Hewlett Packard Enterprise

HPE Security ArcSight ESM

ソフト ウェアバージョン: 6.11.0

ESMインストールガイド

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。

本書は機密文書です。

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。その保有、使用、または複製には、Hewlett Packard Enterpriseから使用許諾を得る必要があります。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

© Copyright 2017 Hewlett Packard Enterprise Development, LP

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

問い合わせ先

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

第1章: CORR-Engineストレージを備えたESMの概要

ESMは、SIEM (Security Information and Event Management) ソリューションであり、ネットワーク上に存在する異なるデバイスからセキュリティデータを収集して分析し、ユーザーに関係するすべてのデバイスのセキュリティステータスをリアルタイムで一元的に表示します。ESMは、イベントを処理して検索を実行する独自のフレームワークであるCORR-Engine (Correlation Optimized Retention and Retrieval Engine) ストレージを使用します。

ESMアプライアンスとESM Expressは、アプライアンスにインストールされるライセンスモデルですが、それぞれ異なります。

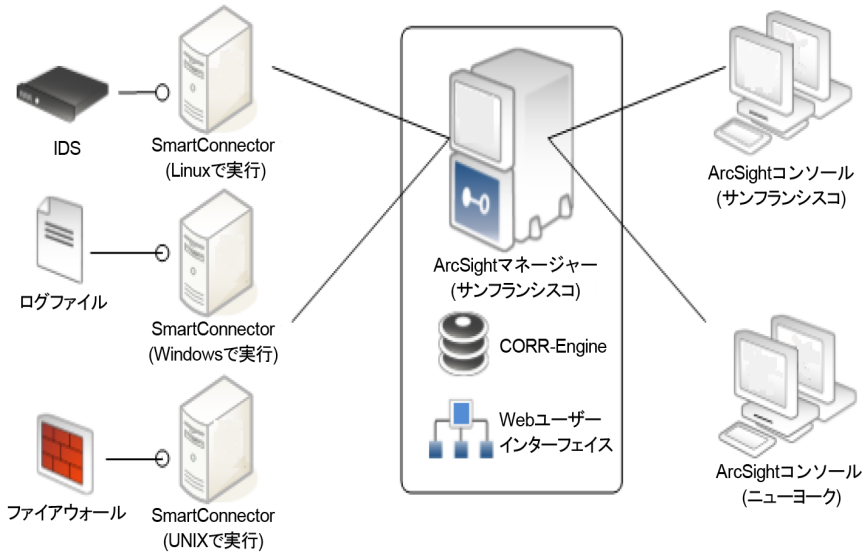
ソフトウェアESMは、ユーザーのハードウェアにインストールされるESMです。

ESMのコンポーネント

ESMシステムは、以下のコンポーネントで構成されています。

- **ESMマネージャー** -- マネージャーは、コネクターからイベントデータを受信し、イベントデータを相互に関連付け、報告し、データベースに格納するサーバーです。マネージャーとCORR-Engineは統合コンポーネントであり、同じマシンにインストールされます。
- **CORR-Engine** -- CORR-Engine (Correlation Optimized Retention and Retrieval Engine) は、長期間にわたるデータの格納と検索を行うエンジンであり、これを搭載した製品は高い頻度でのイベントの受信が可能になります。
- **ArcSightコンソール** -- ArcSightコンソールを使用すると、ESMコンテンツの調整、ルールの作成、ユーザーの管理などの管理タスクを実行できます。ArcSightコンソールは、クライアントマシンに対して個別にインストールされます。
- **ArcSightコマンドセンター** -- ArcSightコマンドセンターは、ArcSightコンソールにある機能の多くを実行できるWebベースのユーザーインターフェイスです。ArcSightコマンドセンターは、ダッシュボード、さまざまな種類の検索、ケース管理、通知、チャネルのほか、コンテンツ、ストレージ、アーカイブ、検索フィルタ、保存された検索、検索設定、ログ検索、ライセンス情報を管理する管理機能を提供します。
- **SmartConnector** -- SmartConnectorは、さまざまなデバイスやセキュリティイベントソースからのセキュリティイベントをESMに転送するソフトウェアコンポーネントです。SmartConnectorは、ESMにはバンドルされていないため、別途インストールします。

以下の図は、これらのコンポーネントをネットワーク上に展開する方法を示しています。



ESMの通信の概要

ArcSightコンソール、マネージャー、SmartConnectorは、HTTPS (HyperText Transfer Protocol Secure) を使用して通信します。HTTPSプロトコルには、データの暗号化、データの整合性の検証、およびサーバーとクライアントの両方の認証機能があります。

SSLは、TCP (Transport Control Protocol) 接続を介して機能します。マネージャーのデフォルトの受信TCPポートは8443です。

マネージャーからコンソールまたはSmartConnectorへの送信接続が確立されることはありません。マネージャーは、独自仕様のプロトコルを使用して、ループバックインターフェイス経由でCORR-Engineに接続します。

コンポーネントで障害が発生した場合の通信への影響

ソフトウェアコンポーネントのいずれかが使用できない状態になると、他のコンポーネント間の通信に影響を及ぼすことがあります。

CORR-Engineが何らかの理由によって使用できない場合、マネージャーはイベントの受け入れを停止して、CORR-Engineにコミットされていないすべてのイベントをキャッシュします。SmartConnectorも受信する新規イベントのキャッシュを開始するため、イベントデータが失われることはありません。コンソールは接続が解除されます。

CORR-Engineの容量が一杯になり、新たなイベントが到着すると、マネージャーは、最も古いイベントから既存のイベントの削除を開始します。

マネージャーを使用できない場合、SmartConnectorがイベントデータの損失を防ぐためにイベントのキャッシングを開始します。CORR-Engineはアイドル状態になり、コンソールは接続が解除されます。

SmartConnectorで障害が発生すると、イベントデータの損失が発生するかどうかは、SmartConnectorのタイプによって決まります。SNMP SmartConnectorなどのデバイスからイベントをリッスンするSmartConnectorは、イベントの受け入れを停止します。ただし、NT Collector SmartConnectorなどのデバイスをポーリングするSmartConnectorは、SmartConnectorがダウンしていた間に生成されたイベントをSmartConnectorの再起動後に収集することができます。

FIPSモードまたはデフォルトモードの選択

ESMは、連邦情報処理規格 (FIPS) 140-2およびSuite Bをサポートします。FIPSは、米国標準技術局 (NIST) によって発行された規格であり、ソフトウェアコンポーネントの暗号化モジュールを認可するために使用されます。米国連邦政府は、SBU (取扱注意ではあるが機密扱いでない) 情報を扱うすべてのIT製品がFIPS 140-2規格に準拠していることを義務付けています。

要件に応じて、次のいずれかのモードでESMコンポーネントをインストールすることができます。

- デフォルトモード (標準暗号化)
- FIPS 140-2モード
- FIPS with Suite Bモード (128ビットまたは192ビット)

FIPS暗号スイート

暗号スイートとは、SSLサーバーとクライアントの間でデータを安全にやり取りするために使用される、認証、暗号化、およびデータの完全性のアルゴリズムのセットです。FIPSモードの設定によって、次の特定の暗号スイートがESMおよびそのクライアントに対して自動的に有効になります。

注: SSLはどのモードでもサポートされていません。TLSはすべてのモードでサポートされています。TLSバージョンのサポートについては、「TLSのサポート」(83ページ) を参照してください。

次の表に、ESMがサポートする3つのモードの基本的な違いをいくつか示します。

モード	デフォルトの暗号スイート	キーストア/ トラストストア
デフォルトモード	• TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_128_GCM_SHA256	キーペアと証明書はキーストア、CACERTSおよびトラストストアにJKS形式で格納されます。
FIPS 140-2モード	• TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_128_GCM_SHA256	キーペアと証明書はキーストアに格納されます。
FIPS with Suite Bモード	• 192ビットモードでは、次の192ビット暗号スイートがサポートされています。 ◦ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA ◦ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • 128ビットモードでは、次の128ビット暗号スイートがサポートされています。 ◦ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ◦ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	キーペアと証明書はキーストアに格納されます。

PKCS#11の使用

ESMでは、コンソールにログインするためのID確認やアクセス制御に使用される90MeterやCAC (Common Access Card) などのPKCS#11トークンの使用がサポートされています。PKCS#11は、RSA Laboratoriesによって公開されているPKCS (Public-Key Cryptography Standard) であり、「Cryptokiと呼ばれる、テクノロジーに依存しない、スマートカードやPCMCIAカードなどの暗号化デバイス用プログラミングインターフェイス」であると説明されています。

PKCS#11認証は、RADIUS、LDAP、およびActive Directoryの認証方式ではサポートされていません。

ESMのインストールディレクトリ構造

デフォルトでは、ESMは単一のルートディレクトリの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、他のサードパーティソフトウェアは、必ずしもこのディレクトリの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へのパスは、`/opt/arcsight`と呼ばれています。

/opt/arcsight配 下 のディレクトリ構 造 も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。以 下 の表 は、マネージャーで一 般 的 に使 用 されているディレクトリの一 部 を示しています。

ポート	ディレクトリ
ESMバイナリ	/opt/arcsight/manager/bin
プロパティファイル	/opt/arcsight/manager/config
ログファイル	/opt/arcsight/manager/logs

