist.gov 0.rhel.pool.org`
	show ntp	現在のNTPサーバーの設定を表示します。 例 `logger> show ntp ntp.arcsight.com time.nist.gov 0.rhel.pool.org`
パスワードコマンド		
	set password	現在のユーザーアカウントのパスワードを設定します。
プロセスコマンド		
	restart process	プロセスを再起動します。
	start process	プロセスを起動します。
	status process	プロセスのステータスを表示します。
	stop process	プロセスを停止します。
SSL証明書コマンド		
	show sslcert	現在Loggerにロードされ ているSSL証明書を表示します。
	reset sslcert	元のデフォルト情報をもとに新しい自己署名証明書を作成してインストールし、HTTPSサーバーを再起動します。
	diag sslcert	SSLセッション情報を表示します。
ステータスコマンド		
	show status	Loggerの設定を表示します。

第3章: Linuxへのソフトウェアのインストール

ソフトウェアLoggerは、LinuxシステムまたはVMware仮想マシン (VM) にインストールできます。この章では、Linuxシステムにソフトウェアをインストールして起動するために必要な情報について説明します。この章には以下のトピックに関する情報が含まれます。

ソフトウェアLoggerをVMware VMにインストールする方法については、「VMwareへのソフトウェアLoggerのインストール」(46ページ)を参照してください。Loggerアプライアンスの初期化については、「Loggerアプライアンスのセットアップ」(16ページ)を参照してください。

開始する前に

ソフトウェアLoggerをインストールするには、サポートされるオペレーティングシステムを実装したサーバーと、使用可能なストレージが必要です。Loggerをインストールして使用できるプラットフォームについての情報は、使用するバージョンのリリースノートおよび『ArcSight Data Platform Support Matrix』を参照してください。これらのドキュメントは、Protect 724のArcSight製品ドキュメントコミュニティからダウンロードできます。

インストールパッケージのダウンロード

インストールパッケージは、HPEソフトウェアデポ (https://h20392.www2.hpe.com/portal/swdepot/index.do) からダウンロードできます。

ダウンロードしたインストール用ソフトウェアの検証

HPEは、お客様が受け取った署名付きのソフトウェアが確実にHPEから提供され、第三者による改ざんが行われていないことを実証できるように、デジタル公開鍵を提供しています。

詳細な情報と手順については、次のサイトを参照してください。

https://h20392.www2.hpe.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning

ソフトウェアLoggerでのライセンスの仕組み

Loggerには、90日間有効な試用版ライセンスが付属しています。試用版ライセンスでは、機能が限定されています。すべての機能にアクセスするには、ArcSight Data Platform LoggerまたはスタンドアロンArcSight Loggerの完全なライセンスをアップロードする必要があります。詳細については、「試用版のライセンス」(11ページ)を参照してください。

ライセンスファイルがない場合は、「ソフトウェアLoggerのライセンスの取得」(28ページ)を参照してください。注文の内容によっては、ソフトウェアLoggerのインスタンスごとに、個別のライセンスが必要です。ライセンスファイルは、Loggerのダウンロードごとに一意に生成されます。

ライセンスの種類は、データボリューム制限機能の仕組みやデータボリュームページに表示される内容に影響します。

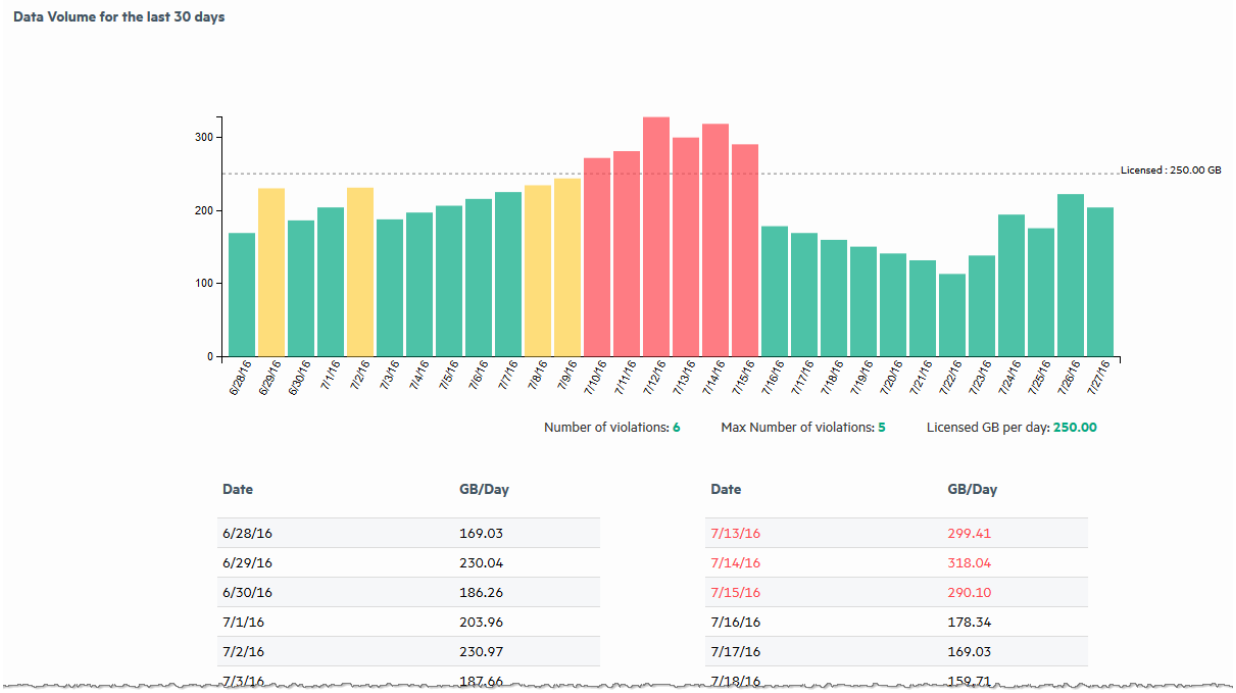
- ADP Loggerの場合、ArcMCがライセンス制限を管理します。詳細については、『ArcMC管理者ガイド』を参照してください。
- スタンドアロン型のArcSight Loggerの場合は、データボリューム制限機能によってライセンス制限が管理されます。

データボリューム制限機能は、ある1日に受信したイベントのサイズの合計を加算して、収集した1日のデータボリューム(1日あたりにLoggerが受信したデータの合計)を計算します。Loggerは、その値とライセンスの1日のデータ制限を比較します。この制限値を超えても、Loggerはイベントを収集して保存するので、イベントが紛失することはありません。ただし、過去30日間のウィンドウ内で制限値を超えた日が6日以上ある場合、検索関連のすべての機能が無効になります。データ制限違反が過去30日間のウィンドウ内で5回以下になるまで、収集したイベントのレポートを転送、検索、または実行することはできません。

たとえば、データの収集限度が20GBであるLoggerソフトウェアを1月1日にインストールし、イベントの収集を開始したとします。Loggerが、1月5日、13日、18日、19日、20日に、20GBを超えるイベントデータを受信します。ここまでで、制限値を超えたのは5回なので、1月21日は保存したイベントデータの転送、検索、レポート作成が可能です。しかし、1月30日に制限値を超えたとすると、許容最大回数を超えるので、1月31日には、転送、検索、レポート作成はできません。(1月31日に実行した検索は失敗し、ユーザーインターフェイスに警告が表示されます。)1月31日から2月4日までの間に、1日のデータ収集制限値を超えることがな

ければ、2月5日には、1月5日の制限値超過が30日間のウィンドウ外になるため、転送、検索、レポート作成の機能が回復します。

[データボリューム] ページ (**[設定] > [詳細] > [データボリューム]**) には、過去30日間にソフトウェアLogger上に保存されたデータが1日単位で表示されます。また、次の図に示すように、データ制限値を超えた日も表示されます。



データ制限値の超過が発生した場合、[検索] ユーザーインターフェイスに警告が表示されます。毎日のデータ制限値の超過が頻繁に発生するようであれば、要求に合ったライセンスの購入を検討してください。新しいライセンスの購入については、HPE ArcSightの営業担当者にお問い合わせください。新しいライセンスを入手したら、『ArcSight Logger管理者ガイド』の説明に従って、ご使用のLoggerに適用してください。

ソフトウェアLoggerのライセンスの取得

ソフトウェアLoggerのインストールには、ライセンスファイルが必要です。ライセンスを取得するには、発注後にHPEから電子メールで受け取るElectronic Delivery Receiptに記載された説明に従ってください。このドキュメントがない場合は、https://softwaresupport.hpe.comのカスタマーサポートに連絡してください。

Loggerのインストール後、[ライセンス情報] および [ライセンスおよび更新] ページで現在のライセンスの詳細を表示できます (**[設定] > [詳細] > [ライセンス情報]**および**[システム管理] > [システム] > [ライセンスおよび更新]**)。詳細については、『Logger管理者ガイド』の「設定」および「システム管理」の各章を参照してください。

インストールの前提条件

Loggerソフトウェアをインストールする前に、以下の前提条件を満たしていることを確認してください。

- Loggerをインストールするプラットフォームがサポートされていることを確認してください。この情報については、リリースノートおよび『ArcSight Data Platform Support Matrix』を参照してください。これらのドキュメントは、Protect 724のArcSight製品ドキュメントコミュニティからダウンロードできます。
- RHEL 7.Xにインストールする場合は、「RHEL 7.Xのlogind設定ファイルの編集」(31ページ)の説明に従って、`logind.conf`ファイルを編集します。
- 「ユーザープロセスの制限値とオープンファイルの最大数の増加」(30ページ)の説明に従って、オペレーティングシステムのユーザープロセスの上限を引き上げます。
- 実稼働環境に展開する前に有効なライセンスファイルを取得します。ライセンスファイルがない場合は、「ライセンスの取得」(48ページ)を参照してください。Loggerのインスタンスごとに、個別のライセンスが必要です。ライセンスファイルは、ダウンロードごとに一意に生成されます。
- Loggerをインストールするシステムにroot以外のユーザーアカウントが存在する必要があります。このアカウントがない場合、インストーラーによってアカウントを作成するように求められます。rootユーザーでインストールする場合でも、root以外のユーザーアカウントが必要です。このアカウントのユーザーIDとそのプライマリグループIDは同じにする必要があります。root以外のユーザーのUIDは1500、GIDは750である必要があります。たとえば、root以外のユーザーを作成するには、`root`ユーザーとして次のコマンドを実行します。

  ```
  groupadd -g 750 arcsight
  useradd -m -g arcsight -u 1500 arcsight
  ```

  これらのコマンドによって、Loggerソフトウェアのインストールで使用できる非rootユーザー`arcsight`が作成されます。
- rootユーザーまたはroot以外のユーザーのどちらでLoggerをインストールするかを決定します。どちらのユーザーを選ぶかにより、インストールオプションが異なります。

  ヒント: root以外のユーザーとしてインストールする場合は、インストールディレクトリとそのサブディレクトリへの書き込み権限が必要です。たとえば、root以外のユーザーarcsightの場合は、`chown -R arcsight:arcsight /opt/arcsight`コマンドを使用します。

  a. rootユーザーとしてインストールする場合、Loggerをサービスとして起動する設定を選択し、Loggerが安全なWeb接続をリッスンするポートを選択することができます。
  b. 非rootユーザーとしてインストールする場合、Loggerはポート9000/tcp上の接続のみをリッスンできます。ポートに別の値を設定することはできません。

> **注:** ユーザーには、インストールディレクトリとそのサブディレクトリへの書き込み権限が必要です (例: `chown –R arcsight /opt/arcsight`)。

c. アップグレードする場合、非rootユーザーによる以前のインストールをrootユーザーによるインストールに変更することはできません。ソフトウェアLoggerへのアクセスは、以前に設定したポート9000/tcpを使用する必要があります。

- 空のフォルダーにインストールします。以前にLoggerをアンインストールしたことがあり、同じ場所にインストールをする場合は、アンインストールで残ったファイルを確実に削除してください。
- Loggerをインストールするマシンのホスト名を「localhost」にすることはできません。ホスト名が「localhost」である場合は、インストールを続行する前に、ホスト名を変更してください。
- IPv6をサポートするには、Loggerをインストールする前に、Loggerをインストールするマシンを IPv6専用モードに設定する必要があります。
- LoggerをインストールするマシンにMySQLのインスタンスをインストールしないでください。マシンにMySQLのインスタンスが存在する場合は、Loggerをインストールする前にそのインスタンスをアンインストールしてください。
- GUIモードでインストールを行うには、X Window Systemサーバーがインストールされている必要があります。X11がインストールされていない場合、インストーラーはデフォルトでコンソールモードになります。
  - LoggerをSSH接続経由でGUIモードを使用してインストールする場合、インストールウィザード画面を見られるように、-Xオプションを使用してX window転送機能を有効にしていることを確認してください。
  - PuTTYを使用する場合は、Loggerをインストールするマシンに接続するマシンにもXクライアントが必要です。

ユーザープロセスの制限値とオープンファイルの最大数の増加

Loggerのインストールまたはアップグレードを実行する前に、`root`ユーザーとしてログインし、デフォルトのユーザープロセスの上限を引き上げる必要があります。これにより、システムは、十分な処理容量を得ます。

デフォルトのユーザープロセスの制限値を増やすには

1. `/etc/security/limits.d/<NN>-nproc.conf`ファイルを開きます。
   (`<NN>`は、RHELまたはCentOS 6.Xの場合は90、RHELおよびCentOS 7.Xの場合は20です)
   - `/etc/security/limits.d/<NN>-nproc.conf file`ファイルがない場合は、作成します (必要な場合は、`limits.d`ディレクトリも作成します)。

- このファイルがすでに存在する場合は、ファイル内のすべてのエントリを削除します。

2. 以下の行を追加します。

```
* soft nproc 10240
* hard nproc 10240
* soft nofile 65536
* hard nofile 65536
```

注意: 新しいエントリには、必ずアスタリスク (*) を含めてください。すべてのエントリを指定どおり正確に追加することが重要です。不足があるとシステムの実行時エラーの原因になります。

3. ログアウトしてから、もう一度ログインします。
4. 新しい設定を確認するために次のコマンドを実行します。`ulimit -a`
5. コマンドの実行結果で、"open files" と "max user processes" が以下の値であることを確認します。

```
open files 65536
max user processes 10240
```

ユーザープロセスの制限値を増やし、その他の前提条件を満たしたら、Loggerをインストールできます。

RHEL 7.Xのlogind設定ファイルの編集

Red Hat Enterprise Linux (RHEL) 7.1または7.2上でLoggerをインストールまたはアップグレードする前に、`logind.conf`ファイルのプロセス間通信 (IPC) 設定を変更する必要があります。

RHEL 7.Xのlogind.confファイルを変更するには

1. `/etc/systemd`ディレクトリに移動し、編集のために`logind.conf`ファイルを開きます。
2. RemoveIPCという行を探します。RemoveIPCをアクティブにして、noに設定する必要があります。

   #があれば削除し、必要であれば`yes`を`no`に変更します。正しいエントリは次のようになります。

```
RemoveIPC=no
```

3. ファイルを保存します。
4. `/etc/systemd`ディレクトリから、次のコマンドを入力して`systemd-logind`サービスを再起動し、変更を有効にします。

```
systemctl restart systemd-logind.service
```

この設定を変更し、その他の前提条件を満たしている場合は、Loggerをインストールする準備ができています。

インストール

ソフトウェアLoggerは、以下の3つの方法でインストールできます。

- GUIモード: ウィザードの手順に従って、ソフトウェアLoggerのインストールと設定を行います。GUIモードを使用するには、OSにX Windowsサーバーがインストールされている必要があります。
- コンソールモード: コマンドラインプロセスに従って、ソフトウェアLoggerのインストールと設定を行います。

  ヒント: リモートインストールで通信速度が問題になる場合は、コンソールモードを使用すると、より早くLoggerをインストールすることができる可能性があります。

- サイレントモード: インストールと設定に必要な入力をファイル経由で提供します。したがって、各サーバーへのインストールと設定のためにインストーラーを操作する必要はありません。ただし、このモードを使用する前に、これ以外のモードの1つを使用してインストールと設定を実行し、入力内容をファイルに記録しておく必要があります。

GUIモードを使用したソフトウェアLoggerのインストール

Loggerをインストールするマシンが、使用するバージョンのリリースノートに記載された仕様を満たしていること、および「インストールの前提条件」(29ページ)に記載された前提条件を満たしていることを確認してください。