ARCSIGHT_HOMEの参 照 先

パスに含 まれる<ARCSIGHT_HOME>は、以 下 の内 容 を表 しています。

- ArcSightマネージャーの場 合 は/opt/arcsight/manager
- ArcSightコンソールのインストール時 に指 定 したパス
- ArcSight SmartConnectorのインストール時 に指 定 したパス

第2章: アプライアンスへのインストール

このセクションは、アプライアンス上にHPEから購入したESMがあるユーザーに適用されます。ユーザーが所有するハードウェアにESMをインストールする方法については、「ソフトウェアESMのインストール」(24ページ)を参照してください。

開始する前に『Release Notes』をお読みください。

アプライアンス上でソフトウェアを準備する必要はありません。また、First Boot Wizardを開始する前に予備の調整を行う機会はありません。

アプライアンスの初めての起動

アプライアンスの電源を入れると、オペレーティングシステムのFirst Boot Wizard (FBW) が自動的に起動します。FBWによって、3種類のネットワーク設定が提示されます。

- IPv4
- IPv6
- IPv4とIPv6の両方 (デュアルスタック)

アプライアンスの初めての起動 - IPv4

この手順は、コマンドラインインターフェイスです。FBWによって、以下の情報を、一度に1つずつ、入力するように求められます (FBWにどの値がオプションであるかが表示されます)。

1. アプライアンスのログイン時に、パスワードarcsightを使用してrootユーザーとしてログインします。
2. rootユーザーの新しいパスワードを設定します。
3. arcsightユーザーの新しいパスワードを設定します。
4. アプライアンスのホスト名を設定します。
5. IPv4の場合は、1を指定します。
6. アプライアンスのIPアドレスを指定します。
7. ネットマスクを指定します。
8. デフォルトゲートウェイを指定します。
9. プライマリDNS IPアドレスを指定します。
10. セカンダリDNS IPアドレスを指定します(オプション)。
11. DNS検索ドメインを指定します。

12. タイムゾーンを指定します。文字を一部だけ入力してTabキーを押すと、システムによってタイムゾーンが自動入力されます。たとえば、Aと入力してTabキーを押すと"America_"が入力されます。Tabキーを2回押すと、"America_" で始まるタイムゾーンエントリのリストが表示されます。
13. 日付を入力します。
日付と時刻はオプションです。NTPサーバーを指定すると、これらの日付と時刻の値が上書きされます。NTPサーバがない場合、これらの日付と時刻の値によってアプライアンスのシステムクロックがリセットされます。空白のままにすると、システムクロックによって日付と時刻が決定されます。
14. 時間を入力します。
15. NTPサーバーを指定します。1行に1つのNTPサーバを記述します。IPアドレスまたはホスト名を使用できます。NTPサーバーを使用することをお勧めします。

設定が完了すると、確認のために、指定した項目のリストが表示されます。Noを選択すると、最初から設定をやり直します。

指定した内容を承認する場合は、「**y**」と入力して**Enter**キーを押します。インストールセッションが終了し、設定ウィザードが自動的に開始します。

ライセンスファイル: IPアドレスが定義されたら、ライセンスファイルをダウンロードしたマシンからアプライアンスにログインし、ライセンスファイルをアプライアンスにコピーすることができます。設定ウィザードの次のセグメントで、アプライアンス上のライセンスファイルの場所を指定するように求められます。

アプライアンスの初めての起動 - IPv6

IPv6では、スタティック設定または自動構成ネットワーキングを指定できます。

この手順は、コマンドラインインターフェイスです。FBWによって、以下の情報を、一度に1つずつ、入力するように求められます (FBWにどの値がオプションであるかが表示されます)。

IPv6スタティックネットワーク設定

1. アプライアンスのログイン時に、パスワードarcsightを使用してrootユーザーとしてログインします。
2. rootユーザーの新しいパスワードを設定します。
3. arcsightユーザーの新しいパスワードを設定します。
4. アプライアンスのホスト名を設定します。
5. IPv6の場合は、2を指定します。
6. スタティックIPv6ネットワーク設定には1を指定します (ここで、IPアドレスを入力します)。
7. アプライアンスのIPアドレスを指定します。
8. デフォルトゲートウェイを指定します。

9. プライマリDNS IPアドレスを指定します。
10. セカンダリDNS IPアドレスを指定します(オプション)。
11. DNS検索ドメインを指定します。
12. タイムゾーンを指定します。文字を一部だけ入力してTabキーを押すと、システムによってタイムゾーンが自動入力されます。たとえば、Aと入力してTabキーを押すと"America_"が入力されます。Tabキーを2回押すと、"America_" で始まるタイムゾーンエントリのリストが表示されます。
13. 日付を入力します。
日付と時刻はオプションです。NTPサーバーを指定すると、これらの日付と時刻の値が上書きされます。NTPサーバーがない場合、これらの日付と時刻の値によってアプライアンスのシステムクロックがリセットされます。空白のままにすると、システムクロックによって日付と時刻が決定されます。
14. 時間を入力します。
15. NTPサーバーを指定します。1行に1つのNTPサーバーを記述します。IPアドレスまたはホスト名を使用できます。NTPサーバーを使用することをお勧めします。

設定が完了すると、確認のために、指定した項目のリストが表示されます。Noを選択すると、最初から設定をやり直します。

指定した内容を承認する場合は、「**y**」と入力して**Enter**キーを押します。インストールセッションが終了し、設定ウィザードが自動的に開始します。

IPv6自動設定ネットワークのセットアップ

1. アプライアンスのログイン時に、パスワードarcsightを使用してrootユーザーとしてログインします。
2. rootユーザーの新しいパスワードを設定します。
3. arcsightユーザーの新しいパスワードを設定します。
4. アプライアンスのホスト名を設定します。
5. IPv6の場合は、2を指定します。
6. ステートレスアドレス自動設定 (SLAAC) を使用するIPv6自動設定ネットワークのセットアップの場合は、2を指定します。プライマリDNS IPアドレスとセカンダリDNS IPアドレス (オプション) を指定します。IPアドレスとゲートウェイアドレスは、DNSによって自動的に検出され、割り当てられます。
7. タイムゾーンを指定します。文字を一部だけ入力してTabキーを押すと、システムによってタイムゾーンが自動入力されます。たとえば、Aと入力してTabキーを押すと"America_"が入力されます。Tabキーを2回押すと、"America_" で始まるタイムゾーンエントリのリストが表示されます。
8. 日付を入力します。
日付と時刻はオプションです。NTPサーバーを指定すると、これらの日付と時刻の値が上書きされます。NTPサーバーがない場合、これらの日付と時刻の値によってアプライアンス

のシステムクロックがリセットされます。空白のままにすると、システムクロックによって日付と時刻が決定されます。

9. 時間を入力します。
10. NTPサーバーを指定します。1行に1つのNTPサーバーを記述します。IPアドレスまたはホスト名を使用できます。NTPサーバーを使用することをお勧めします。

設定が完了すると、確認のために、指定した項目のリストが表示されます。Noを選択すると、最初から設定をやり直します。

指定した内容を承認する場合は、「**y**」と入力して**Enter**キーを押します。インストールセッションが終了し、設定ウィザードが自動的に開始します。

ライセンスファイル: IPアドレスが定義されたら、ライセンスファイルをダウンロードしたマシンからアプライアンスにログインし、ライセンスファイルをアプライアンスにコピーすることができます。設定ウィザードの次のセグメントで、アプライアンス上のライセンスファイルの場所を指定するように求められます。

アプライアンスの初めての起動 - デュアルスタック

この手順は、コマンドラインインターフェイスです。FBWによって、以下の情報を、一度に1つずつ、入力するように求められます (FBWにどの値がオプションであるかが表示されます)。

1. アプライアンスのログイン時に、パスワードarcsightを使用してrootユーザーとしてログインします。
2. rootユーザーの新しいパスワードを設定します。
3. arcsightユーザーの新しいパスワードを設定します。
4. アプライアンスのホスト名を設定します。
5. IPv4とIPv6の両方の場合は、3を指定します。
6. 「アプライアンスの初めての起動 - IPv4」(13ページ)の手順に従って、IPv4ネットワーク設定の選択項目を完了します。
7. 「アプライアンスの初めての起動 - IPv6」(14ページ)の手順に従って、IPv6ネットワーク設定の選択項目を完了します。

設定が完了すると、確認のために、IPv4とIPv6の両方について指定した項目のリストが表示されます。Noを選択すると、最初から設定をやり直します。

IPv4とIPv6の両方について指定した内容を承認する場合は、「**y**」と入力して**Enter**キーを押します。インストールセッションが終了し、設定ウィザードが自動的に開始します。

ライセンスファイル: IPアドレスが定義されたら、ライセンスファイルをダウンロードしたマシンからアプライアンスにログインし、ライセンスファイルをアプライアンスにコピーすることができます。設定ウィザードの次のセグメントで、アプライアンス上のライセンスファイルの場所を指定するように求められます。

設定ウィザードの使用

アプライアンスにインストールすると、設定ウィザードが自動的に開始します。(設定ウィザードを開始するために、手動でコマンドを入力する必要はありません)ソフトウェアESMをGUIモードでインストールすると、設定ウィザードが自動的に開始します。コンソールモードのソフトウェアESMでは、次のコマンドを使用して手動で設定ウィザードを開始します。

```
/opt/arcsight/manager/bin/arcsight firstbootsetup -boxster -soft -i console
```

1. Welcomeメッセージが表示されます。ライセンスファイルにアクセスできる場合は、「**yes**」と入力して続行します。
2. [**Language Options**] で、インターフェイスの表示言語を選択します。**Enter**キーを押して続行します。
3. [**CORR-Engine Password**] の下で、**Enter**キーを押して難読化されたパスワードを使用して続行するか、「**no**」と入力して**Enter**キーを押し、パスワードを画面に表示させます。
4. [**CORR-Engine Password]** の下で、CORR-Engine用のパスワードを設定し、確認のために再入力します。**Enter**キーを押します。パスワード制限の詳細は、『ESM Administrator's Guide』の「Configuration」の章で「Managing Password Configuration」を参照してください。
5. [**CORR Engine Configuration**] で、CORR-Engineストレージ割り当て情報を入力し、**Enter**キーを押します。

   System Storage Size - リソースの格納領域とは別に設定されるストレージ領域のサイズ

   Event Storage Size - イベントの格納領域とは別に設定されるストレージ領域のサイズ

   Online Event Archive Size - イベントアーカイブ用のディスク領域の最大ギガバイト数。これは、デフォルトのオンラインイベントアーカイブにのみ適用されます。

   Retention Period - イベントがシステムからパージされる前にイベントを保持しておく期間
6. [**Notification Emails**]で、次の電子メールアドレスを指定します。

   Error Notification Recipient: マネージャーがダウンした場合や他の問題が発生した場合に、メール通知を受信する電子メールアカウントのメールアドレスを1つ指定します。電子メールアドレスをさらに指定する必要がある場合は、『ESM Administrator's Guide』の「Running the Manager Configuration Wizard」の説明に従って、マネージャー設定ウィザードを使用して指定できます。

   From email address: 通知の送信者に使用されるメールアドレス。

   値が正しい場合は、「**yes**」と入力し、**Enter**キーを押して続行します。電子メールは、システムが次の状態を検出したときに送信されます。

- サブシステムのステータスが変更された。変更の内容と、変更を行ったユーザーが電子メールに記されます。
- レポートが正常にアーカイブされた。
- アカウントのパスワードがリセットされた。
- アーカイブレポートの生成が失敗した。
- 通知先で受信された通知が多すぎる。
- イベントアーカイブの場所が上限に達した。イベントアーカイブを別の場所に移動して、スペースを解放するように求められます。
- ユーザーがArcSightコンソールの設定を電子メールで送信することを選択した。
- ユーザーがパーティションアーカイブコマンドを送信した。
- 十分なスペースがないため、アーカイブが失敗する。
- データベースへの接続に失敗した。

7. [**License File**] に、ダウンロードしたライセンスファイルのパスとファイル名を入力し、**Enter**キーを押します。
8. [**Select the Product Mode**] でデフォルトモードでインストールするか、FIPSモードでインストールするかを選択します。**Enter**キーを押して続行します。

注意:

- 本製品をFIPSモードでインストールすることを選択した場合は、コンソールもFIPSモードでインストールしてください。コンソールをFIPSモードでインストールする方法については、「FIPSモードでのArcSightコンソールのインストール」(85ページ)を参照してください。
- FIPSモードでソフトウェアを構成した場合は、再インストールしないと、デフォルトモードに切り替えることはできません。
- デフォルトモードのインストールからFIPS-140-2モードへの切り替えはサポートされています。切り替える必要がある場合は、『Administrator's Guide』で手順を参照してください。
- ESMのデフォルトでは、自己署名証明書が使用されます。CA署名証明書を使用する場合は、設定ウィザードが正常に完了した**後**、CA署名証明書を手動でインポートする必要があります。CA署名証明書の使用方法の詳細については、『ESM Administrator's Guide』を参照してください。

9. FIPSモードを選択した場合は、選択内容を確認します。FIPSモードを選択していない場合は、Manager Informationのステップにスキップします。
10. [**Select the Cipher Suite Options**] パネルでFIPSモードを選択した場合は、暗号ス

イートを選択します。

Suite Bでは、2つのセキュリティレベル(128ビットと192ビット)が定義されます。この2つのセキュリティレベルは、Suite Bによって提供される全体的なセキュリティの代わりに使用されるAES (Advanced Encryption Standard) のキーサイズに基づいています。128ビットのセキュリティレベルでは、128ビットのAESキーサイズが使用されますが、192ビットのセキュリティレベルでは、256ビットのAESキーサイズが使用されます。キーサイズが大きくなるとセキュリティも強化されますが、時間とリソース(CPU)消費の点で計算コストも高くなります。ほとんどのシナリオでは、128ビットのキーサイズで十分です。

11. [**Manager Information**] で、マネージャーのホスト名を入力し、管理ユーザーのユーザーIDとパスワードを設定して、**Enter**キーを押します。

注意:

- マネージャーのホスト名は、マネージャーがインストールされているマシンのIPアドレス(IPv4のみ)、または完全修飾ドメイン名です。この名前は、すべてのクライアント(ArcSightコンソールなど)がマネージャーと接続するために指定する名前です。柔軟性を確保するために、IPアドレスの代わりに完全修飾ドメイン名を使用することを推奨します。
- [**IP Version**] の選択 (IPv4またはIPv6) は、アプライアンスなどのデュアルスタックマシンがある場合に表示されます。このオプションが表示された場合、選択内容は次のような影響を及ぼします。
  - ホスト名が指定されている場合、サードパーティのソフトウェアが使用するIPアドレスを制御します (例: マネージャーセットアップの電子メールサーバー)。
  - ホスト名が指定されている場合、ピアリングページで試行されるIPアドレスを制御します。
  - マネージャーアセットに対してIPv4アドレスまたはIPv6アドレスのどちらを選択するかを制御します。
- 複数のホスト名が存在する可能性があり、デフォルトはhostnameコマンドで返されたものと同じではない可能性があります。高可用性モジュールを使用している場合は、両方のサーバー(プライマリとセカンダリ)に共通のサービスホスト名をマネージャーのIPまたはホスト名として使用します。それ以外の場合は、コネクター、コンソールおよびその他のクライアントの設定に便利で、正常に機能すると考えられるホスト名を選択します。完全修飾ドメイン名を使用することが、最善の方法であることに注意してください。
- DNSサーバー上でホスト名を使用しない場合は、`/ etc / hosts`ファイルに静的ホストエントリを追加して、ホスト名をローカルで解決してください。
- マネージャーのホスト名は、自己署名証明書を生成するために使用されます。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。

- マネージャーではデフォルトで自己署名証明書が使用されますが、必要に応じて、CA署名証明書を使用するように切り替えることができます。切り替えはインストール後に行います。手順については、『ESM Administrator's Guide』を参照してください。

12. Event Brokerへの接続をセットアップするかどうかを選択します (Event BrokerがESMの実装の一部である場合)。Event BrokerをFIPSモードでセットアップする必要がある場合は、「Event Brokerへのアクセスの設定 - FIPSモード (サーバー認証のみ) (オプション)」(89ページ) を参照してください。

    クライアント認証がEvent Brokerで有効になっている場合は、「Event BrokerとESM間のSSLクライアント側認証の設定 - 非FIPSモード」(47ページ) または「Event BrokerとESMの間のSSLクライアント側認証の設定 - FIPSモード」(90ページ) を参照してください。

    接続を設定する場合は **[Yes]** を選択し、続行する場合は **[No]** を選択します。**[Yes]** を選択した場合は、以下を指定します。

    a. **Host: Port(s)**: Event Broker内のノードのホストとポートの情報を入力します。マスターノードだけでなく、複数のノード環境内のすべてのノードのホスト (ホスト名またはIPアドレス) とポートの情報を含めます。入力する内容は、カンマ区切りのリストです (例: <host>:<port>,<host>:<port>)。Event Brokerが受け入れることができるのは、ESMからのIPv4接続だけであることに注意してください。

    b. **Topic to read from**: Event Brokerから購読するトピックを指定します。これにより、データソースが決定されます。『Event Broker管理者ガイド』の「Event Brokerのトピックの管理」の章を参照してください。

    c. **Path to the Event Broker root cert**: ESMは、TLS経由でEvent Brokerと通信します。これを有効にするには、Event Brokerのルート証明書をESMのクライアントのトラストストアにインポートする必要があります。
    Event Brokerのルート証明書を、Event Brokerマシン (`/opt/arcsight/kubernetes/ssl/ca.crt`) からESMマシン上のローカルフォルダーにコピーします。証明書のパスを入力して **[Next]** をクリックすると、Event Brokerのルート証明書がESMのクライアントのトラストストアにインポートされ、Event Brokerへの接続が検証されます。問題がある場合は、エラーまたは警告メッセージが表示されます。メッセージが表示されず、ウィザードが次の画面に進んだ場合、Event BrokerとESMの間の接続が正常に検証されたことを意味します。

13. ArcSight Investigateをセットアップするかどうかを選択します。統合を有効にする場合は **[Yes]** を選択し、続行する場合は **[No]** を選択します。**[Yes]** を選択した場合は、ArcSight Investigateの展開の **[Search URL]** を指定します。

14. **[Packages]** パネルで**Enter**キーを押して続行します。それ以外の場合は、使用を許可されているオプションパッケージを選択します。これらのオプションパッケージに加えて、ArcSightマネージャーに自動的にインストールされるデフォルトの標準コンテンツパッケージがあります。これらのデフォルトパッケージは、システムヘルスと状態の運用に不可欠なものであり、すぐに使用してネットワークを監視し、保護することができます。