インストールの前に、「ユーザープロセスの制限値とオープンファイルの最大数の増加」(30ページ)の説明に従って、OSのユーザープロセスの制限値を増やす必要があります。RHEL 7.Xの場合に限り、「RHEL 7.Xのlogind設定ファイルの編集」(31ページ)の説明に従って、`logind.conf`ファイルを変更します。

「ダウンロードしたインストール用ソフトウェアの検証」(27ページ)の説明に従って、用意したインストールファイルが正しいことを確認できます。

Loggerは、rootユーザーとしても、root以外のユーザーとしてもインストールできます。詳細と制約については、「インストールの前提条件」(29ページ)を参照してください。

注: ソフトウェアLoggerをSSH接続経由でGUIモードを使用してインストールする場合、インストールウィザード画面を見られるように、-xオプションを使用してX window転送機

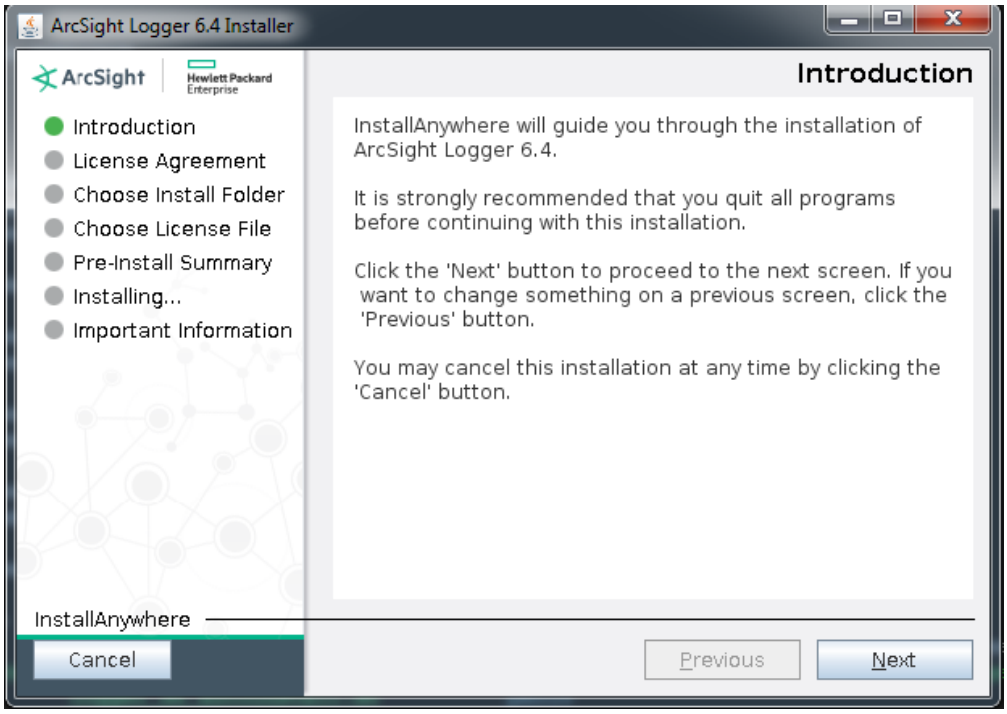
能を有効にしていることを確認してください。PuTTYを使用する場合は、Loggerをインストールするマシンに接続するマシンにもXクライアントが必要です。

Loggerソフトウェアのインストール

1. 以下のコマンドをLoggerのインストール用ファイルをコピーしたディレクトリから実行します。

   ```
   chmod u+x ArcSight-logger-6.4.0.XXXX.0.bin
   ./ArcSight-logger-6.4.0.XXXX.0.bin
   ```

2. インストールウィザードが起動します。**[Next]** をクリックします。



インストール処理のどの時点でも、[**Cancel**] をクリックしてインストール処理を中断できます。

注意： インストーラーを終了するためにCtrl+Cを使用しないでください。Ctrl+Cキーの操作によりインストールを終了し、続いてLoggerをアンインストールすると、アンインストール処理によって`/tmp`ディレクトリが削除されることがあります。

3. [License Agreement] 画面が表示されます。ライセンス契約を確認するために、契約の最後までスクロールし、[I accept the terms of the License Agreement] ボタンを有効にします。
4. [**I accept the terms of the License Agreement**] を選択し、[**Next**] をクリックします。
5. インストールの前提条件が満たされているかどうかが、インストーラーによってチェックされます。

- オペレーティングシステムのチェック - デバイスが実行しているオペレーティングシステムがサポート対象かどうかがチェックされます。サポートされていないオペレーティングシステムが実行されている場合、メッセージは表示されますが、Loggerソフトウェアのインストールが中止されるわけではありません。一部の更新シナリオでは、古いOSが使用されているため、このメッセージが発生します。

  注: HPE ArcSightでは、インストールの前にサポート対象のOSにアップグレードすることを強くお勧めします。サポートされているオペレーティングシステムプラットフォームのリストについては、『ArcSight Data Platform Support Matrix』を参照してください。

- インストールの前提条件のチェック - 確認に失敗すると、Loggerにメッセージが表示されます。先に進む前に、問題点を解決する必要があります。

例

ユーザーの操作を要求するメッセージが表示され、`etc/logind.conf`ファイル内のパラメーターを`yes`から`no`に変更する必要があることが通知されます。このメッセージには、必要な処理が書かれています。この例では、インストーラーを終了し、「RHEL 7.Xのlogind設定ファイルの編集」(31ページ)の手順に従います。ファイルを変更して保存したら、もう一度インストールコマンドを入力します。

すべてのチェックが完了すると、[Choose Install Folder] 画面が表示されます。

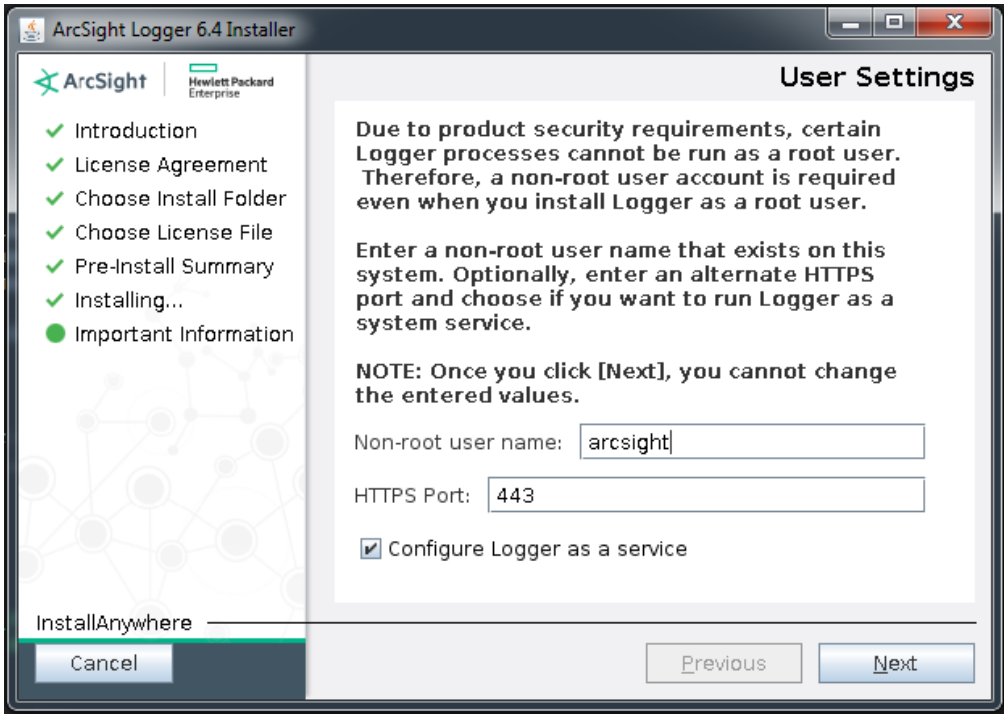
6. Loggerをインストールする場所に移動するか、場所を指定します。

   デフォルトのインストールパスは、`/opt`です。この場所にインストールすることも、別の場所にインストールすることもできます。

7. [**Next**] をクリックして、選択した場所にインストールします。
   - 指定された場所に、ソフトウェアをインストールする十分なスペースがない場合、メッセージが表示されます。インストールを続行するには、別の場所を指定するか、指定の場所に十分なスペースを確保します。[**Previous**] をクリックして別の場所を指定するか、[**Quit**] をクリックしてインストーラーを終了します。
   - 指定した場所にLoggerがすでにインストールされている場合、メッセージが表示されます。[**Upgrade**] をクリックして処理を続行するか、[**Previous**] をクリックして別の場所を指定します。アップグレードの説明については、使用するバージョンのリリースノートを参照してください。
8. インストール前の概要を確認し、[**Install**] をクリックします。

   インストールには数分かかることがあります。しばらくお待ちください。インストールが完了すると、次の画面が表示されます。
9. rootでログインしている場合、以下のフィールドの入力を要求されます。フィールドに記入してから [**Next**] をクリックします。

フィールド	説明
Non-root user name	このユーザーがまだシステムに存在しない場合は、ユーザー名の入力が求められます。
HTTPS Port	Logger UIにアクセスするときに使用するポート番号。 デフォルトのHTTPSポート (443/tcp) を使用することも、ご希望のポートを入力することもできます。443/tcp以外のポートを指定する場合、ユーザーはLogger UIへのアクセスに使用するURLにそのポート番号を入力する必要があります。
Configure Logger as a service	Loggerをサービスとして実行するように設定するかどうかを示します。 このオプションを選択すると、`arcsight_logger`という名前のサービスを作成し、レベル2、3、4、5で実行可能にします。 インストール処理中にLoggerをサービスとして起動するように設定しなかった場合でも、後からそのように設定することができます。インストール後にLoggerをサービスとして起動する方法については、「ソフトウェアLoggerのコマンドラインオプションの使用」(43ページ)を参照してください。



10. このインストールのロケールを選択し、[**Next**] をクリックします。
11. ライセンスファイルのパスと名前を入力し、[**Next**] をクリックします。

> **注:** ライセンスファイルを指定しない場合は、機能に大幅な制限のある90日間の試用版ライセンスがインストールされます。「試用版のライセンス」(11ページ)を参照してください。

初期化画面が表示されます。

12. もう一度 [**Next**] をクリックして、Loggerコンポーネントを初期化します。初期化には数分かかることがあります。しばらくお待ちください。初期化が完了すると、設定画面が表示されます。
13. [**Next**] をクリックして、Loggerがストレージグループとストレージボリュームを設定することを許可します。設定には数分かかることがあります。しばらくお待ちください。

    設定が完了すると、Loggerが起動し、設定が完了したことを通知するウィンドウにLoggerユーザーインターフェイスのURLが表示されます。
14. URLをメモし、[**Done**] をクリックしてインストーラーを終了します。

Loggerのインストールと初期化が完了したら、インストール中にメモしたURLを使用してLoggerに接続できます。この手順については、「ソフトウェアLoggerへの接続」(42ページ)を参照してください。

コンソールモードを使用したソフトウェアLoggerのインストール

Loggerをインストールするマシンが、使用するバージョンのリリースノートに記載された仕様を満たしていること、および「インストールの前提条件」(29ページ)に記載された前提条件を満たしていることを確認してください。

インストールの前に、「ユーザープロセスの制限値とオープンファイルの最大数の増加」(30ページ)の説明に従って、OSのユーザープロセスの制限値を増やす必要があります。RHEL 7.Xの場合に限り、「RHEL 7.Xのlogind設定ファイルの編集」(31ページ)の説明に従って、`logind.conf`ファイルを変更します。

「ダウンロードしたインストール用ソフトウェアの検証」(27ページ)の説明に従って、用意したインストールファイルが正しいことを確認できます。

Loggerは、rootユーザーとしても、root以外のユーザーとしてもインストールできます。詳細と制約については、「インストールの前提条件」(29ページ)を参照してください。

Loggerソフトウェアのインストール

1. 以下のコマンドをLoggerのインストール用ファイルをコピーしたディレクトリから実行します。

   ```
   chmod u+x ArcSight-logger-6.4.0.XXXX.0.bin
   ./ArcSight-logger-6.4.0.XXXX.0.bin -i console
   ```
2. インストールウィザードがコマンドラインモードで起動します。**Enter**キーを押して続行します。

   ```
   ===============================================================

   Introduction
   ------------
   ```

```
InstallAnywhere will guide you through the installation of ArcSight Logger
6.4.

It is strongly recommended that you quit all programs before continuing
with this installation.

Respond to each prompt to proceed to the next step in the installation.If
you want to change something on a previous step, type 'back'.

You may cancel this installation at any time by typing 'quit'.

PRESS <ENTER> TO CONTINUE:
```

3. 以降の数画面は、エンドユーザーライセンス契約を表示します。以下のプロンプトが表示されるまで、**Enter**キーを押して、ライセンス契約の各部分を表示します。

   ```
   DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N):
   ```

4. Yと入力し、**Enter**キーを押してライセンス契約を承認します。

   インストール処理のどの時点でも、「quit」と入力し、**Enter**キーを押してインストール処理を中止できます。

5. インストールの前提条件が満たされているかどうかが、インストーラーによってチェックされます。
   - オペレーティングシステムのチェック - デバイスが実行しているオペレーティングシステムがサポート対象かどうかがチェックされます。サポートされていないオペレーティングシステムが実行されている場合、メッセージは表示されますが、Loggerソフトウェアのインストールが中止されるわけではありません。一部の更新シナリオでは、古いOSが使用されているため、このメッセージが発生します。

     注: HPE ArcSightでは、インストールの前にサポート対象のOSにアップグレードすることを強くお勧めします。サポートされているオペレーティングシステムプラットフォームのリストについては、『ArcSight Data Platform Support Matrix』を参照してください。

   - インストールの前提条件のチェック - 確認に失敗すると、Loggerにメッセージが表示されます。先に進む前に、問題点を解決する必要があります。

例

このマシン上でLoggerが実行されている場合は、ユーザーの操作を要求するメッセージが表示されます。

```
================================================================================

Intervention Required

--------------------

ArcSight Logger processes are active.

All ArcSight Logger processes must be stopped to allow installation to
proceed.

Type 'Quit' to exit this installer or 'Continue' to stop all ArcSight
Logger processes and continue with the installation.

->1- Continue

  2- Quit

ENTER THE NUMBER OF THE DESIRED CHOICE, OR PRESS <ENTER> TO ACCEPT THE
DEFAULT:
```

この場合、Loggerプロセスを停止するには「1」を入力します (または**Enter**キーを押します)。プロセスを実行するか、インストーラーを終了するには、「2」を入力します。

すべてのチェックが完了すると、インストールが続行し、[Choose Install Folder] 画面が表示されます。

6. [Choose Install Folder] 画面で、Loggerのインストールパスを入力し、**Enter**キーを押します。

   デフォルトのインストールパスは、/optです。この場所にインストールすることも、別の場所にインストールすることもできます。

7. 「Y」と入力し、**Enter**キーを押してインストールの場所を確認します。
   - 指定された場所に、ソフトウェアをインストールする十分なスペースがない場合、メッセージが表示されます。インストールを続行するには、別の場所を指定するか、指定の場所に十分なスペースを確保します。インストールを中止するには、「quit」と入力し、**Enter**キーを押します。
   - Loggerが指定の場所にすでにインストールされている場合は、メッセージが表示されます。アップグレードを続行する場合は「2」を入力し、別の場所を指定する場合は「1」を入力します。アップグレードの説明については、使用するバージョンのリリースノートを参照してください。
8. インストール前の概要を確認し、**Enter**キーを押してLoggerをインストールします。