パッケージの詳細については、『ArcSight Administration and ArcSight System Standard Content Guide』を参照してください。

15. **About to Configure ESM**の下で

> **注意:**「**yes**」と入力して**Enter**キーを押すと、製品は指定されたとおりにインストールされます。

16. 「**Configuration Completed Successfully**」と表示されたら、「**yes**」と入力し、**Enter**キーを押して終了します。
17. **重要:** このステップは、サービスを起動するために必要になります。ルートユーザーでログインし、以下のスクリプトを実行して必要なサービスをセットアップします。

```
/opt/arcsight/manager/bin/setup_services.sh
```

インストールが完了したら、ストレージボリュームの場所とサイズを確認して、必要な変更を加えます。変更は、ArcSightコマンドセンターで行うことができます。ストレージボリュームに関する詳細については、『ArcSight Command Center User's Guide』の「Administration」の章の「Storage and Archive」を参照してください。

> 設定ウィザードは、[About to Configure ESM v6.11.0] という最初の構成画面が表示される**前**の任意の時点で終了した場合のみ、手動で再実行できます。詳細については、「ESM設定ウィザードの再実行」(44ページ)を参照してください。

開いたままにしておくTCPポート

アプライアンスでは、これらのポートはすでに開いています。

外部の受信接続用のポート:

8443/tcp
22/tcp (ssh)

コンポーネント間の通信用に内部で使用されるTCPポート:

1976、28001、2812、3306、5555、6005、6009、7777、7778、7779、7780、8005、8009、8080、8088、8089、8666、8766、8808、8880、8888、8889、9095、9090、9123、9124、9999、45450

ピアリングの有効化

このトピックは、ピアリングを含むESMライセンスを使用してアプライアンスをインストールするためのものです。

デフォルトでは、アプライアンスはポート9000を無効にして出荷されます。ピアリングにはこのポートが必要です。アプライアンスでピアリングを機能させるには、次のコマンドを使用してポート9000を有効にします。

```
[root@rhel7 ~]# firewall-cmd --zone=public --add-port=9000/tcp --permanent

[root@rhel7 ~]# firewall-cmd --reload
```

次のコマンドを使用して、ポート9000が有効になっていることを確認します。

```
[root@rhel7 ~]# iptables-save | grep 9000
```

次のような応答が得られます。

```
 -A IN_public_allow -p tcp -m tcp --dport 9000 -m conntrack --ctstate NEW -j
ACCEPT
```

ピアリングは、同じIPバージョンを使用するESMマネージャー間で機能することに注意してください。ただし、ESMマネージャーがデュアルスタックマシン上にある場合は、詳細について『ArcSight Command Center User's Guide』を参照してください。「Administration Configuration」のセクションの「Peers」を参照してください。

暗号化されたアプライアンスでのESMの実行

ESM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。これには、High Availabilityモジュールを使用するシステムが含まれます。HAの機能に変わりはありません。

Server Management Software > HP Secure Encryption Webページから入手可能なHPE Secure Encryptionを使用して、G9 ESM Expressアプライアンス(B7600またはE7600など)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。

G9アプライアンス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。ハードウェアの暗号化は、ESMをインストールする前または後のどちらでも実行できます。HAがすでにインストールされている場合は、1回だけフェイルオーバーすれば済むように、セカンダリを最初に暗号化します。

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Gen 9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ESMを使用できます。ESM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: ESM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。

アプライアンスのアウトオブバンドリモートアクセスの設定

応答不能になったアプライアンスにカスタマーサポートがアクセスしてトラブルシューティングできるように、アプライアンスにアウトオブバンドリモートアクセスを設定します。すべてのアプライアンスモデルには、HPE Integrated Lights-Out (iLO) 拡張リモート管理カードが装備されています。詳細な情報およびドキュメントについては、https://www.hpe.com/us/en/servers/integrated-lights-out-ilo.htmlにアクセスしてください。

第3章: ソフトウェアESMのインストール

ESMのインストールを開始する前に、『ESM Release Note』を参照することを推奨します。

HPE製のアプライアンス上にあるESM Expressをインストールする場合は、「アプライアンスへのインストール」(13ページ)を参照してください。

ESMとともにESM高可用性モジュールを使用する予定で、これがESMの新規インストールの場合は、最初に高可用性モジュールをインストールします。手順については、『ESM High Availability Module Guide』を参照してください。

ESMはオペレーティングシステムとバージョンの影響を受けます。適切な動作を確保するため、このインストーラーでは、『HPE ArcSight ESM Support Matrix』に記載されている特定のオペレーティングシステムとバージョンにのみインストールできます。『HPE ArcSight ESM Support Matrix』は、Protect 724 (https://www.protect724.hpe.com) でダウンロードできます。

ESMシステムの保護

以下の各セクションの情報を使用して、ArcSightのコンポーネントを保護します。

ArcSightマネージャーの保護

本番環境では、デモ用の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からデモ用のCAを必ず削除してください。

ユーザーにはタスクの完了に必要な権限のみを付与するという最小権限の原則に基づいて、ファイルへのアクセスを厳密に管理します。以下は、特に機密性のあるファイルです。

注: `<ARCSIGHT_HOME>`はコンポーネントのルートディレクトリです。たとえば、マネージャーコンポーネントの場合、`<ARCSIGHT_HOME>`は`/opt/arcsight/manager`です。

- `<ARCSIGHT_HOME>/config/jetty/keystore` (ArcSightマネージャー秘密キーの盗難を防ぐためのファイル)
- `<ARCSIGHT_HOME>/config/jetty/truststore` (新しい信頼済みCAの挿入を防ぐために、SSLクライアント認証でのみ使用されるファイル)
- `<ARCSIGHT_HOME>/config/server.properties` (キーストアとデータベースのパスワードがあるファイル)
- `<ARCSIGHT_HOME>/config/jaas.config` (RADIUSまたはSecurID対応の場合のみ、共

有ノードシークレットが含まれるファイル)

- `<ARCSIGHT_HOME>/config/client.properties` (SSLクライアント認証の場合のみ、キーストアパスワードが含まれるファイル)
- `<ARCSIGHT_HOME>/reports/sree.properties` (レポートライセンスを保護するためのファイル)
- `<ARCSIGHT_HOME>/reports/archive/*` (アーカイブされたレポートの盗難を防ぐためのファイル)
- `<ARCSIGHT_HOME>/jre/lib/security/cacerts` (新しい信頼済みCAの挿入を防ぐためのファイル)
- `<ARCSIGHT_HOME>/lib/*` (悪意のあるコードの挿入を防ぐためのファイル)
- `<ARCSIGHT_HOME>/rules/classes/*` (コードの挿入を防ぐためのファイル)

ESMを (アプライアンスではなく) 所有するハードウェアにインストールする場合は、ホストベースのファイアウォールを使用してください。ArcSightマネージャーでは、以下の表のポートを除くすべてがブロックされます。これらのポートに実際に接続して通信する可能性があるリモートIPアドレスは厳重に管理してください。

ポート	フロー	説明
22/TCP	インバウンド	SSHログイン (UNIXのみ)
53/UDP	インバウンド/アウトバウンド	DNSの要求と応答
8443/TCP	インバウンド	SmartConnectorとコンソール
25/TCP	アウトバウンド	メールサーバー向けのSMTP
110/TCP	アウトバウンド	メールサーバー向けのPOP3 (該当する場合)
143/TCP	アウトバウンド	メールサーバー向けのIMAP (該当する場合)
1645/UDP	インバウンド/アウトバウンド	RADIUS (該当する場合)
1812/UDP	インバウンド/アウトバウンド	RADIUS (該当する場合)
389/TCP	アウトバウンド	LDAPサーバー向けのLDAP (該当する場合)
636/TCP	アウトバウンド	LDAPサーバー向けのLDAP over SSL (該当する場合)

IPv4のみに適用:

別の防御レイヤーとして (または、ホストベースのファイアウォールを使用できない場合)、server.propertiesファイルの以下のプロパティを使用して、ArcSightマネージャーによって許可される接続を制限することができます。

```
xmlrpc.accept.ips=
agents.accept.ips=
```

これらの各プロパティは、カンマまたはスペースで区切られた、IPアドレスまたはサブネットを指定したリストを取り込みます。一度指定すると、リストにあるアドレスからの接続のみが許可されます。

- `xmlrpc.accept.ips`プロパティは、ArcSightコンソールのアクセスを制限します。
- `agents.accept.ips`プロパティは、SmartConnectorのアクセスを制限します。登録時は、SmartConnectorを`xmlrpc.accept.ips`にも含めて、登録可能にしておく必要があります(「登録されている」ということが、削除可能であることを意味するわけではありません)。

サブネットの指定形式は、以下の例に示されているようにフレキシブルです。

```
xmlrpc.accept.ips=192.0.2.0 192.0.2.5
agents.accept.ips=10.*.*.*,192.0.0.0-192.0.255.255
```

組み込みセキュリティ

ESMのユーザーアカウントには、ユーザーがArcSightマネージャーでアクセスできる機能を制御するユーザータイプがあります。最も多くの権限は「Normal User」タイプに付与されています。可能な場合は、自動ユーザーアカウントには「Manager SmartConnector」、「Management Tool」、または「Archive Utility」などの制限付きのタイプを使用します。このことは、自動実行を行うためにスクリプトにユーザーパスワードを格納する必要がある場合は特に重要です。