   インストールには数分かかることがあります。しばらくお待ちください。インストールが完了すると、次の画面が表示されます。

9. rootでログインしている場合、以下のフィールドの入力を要求されます。各フィールドに回

答を入力し、**Enter**キーを押します。

フィールド	説明
User Name	このユーザーがまだシステムに存在しない場合は、ユーザー名の入力が求められます。 **ヒント:** VMWare VM上にLoggerをインストールする場合は、システムにあらかじめ構成されている非rootユーザー`arcsight`を使用します。
HTTPS Port	Logger UIにアクセスするときに使用するポート番号。 デフォルトのHTTPSポート (443) を使用することも、ご希望のポートを入力することもできます。443以外のポートを指定する場合、ユーザーはLogger UIへのアクセスに使用するURLにそのポート番号を入力する必要があります。
Choose if you want to run Logger as a system service.	「`1`」を入力してEnterキーを押し、Loggerをサービスとして設定するか、「`2`」を入力してEnterキーを押し、Loggerをスタンドアロン型に設定します。 このオプションを選択すると、`arcsight_logger`という名前のサービスが作成され、レベル2、3、4、5で実行可能になります。 インストール処理中にLoggerをサービスとして起動するように設定しなかった場合でも、後からそのように設定することができます。インストール後にLoggerをサービスとして起動する方法については、『Logger管理者ガイド』を参照してください。

10. 希望するロケールに対応する番号を入力して**Enter**キーを押します。
    - 英語の場合は1
    - 日本語の場合は2
    - 簡体字中国語の場合は3
    - 繁体字中国語の場合は4
11. ライセンスファイルへの絶対パスを入力し、**[Next]** をクリックします。

    注: ライセンスファイルを指定しない場合は、機能に大幅な制限のある90日間の試用版ライセンスがインストールされます。「Loggerアプライアンスのライセンスの取得」(20ページ) を参照してください。

    初期化画面が表示されます。
12. **Enter**キーをもう一度押して、Loggerコンポーネントを初期化します。

    初期化には数分かかることがあります。しばらくお待ちください。初期化が完了すると、設定画面が表示されます。
13. **[Next]** をクリックして、ストレージグループとストレージボリュームを設定し、Loggerを再起動します。

    設定には数分かかることがあります。しばらくお待ちください。

    設定が完了すると、Loggerが起動し、次の画面にLoggerへの接続に使用するURLが表示されます。
14. URLをメモし、**Enter**キーを押してインストーラーを終了します。

Loggerのインストールと初期化が完了したら、インストール中にメモしたURLを使用してLoggerに接続できます。この手順については、「ソフトウェアLoggerへの接続」(42ページ)を参照してください。

サイレントモードを使用したソフトウェアLoggerのインストール

ソフトウェアLoggerをサイレントモードでインストールする前に、サイレントモードのインストールで必要になるプロパティファイルを作成する必要があります。ファイルを作成したら、サイレントモードのインストールに使用します。

サイレントモードのインストール用ライセンス

Loggerのインストールでは、サイレントモードのインストールごとに固有のライセンスファイルが必要です。「ソフトウェアLoggerのライセンスの取得」(28ページ)で説明されているようにライセンスを取得し、それを、Loggerをサイレントモードでインストールするマシンまたは、そのマシンからアクセスできる場所に置きます。

サイレントモードインストール用プロパティファイルの生成

サイレントインストールに使用するプロパティファイルを生成するには

1. インストール用のプロパティファイルを生成するために、ソフトウェアLoggerをインストールするマシンにログインします。

   サイレントモードのインストールをrootユーザーとして実行したい場合は、rootユーザーでログインします。そうでない場合は、root以外のユーザーでログインします。
2. 以下のコマンドを実行します。

   ```
   chmod u+x ArcSight-logger-6.4.0.XXXX.0.bin
   ./ArcSight-logger-6.4.0.XXXX.0.bin -r <path_for_generated_file>
   ```

   <path_for_generated_file>は、生成したプロパティファイルを置くディレクトリです。生成されたプロパティファイルは、installer.propertiesという名前です。この名前を変更したり、別の名前を指定したりすることはできません。
3. LoggerをGUIモードでインストールします。「GUIモードを使用したソフトウェアLoggerのインストール」(32ページ)を参照してください。
4. インストールが完了したら、installer.propertiesファイル用に指定したディレクトリに移動します。次に、「サイレントモードでのソフトウェアLoggerのインストール」(41ページ)の手順を続けます。

   以下は、生成されたinstaller.propertiesファイルの例です。

```
# Wed Aug 14 18:27:49 PDT 2016
# Replay feature output
# ---------------------
# This file was built by the Replay feature of InstallAnywhere.
#It contains variables that were set by Panels, Consoles or Custom Code.

#Choose Install Folder
#---------------------
USER_INSTALL_DIR=/opt/Logger

#License Information
#-------------------
LICENSE_LOCATION=/home/user/arcsight.lic
```

サイレントモードでのソフトウェアLoggerのインストール

ソフトウェアLoggerをインストールするマシンが、インストールするバーのリリースノートに記載されたプラットフォーム要件を満たしていること、および「インストールの前提条件」(29ページ)に記載された前提条件を満たしていることを確認してください。

rootユーザーとしてインストールする場合、サイレントモードプロパティファイルを生成するときに使用したroot以外のユーザーのアカウントが、サイレントモードを使用してLoggerをインストールするマシン上に存在することを確認します。

サイレントモードを使用してソフトウェアLoggerをインストールするには

1. 以前に生成したサイレントモードプロパティファイルを、新しいシステム上のLoggerソフトウェアをコピーした同じ場所にコピーします。
2. サイレントモードプロパティファイルのLICENSE_LOCATIONプロパティを編集し、このインストールインスタンス用のライセンスファイルの場所を設定します。(インストールインスタンスごとに固有のライセンスファイルが必要です。)

   または

   LICENSE_LOCATIONプロパティが、たとえばlogger_license.zipを指し示すように設定します。次に、サイレントモードのインストールインスタンスごとに、関連するライセンスファイルを該当の箇所にコピーして、ファイル名をlogger_license.zipに変更します。これにより、結合したプロパティファイルをインストールごとに更新する必要がなくなります。
3. Loggerソフトウェアをコピーしたディレクトリから以下のコマンドを実行します。

   ```
   chmod u+x ArcSight-logger-6.4.0.XXXX.0.bin
   ./ArcSight-logger-6.4.0.XXXX.0.bin -i SILENT -f <path to
   installer.properties>
   ```

これ以降のインストールと設定は、ユーザーの入力を必要としないで進みます。

インストールと初期化が完了すると、インストール中に作成したURLを使用してLoggerに接続できます。この手順については、「ソフトウェアLoggerへの接続」(42ページ)を参照してください。

ソフトウェアLoggerへの接続

Loggerのユーザーインターフェイス(UI)は、暗号化されたHTTPS接続を使用し、パスワードで保護されたWebブラウザーアプリケーションです。Logger 6.4のブラウザーのサポートに関する詳細は、Protect 724サイトで提供されている『ADP Support Matrix』ドキュメントを参照してください。

パブリックにアクセス可能なLoggerのポートは、任意のファイアウォールルールで許可する必要があります。ソフトウェアLoggerの場合、ファイアウォールの設定はユーザーが行います。Loggerアプライアンスでは、ファイアウォールのルールはあらかじめ設定されています。詳細については、「ファイアウォールルール」(15ページ)を参照してください。

- rootユーザーによるインストールの場合は、UDPレシーバー用のポート`514/udp`やTCPレシーバー用のポート`515/tcp`などのLoggerレシーバーが必要とするすべてのプロトコル用のポートに加え、ポート`443/tcp`へのアクセスも許可します。
- root以外のユーザーによるインストールの場合は、UDPレシーバー用のポート`8514/udp`やTCPレシーバー用のポート`8515/tcp`などのLoggerレシーバーが必要とするすべてのプロトコル用のポートに加え、ポート`9000/tcp`へのアクセスも許可します。

  注: ここで挙げたポートはデフォルトポートです。ご使用のLoggerでは、異なるポートを使用する場合があります。

JavaScriptとCookieは有効にしておく必要があります。

Loggerに接続するには

Loggerのインストール時に設定したURLを使用し、サポートされているブラウザーからLoggerに接続します。

ソフトウェアLoggerの場合: `https://<hostname or IP address>:<configured_port>`

Loggerアプライアンスの場合: `https://<hostname or IP address>`

hostname or IP addressはLoggerソフトウェアがインストールされているシステムのホスト名またはIPアドレスであり、configured_portは、Loggerのインストール時に設定したポートです(該当する場合)。

注: IPv6アドレスは、ブラウザーが認識できるように、角カッコで囲む必要があります。

接続すると、[ログイン]画面が表示されます。

ログインするには

[ログイン] ダイアログが表示されたら、ユーザー名とパスワードを入力して [**ログイン**] をクリックします。

初めて接続する場合は、次のデフォルトの資格情報を使用します。

ユーザー名: admin
パスワード: password

> **注:** デフォルトのユーザー名とパスワードで初めてログインすると、パスワードの変更を求めるプロンプトが表示されます。プロンプトに従って、新しいパスワードを入力して確認します。

ログイン画面とLoggerへの接続方法の詳細については、『Logger管理者ガイド』の「ユーザーインターフェイスとダッシュボード」の章を参照してください。

正常にログインしたら、保有ポリシーの実装に必要な、設定済みレシーバーと設定デバイス、デバイスグループ、およびストレージグループを有効にできます。Loggerをセットアップしてイベントの受信を開始する方法については、「Loggerの設定」(60ページ) および『Logger管理者ガイド』の「設定」の章を参照してください。

ソフトウェアLoggerのコマンドラインオプションの使用

`loggerd`コマンドを使用すると、マシン上で動作しているLoggerソフトウェアを起動または停止できます。また、このコマンドにはいくつかのサブコマンドが含まれ、Loggerソフトウェアの一部として動作する他のプロセスを制御するために使用できます。

> **注:** Loggerが、システムサービスとして動作するようにインストールされている場合は、オペレーティングシステムの`service`コマンドを使用して、Logger上のプロセスの起動、停止、ステータス確認を行うことができます。

```
<install_dir>/current/arcsight/logger/bin/loggerd
{start|stop|restart|status|quit}<install_dir>
```

```
/current/arcsight/logger/bin/loggerd {start <process_name> | stop <process_
name> | restart <process_name>}
```

`loggerd`を使用して起動、停止、再起動できるプロセスを表示するには、最上位のメニューバーの [**システム管理**] をクリックします。次に、[**システム**] の中の [**プロセス ステータス**] をクリックします。プロセスは、右側の [**プロセス**] の下に表示されます。

次の表では、loggerdで使用できるサブコマンドとその用途について説明します。

コマンド	用途
loggerd start	[システム] セクションと[プロセス] セクションに表示されているすべてのプロセスを起動します。このコマンドは、Loggerを起動するために使用します。
loggerd stop	[プロセス] セクションに表示されているプロセスのみを停止します。このコマンドは、loggerdを実行したまま、他のすべてのプロセスを停止する場合に使用します。
loggerd restart	このコマンドは、[プロセス] セクションに表示されているプロセスのみを再起動します。 **注:** loggerd restartコマンドを使用してLoggerを再起動する場合、「aps」プロセスのステータスメッセージに次のメッセージが表示されます。 Process 'aps' Execution failed メッセージは数秒後に次のように変わります。 Process 'aps' running
loggerd status	すべてのプロセスのステータスを表示します。
loggerd quit	[システム] セクションと[プロセス] セクションに表示されているすべてのプロセスを停止します。このコマンドは、Loggerを停止するために使用します。
loggerd start <process_name>	指定したプロセスを起動します。例: loggerd start apache
loggerd stop <process_name>	指定したプロセスを停止します。例: loggerd stop apache
loggerd restart <process_name>	指定したプロセスを再起動します。例: loggerd restart apache

[システム管理] > [システム] > [プロセス ステータス] ページからLoggerプロセスの起動、停止、ステータス確認ができます。詳細については、『Logger管理者ガイド』またはオンラインヘルプを参照してください。

Loggerのアンインストール

ソフトウェアLoggerをSSH接続経由でGUIモードを使用してアンインストールしたい場合、アンインストールウィザード画面を見られるように、-xオプションを使用してX window転送機能を有効にしていることを確認してください。PuTTYを使用する場合は、Linuxマシンに接続するマシンにもXクライアントが必要です。

Loggerをアンインストールする前に、「ソフトウェアLoggerへの接続」(42ページ)の説明に従って、loggerd stopコマンドを使用してLoggerプロセスを停止します。

Loggerソフトウェアをアンインストールするには

1. インストールディレクトリで、次 のコマンドを入 力します。

   ```
   ./UninstallerData/Uninstall_ArcSight_Logger_6.4
   ```

   アンインストールウィザード が起 動 されます。
2. [**Uninstall**] をクリックするか、**Enter**キーを押して、Loggerのアンインストールを開 始します。

第4章: VMwareへのソフトウェアLoggerのインストール

ソフトウェアLoggerは、LinuxシステムまたはVMware VMにインストールできます。この章では、VMware VMにソフトウェアLoggerをインストールして起動するために必要な情報について説明します。この章には以下のトピックに関する情報が含まれます。

ソフトウェアLoggerをLinuxにインストールする方法の詳細は、「LinuxへのソフトウェアLoggerのインストール」(26ページ)を参照してください。Logger**アプライアンス**の初期化については、「Loggerアプライアンスのセットアップ」(16ページ)を参照してください。

開始する前に

VMware ESXiサーバーバージョン5.5に、Logger仮想マシン(VM)を展開できます。VMイメージには、12GB RAMと4つの物理(8つの論理)コアで構成された64ビットCentOS 7.3上のLogger 6.4インストーラーが含まれます。リリースの詳細については、リリースノートおよび『ArcSight Data Platform Support Matrix』を参照してください。これらのドキュメントは、Protect 724のArcSight製品ドキュメントコミュニティからダウンロードできます。

インストールパッケージのダウンロード

インストールパッケージLogger6.4_LXXXX_Q1001.ovaは、HPEソフトウェアデポ(https://h20392.www2.hpe.com/portal/swdepot/index.do)からダウンロードできます。

ダウンロードしたインストール用ソフトウェアの検証

HPEは、お客様が受け取った署名付きのソフトウェアが確実にHPEから提供され、第三者による改ざんが行われていないことを実証できるように、デジタル公開鍵を提供しています。

詳細な情報と手順については、次のサイトを参照してください。

https://h20392.www2.hpe.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning

ソフトウェアLoggerでのライセンスの仕組み

Loggerには、90日間有効な試用版ライセンスが付属しています。試用版ライセンスでは、機能が限定されています。すべての機能にアクセスするには、ArcSight Data Platform LoggerまたはスタンドアロンArcSight Loggerの完全なライセンスをアップロードする必要があります。詳細については、「試用版のライセンス」(11ページ)を参照してください。

ライセンスファイルがない場合は、「ソフトウェアLoggerのライセンスの取得」(28ページ)を参照してください。注文の内容によっては、ソフトウェアLoggerのインスタンスごとに、個別のライセンスが必要です。ライセンスファイルは、Loggerのダウンロードごとに一意に生成されます。

ライセンスの種類は、データボリューム制限機能の仕組みやデータボリュームページに表示される内容に影響します。

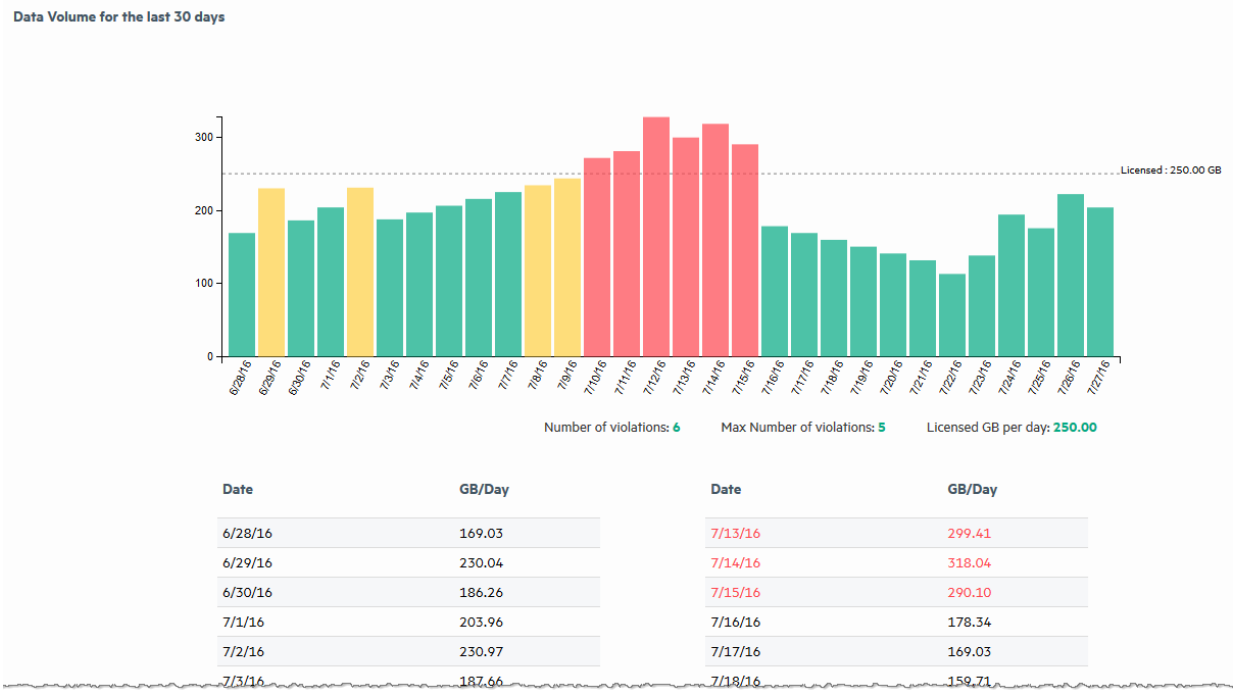
- ADP Loggerの場合、ArcMCがライセンス制限を管理します。詳細については、『ArcMC管理者ガイド』を参照してください。
- スタンドアロン型のArcSight Loggerの場合は、データボリューム制限機能によってライセンス制限が管理されます。

データボリューム制限機能は、ある1日に受信したイベントのサイズの合計を加算して、収集した1日のデータボリューム(1日あたりにLoggerが受信したデータの合計)を計算します。Loggerは、その値とライセンスの1日のデータ制限を比較します。この制限値を超えても、Loggerはイベントを収集して保存するので、イベントが紛失することはありません。ただし、過去30日間のウィンドウ内で制限値を超えた日が6日以上ある場合、検索関連のすべての機能が無効になります。データ制限違反が過去30日間のウィンドウ内で5回以下になるまで、収集したイベントのレポートを転送、検索、または実行することはできません。

たとえば、データの収集限度が20GBであるLoggerソフトウェアを1月1日にインストールし、イベントの収集を開始したとします。Loggerが、1月5日、13日、18日、19日、20日に、20GBを超えるイベントデータを受信します。ここまでで、制限値を超えたのは5回なので、1月21日は保存したイベントデータの転送、検索、レポート作成が可能です。しかし、1月30日に制限値を超えたとすると、許容最大回数を超えるので、1月31日には、転送、検索、レポート作成はできません。(1月31日に実行した検索は失敗し、ユーザーインターフェイスに警告が表示されます。)1月31日から2月4日までの間に、1日のデータ収集制限値を超えることがな

ければ、2月5日には、1月5日の制限値超過が30日間のウィンドウ外になるため、転送、検索、レポート作成の機能が回復します。

[データボリューム] ページ (**[設定] > [詳細] > [データボリューム]**) には、過去30日間にソフトウェアLogger上に保存されたデータが1日単位で表示されます。また、次の図に示すように、データ制限値を超えた日も表示されます。



Date	GB/Day	Date	GB/Day
6/28/16	169.03	7/13/16	299.41
6/29/16	230.04	7/14/16	318.04
6/30/16	186.26	7/15/16	290.10
7/1/16	203.96	7/16/16	178.34
7/2/16	230.97	7/17/16	169.03
7/3/16	187.66	7/18/16	159.71

データ制限値の超過が発生した場合、[検索] ユーザーインターフェイスに警告が表示されます。毎日のデータ制限値の超過が頻繁に発生するようであれば、要求に合ったライセンスの購入を検討してください。新しいライセンスの購入については、HPE ArcSightの営業担当者にお問い合わせください。新しいライセンスを入手したら、『ArcSight Logger管理者ガイド』の説明に従って、ご使用のLoggerに適用してください。

ライセンスの取得

ソフトウェアLoggerのインストールには、ライセンスファイルが必要です。ライセンスを取得するには、発注後にHPEから電子メールで受け取るElectronic Delivery Receiptに記載された説明に従ってください。このドキュメントがない場合は、https://softwaresupport.hpe.comのカスタマーサポートに連絡してください。

Loggerのインストール後、[ライセンス情報] および [ライセンスおよび更新] ページで現在のライセンスの詳細を表示できます (**[設定] > [詳細] > [ライセンス情報]**および**[システム管理] > [システム] > [ライセンスおよび更新]**)。詳細については、『Logger管理者ガイド』の「設定」および「システム管理」の各章を参照してください。

ソフトウェアLoggerのライセンスの取得

Loggerの一部の機能は、アクセスするために、有効なライセンスファイルをLoggerに適用する必要があります。詳細と手順については、「試用版のライセンス」(11ページ)を参照してください。ライセンスを取得するには、発注後にHPEから電子メールで受け取るElectronic Delivery Receiptに記載された説明に従ってください。

注: 複数のLoggerがある場合、注文の内容によっては、それぞれのLoggerについてライセンスファイルが必要です。

Loggerのインストール後、[ライセンス情報] および [ライセンスおよび更新] ページで現在のライセンスの詳細を表示できます (**[設定] > [詳細] > [ライセンス情報]** および **[システム管理] > [システム] > [ライセンスおよび更新]**)。詳細については、『Logger管理者ガイド』の「設定」および「システム管理」の各章を参照してください。

仮想マシンの準備

Loggerソフトウェアをインストールする前に、VMをインポートして設定する必要があります。この項では、VMのインポートと設定を手順を追って説明します。Loggerをインストールする前に、オペレーティングシステムの設定プロセスの一部として、2番目のハードディスクを作成する必要があります。2番目のハードディスクを追加し、システムの電源を投入した後、起動スクリプトが2番目のハードディスクを接続し、XFSパーティションの形式でフォーマットします。このパーティションは、Loggerデータの保存に使用されます。

注: 以下の手順は、OVAファイルをインポートし、展開するための参考となるものです。正確な手順は、ESXiの特定の環境と展開ツールによって異なる可能性があります。特定の環境およびOVAファイルの展開手順の詳細については、ESXiまたはシステムの管理者に相談してください。

仮想マシンをインポートするには

1. vSphereクライアントを開き、ESXiサーバーに接続します。
2. vSphereクライアント上で [File] メニューを開き、[**Deploy OVF Template…**] を選択し、[**Next**] をクリックします。
3. [Source] パネルで、ダウンロードしたLoggerインストールファイル (`Logger6.4_LXXXX_Q1001.ova`) を選択します。[**Open**] をクリックし、次に [**Next**] をクリックします。
4. [OVF Template Details] パネルに製品の詳細が表示されます。[**Next**] をクリックします。
5. [Name and Location] パネルで仮想マシンの名前を入力し、[**Next**] をクリックします。
6. 使用可能なストレージの場所が複数ある場合、仮想マシンを保存する場所を選択します。[**Next**] をクリックします。

7. [Disk Format] パネルで [**Thick Provision Lazy Zeroed**] を選択し、[**Next**] をクリックします。
8. [Ready to Complete] パネルに、選択したオプションが表示されます。オプションを確認後、[**Finish**] をクリックして、仮想マシンを展開します。

   進捗バーが進捗を表示します。展開が完了すると、ユーザーが作成したVMが、ESXiサーバーのリストに表示されます。

既存のハードディスクは、Loggerソフトウェア用です。Loggerデータを保存するために、別の仮想ハードディスクを作成する必要があります。

2番目のハードディスクを追加するには

1. ESXiサーバーのリストから新しいVMを選択し、電源がオフであることを確認します。
2. VMを右クリックし、ドロップダウンメニューを開き、[**Edit Settings**] を選択します。
3. [Virtual Machine Properties] ダイアログボックスが開きます。[**Add...**] をクリックします。

   [Device Type] パネルに、追加可能なデバイスのリストが表示されます。
4. [**Hard Disk**] を選択し、[**Next**] をクリックします。
5. [Select a Disk] パネルに、使用可能なディスクのタイプが表示されます。[**Create a new virtual disk**] を選択し、[**Next**] をクリックします。
6. [Create a Disk] パネルに、仮想ディスクサイズとプロビジョニングのオプションが表示されます。
   - [**Disk Size**] を設定します。

     注意: ディスクサイズは、可能な限り大きな値を設定します。一度作成したハードディスクは、拡張できません。最小サイズは40GBです。Logger 6.4は、最大12 TBをサポートします。
   - [**Thick Provision Lazy Zeroed**] を選択します。
   - [**Next**] をクリックします。
7. [Advanced Options] パネルに、その他のオプションが表示されます。デフォルトの仮想デバイスノードを受け入れ、[**Next**] をクリックします。
8. [Ready to complete] パネルに、選択したオプションが表示されます。オプションを確認後、[**Finish**] をクリックして、ハードディスクを追加します。

   新たに作成されたハードディスクは、ハードウェアリストに表示されます。
9. [**OK**] をクリックして、新しいVMの電源をオンにします。2番目のハードディスクが接続されます。

インストールの前提条件

VMにはデフォルトのrootパスワード「arcsight」が設定されています。パスワードを持たない、root以外のユーザー「arcsight」も含まれています。このユーザーはインストールに必要です。

注意：セキュリティ上の理由およびSCPまたはSSHを使用してファイルをマシンに転送できるようにするため、できるだけ早くrootパスワードを変更し、arcsightユーザーのパスワードを追加してください。

Loggerソフトウェアを VMにインストールする前に、以下の前提条件を満たしていることを確認してください。

- インストールを進める前に、VM上でオペレーティングシステムを起動してログインし、タイムゾーンおよびその他の必要な設定を行います。
- VM上のネットワークを、ご使用の環境に合わせて設定します。DNSサーバーまたは/etc/hostsの設定によりホスト名を解決できる必要があります。
- OS上でSELinuxおよびSSHは有効になっていますが、ファイアウォールは無効になっています。Loggerへの適切なアクセスを確実にするため、できるだけ早くファイアウォールを有効にし、デバイスを許可または拒否するファイアウォールポリシーを追加します。詳細については、「ファイアウォールルール」(15ページ)を参照してください。
- 実稼働環境に展開する前に有効なライセンスファイルを取得します。ライセンスファイルがない場合は、「ライセンスの取得」(48ページ)を参照してください。Loggerのインスタンスごとに、個別のライセンスが必要です。ライセンスファイルは、ダウンロードごとに一意に生成されます。
- ライセンスをSCPでVMに転送し、ファイル名と場所をメモしておいてください。インストールプロセス中にその情報が必要になります。
- rootユーザーまたはroot以外の設定済みユーザー(arcsight)のどちらでLoggerをインストールするかを決定します。どちらのユーザーを選ぶかにより、インストールオプションが異なります。
  a. rootユーザーとしてインストールする場合、Loggerをサービスとして起動する設定を選択し、Loggerが安全なWeb接続をリッスンするポートを選択することができます。
  b. 非rootユーザーとしてインストールする場合、Loggerはポート9000/tcp上の接続のみをリッスンできます。ポートに別の値を設定することはできません。

     注：ユーザーには、インストールディレクトリとそのサブディレクトリへの書き込み権限が必要です(例：chown –R arcsight /opt/arcsight)。

  c. アップグレードする場合、非rootユーザーによる以前のインストールをrootユーザーによるインストールに変更することはできません。ソフトウェアLoggerへのアクセスは、以前に設定したポート9000/tcpを使用する必要があります。
- 空のフォルダーにインストールします。以前にLoggerをアンインストールしたことがある場合

は、アンインストールで残ったファイルを確実に削除してください。

- Loggerをインストールするマシンのホスト名を「localhost」にすることはできません。ホスト名が「localhost」である場合は、インストールを続行する前に、ホスト名を変更してください。
- IPv6をサポートするには、Loggerをインストールする前に、Loggerをインストールするマシンを IPv6専用モードに設定する必要があります。
- LoggerをインストールするマシンにMySQLのインスタンスをインストールしないでください。マシンにMySQLのインスタンスが存在する場合は、Loggerをインストールする前にそのインスタンスをアンインストールしてください。

仮想マシンへのLoggerのインストール

ソフトウェアLoggerをインストールするマシンが、使用するバージョン用のリリースノートに記載された仕様を満たしていること、および、「インストールの前提条件」(51ページ)に記載された前提条件を満たしていることを確認してください。

インストール前：

「ダウンロードしたインストール用ソフトウェアの検証」(47ページ)の説明に従って、用意したインストールファイルが正しいことを確認できます。

Loggerは、rootユーザーとして、またはrootではないarcsightユーザーとしてインストールできます。詳細と制約については、「インストールの前提条件」(51ページ)を参照してください。

注： Loggerは、`/opt/arcsight/logger`ディレクトリにインストールする必要があります。

Loggerソフトウェアのインストール

1. 以下のコマンドをLoggerのインストール用ファイルをコピーしたディレクトリから実行します。

   ```
   chmod u+x ArcSight-logger-6.4.0.XXXX.0.bin
   ./ArcSight-logger-6.4.0.XXXX.0.bin -i console
   ```

2. インストールウィザードがコマンドラインモードで起動します。**Enter**キーを押して続行します。

   ```
   ===============================================================

   Introduction
   ------------

   InstallAnywhere will guide you through the installation of ArcSight Logger
   6.4.
   ```

```
It is strongly recommended that you quit all programs before continuing
with this installation.

Respond to each prompt to proceed to the next step in the installation.If
you want to change something on a previous step, type 'back'.

You may cancel this installation at any time by typing 'quit'.

PRESS <ENTER> TO CONTINUE:
```

3. 以降の数画面は、エンドユーザーライセンス契約を表示します。以下のプロンプトが表示されるまで、**Enter**キーを押して、ライセンス契約の各部分を表示します。

```
DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N):
```

4. Yと入力し、**Enter**キーを押してライセンス契約を承認します。
   インストール処理のどの時点でも、「quit」と入力し、**Enter**キーを押してインストール処理を中止できます。
5. インストールの前提条件が満たされているかどうかが、インストーラーによってチェックされます。
   - オペレーティングシステムのチェック - デバイスが実行しているオペレーティングシステムがサポート対象かどうかがチェックされます。サポートされていないオペレーティングシステムが実行されている場合、メッセージは表示されますが、Loggerソフトウェアのインストールが中止されるわけではありません。一部の更新シナリオでは、古いOSが使用されているため、このメッセージが発生します。

     注: HPE ArcSightでは、インストールの前にサポート対象のOSにアップグレードすることを強くお勧めします。サポートされているオペレーティングシステムプラットフォームのリストについては、『ArcSight Data Platform Support Matrix』を参照してください。

   - インストールの前提条件のチェック - 確認に失敗すると、Loggerにメッセージが表示されます。先に進む前に、問題点を解決する必要があります。

   例

   このマシン上でLoggerが実行されている場合は、ユーザーの操作を要求するメッセージが表示されます。

```
================================================================================

Intervention Required

---------------------

ArcSight Logger processes are active.

All ArcSight Logger processes must be stopped to allow installation to
proceed.
```

```
Type 'Quit' to exit this installer or 'Continue' to stop all ArcSight
Logger processes and continue with the installation.

->1- Continue

  2- Quit

ENTER THE NUMBER OF THE DESIRED CHOICE, OR PRESS <ENTER> TO ACCEPT THE
DEFAULT:
```

この場合、Loggerプロセスを停止するには「1」を入力します (または**Enter**キーを押します)。プロセスを実行するか、インストーラーを終了するには、「2」を入力します。

すべてのチェックが完了すると、インストールが続行し、[Choose Install Folder] 画面が表示されます。

6. [Choose Install Folder] 画面で、Loggerのインストールパスを入力し、**Enter**キーを押します。

   デフォルトのインストールパスは、/optです。VMイメージ上のインストールパスは、/opt/arcsight/loggerです。必ずこの場所を使用してください。別の場所を指定しないでください。

7. 「Y」と入力し、**Enter**キーを押してインストールの場所を確認します。
   - 指定された場所に、ソフトウェアをインストールする十分なスペースがない場合、メッセージが表示されます。インストールを続行するには、別の場所を指定するか、指定の場所に十分なスペースを確保します。インストールを中止するには、「quit」と入力し、**Enter**キーを押します。
   - Loggerが指定の場所にすでにインストールされている場合は、メッセージが表示されます。アップグレードを続行する場合は「2」を入力し、別の場所を指定する場合は「1」を入力します。アップグレードの説明については、使用するバージョンのリリースノートを参照してください。
8. インストール前の概要を確認し、**Enter**キーを押してLoggerをインストールします。