ESMにユーザーアカウントを作成する場合、およびリソースやイベントへのアクセス権を付与する場合には最小権限の原則を適用します。ユーザーにはそれぞれのタスクに必要とされる以上の権限を付与しないでください。

デフォルトでは、パスワードの最小長は6文字、最大長は20文字です。パスワードの制限の詳細については、『Administrator's Guide』の第2章「Configuration」の「Managing Password Configuration」の中にある「Password Character Sets」を参照してください。

ハードウェアの物理セキュリティ

パスワード、キーストア、および他のソフトウェア機能のセキュリティポリシーを確立することに加えて、ESMシステムによって使用されるハードウェアに物理的なセキュリティを施すことが重要です。物理的なハードウェアには、ArcSightコンソール、およびSmartConnectorソフトウェアを実行しているコンピューターに加えて、それらのコンピューターに接続するネットワークが含まれます。

ArcSightソフトウェアを実行しているコンピューターへの物理的なアクセスは制限する必要があります。

- ほとんどのラックマウントケースで提供されているケーブルロックメカニズムを使用して、悪意によるまたは偶発的なマシンの改ざんを防止する
- ディスクドライブエンクロージャーにはロックを使用する
- 冗長電源装置およびUPS (無停電電源装置) を使用する

- 以下の方法で、BIOS (x86システムのみ) またはファームウェアを保護する
  - ブート用のすべてのCD-ROMドライブを無効にして、ハードディスクからのみシステムを起動可能にする
  - COMポート、パラレルポート、およびUSBポートを無効にして、データ抽出に使用できなくする
  - 電源管理を無効にする

オペレーティングシステムのセキュリティ

- Linuxでは、ブートローダーパスワードをセットアップして、許可を得ていない人間がシングルユーザーモードで起動するのを防ぎます (詳細については、iLOまたはGRUBのドキュメントを参照してください)。
- Linuxでは、`/etc/inittab`でCtrl-Alt-Delによる再起動を無効にします。「ctrlaltdel」を参照している行をコメントにします。
- 適度に短い経過時間 (5分など) でパスワードのプロンプトが表示されるスクリーンセーバーをセットアップします。
- OSの電源管理を無効にします。
- OSのインストール時には、パッケージを個別に選択し、内容を把握しているパッケージのみインストールします。不足しているパッケージは、必要になったときにいつでもインストールできます。
- 自動アップデートツールを実行して、すべてのセキュリティ修正プログラムを取得します。Red Hat Linuxでは`up2date`を使用します (Red Hat Networkのサブスクリプションが必要な場合あり)。
- 必要のないサービスをすべてアンインストールします (または、少なくとも停止します)。具体的には、finger、r-services、telnet、ftp、httpd、linuxconf (Linux)、Remote Administration ServicesおよびIIS Services (Windows) が対象です。
- UNIXマシンでは、リモートルートログインを禁止します (OpenSSHの場合は、`/etc/ssh/sshd_config`の`PermitRootLogin` noディレクティブを使用して禁止できます)。この結果、リモートユーザーはルート以外のユーザーとしてログインして、ルートに`su`することになり、システムへのルートアクセスを獲得するためには2つのパスワードを知っている必要があります。「wheel group」PAM (Pluggable Authentication Module) を使用して、`su`へのアクセスを制限し、マシン上の1人の非ルートユーザーだけがルートに`su`できるようにします。対象ユーザーはarcsightユーザーとは別のユーザーにします。そうすることで、攻撃者はルートパスワードがわかっていて、何らかの方法でESMを介してアクセスを獲得した場合でも、ルートとしてログインすることはできません。
- 管理者/ルートアカウントの名前を変更して、ブルートフォース攻撃の実行を難しくします。

セキュリティに関する一般的なガイドラインとポリシー

ユーザーアカウント情報を盗むために使われる「ソーシャルエンジニアリング」の手口をシステムユーザーに教育します。HPEの従業員がユーザーのパスワードを要求することは決してありません。HPEの担当者が現場にいる場合は、システム管理者にパスワードの入力をお願いしています。また、HPEのチームが効率的に作業できるよう、必要に応じてパスワードを一時的に変更していただくようお願いする場合があります。

設定情報やログファイルをHPEに転送する場合、通信にはセキュアな手段 (アップロード用のSSLやメール用のPGPなど) を使用するようにユーザーを教育します。

システムの使用や誤使用の結果に関する法的な方針が記載されているログインバナーをセットアップします(ログインバナーの作成手順はプラットフォームによって異なります)。ArcSightコンソールにはカスタムログインバナーも表示できます。詳細については、HPE SSOサイトからCustomer Supportに連絡して確認してください。

セキュアなパスワードを選びます(1つのパスワードを2か所で使用しない、ランダムな文字シーケンスにする、8文字以上にする、数字と特殊文字を含んでいる)。パスワードの制限の詳細については、『Administrator's Guide』の第2章「Configuration」の「Managing Password Configuration」を参照してください。

パスワードは以下で使用されます。いずれかでパスワードが破られると、システムが危険にさらされます。

- すべてのデータベースアカウント (arcsight)
- ArcSightマネージャーを実行するシステム上の「arcsight」ユーザーとルートユーザー
- ESMで作成されるすべてのユーザー
- SSLキーストア
- ブートローダー (Linux)
- BIOS (x86システムのみ)
- RADIUSノードシークレット
- ArcSightマネージャーのLDAPパスワード (基本認証の場合のみ、かつ該当する場合)
- ArcSightマネージャーのActive Directoryドメインユーザーパスワード (該当する場合)

コンソールおよびSmartConnector上でSSLクライアント認証を有効にするために、PKIソリューションの購入と使用を検討します。

二要素認証ソリューション (RSA SecurIDなど) の購入と使用を検討します。

ESMが通信するすべてのサーバー (DNS、メール、RADIUSなど) のセキュリティが同等に強化されていることを確認します。

ファイアウォールと侵入検知システムを使用して、ArcSightマネージャーCORR_Engineが使用するネットワークを保護します。

インストールの準備

ソフトウェアESMのインストールファイルを実行する前に、システムを準備する必要があります。

システム要件

ESM 6.11.0のハードウェア要件は以下のとおりです。

	最小構成	ミッドレンジ構成	高性能構成
プロセッサー	8コア (推奨は16コア)	32コア	40コア
メモリ	48 GB RAM (推奨は64GB)	192 GB RAM	512 GB RAM
ハードディスク	6 x 600GBディスク (1.5TB) (RAID 10) 15,000RPM	20 x 1 TBディスク (10 TB) (RAID 10) 10,000RPM	12 TB (RAID 10) ソリッドステート

注意 : 「最小構成」の値は、低EPS (研究室の環境では一般的) でベースシステムコンテンツを実行しているシステムに適用します。大量のカスタマー作成リソースを実行しているシステム、または高いイベントレートを処理する必要があるシステムには使用しないでください。「ミッドレンジ構成」または「高性能構成」の仕様は、かなり大きなEPS負荷に加えて追加コンテンツやユーザーアクティビティに対応する本番環境に使用します。

パターン検出または多数のアセットやアクターを使用すると、システムの負荷が増え、検索やイベント処理のパフォーマンスが低下することになります。ESMのインストールのサイジングに関するサポートについては、HPEの営業またはフィールドの担当者にお問い合わせください。

大規模なリストが必要になる予定の場合は、システムがミッドレンジ以上の要件を満たしていることを確認してください。

マネージャーのホスト名の解決

ESMをインストールする前に、ホストマシンのホスト名が解決可能であることを確認してください。ホスト名を解決できない場合、マネージャーのセットアップは正常に完了しません。`ping`を使用してホスト名を確認し、問題を解決して、マネージャーのセットアップ中にエラーが発生しないようにします。

127.0.0.1のローカルホストへのマッピング

IPアドレス127.0.0.1が`/etc/hosts`ファイルで`localhost`に解決されていることを確認してください。解決されていない場合、ESMのインストールは失敗します。これは、IPv4およびIPv6システムに適用されます。

モニター要件

ArcSightコマンドセンターを表示するには、少なくとも1450ピクセルの幅があるモニターを使用します。これは、すべてのトップメニュー項目をはみ出さずに表示するために必要な最小の幅です。この最小幅は、大きなモニターで、ブラウザーウィンドウのサイズを縮小するときにも適用されます。

サポート対象のプラットフォーム

ESM6.11.0は、64ビットのRed Hat Enterprise LinuxおよびCentOSでサポートされています。サポートされるバージョン番号については、『HPE ArcSight ESM Support Matrix』を参照してください。このドキュメントは、Protect 724 (https://www.protect724.hpe.com) からダウンロードできます。ESMは、少なくともインストール時に「Web Server」オプションを使用し、「互Compatibility Libraries」と「Development Tools」を追加して、インストールしてください。ESMはオペレーティングシステムとバージョンの影響を受けます。

注:

- GUIモードで製品をインストールするには、X Windowシステムパッケージをインストールします。X Windowの使用は任意です。使用する場合は、RHELまたはCentOS用の `xorg-x11-server-utils-7.5-13.el6.x86_64`以降のバージョンを使用してください。X Windowを使用しない場合は、コンソールモードでESMをインストールできます。
- インストール時には、XFSおよびEXT4ファイルシステム形式がサポートされています。
- ESMは、最初にインストールされたファイルシステムに自動で設定されます。インストール後は、アップグレードの場合でもファイルシステムの種類を変更することはできません。
- `atd`サービスは常時実行している必要があります。ESMのインストールの最後になっても、このサービスがまだ実行していない場合は、`setup_services.sh`コマンドを実行すると起動します。
- RHELまたはCentOSをインストールすると、特定のオプションが提示されます。**Web Server**、**Compatibility Libraries**、および**Development Tools**オプションを選択してください。

インストールパッケージのダウンロード

ESM 6.11.0インストールパッケージは、HPEのサイトのhttps://softwaresupport.hpe.com/からダウンロードできます。`ArcSightESMSuite-6.11.0.xxxx.0.tar`ファイルをダウンロードして、ESMをインストールするシステムにコピーします。ファイル名のxxxxの部分は、ビルド番号を表しています。

HPEが提供するデジタル公開鍵により、お客様が受け取る署名付きのソフトウェアの提供元が確かにHPEであり、第三者による改ざんが行われていないことを検証できます。

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

HPE Software Depotから.tarファイルをダウンロードしたら、注文後にHPEからのメールに含まれているElectronic Delivery Receiptの指示に従い、ライセンスの調達を開始します。

システムの準備

1. rootユーザーでログインします。
2. 以下のコマンドを実行して、ファイルを解凍します。
   `tar xvf ArcSightESMSuite-6.11.0.xxxx.0.tar`
   `ArcSightESMSuite-6.11.0.xxxx.0.tar`ファイルを解凍すると、ファイルの解凍先にある`Tools`というサブディレクトリに`prepare_system.sh`スクリプトが格納されます。
3. `prepare_system.sh`を実行します。
4. tarファイルから抽出されたすべてのファイルとフォルダーの所有権を変更して、arcsightユーザーに所有権を割り当てます。
5. システムを再起動します。
6. 正常に実行されたことを確認します。rootユーザーとしてログインし、次のコマンドを実行します。
   `ulimit -a`
   次の2行を確認します。
   `open files 65536`
   `max user processes 10240`

開いたままにしておくTCPポート

ソフトウェアESMの場合は、インストールの前に、システム上の次のポートを開き(開いていない場合)、他のプロセスがポートを使用していないことを確認します。

外部の受信接続用のポート:

8443/tcp
9000/tcp
694/udp (HAの場合)
7789/tcp (HAの場合)
22/tcp (ssh)

コンポーネント間の通信用に内部で使用されるTCPポート:

1976、28001、2812、3306、5555、6005、6009、7777、7778、7779、7780、8005、8009、8080、8088、8089、8666、8766、8808、8880、8888、8889、9000、9095、9090、9123、9124、9999, 45450

タイムゾーンパッケージのインストール

ESMでは、タイムゾーンの変更や標準時間と夏時間の変更を処理するためにタイムゾーンパッケージを使用します。ESMのインストール時、インストールされているオペレーティングシステムのタイムゾーンパッケージが正しいものであるかがチェックされます。正しくない場合は、インストーラーを終了してタイムゾーンパッケージの最新アップデートをインストールするか、ESMコンポーネントのタイムゾーンアップデートはスキップしてESMのインストールを続行することができます。タイムゾーンのアップデートパッケージをインストールすることをお勧めします。

RHEL 7.3およびCentOS 7.3の場合は、`tzdata-2016g-1.el7.noarch.rpm`以降のバージョンの`rpm`パッケージを使用します。

RHELまたはCentOS 7.3の場合

RHELまたはCentOS 7.3にパッケージをインストールするには、次のコマンドを使用します。

```
rpm -Uvh <package>
```

次のコマンドを使用して、タイムゾーンの設定を確認します。

```
timedatectl
```

タイムゾーンが設定されていないか、目的のタイムゾーンでない場合は、次のコマンドを使用して別のタイムゾーンを指定します。

```
timedatectl set-timezone <time_zone>
```

例:

```
timedatectl set-timezone America/Los_Angeles
```

RHELまたはCentOS 6.8の場合

RHELまたはCentOS 6.8にパッケージをインストールするには、次のコマンドを使用します。

```
rpm -Uvh <package>
```

次のコマンドを実行して、`/etc/localtime`リンクが有効なタイムゾーンを指していることを確認します。

```
ls -altrh /etc/localtime
```

タイムゾーンが正しい場合は、以下のような応答が得られます。ここで、<ZONE>は米国/ロサンゼルスのようなタイムゾーンです。

```
lrwxrwxrwx.1 root root 39 Nov 27 08:28 /etc/localtime ->
/usr/share/zoneinfo/<ZONE>
```

注: /etc/localtimeリンクが有効なタイムゾーンを指していない場合、ESMのインストールは停止します。この場合、リンクを有効なタイムゾーンに手動で設定する必要があります。

この時点でインストールしない場合

必要なtzdata rpmパッケージをインストールしないでESMのインストールを完了した場合は、ESMのインストールが完了した後にタイムゾーン更新を設定できます。正しいtzdataパッケージをダウンロードしてインストールし、/etc/localtimeリンクを正しく設定してから、以下の手順に従います。(これはESMのインストールが完了した後の手順です)。

1. arcsightユーザーで、すべてのarcsightサービスをシャットダウンします(これは重要です)。次のコマンドを実行します。
   ```
   /etc/init.d/arcsight_services stop all
   ```
2. rootユーザーで、以下のコマンドを実行します(実際には1行です) 。
   ```
   /opt/arcsight/manager/bin/arcsight tzupdater /opt/arcsight /opt/arcs
   ight/manager/lib/jre-tools/tzupdater
   ```
3. 次のコマンドを使用して、すべてのarcsightサービスを開始します。
   ```
   /etc/init.d/arcsight_services start all
   ```

/etc/systemd/logind.confへのRemoveIPC = noの追加 - RHELおよびCentOS 7.3のみ

プリフライトチェックが失敗した場合は、/etc/systemd/logind.confファイルのRemoveIPC = noプロパティの値を追加するか、編集します。

値を追加するには:

1. rootユーザーとして、/etc/systemd/logind.confファイルを編集します。
2. RemoveIPCを検索し、このプロパティが1つしかないことを確認します。
3. プロパティが存在する場合は、編集して値を**no**にします (存在しない場合は、プロパティを追加します)。
   ```
   RemoveIPC=no
   ```
4. 次のコマンドを実行します。
   ```
   systemctl restart systemd-logind.service
   ```

ディレクトリサイズの設定

/tmpディレクトリが存在するパーティションに少なくとも5 GBの領域があることを確認します。

/opt/arcsightディレクトリが存在するパーティションに少なくとも50 GBの領域があることを確認します。

CORR-Engineのサイジングのガイドライン

ESM 6.11.0のインストール時には、CORR-Engineのデフォルトのストレージサイズは、以下の表に記載されているデフォルト値に従い、使用しているハードウェアに基づき自動的に計算されます。表の内容は、推奨サイジングに関するガイドラインです。ウィザードの[CORR-Engine Configuration]パネルでは、すべてのデフォルトのストレージサイズを変更できますが、ストレージのサイズを変更する場合は、最小値と最大値を考慮する必要があります。

注: オフラインアーカイブからオンラインアーカイブにインポートされるイベントは、合計12 TB (またはライセンスにより決定) のストレージ制限の一部として計算されます。オフラインアーカイブをオンラインアーカイブに戻したために、保存容量の制限を超えてしまったということは避けなければなりません。オフラインアーカイブをオンラインにする際には慎重に判断し、作業を終えたら再度オフラインに戻してください。

システムストレージ - リソース、トレンド、リストなど、イベント以外のストレージ

イベントストレージ - イベントのストレージ

イベントアーカイブサイズ - オンラインイベントのアーカイブ

	推奨	最小値	最大値
システムストレージサイズ	デフォルトは、使用可能スペースの約6分の1で、最小値は3 GB、最大値は1,500 GBです。インストールの際には、デフォルトを受け入れることをお勧めします。	3 GB	1,500 GB
イベントストレージサイズ	インストール時に表示される使用可能スペースの約3分の2を指定します。	10 GB	12 TB
イベントアーカイブサイズ	システムストレージとイベントストレージを割り当てた後の残りの領域を指定することができます。	1 GB	制限は、ファイルシステムのサイズを前提としています。