   インストールには数分かかることがあります。しばらくお待ちください。インストールが完了すると、次の画面が表示されます。

9. rootでログインしている場合、以下のフィールドの入力を要求されます。各フィールドに回答を入力し、**Enter**キーを押します。

フィールド	説明
User Name	このユーザーがまだシステムに存在しない場合は、ユーザー名の入力が求められます。 **ヒント:** VMWare VM上にLoggerをインストールする場合は、システムにあらかじめ構成されている非rootユーザー`arcsight`を使用します。
HTTPS Port	Logger UIにアクセスするときに使用するポート番号。 デフォルトのHTTPSポート (443) を使用することも、ご希望のポートを入力することもできます。443以外のポートを指定する場合、ユーザーはLogger UIへのアクセスに使用するURLにそのポート番号を入力する必要があります。
Choose if you want to run Logger as a system service.	「`1`」を入力してEnterキーを押し、Loggerをサービスとして設定するか、「`2`」を入力してEnterキーを押し、Loggerをスタンドアロン型に設定します。 このオプションを選択すると、`arcsight_logger`という名前のサービスが作成され、レベル2、3、4、5で実行可能になります。 インストール処理中にLoggerをサービスとして起動するように設定しなかった場合でも、後からそのように設定することができます。インストール後にLoggerをサービスとして起動する方法については、『Logger管理者ガイド』を参照してください。

10. 希望するロケールに対応する番号を入力して**Enter**キーを押します。
    - 英語の場合は1
    - 日本語の場合は2
    - 簡体字中国語の場合は3
    - 繁体字中国語の場合は4
11. ライセンスファイルへの絶対パスを入力し、**[Next]** をクリックします。

    注: ライセンスファイルを指定しない場合は、機能に大幅な制限のある90日間の試用版ライセンスがインストールされます。「Loggerアプライアンスのライセンスの取得」(20ページ) を参照してください。

    初期化画面が表示されます。
12. **Enter**キーをもう一度押して、Loggerコンポーネントを初期化します。

    初期化には数分かかることがあります。しばらくお待ちください。初期化が完了すると、設定画面が表示されます。
13. **[Next]** をクリックして、ストレージグループとストレージボリュームを設定し、Loggerを再起動します。

    設定には数分かかることがあります。しばらくお待ちください。

    設定が完了すると、Loggerが起動し、次の画面にLoggerへの接続に使用するURLが表示されます。
14. URLをメモし、**Enter**キーを押してインストーラーを終了します。

Loggerのインストールと初期化が完了したら、インストール中にメモしたURLを使用してLoggerに接続できます。この手順については、「ソフトウェアLoggerへの接続」(42ページ)を参照してください。

ソフトウェアLoggerへの接続

Loggerのユーザーインターフェイス(UI)は、暗号化されたHTTPS接続を使用し、パスワードで保護されたWebブラウザーアプリケーションです。Logger 6.4のブラウザーのサポートに関する詳細は、Protect 724サイトで提供されている『ADP Support Matrix』ドキュメントを参照してください。

パブリックにアクセス可能なLoggerのポートは、任意のファイアウォールルールで許可する必要があります。ソフトウェアLoggerの場合、ファイアウォールの設定はユーザーが行います。Loggerアプライアンスでは、ファイアウォールのルールはあらかじめ設定されています。詳細については、「ファイアウォールルール」(15ページ)を参照してください。

- rootユーザーによるインストールの場合は、UDPレシーバー用のポート`514/udp`やTCPレシーバー用のポート`515/tcp`などのLoggerレシーバーが必要とするすべてのプロトコル用のポートに加え、ポート`443/tcp`へのアクセスも許可します。
- root以外のユーザーによるインストールの場合は、UDPレシーバー用のポート`8514/udp`やTCPレシーバー用のポート`8515/tcp`などのLoggerレシーバーが必要とするすべてのプロトコル用のポートに加え、ポート`9000/tcp`へのアクセスも許可します。

  注: ここで挙げたポートはデフォルトポートです。ご使用のLoggerでは、異なるポートを使用する場合があります。

JavaScriptとCookieは有効にしておく必要があります。

Loggerへの接続:

Loggerのインストール時に設定したURLを使用し、サポートされているブラウザーからLoggerに接続します。

ソフトウェアLoggerの場合: `https://<hostname or IP address>:<configured_port>`

Loggerアプライアンスの場合: `https://<hostname or IP address>`

hostname or IP addressはLoggerソフトウェアがインストールされているシステムのホスト名またはIPアドレスであり、configured_portは、Loggerのインストール時に設定したポートです(該当する場合)。

注: IPv6アドレスは、ブラウザーが認識できるように、角カッコで囲む必要があります。

Loggerへのログイン

[ログイン] ダイアログが表示されたら、ユーザー名とパスワードを入力して [**ログイン**] をクリックします。

初めて接続する場合は、次のデフォルトの資格情報を使用します。

ユーザー名: admin
パスワード: password

> **注:** デフォルトのユーザー名とパスワードで初めてログインすると、パスワードの変更を求めるプロンプトが表示されます。プロンプトに従って、新しいパスワードを入力して確認します。

ログイン画面とLoggerへの接続方法の詳細については、『Logger管理者ガイド』の「ユーザーインターフェイスとダッシュボード」の章を参照してください。

正常にログインしたら、保有ポリシーの実装に必要な、設定済みレシーバーと設定デバイス、デバイスグループ、およびストレージグループを有効にできます。Loggerをセットアップしてイベントの受信を開始する方法については、「Loggerの設定」(60ページ) および『Logger管理者ガイド』の「設定」の章を参照してください。

ソフトウェアLoggerのコマンドラインオプションの使用

loggerdコマンドを使用すると、マシン上で動作しているLoggerソフトウェアを起動または停止できます。また、このコマンドにはいくつかのサブコマンドが含まれ、Loggerソフトウェアの一部として動作する他のプロセスを制御するために使用できます。

> **注:** Loggerが、システムサービスとして動作するようにインストールされている場合は、オペレーティングシステムのserviceコマンドを使用して、Logger上のプロセスの起動、停止、ステータス確認を行うことができます。

```
<install_dir>/current/arcsight/logger/bin/loggerd
{start|stop|restart|status|quit}<install_dir>
```

```
/current/arcsight/logger/bin/loggerd {start <process_name> | stop <process_
name> | restart <process_name>}
```

loggerdを使用して起動、停止、再起動できるプロセスを表示するには、最上位のメニューバーの [**システム管理**] をクリックします。次に、[**システム**] の中の [**プロセス ステータス**] をクリックします。プロセスは、右側の [**プロセス**] の下に表示されます。

次の表では、loggerdで使用できるサブコマンドとその用途について説明します。

コマンド	用途
loggerd start	[システム] セクションと[プロセス] セクションに表示されているすべてのプロセスを起動します。このコマンドは、Loggerを起動するために使用します。
loggerd stop	[プロセス] セクションに表示されているプロセスのみを停止します。このコマンドは、loggerdを実行したまま、他のすべてのプロセスを停止する場合に使用します。
loggerd restart	このコマンドは、[プロセス] セクションに表示されているプロセスのみを再起動します。 **注:** loggerd restartコマンドを使用してLoggerを再起動する場合、「aps」プロセスのステータスメッセージに次のメッセージが表示されます。 Process 'aps' Execution failed メッセージは数秒後に次のように変わります。 Process 'aps' running
loggerd status	すべてのプロセスのステータスを表示します。
loggerd quit	[システム] セクションと[プロセス] セクションに表示されているすべてのプロセスを停止します。このコマンドは、Loggerを停止するために使用します。
loggerd start <process_name>	指定したプロセスを起動します。例: loggerd start apache
loggerd stop <process_name>	指定したプロセスを停止します。例: loggerd stop apache
loggerd restart <process_name>	指定したプロセスを再起動します。例: loggerd restart apache

[システム管理] > [システム] > [プロセス ステータス] ページからLoggerプロセスの起動、停止、ステータス確認ができます。詳細については、『Logger管理者ガイド』またはオンラインヘルプを参照してください。

Loggerのアンインストール

Loggerソフトウェアをアンインストールするには、単純にVMを削除します。また、VMからソフトウェアLoggerをアンインストールすることもできます。

ソフトウェアLoggerをSSH接続経由でGUIモードを使用してアンインストールしたい場合、アンインストールウィザード画面を見られるように、-xオプションを使用してX window転送機能を有効にしていることを確認してください。PuTTYを使用する場合は、Linuxマシンに接続するマシンにもXクライアントが必要です。

Loggerをアンインストールする前に、「ソフトウェアLoggerへの接続」(42ページ)の説明に従って、`loggerd stop`コマンドを使用してLoggerプロセスを停止します。

Loggerソフトウェアをアンインストールするには

1. インストールディレクトリで、次のコマンドを入力します。

   ```
   ./UninstallerData/Uninstall_ArcSight_Logger_6.4
   ```

   アンインストールウィザードが起動されます。
2. [**Uninstall**] をクリックするか、**Enter**キーを押して、Loggerのアンインストールを開始します。

第5章: Loggerの設定

この章では、以下のトピックに関する基本的な展開と設定の情報を説明します。この章の内容は、Loggerのすべてのタイプに適用されます。複数のLoggerをインストールしている場合は、各Loggerに接続して個別に設定するか、ArcSight Management Centerを使用して一括で設定を変更する必要があります。

Loggerを直接設定し、管理する方法の詳細については、『Logger管理者ガイド』を参照してください。ArcMCを使用したLoggerの設定と管理に関する詳細については、『ArcSight Management Center管理者ガイド』を参照してください。コネクターの設定についての詳細は、各コネクターのドキュメントを参照してください。

イベントとログの受信

Loggerには、あらかじめいくつかのレシーバーが設定されています。これらのレシーバーは、ご使用のネットワーク上のデバイスやシステム (たとえば、syslogサーバー、NFS、CIFS、SANシステム) から直接イベントやログファイルを受信できます。

Loggerは、さらに、ネットワーク上のソースからイベントデータを収集するArcSight SmartConnectorからイベントを受信することができます。ArcSightSmartConnectorの一部は試用版のLoggerでサポートされ、Loggerをダウンロードした場所と同じ場所からダウンロードできます。サポートされているSmartConnectorの設定ガイドは、同じWebサイトに掲載され、そこから入手できます。ArcSightSmartConnectorについての詳細は、http://www8.hp.com/us/en/software-solutions/enterprise-security.htmlにアクセスしてください。

レシーバー

Loggerのインストールを完了したら、イベントを受信するためのレシーバーを設定できます。Loggerには、あらかじめいくつかのレシーバーが設定されています。これらのレシーバーは、ご使用のネットワーク上のデバイスやシステム (たとえば、syslogサーバー、NFS、CIFS、SANシステム) から直接イベントやログファイルを受信できます。設定済みのレシーバーを使用することも、ユーザー自身のレシーバーを追加することも可能です。レシーバーを無効にし、後で再度有効にすることができます。必要に応じて、レシーバーの追加、変更、削除ができます。

設定済みのレシーバーには、TCPレシーバー、UDPレシーバー、および、SmartMessageレシーバーがあり、すでに有効化され、イベントの受信が可能になっています。また、LoggerにはLoggerのApacheアクセスエラーログ、システムメッセージログ、およびシステム監査ログ (ご使用のLinux OSで監査が有効になっている場合) 用のフォルダーフォロワーレシーバーが設定されています。

データを受信するには、任意のファイアウォールルールでレシーバーのポートを許可する必要があります。詳細については、「ファイアウォールルール」(15ページ)を参照してください。これらのレシーバーを使用するには、有効化する必要があります。手順については、「設定済みフォルダーフォロワーレシーバーの有効化」(62ページ)を参照してください。

設定済みのレシーバーについては、「レシーバー」(13ページ)で詳細に説明しています。レシーバーの詳細については、『Logger管理者ガイド』の「設定」の章を参照してください。

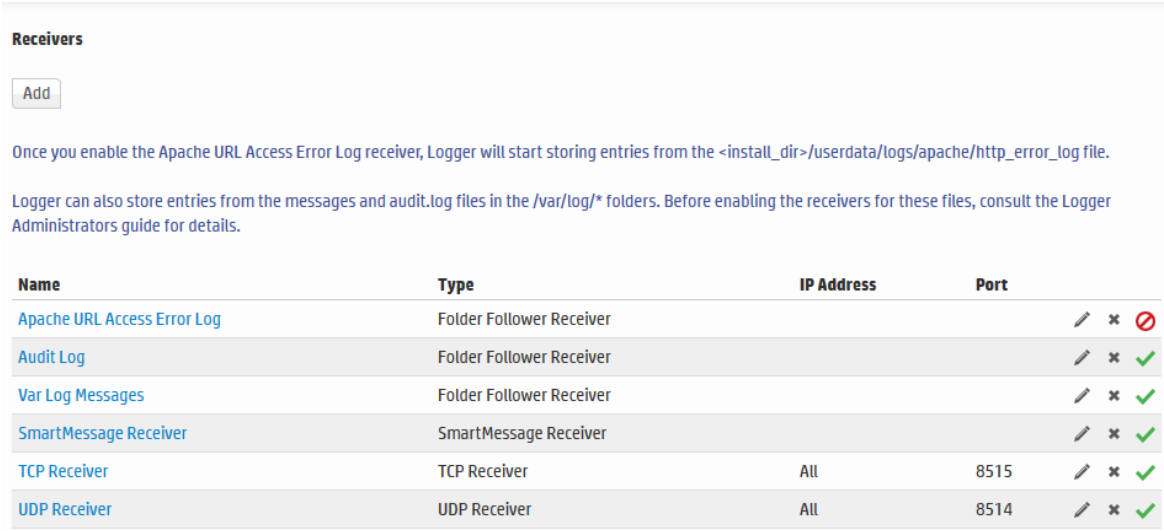
Loggerは、さらに、ネットワーク上のソースからイベントデータを収集するArcSight SmartConnectorからイベントを受信することができます。ArcSight SmartConnectorについてのSmartConnectorの詳細は、https://www.hpe.com/us/en/solutions/security.htmlにアクセスしてください。

設定済みフォルダーフォロワーレシーバーの有効化

設定済みのレシーバーについては、「レシーバー」(13ページ) で詳細に説明しています。レシーバーの詳細については、『Logger管理者ガイド』の「設定」の章を参照してください。

設定したURLを使用して最初にLoggerにログインしたとき、設定済みのフォルダーフォロワーレシーバーは無効になっています。ホームページに [データの追加] ボタンが表示されます。**[データの追加]** (Add Data) をクリックしてレシーバーのページを開き、レシーバーを有効化します。

ヒント: これらのレシーバーを有効にする前に、Loggerのインストール中に指定した、またはインストールに使用したrootでないユーザーが`/var/log/audit/audit.log`および`/var/log/`のメッセージを読み取れるようにします。



レシーバーを有効にするには、行末にある無効アイコン (⊘) をクリックします。

また、メニューからレシーバーのページに移動してレシーバーを有効にすることもできます。

メニューからレシーバーのページを開き、レシーバーを有効にするには

1. **[設定] > [データ]** メニューを開き、**[レシーバー]** をクリックします。
2. 有効にするレシーバーを特定し、行末にある無効アイコン (⊘) をクリックします。

設定済みのSmartMessageレシーバーの使用方法については、「SmartConnectorを使用したイベント収集」(64ページ) を参照してください。

新しいレシーバーの設定

あらかじめ設定されたレシーバーに加えて、ニーズに合わせて他のレシーバーを設定することもできます。レシーバータイプには、UDP、TCP、SmartMessageと、ファイル転送、ファイルレシーバー、フォルダーフォロワーレシーバーの3種類のファイルフォロワーがあります。

Loggerでは、以下のタイプのレシーバーを設定できます。

- **UDPレシーバー**: UDPレシーバーは、指定したポート上でUDPメッセージをリッスンします。プリインストールされているUDPレシーバーは、デフォルトで有効になっています。
- **CEF UDPレシーバー**: 共通イベントフォーマットのイベントを受信するUDPレシーバーです。
- **TCPレシーバー**: TCPレシーバーは、指定したポート上でTCPメッセージをリッスンします。プリインストールされているTCPレシーバーは、デフォルトで有効になっています。
- **CEF TCPレシーバー**: 共通イベントフォーマットのイベントを受信するTCPレシーバーです。
- **ファイルレシーバー**: ファイルレシーバーは、Loggerのタイプに応じて、ローカルファイルシステム、NFS (Network File System)、CIFS (Common Internet File System)、SAN (Storage Area Network) からログファイルを読み込みます。ファイルレシーバーは、単一行または複数行のログファイルを読み込みます。ファイルレシーバーは、ある時点のログファイルのスナップショットを提供します。
- **フォルダーフォロワーレシーバー:** フォルダーフォロワーレシーバーは、指定したディレクトリ内のログファイルが更新されると、継続的にそれを読み込みます。ソースディレクトリに異なる種類のログファイルが格納されている場合、監視するファイルの種類ごとにレシーバーを作成できます。プリインストールされたフォルダーフォロワーレシーバーを使用するには、レシーバーを有効にする必要があります。
- **ファイル転送**: ファイル転送レシーバーは、セキュアコピープロトコル (SCP)、セキュアファイル転送プロトコル (SFTP) またはファイル転送プロトコル (FTP) を使用して、リモートログファイルを読み取ります。これらのレシーバーは、単一行または複数行のログファイルを読み込みます。1つまたは複数のファイルを定期的に読み込むようにレシーバーをスケジュールできます。

  注意: Loggerアプライアンス上のSCPおよびSFTPプロトコルは、FIPSに準拠していません。

  注: SCP、SFTP、およびFTPファイル転送レシーバーは、システムにインストールされているFTP、SCP、およびSFTPクライアントを利用します。

- **SmartMessageレシーバー**: SmartMessageレシーバーは、ArcSight SmartConnectorからの暗号化メッセージをリッスンします。プリインストールされたレシーバーの使用を開始するには、レシーバーにイベントを送信するように、SmartConnectorを設定する必要があります。手順については、「LoggerにイベントをSmartConnectorの設定」(65ページ)を参照してください。

Loggerへの構造化データの送信

Loggerはメッセージの形式に依存しませんが、イベントやログを生成するデバイスを相互運用するための業界標準である、共通イベントフォーマット (CEF) に準拠したメッセージであれば、高度な処理を実行できます。共通イベントフォーマット (CEF) のイベントには、より多くの列が定義されており、データがより利用しやすくなっています。

Loggerは、「Loggerの仕組み」(8ページ) の図のように、ArcSight SmartConnector から正規化されたCEFイベントの形式で構造化データを受け取ることができます。

共通イベントフォーマット (CEF) の詳細については、『Implementing ArcSight CEF』を参照してください。このガイドのダウンロード可能なコピーについては、Protect 724のArcSight製品ドキュメントコミュニティで「ArcSight Common Event Format (CEF) Guide」を検索してください。

SmartConnectorを使用したイベント収集

ArcSightマネージャーと同様に、LoggerもArcSight SmartConnectorを利用してイベントを収集します。SmartConnectorは、ネットワーク上の異種のデバイス (たとえば、ファイアウォールとサーバー) からセキュリティ上のイベントを読み取り、関心のあるイベントに絞り込み (必要に応じて集約し)、Loggerレシーバーに送信します。Loggerは、SmartConnectorから正規化された共通イベントフォーマット (CEF) の形式で構造化データを受信します。

この項では、以下のトピックに対する基本的な情報を説明します。詳細については、該当するコネクターのドキュメントおよび『SmartConnectorユーザーガイド』(Protect 724のArcSight製品ドキュメントコミュニティからダウンロード可能) を参照してください。

SmartMessage

SmartMessageは、ArcSight SmartConnectorとLoggerとの間で共通イベントフォーマット (CEF) 形式のイベントを送受信するためのセキュアなチャネルを提供するHPE ArcSight のテクノロジーです。

SmartMessageは、TLS (Transport Layer Security) を使用し、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。一方の端は、ArcSight SmartConnectorで、ArcSight

SmartConnectorがサポートする多数のデバイスからイベントを受信します。もう一方の端は、Logger上のSmartMessageレシーバーです。

注: SmartMessageのセキュアチャネルは、TLS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、SmartConnectorとArcSightマネージャーの間で使用されている暗号化バイナリプロトコルに似ていますが、異なるものです。

LoggerにイベントをSmartConnectorの設定

Loggerは、SmartMessageレシーバーがあらかじめ設定された状態で出荷されています。これを使用してSmartConnectorからイベントを受信するには、以下の説明に従ってSmartConnectorを設定する必要があります。また、新しいSmartMessageレシーバーを作成し、この新たに作成したレシーバーを使用してSmartConnectorを設定することもできます。SmartConnectorを設定する際には、必ず正しいレシーバー名を指定してください。

LoggerにイベントをSmartConnectorを設定するには

1. 『SmartConnectorユーザーガイド』を参考にしながら、SmartConnectorコンポーネントをインストールします。通知先として、ArcSight ESMやCEFファイルではなく、Loggerを指定します。

   注: 手順については、SmartConnectorに付属しているドキュメントを参照してください。

2. 必要なパラメーターを指定します。Loggerのホスト名またはIPアドレスと、SmartMessageレシーバーの名前を入力します。これらの設定は、このコネクターからのイベントをリッスンするLogger内のレシーバーに一致している必要があります。
   - 設定済みのレシーバーを使用するには、[**Receiver Name**] に「SmartMessage Receiver」を指定します。
   - SmartMessageを使用して、ArcSight SmartConnectorとLoggerアプライアンスとの間の通信を行うには、ポート443/tcpを使用するようにSmartConnectorを設定します。
   - ArcSight SmartConnectorとソフトウェアLoggerの間で通信するには、ソフトウェアLoggerで設定されているポートを使用するようにSmartConnectorを設定します。
   - 暗号化されていないCEF syslogの場合は、Loggerのホスト名またはIPアドレスと目的のポートを入力し、UDPまたはTCP出力を選択します。

LoggerとArcSightマネージャーにイベントを送信するためのSmartConnectorの設定

SmartConnectorを設定して、LoggerにCEF syslog出力を、ArcSightマネージャーにイベントを同時に送信できます。

共通イベントフォーマット (CEF) の詳細については、『Implementing ArcSight CEF』を参照してください。このガイドのダウンロード可能なコピーについては、Protect 724のArcSight製品ドキュメントコミュニティで「ArcSight Common Event Format (CEF) Guide」を検索してください。

1. SmartConnectorを通常どおりにインストールします。SmartConnectorを、実行中のArcSightマネージャーに登録し、SmartConnectorが正常に動作しているかテストします。
2. `$ARCSIGHT_HOME/current/bin/runagentsetup`スクリプト (または`arcsight agentsetup -w`) を使用してSmartConnectorの設定プログラムを再起動します。
3. [**I want to add/remove/modify ArcSight Manager destinations**] を選択し、次に [**Add new destination**] を選択します。
4. Loggerを選択し、要求されたパラメーターを指定します。SmartConnectorを再起動し、変更を有効にします。

SmartConnectorのフェイルオーバー先の設定

プライマリ接続が使用できなくなったときにセカンダリ (フェイルオーバー先) にイベントを送信するようにSmartConnectorを設定できます。

フェイルオーバー先を設定するには以下の手順を実行します。

1. 前述のように、プライマリLogger用にSmartConnectorを設定します。トランスポートは、フェイルオーバーの原因となる転送エラーを検出できるよう、raw TCPである必要があります。
2. `$ARCSIGHT_HOME/current/user/agent`ディレクトリの`agent.properties`ファイルを編集します。`$ARCSIGHT_HOME`は、SmartConnectorコンポーネントをインストールしたルートディレクトリです。
   a. 次のプロパティを追加します。`transport.types=http,file,cefsyslog`
   b. 次のプロパティを削除します。`transport.default.type`
3. `$ARCSIGHT_HOME/current/bin/runagentsetup`スクリプト (または`arcsight agentsetup -w`) を使用してSmartConnectorの設定プログラムを再起動します。
4. **[I want to add/remove/modify]** を選択し、プライマリLoggerを選択した状態で **[Modify]** を選択します。次に **[Add failover destination]** を選択します。
5. セカンダリLogger用の情報を入力します。

6. SmartConnectorを再起動し、変更を有効にします。
7. ArcSight SmartConnectorのインストールと設定についての詳細は、Protect 724のArcSight製品ドキュメントコミュニティから入手できる『ArcSight SmartConnectorユーザーガイド』、または特定の『SmartConnector Configuration Guide』を参照してください。

SmartConnectorのダウンロード

サポートされるSmartConnectorをダウンロードする場所については、HPE ArcSightの営業担当者またはカスタマーサポートにお問い合わせください。ArcSight SmartConnectorの詳細については、https://www.hpe.com/us/en/solutions/security.htmlにアクセスしてください。

デバイス

有効化されたレシーバーがデータを受信するか、ファイルレシーバーの場合にファイルが使用可能になると、Loggerはイベントの保存を開始します。自動検出と呼ばれるプロセスを使用してLoggerはデバイスと呼ばれるリソースを自動作成し、ソースIPアドレスを追跡し、DNSを使用してホスト名にマッピングします。最終的には、Loggerがイベントを受信したデバイスすべてについて、デバイスが作成されます。

Loggerにイベントを送信すると想定されるデータソースのIPアドレスまたはホスト名を入力することで、先行してデバイスを作成することもできます。自動検出を待ちたくない場合や、各デバイスの最初のデバイス名を管理したい場合に、この方法を使用できます。検出されたデバイスは、そのホスト (またはDNSルックアップに失敗した場合は、そのIPアドレス) とレシーバーに由来した名前が付けられます。デバイスの作成の詳細については、『Logger管理者ガイド』の「設定」の章を参照してください。

デバイスグループ

デバイスグループは、フォルダー (またはディレクトリ) にファイルが格納されるのと同じように、デバイスを格納したり、論理的なグループに分けたりします。デバイスグループとは、グループ化されたデバイスの名前です。1つのデバイスが複数のグループのメンバーになることが可能です。各デバイスグループは、保有ポリシーを割り当てる特定のストレージグループと関連付けることができます。

デバイスグループは、必要に応じて、自由に変更したり、削除したりできます。デバイスグループの設定を必ず最初に実行する必要はありません。デバイスグループに割り当てられていないイベントは、デフォルトのデバイスグループに送られます。デバイスグループの設定の詳細については、『Logger管理者ガイド』の「設定」の章を参照してください。

ストレージルール

特に指定がない限り、イベントはデフォルトストレージグループに格納されます。ストレージルールは、あるデバイスグループからあるストレージグループへイベントを送るための方法です。ストレージルールは、追加の保有ポリシーを実装するために使用できます。

追加のストレージグループを作成し、イベントをそこに送信する場合は、ストレージルールを使用して実現できます。ストレージルールを作成しない場合、すべてのデバイスからのイベントはデフォルトストレージグループに送信され、デフォルトストレージグループで指定されている保有ポリシーが使用されます。

複数の保有ポリシーを実装する場合は、ストレージルールを作成して、特定のデバイスグループと、目的の保有ポリシーを実装しているストレージグループを関連付けます。

たとえば、1つの保有ポリシーに対して1つのデバイスグループを作成するという方法もありますが、管理しやすくするために、デバイスグループをストレージグループとストレージルールに関連付け、ストレージルールを使用してイベントを分類するという方法もあります。たとえば、特定のデバイスグループの中で特定のパターンに合致するイベントを検索し、そのイベントを特定のストレージグループに送り、イベントカテゴリに基づいて保有します。

ストレージルールは、重要度順に評価されます。最初に合致したルールにより、イベントを送るストレージグループが決定されます。この方法だと、1つのデバイスを複数のデバイスグループに所属させることができ、最終的にイベントを送信するストレージグループの決定が曖昧になることがありません。

ストレージルールの詳細については、『Logger管理者ガイド』の「設定」の章を参照してください。

ArcSight ESMからLoggerへのイベントの送信

ArcSight Forwarding SmartConnectorは、ArcSightマネージャーからイベントを読み取り、これをCEF形式のsyslogメッセージとしてLoggerに転送します。

注: Forwarding SmartConnectorは個別にインストール可能なファイルで、以下のような名前が付けられています。

```
ArcSight-x.x.x.<build>.x-SuperConnector-<platform>.exe
ArcSight-x.x.x.<build>.x-SuperConnector-<platform>.bin
```

Loggerとの互換性のために、ビルド4810以降を使用してください。

ArcSight Forwarding SmartConnectorを設定してLoggerにイベントを送信するには

1. SmartConnectorコンポーネントを通常どおりにインストールします。ただし、ターゲットマネージャーがデモ用証明書を使用しているかどうかを尋ねる質問がSmartConnectorウィザードに表示されたらインストールをキャンセルします。

   SmartConnector設定ウィザードの最初の画面で、デモ証明書に関する質問が表示されたら、[**Cancel**] をクリックします。
2. ウィザードの終了を確定し、[**Done**] をクリックしてインストールウィザードを終了します。これにより、設定は行われずに、SmartConnectorがインストールされます。
3. `$ARCSIGHT_HOME/current/user/agent`ディレクトリに**agent.properties**という名前のファイルを作成します。`$ARCSIGHT_HOME`は、SmartConnectorコンポーネントをインストールしたルートディレクトリです。このファイルは、以下の行のみを含むようにします。

   ```
   transport.default.type=cefsyslog
   ```
4. `$ARCSIGHT_HOME/current/bin/runagentsetup`スクリプト (または`arcsight agentsetup -w`) を使用してSmartConnectorの設定プログラムを再起動します。
5. CEF出力に必要なパラメーターを指定します。UDPまたはTCP出力のための希望のポートを入力します。これらの設定は、ArcSight ESMからのイベントを受信するためにLoggerで作成したレシーバーと合致する必要があります。

パラメーター	説明
IP/Host	LoggerのIPアドレスまたはホスト名
Port	514またはレシーバーに合致する他のポート
Protocol	UDPまたはRaw TCP
ArcSight Source Manager Host Name	ソースArcSightマネージャーのIPアドレスまたはホスト名
ArcSight Source Manager Port	8443 (デフォルト)
ArcSight Source Manager User Name	ソースマネージャー上でイベントを読み取るための十分な権限を持つユーザーアカウント
ArcSight Source Manager Password	指定されたマネージャーのユーザーアカウントのパスワード
SmartConnector Name	ESMからLoggerへのコネクター (マネージャーで認識可能) の名前
SmartConnector Location	コネクターがインストールされた場所の通知
Device Location	ソースマネージャーがインストールされた場所の通知
Comment	コメント (オプション)

Forwarding SmartConnectorを設 定してLoggerにCEF出 力を送 信し、同 時 に別 の ArcSightマネージャーにイベントを送 信 する方 法 については、「LoggerとArcSightマネージャーにイベントを送 信 するためのSmartConnectorの設 定 」(66ページ) を参 照してください。

共 通 イベントフォーマット (CEF) の詳 細 については、『Implementing ArcSight CEF』を参 照してください。このガイドのダウンロード可 能 なコピーについては、Protect 724のArcSight製 品 ドキュメントコミュニティで「ArcSight Common Event Format (CEF) Guide」を検 索してください。

第7章: アラート

Loggerを設定して、特定のクエリに一致する新しいイベントを受信した場合、または所定の時間内に指定された回数の一致が発生した場合に、電子メール、SNMPトラップ、またはSyslogメッセージを使用してアラートを出すことができます。

また、[分析] タブの下で [アラート] プルダウンサブメニューから、アラートを表示することもできます。アラートが起動されると、Loggerはアラートイベントを作成し、設定した通知先に通知を送信します。