`/opt/arcsight`パーティションの10%は、システム使用領域として予約されています。

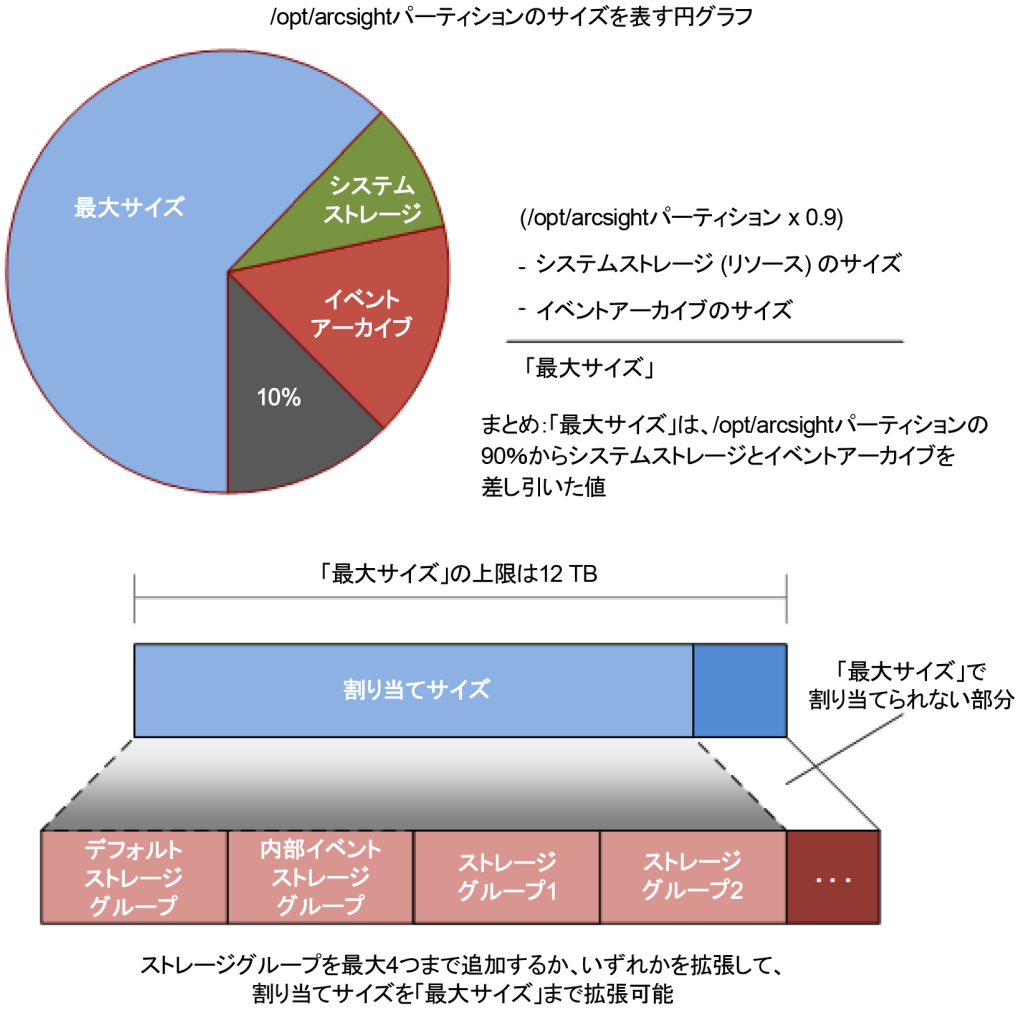
インストール時には、`/opt/arcsight`パーティションのサイズは「Available Space」として表示され、そのサイズの10%未満が「Usable Space」として予約されます。イベントストレージボリュームの最大サイズは、以下の式を使用して計算されます。
イベントストレージの最大値 = `/opt/arcsight`パーティション x `0.9` - システムストレージ - イベントアーカイブ。

インストール後、割り当て済みのイベントストレージ領域は、デフォルトのストレージグループ、およびインストーラーによってサイズが初期設定されている内部ストレージグループで構成されます。これらのストレージグループによって、イベントストレージボリュームの最大サイズが満たされることはありません。割り当て済みのイベントストレージのサイズがイベントストレージボリュームの最大サイズに達するまで、これらのストレージグループのサイズを拡張するか、または独自

のストレージグループを4つまで追加することができます。ArcSightコマンドセンターのユーザーインターフェイスを使用して、ストレージグループのサイズを追加または変更します。

ArcSightコマンドセンターで **[管理] > [ストレージとアーカイブ]** を選択して、ストレージの割り当てを確認して変更します。詳細については、『ArcSight Command Center User's Guide』を参照してください。

以下の図には、設定ウィザードやArcSightコマンドセンターのユーザーインターフェイスで使用されるさまざまな条件が説明されています。



各言語のUTFファイルのエクスポート

以下のコマンドを実行します。

```
export LC_ALL=[language].UTF-8
```

[language]は、以下のいずれかです。
en_US (英語)
zh_CN (簡体字中国語)

zh_TW (繁体字中国語)
ja_JP (日本語)
fr_FR (フランス語)
ko_KR (韓国語)
ru_RU (ロシア語)

例: export LC_ALL=en_US.UTF-8

インストーラーの起動

インストールは、arcsightユーザーでログインしている間に開始します。

ArcSightESMSuite.binファイルに実行パーミッションを付与します (まだ付与されていない場合)。付与する場合は、以下のコマンドを入力します。

```
chmod +x ArcSightESMSuite.bin
```

以下のインストールファイルを実行します。

```
./ArcSightESMSuite.bin -i console
```

(またはX Windowを使用しているGUIモードの場合は、./ArcSightESMSuite.bin)

インストールが開始されます。

注:

- GUIモードで実行する場合は、X Windowを実行する必要があります。X Windowが実行中でない場合、インストーラーは自動的にコンソールモードで実行されます。GUIモードは完全にオプションです。
- コンソールモードで実行する場合は、X Windowが実行中でないことを確認します。GUIモードで必要な情報はコンソールモードと同じなので、個別に記述することはありません。
- このインストールのログファイルは、/home/arcsightディレクトリに表示されます。

次のトピックでは、インストーラーの起動後を扱います。

インストールファイルの実行

次の手順では、ESMインストーラーについて説明します。

1. [**Introduction**] メッセージを読み、**Enter**キーを押します。
2. [**License Agreement**] パネルで、**Enter**を押して契約に目を通します。GUIモードでは、[I accept the terms of the License Agreement] チェックボックスは、契約テキストの最後までスクロールするまでは無効になっています。使用許諾契約に同意する場合は、「**y**」と入力して**Enter**キーを押します。

3. [**Special Notice**] の内容を読み、**Enter**キーを押します。
4. [**Choose Link Location**] で、インストーラーがこのインストールのリンクを配置する場所の番号を入力し、**Enter**キーを押します。
5. [**Pre-Installation Summary**] の内容を確認します。**[Enter]**を入力して続行します。

   [**Installing**] の下に進行状況バーが表示されます。

Suite Installerによって各コンポーネントがインストールされます。

- コンソールモードでは、コンポーネントがインストールされた後に、「**Installation Complete**」と表示されます。**Enter**キーを押して、インストーラーを終了します。次のトピック「コンソールモードでの設定ウィザードの起動」(37ページ)に進んでください。
- GUIモードでは、コンポーネントがインストールされた後に、設定ウィザードのGUIが自動的に開きます。ESMの設定の詳細については、「設定ウィザードの使用」(37ページ)を参照してください。

> **注:** GUIモードでエラーまたは問題を報告するダイアログボックスが表示され、アクションボタンに「**Quit**」と表示された場合は、[**Quit**] ボタンを使用します。ダイアログの右上隅にある**X**を使用すると、プロセスは中止されませんが、報告されたエラーのため正常に完了することができません。

コンソールモードでの設定ウィザードの起動

ソフトウェアESMをGUIモードでインストールする場合、またはESM Expressをインストールする場合は、設定ウィザードが自動的に起動し、初期インストールのこの手順をスキップできます。

コンソールモードでコマンドラインからソフトウェアESMをインストールする場合、Suite Installerの完了時にインストールが停止しますが、設定ウィザードは自動的に実行されません。以下のコマンドを実行して、設定ウィザードを手動で開始してください。

```
/opt/arcsight/manager/bin/arcsight firstbootsetup -boxster -soft -i console
```

設定ウィザードの使用

アプライアンスにインストールすると、設定ウィザードが自動的に開始します。(設定ウィザードを開始するために、手動でコマンドを入力する必要はありません)ソフトウェアESMをGUIモードでインストールすると、設定ウィザードが自動的に開始します。コンソールモードのソフトウェアESMでは、次のコマンドを使用して手動で設定ウィザードを開始します。

```
/opt/arcsight/manager/bin/arcsight firstbootsetup -boxster -soft -i console
```

1. Welcomeメッセージが表示されます。ライセンスファイルにアクセスできる場合は、「**yes**」と入力して続行します。
2. [**Language Options**] で、インターフェイスの表示言語を選択します。**Enter**キーを押し

て続行します。

3. [**CORR-Engine Password**] の下で、**Enter**キーを押して難読化されたパスワードを使用して続行するか、「**no**」と入力して**Enter**キーを押し、パスワードを画面に表示させます。
4. [**CORR-Engine Password]** の下で、CORR-Engine用のパスワードを設定し、確認のために再入力します。**Enter**キーを押します。パスワード制限の詳細は、『ESM Administrator's Guide』の「Configuration」の章で「Managing Password Configuration」を参照してください。
5. [**CORR Engine Configuration**] で、CORR-Engineストレージ割り当て情報を入力し、**Enter**キーを押します。

   System Storage Size - リソースの格納領域とは別に設定されるストレージ領域のサイズ

   Event Storage Size - イベントの格納領域とは別に設定されるストレージ領域のサイズ

   Online Event Archive Size - イベントアーカイブ用のディスク領域の最大ギガバイト数。これは、デフォルトのオンラインイベントアーカイブにのみ適用されます。

   Retention Period - イベントがシステムからパージされる前にイベントを保持しておく期間
6. [**Notification Emails**]で、次の電子メールアドレスを指定します。