アラートの種類

Loggerには、以下の2種類のアラートがあります。

- リアルタイムアラート
- 保存された検索アラート

次の表では、2種類のアラートについて比較します。

リアルタイムアラート	保存された検索アラート
定義できるアラートの数に制限はありません。 同時に有効にできるアラートは25個までです。	アラートはいくつでも定義できます。定義されたすべてのアラートを有効にできますが、同時に実行できるアラートは最大50個です。
設定される電子メールの通知先の数に制限はありませんが、セットアップできるのは、1つのSNMP、1つのSyslog、および1つのESM通知先だけです。	設定される電子メールの通知先の数に制限はありませんが、セットアップできるのは、1つのSNMP、1つのSyslog、および1つのESM通知先だけです。
アラートはリアルタイムで起動されます。つまり、指定されたしきい値内に、クエリとの一致が指定した回数に達すると、**すぐに**アラートが起動されます。	これらのアラートは、スケジュールされた間隔で起動されます。つまり、指定されたしきい値内に、クエリとの一致が指定した回数に達すると、**スケジュールされた次の間隔で**アラートが起動されます。
これらのアラートには、正規表現クエリのみを指定できます。	これらのアラートのクエリは、フローベースの検索言語を使用して定義されます。この言語では、正規表現を含む複数の検索コマンドをパイプライン形式で指定できます。chartやtopなどの集約演算子を検索クエリに含めることはできません。
リアルタイムアラートを定義するには、クエリ、一致数、しきい値、1つ以上の通知先を指定します。 リアルタイムアラートのために定義されたクエリには、時間範囲は関係しません。そのため、指定されたしきい値内に、クエリとの一致が指定した回数に達すると、アラートが起動されます。	保存された検索アラートを定義するには、保存された検索 (時間範囲を含むクエリ)、一致数、しきい値、1つ以上の通知先を指定します。 保存された検索アラートに関連するクエリには、時間範囲 (イベントを検索する時間範囲) が指定されます。そのため、指定された時間範囲内で、指定され

リアルタイムアラート	保存された検索アラート
	たしきい値内に、クエリとの一致が指定した回数に達する必要があります。また、動的な時間範囲を使用することもできます (たとえば、$Now-1d、$Nowなど)。 たとえば、保存された検索クエリの開始および終了時刻が次のようになっているとします。 開始時刻: 5/11/2016 10:38:04 終了時刻: 5/12/2016 10:38:04 そして、一致数としきい値が以下のようになっているとします。 マッチ数 5 しきい値: 3600 2016年5月11日 10:38:04から2016年5月12日 10:38:04までの間で、1時間以内に5つ以上のイベントが発生すると、アラートが起動します。

アラートの設定

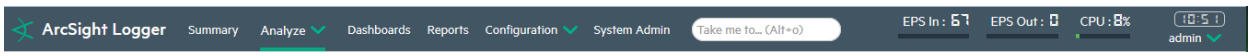
2種類のアラートの作成方法の詳細については、『ArcSight Logger管理者ガイド』を参照してください。

第8章: Loggerのユーザーインターフェイスの概要

この項では、検索インターフェイスを中心に、Loggerのユーザーインターフェイスの概要を説明します。詳細情報およびこの項で説明していないユーザーインターフェイスについては、『ArcSight Logger管理者ガイド』を参照してください。

ユーザーインターフェイスの操作

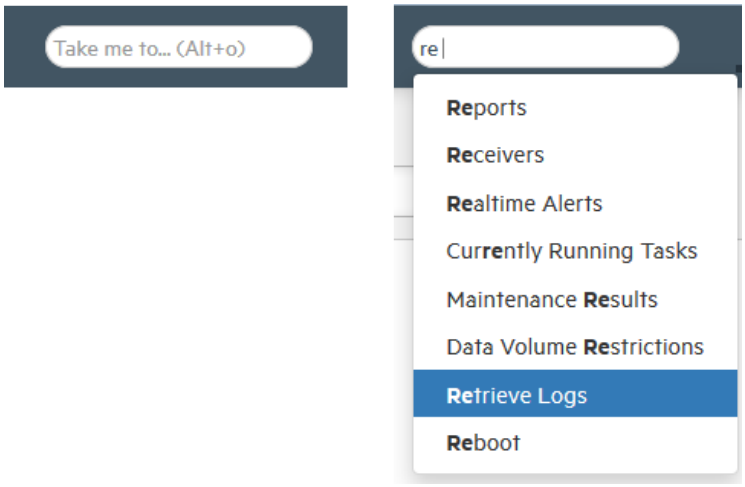
ユーザーインターフェイスのすべてのページの上部には、操作と情報のための帯状の領域があります。ここには、メニュータブ、クイックナビゲーションフィールド、イベントゲージ、時計のほかに、オプション、ヘルプ、バージョン情報、ログアウトを含むメニューがあります。



画面の上部にあるゲージには、スループットとCPU使用率の情報が表示されます。詳細は[モニター] ダッシュボード (「ダッシュボード」(76ページ)) に表示されます。[オプション] ページでゲージの範囲を変更することができます。ログインしているユーザーの名前は、時計の下、ゲージの右側に表示されます。

移動

メニュータブの右にある **[移動... (Take me to...)]** ナビゲーションボックスでは、ユーザーインターフェイス (UI) の任意の場所に素早く簡単に移動できます。[移動... (Take me to...)] 機能を使用すると、機能名を入力するだけで、Loggerの任意の機能に移動できます。



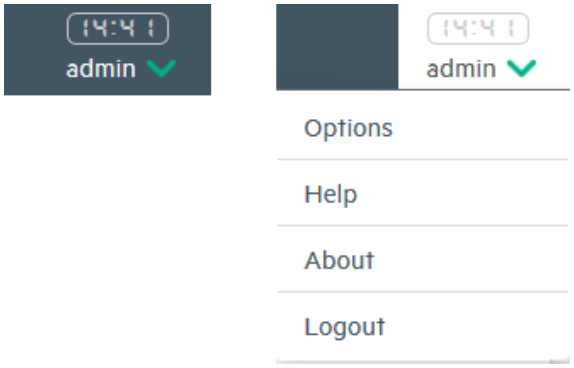
[移動... (Take me to...)] ナビゲーションボックスにアクセスするには、このボックスをクリックするか、ホットキーAlt+o、Alt+p、またはCtrl+Shift+oを使用します。入力すると、一致する機能の一覧がドロップダウンに表示されます。リスト中の項目をクリックするか、Enterキーを押して指定した機能に移動します。

注: 現在のUIページのヘルプを開くには、**[移動... (Take me to...)]** 検索ボックスに「`help`」と入力します。

サーバークロック、現在のユーザー、オプションドロップダウン

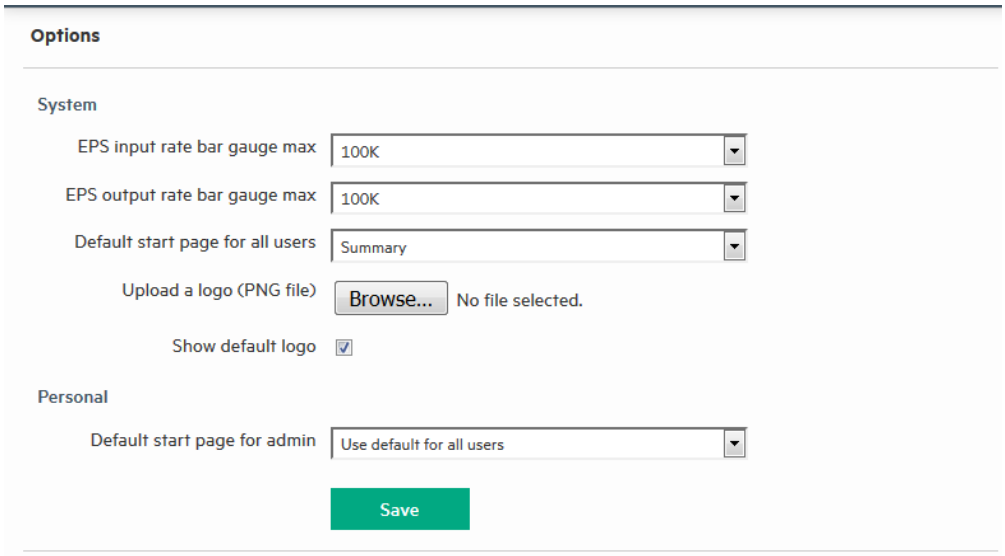
ゲージの右には、サーバークロック、現在ログインしているユーザーの名前、オプションドロップダウンが表示されます。

サーバークロックには、Logger サーバーのシステム時刻が表示されます。これは、ユーザーのローカル時刻と違っている可能性があります。ユーザー名の横のドロップダウンをクリックすると、[オプション (Options)]、[ヘルプ (Help)]、[バージョン情報 (About)]、および [Logout (ログアウト)] リンクにアクセスできます。



[オプション] ページ

[オプション (Options)] ページでは、EPSの入出力を表すゲージの範囲を設定できます。イベントレートが指定した最大を超えると、範囲が自動的に広がります。



このページからは、**ロゴ (.pngファイル) をアップロード**して、Logger ArcSight のロゴをカスタムロゴで置き換えることができます。ロゴは.png形式でなければなりません。推奨サイズは150 X 30ピクセル、最大ファイルサイズは1 MBです。

また、このページでは、すべてのユーザーのデフォルト開始ページ (ホームページ) と、個々のユーザー専用の開始ページを設定できます。開始ページは、ユーザーがログインしたときにLoggerに表示されるユーザーインターフェイスページです。

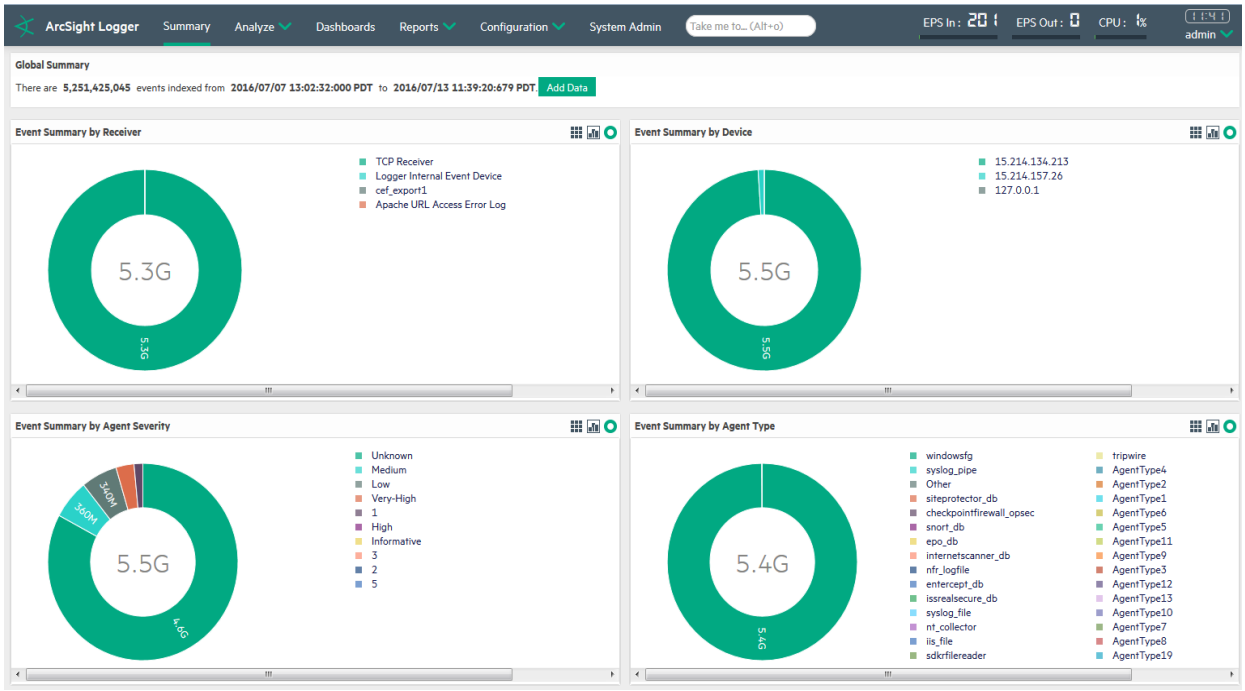
ログアウト

どのページでも [ログアウト] リンクをクリックすると、[ログイン] 画面に戻ります。ログアウトは、ユーザーがいない放置されたLoggerセッションが不正に使用されることを防ぐ適切なセキュリティの方法です。

Loggerは、ユーザーが設定した時間 (デフォルトでは15分) が経過すると、自動的にログアウトします。この時間を変更する方法については、『ArcSightLogger管理者ガイド』を参照してください。

サマリー

[サマリー (Summary)] ページは、Loggerに関するイベント情報の概要を1画面に表示する全体的なダッシュボードです。このページでは、受信イベントアクティビティやインデックス作成の状況を確認できます。



ダッシュボード

ダッシュボードは、関心のあるLogger情報を1か所で表示できるようにしたものです。関心のあるイベントに一致するさまざまな検索クエリや、レシーバー、フォワーダー、ストレージ、CPU、ディスクなどのLoggerコンポーネントのステータス、またはその両方を組み合わせて、1つのダッシュボードに表示し、一目で確認することができます。

各ダッシュボードには、検索結果またはモニターという種類のパネルが1つ以上含まれています。[検索結果] パネルには、パネルに関連付けられているクエリに一致するイベントが表示されます。[モニター] パネルには、レシーバー、フォワーダー、ストレージ、CPU、ディスクなど、Loggerの各種コンポーネントのリアルタイムなステータスと履歴ステータスが表示されます。

ダッシュボードの詳細については、『ArcSight Logger管理者ガイド』を参照してください。

第9章: イベントの検索

ネットワーク上の多様なソースから収集したイベントがLoggerに格納されると、失敗したログイン試行、ソース別のイベント数、SSH認証など、幅広い用途でイベントを検索することができます。さらに、一致するイベントをレポートに含めたり、ArcSight ESMなどの別のシステムにイベントを転送したりすることもできます。

イベントを検索するには、クエリを作成する必要があります。クエリは、「login」などの一致する単語やIPアドレスなど、シンプルな場合もあれば、複数のIPアドレスとポートを含み、かつ特定のデバイスグループに属するデバイスで特定の時間範囲の間に発生したイベントを検索するなど、より複雑なものにすることもできます。

Loggerでは、保存されたイベントをとても簡単に直感的に検索できます。Loggerでは、フローベースの検索言語がサポートされており、複数の検索コマンドをパイプライン形式で指定できます。また、検索結果の表示をカスタマイズしたり、検索結果をグラフで表示したりすることができます。

クエリの例

シンプルなクエリの例:

- `error`
- `sourceAddress=192.0.2.0`
- `hostA.companyxyz.com`

複雑なクエリの例:

```
_storageGroup IN ["Default Storage Group"] _deviceGroup IN ["192.168.22.120
[TCPC]"] name="*[4924TestAlert]*" AND ("192.168.*"OR categoryBehavior
CONTAINS Stop) | REGEX=":\d31" | cef name deviceEventCategory | chart _count
by name
```

クエリの構文

Loggerの検索クエリには、以下の種類の式が1つ以上含まれます。

クエリ要素	説明

キーワード	キーワード: プレーンテキストで表現された単語。以下に例を示します。
	`warning`
	`failed`
	`login`

フィールドベースの式:	フィールドベースの式: イベントのフィールド内の値を検索します。これには、特定のフィールドにおける一般的ではない値の検索が含まれます。以下に例を示します。
	`name="failed login"`
	`message!="failed login"`
	`sourceAddress=192.0.2.0`

検索演算子を使用した式	検索演算子を使用した式: この式では、検索演算子を使用して、キーワードとフィールドベースの式で指定された式と一致するデータに絞り込みます。 Logger6.4では、次の検索演算子を利用できます。 `cef`、`chart`、`dedup`、`eval`、`extract`、`fields`、`head`、`keys`、`rare`、`regex`、`rename`、`replace`、`rex`、`sort`、`tail`、`top`、`transaction`、`where`

抽出演算子を使用した式	`rex`検索演算子は、syslogイベント (rawデータまたは構造化されていないデータ) に便利に使用できます。また、あるイベントの15文字目など、イベントの特定の場所から情報を抽出する場合にも役に立ちます。
	たとえば、次のイベントからIPアドレスを抽出して
	`[Thu Jul 30 01:20:06 2009] [error] [client 69.63.180.245] PHP Warning: Can't connect to 10.4.31.4:11211`
	抽出した情報を"IP_Address" というフィールドに割り当てるには、次の`rex`式を使用します。
	`| rex "(?<IPAddress>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})"`

暗黙的なフィールド抽出演算子	イベントフィールドを直接クエリで指定できます。以下に例を示します。
	デバイスアドレスの一意の値を検索し、その数をグラフ形式で表示します。
	`failed | chart _count by deviceAddress`
	`deviceAddress`フィールド内で高頻度で現れる値の検索結果を表形式で表示します。つまり、値は頻度の高い値から少ない値の順に表示されます。
	`failed | top deviceAddress`

検索式の詳細な使用法と例については、『ArcSight Logger管理者ガイド』を参照してください。

クエリの作成

クエリを作成するときは、次の要素を指定する必要があります。

- **クエリ式**: イベントを選択または拒否するときに使用する検索条件。
- **時間範囲**: 検索の対象となる時間範囲。
- **フィールドセット**: 一致するイベントについて表示するイベントのフィールド。たとえば、一致するイベントのdeviceAddressとdeviceReceiptTimeフィールドだけを表示するように選択することができます。

さらに、検索対象を特定のストレージグループやストレージグループに限定する制約を含めることもできます。制約の指定についての詳細は、『ArcSight Logger管理者ガイド』を参照してください。

- ストレージグループを使用すると、グループに保有ポリシーを関連付けることができます。したがって、複数のストレージグループを定義して、異なる期間でイベントを保存できます。
- デバイスグループを使用すると、選択したデバイスをグループに分類できます。デバイスグループは、ストレージルールに関連付けることができます。ストレージルールは、特定のデバイスグループのイベントをどのストレージグループに保存するかを定義しています。

クエリの実行

クエリを実行するには

1. [**分析**] > [**検索**] をクリックします。
2. [検索] テキストボックスにクエリ式を指定します。
3. 時間範囲とフィールドセット (オプション) を選択します。
4. [**実行**] をクリックします。

> **ヒント:** クエリの実行中に構文エラーが表示された場合は、クエリの構文が『ArcSight Logger管理者ガイド』の「クエリ式の構文リファレンス」の項で指定されている要件に従っていることを確認してください。

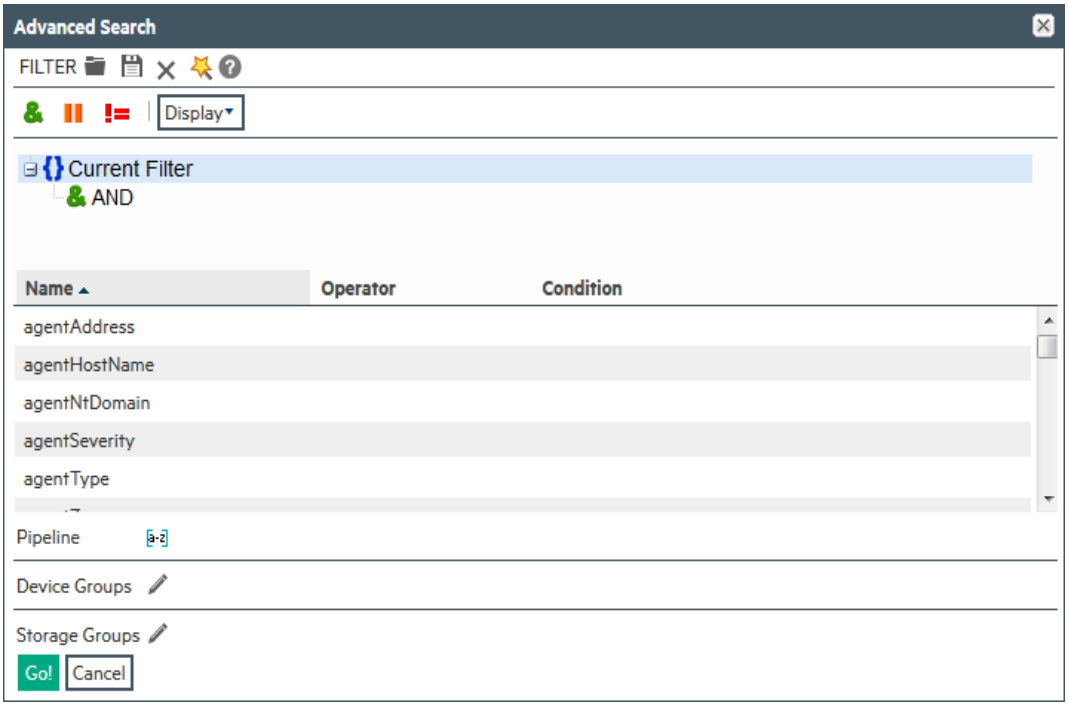
クエリ作成ツール

Loggerには、複雑なクエリの作成に役立つ以下のツールが用意されています。

- Search Builder

  Search Builderツールは、検索クエリを素早く正確に作成するための論理条件エディターです。このツールでは、クエリに含める条件が視覚的に表現されます。このツールを使用して、キーワード、フィールドベースの条件、正規表現を指定できます。また、このツールでデバイスグループやストレージグループなどの検索の制約を指定することもできます。

  このツールにアクセスするには、[検索]テキストボックスの下 [**検索の詳細設定**]をクリックします。このツールの使用方法については、『ArcSight Logger管理者ガイド』を参照してください。



- Regex Helper

  rex抽出演算子用の正規表現の作成は、複雑で間違いが起きやすい作業です。Regex Helperツールを使用すると、rexパイプライン演算子と合わせて使用する正規表現を作成し、関心のあるフィールドをイベントから抽出することができます。このツールは、rex演算子用の正規表現を簡単に作成できるようにするだけでなく、正規表現を効率的で誤りのないものにします。このツールについては、『ArcSight Logger管理者ガイド』を参照してください。

- Search Helper

  Search Helperは、検索に特化したユーティリティで、以下のような機能を提供します。

  - **検索履歴**: 最近実行されたクエリをLoggerに表示します。クエリを選択して再利用できるため、入力する手間が省けます。
  - **検索演算子履歴**: [検索] テキストボックスに入力した検索演算子を使用したことのあるフィールドが表示されます。
  - **例**: 入力した最近のクエリ演算子に関連する例をリストします。
  - **推奨される次の演算子**: 現在のクエリの後に使用されることが多い演算子のリストです。たとえば、`logger`と入力すると、その後に続くことが多い演算子は`rex`、`extract`、または`regex`です。
  - **ヘルプ**: クエリ内で最後に記述された演算子に関するコンテキスト依存のヘルプを提供します。
  - **フィールドと演算子のリスト**: 入力したクエリに応じて、現在入力しているフィールド名に一致する可能性のあるフィールド名の完全なリスト、または使用可能な演算子のリストを表示します。

検索結果のエクスポート

検索結果を次の形式でエクスポートできます。

- PDF: 検索結果の簡易レポートを生成するのに便利です。レポートには、検索結果の表と、結果用に生成されたすべてのグラフが含まれています。rawイベントとCEFイベントの両方を、エクスポートするレポートに含めることができます。
- CSV (Comma-Separated Values) ファイル: 他のソフトウェアアプリケーションでさらに分析するのに便利です。レポートには、検索結果の表が含まれています。この形式にはグラフを含めることができません。

検索結果をエクスポートするには

1. 検索クエリを実行します。
2. [**結果のエクスポート**] ( ) をクリックします。

後で使用するためのクエリの保存

同じクエリを定期的に実行する必要がある場合は、次の2つの方法でクエリを保存できます。

- 保存されたフィルター: クエリ式を保存しますが、時間範囲やフィールドセット情報は保存しません。
- 保存された検索: クエリ式と時間範囲を保存します。

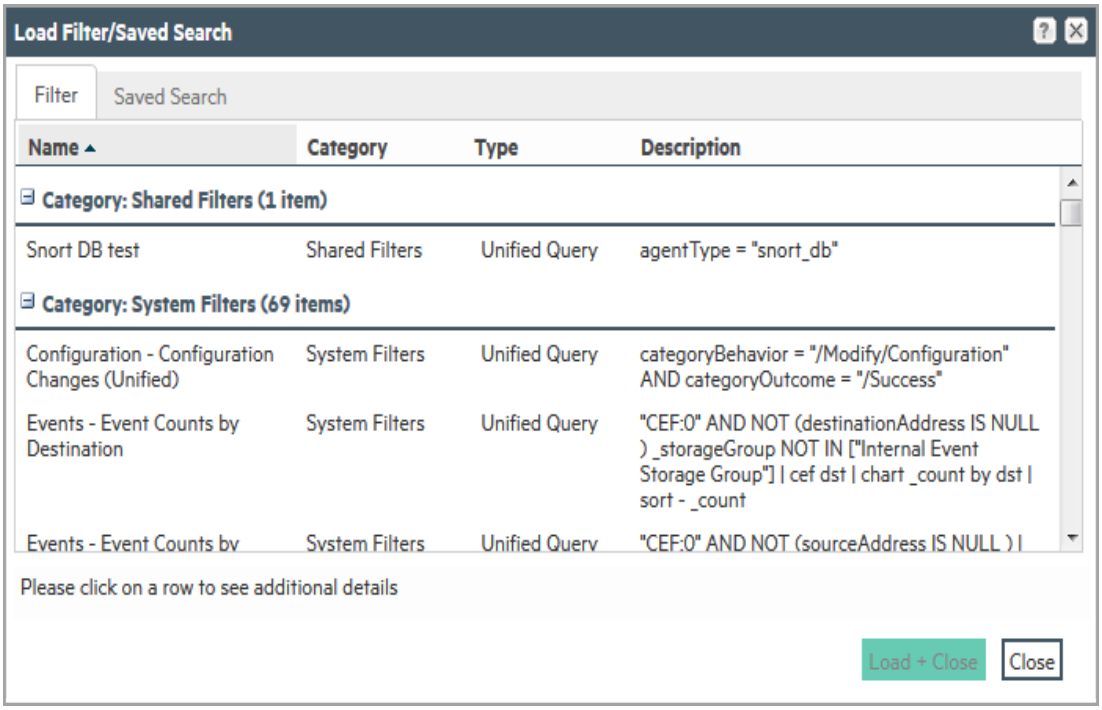
  クエリの保存と再利用についての詳細は、『ArcSight Logger管理者ガイド』を参照してください。

システムフィルター (定義済みフィルター)

Loggerには、いくつかの定義済みファイルター (システムフィルターとも呼びます) が用意されています。これらのフィルターは、失敗したログインの試行やソース別のイベント数など、よく検索されるイベントのクエリを定義しています。

システムフィルターを使用するには

1. [**分析**] > [**検索**] をクリックします。
2. [保存されているフィルターの読み込み] アイコン () をクリックして、すべてのシステムフィルターのリストを表示します。



3. **[読み込み + クローズ (Load+Close)]** をクリックします。

検索パフォーマンスの調整

検索パフォーマンスは多くの要因の影響を受け、クエリによって異なります。検索パフォーマンスに影響を与える可能性がある要因の一部を以下に示します。

検索パフォーマンスを最適化するには、以下の推奨事項に従ってください。

- 検索速度を最速にするには、可能な限りスーパーインデックスを利用します。スーパーインデックスフィールドの検索方法の詳細については、『ArcSight Logger管理者ガイド』を参照してください。
- 検索にかかる時間は、検索する必要のあるデータセットのサイズ、クエリの複雑さ、および検索が複数のピアに分散されているかどうかに依存します。データセットを制限するには、膨大な数のイベントをスキャンする必要がないように、クエリの時間範囲を指定します。
- 特定のストレージグループまたはピアに検索を限定すると、通常、ストレージグループまたはピアが指定されていない場合よりも検索パフォーマンスが向上します。
- クエリを実行する必要があるときは、スケジュールされたジョブ、複数のレポートの実行、多数のイベントの受信などのシステムへの負荷を軽減します。

ヒント: 推奨されるフィールドセットに対する全文インデックスとフィールドベースのインデックスの作成は、Loggerの初期化時に自動的に有効になります。これらのフィールドに加え、検索クエリとレポートクエリで使用するフィールドのインデックスを作成することを強

くお勧 めします。フィールド のインデックス作 成 の詳 細 については、『ArcSight Logger管 理 者 ガイド』を参 照してください。

第 10章 : クエリの例

このセクションでは、Loggerで使 用 できるクエリの例 をいくつか紹 介します。これらのクエリは、Loggerがイベントを受 信して、格 納していることを前 提 にしています。これらのクエリは、ニーズに合 わせて変 更 することもできます。

ヒント : rex式 を作 成 するには、Loggerで利 用 可 能 なRegex Helperツールを使 用します。Regex Helperツールの詳 細 については、『ArcSight Logger管 理 者 ガイド』を参 照してください。

- 次 のクエリは、"failed" という単 語 を含 むイベントからIPアドレスを抽 出し、一 番 上 のIPアドレスを表 示します。

  ```
  failed | rex “(?<src_ip>[^ ]\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})” | top
  <src_ip>
  ```

- 次 のクエリは、IPアドレスからネットワークIDを抽 出します。

  最 初 のrex式 でIPアドレスを取 得し、取 得したIPアドレスからIPアドレスが属 するネットワークID (IPアドレスの最 初 の3バイトが表 現 していると仮 定) を抽 出します。

  ```
  error | rex “(?<src_ip>[^ ]\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})” | rex
  field=src_ip “(?<net_id>\d{1,3}\.\d{1,3}\.\d{1,3})”
  ```

- 次 のクエリは、イベントからすべてのURLを抽 出し、空 のURLを除くURL数 のグラフを生 成します。

  ```
  http | rex “http://(?<customURL>[^ ]*)” | where customURL is not null |
  chart _count by customURL | sort - _count
  ```

- 次 のクエリは、単 語「user」(単 語 の後 に1個 のスペース) または「user=」の後 の最 初 の単 語を抽 出します。

  この場 合 、単 語「user」は大 文 字 と小 文 字 を区 別 せず、その前 にスペース文 字 が必 要 です。つまり、「ruser」や「suser」などの単 語 は一 致しません。

  ```
  user | rex “\s[u|U][s|S][e|E][r|R][\s|=](?<CustomUser>[^ ]*)” | chart _
  count by CustomUser
  ```

第 11章 : Loggerのその他 の機 能

Loggerには、このガイド で強 調 されている機 能 のほかにも多 くの機 能 があります。この項 で は、これらの機 能 の一 部 について説 明 します。Loggerの詳 細 な理 解 と使 用 方 法 について は、『ArcSight Logger管 理 者 ガイド』および『ArcSight Logger Web Services API Guide』を 参 照 してください。

タスクのスケジュール設 定

Loggerを設 定 して、設 定 バックアップ、イベントアーカイブ、ファイル転 送 、保 存 された検 索 な どのジョブを繰 り返 し実 行 することができます。

イベント のアーカイブ

イベントアーカイブを使 用 すると、現 在 の日 を除 く、過 去 の任 意 の日 のイベントを保 存 できま す。アーカイブの場 所 には、ローカルディレクトリか、Loggerソフト ウェアがインスト ールされている システム上 に作 成 したマウント ポイントを指 定 できます。イベントを毎 日 アーカイブするようにス ケジュールすることもできます。インデックス情 報 は、イベントアーカイブには含 まれません。ただ し、アーカイブが追 加 された後 にインデックスを作 成 することはできます。これにより、ライブスト レージ内 の検 索 と同 等 の速 さで、アーカイブされたイベントを検 索 できるようになります。

Loggerユーザーのアクセス制 御

Logger上 にさまざまなアクセス権 限 を持 つユーザーを作 成 することができます。たとえば、 Loggerの検 索 権 限 だけを持 つユーザーJoeを作 成 し、ユーザーJaneにはLoggerの検 索 およ び管 理 権 限 を付 与 します。

静 的 相 関 によるデータの強 化

ルックアップ機 能 を使 用 すると、Loggerの中 にあるデータを外 部 ファイルからのデータで増 強 し、このデータを検 索 結 果 に表 示 できます。これにより、静 的 相 関 にもとづくジオタグやアセット タグの追 加 、ユーザーの識 別 などが可 能 になります。たとえば、ソースIPアドレスが存 在 する 国 を検 索 結 果 に含 める場 合 、IPアドレスと国 の一 覧 を記 載 したファイルを作 成 し、そのファイ ルをLoggerにルックアップファイルとしてアップロード できます。その後 、lookup検 索 演 算 子 を使 用 してイベントのsourceAddressフィールドとルックアップファイルのIPアドレス列 を関 連 付 け、 検 索 結 果 に国 を表 示 できます。

Webサービス

Loggerには、Logger機 能 をユーザーのアプリケーションに統 合 するために使 用 できるSOAPおよびREST Webサービスが含 まれています。たとえば、保 存 されているLoggerイベントに対して検 索 を実 行したり、Loggerレポートを実 行してユーザーのサード パーティシステムにレポートをフィード バックしたりするプログラムを作 成 できます。この機 能 の詳 細 については、『Logger Web Services API Guide』を参 照してください。

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。

インストールおよび構成ガイド (Logger 6.4) に関するフィードバック

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。