   Error Notification Recipient: マネージャーがダウンした場合や他の問題が発生した場合に、メール通知を受信する電子メールアカウントのメールアドレスを1つ指定します。電子メールアドレスをさらに指定する必要がある場合は、『ESM Administrator's Guide』の「Running the Manager Configuration Wizard」の説明に従って、マネージャー設定ウィザードを使用して指定できます。

   From email address: 通知の送信者に使用されるメールアドレス。

   値が正しい場合は、「**yes**」と入力し、**Enter**キーを押して続行します。電子メールは、システムが次の状態を検出したときに送信されます。

   - サブシステムのステータスが変更された。変更の内容と、変更を行ったユーザーが電子メールに記されます。
   - レポートが正常にアーカイブされた。
   - アカウントのパスワードがリセットされた。
   - アーカイブレポートの生成が失敗した。
   - 通知先で受信された通知が多すぎる。
   - イベントアーカイブの場所が上限に達した。イベントアーカイブを別の場所に移動して、スペースを解放するように求められます。
   - ユーザーがArcSightコンソールの設定を電子メールで送信することを選択した。
   - ユーザーがパーティションアーカイブコマンドを送信した。

- 十分なスペースがないため、アーカイブが失敗する。
- データベースへの接続に失敗した。

7. [**License File**] に、ダウンロードしたライセンスファイルのパスとファイル名を入力し、**Enter**キーを押します。
8. [**Select the Product Mode**] でデフォルトモードでインストールするか、FIPSモードでインストールするかを選択します。**Enter**キーを押して続行します。

注意:

- 本製品をFIPSモードでインストールすることを選択した場合は、コンソールもFIPSモードでインストールしてください。コンソールをFIPSモードでインストールする方法については、「FIPSモードでのArcSightコンソールのインストール」(85ページ)を参照してください。
- FIPSモードでソフトウェアを構成した場合は、再インストールしないと、デフォルトモードに切り替えることはできません。
- デフォルトモードのインストールからFIPS-140-2モードへの切り替えはサポートされています。切り替える必要がある場合は、『Administrator's Guide』で手順を参照してください。
- ESMのデフォルトでは、自己署名証明書が使用されます。CA署名証明書を使用する場合は、設定ウィザードが正常に完了した**後**、CA署名証明書を手動でインポートする必要があります。CA署名証明書の使用方法の詳細については、『ESM Administrator's Guide』を参照してください。

9. FIPSモードを選択した場合は、選択内容を確認します。FIPSモードを選択していない場合は、Manager Informationのステップにスキップします。
10. [**Select the Cipher Suite Options**] パネルでFIPSモードを選択した場合は、暗号スイートを選択します。

    Suite Bでは、2つのセキュリティレベル(128ビットと192ビット)が定義されます。この2つのセキュリティレベルは、Suite Bによって提供される全体的なセキュリティの代わりに使用されるAES (Advanced Encryption Standard) のキーサイズに基づいています。128ビットのセキュリティレベルでは、128ビットのAESキーサイズが使用されますが、192ビットのセキュリティレベルでは、256ビットのAESキーサイズが使用されます。キーサイズが大きくなるとセキュリティも強化されますが、時間とリソース(CPU)消費の点で計算コストも高くなります。ほとんどのシナリオでは、128ビットのキーサイズで十分です。
11. [**Manager Information**] で、マネージャーのホスト名を入力し、管理ユーザーのユーザーIDとパスワードを設定して、**Enter**キーを押します。

注意:

- マネージャーのホスト名は、マネージャーがインストールされているマシンのIPアドレス(IPv4のみ)、または完全修飾ドメイン名です。この名前は、すべてのクライアント(ArcSightコンソールなど)がマネージャーと接続するために指定する名前です。柔軟性を確保するために、IPアドレスの代わりに完全修飾ドメイン名を使用することを推奨します。
- [**IP Version**]の選択(IPv4またはIPv6)は、アプライアンスなどのデュアルスタックマシンがある場合に表示されます。このオプションが表示された場合、選択内容は次のような影響を及ぼします。
  - ホスト名が指定されている場合、サードパーティのソフトウェアが使用するIPアドレスを制御します(例：マネージャーセットアップの電子メールサーバー)。
  - ホスト名が指定されている場合、ピアリングページで試行されるIPアドレスを制御します。
  - マネージャーアセットに対してIPv4アドレスまたはIPv6アドレスのどちらを選択するかを制御します。
- 複数のホスト名が存在する可能性があり、デフォルトはhostnameコマンドで返されたものと同じではない可能性があります。高可用性モジュールを使用している場合は、両方のサーバー(プライマリとセカンダリ)に共通のサービスホスト名をマネージャーのIPまたはホスト名として使用します。それ以外の場合は、コネクター、コンソールおよびその他のクライアントの設定に便利で、正常に機能すると考えられるホスト名を選択します。完全修飾ドメイン名を使用することが、最善の方法であることに注意してください。
- DNSサーバー上でホスト名を使用しない場合は、`/ etc / hosts`ファイルに静的ホストエントリを追加して、ホスト名をローカルで解決してください。
- マネージャーのホスト名は、自己署名証明書を生成するために使用されます。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。
- マネージャーではデフォルトで自己署名証明書が使用されますが、必要に応じて、CA署名証明書を使用するように切り替えることができます。切り替えはインストール後に行います。手順については、『ESM Administrator's Guide』を参照してください。

12. Event Brokerへの接続をセットアップするかどうかを選択します(Event BrokerがESMの実装の一部である場合)。Event BrokerをFIPSモードでセットアップする必要がある場合は、「Event Brokerへのアクセスの設定 - FIPSモード(サーバー認証のみ)(オプション)」(89ページ)を参照してください。

    クライアント認証がEvent Brokerで有効になっている場合は、「Event BrokerとESM間のSSLクライアント側認証の設定 - 非FIPSモード」(47ページ)または「Event BrokerとESMの間のSSLクライアント側認証の設定 - FIPSモード」(90ページ)を参照してください。

    接続を設定する場合は[**Yes**]を選択し、続行する場合は[**No**]を選択します。[**Yes**]を選択した場合は、以下を指定します。

a. **Host: Port(s)**: Event Broker内のノードのホストとポートの情報を入力します。マスターノードだけでなく、複数のノード環境内のすべてのノードのホスト (ホスト名またはIPアドレス) とポートの情報を含めます。入力する内容は、カンマ区切りのリストです (例: <host>:<port>,<host>:<port>)。Event Brokerが受け入れることができるのは、ESMからのIPv4接続だけであることに注意してください。

b. **Topic to read from**: Event Brokerから購読するトピックを指定します。これにより、データソースが決定されます。『Event Broker管理者ガイド』の「Event Brokerのトピックの管理」の章を参照してください。

c. **Path to the Event Broker root cert**: ESMは、TLS経由でEvent Brokerと通信します。これを有効にするには、Event Brokerのルート証明書をESMのクライアントのトラストストアにインポートする必要があります。
Event Brokerのルート証明書を、Event Brokerマシン (`/opt/arcsight/kubernetes/ssl/ca.crt`) からESMマシン上のローカルフォルダーにコピーします。証明書のパスを入力して [**Next**] をクリックすると、Event Brokerのルート証明書がESMのクライアントのトラストストアにインポートされ、Event Brokerへの接続が検証されます。問題がある場合は、エラーまたは警告メッセージが表示されます。メッセージが表示されず、ウィザードが次の画面に進んだ場合、Event BrokerとESMの間の接続が正常に検証されたことを意味します。

13. ArcSight Investigateをセットアップするかどうかを選択します。統合を有効にする場合は [**Yes**] を選択し、続行する場合は [**No**] を選択します。[**Yes**] を選択した場合は、ArcSight Investigateの展開の [**Search URL**] を指定します。
14. [**Packages**] パネルで**Enter**キーを押して続行します。それ以外の場合は、使用を許可されているオプションパッケージを選択します。これらのオプションパッケージに加えて、ArcSightマネージャーに自動的にインストールされるデフォルトの標準コンテンツパッケージがあります。これらのデフォルトパッケージは、システムヘルスと状態の運用に不可欠なものであり、すぐに使用してネットワークを監視し、保護することができます。

    パッケージの詳細については、『ArcSight Administration and ArcSight System Standard Content Guide』を参照してください。
15. **About to Configure ESM**の下で

    注意: 「**yes**」と入力して**Enter**キーを押すと、製品は指定されたとおりにインストールされます。

16. 「**Configuration Completed Successfully**」と表示されたら、「**yes**」と入力し、**Enter**キーを押して終了します。
17. **重要:** このステップは、サービスを起動するために必要になります。ルートユーザーでログインし、以下のスクリプトを実行して必要なサービスをセットアップします。

    ```
    /opt/arcsight/manager/bin/setup_services.sh
    ```

    インストールが完了したら、ストレージボリュームの場所とサイズを確認して、必要な変更を加えます。変更は、ArcSightコマンドセンターで行うことができます。ストレージボリューム

に関する詳細については、『ArcSight Command Center User's Guide』の「Administration」の章の「Storage and Archive」を参照してください。

設定ウィザードは、[About to Configure ESM v6.11.0] という最初の構成画面が表示される**前**の任意の時点で終了した場合のみ、手動で再実行できます。詳細については、「ESM設定ウィザードの再実行」(44ページ)を参照してください。

タイムゾーンアップデートエラーの対応

インストーラーによりESMコンポーネントのタイムゾーン情報がアップデートされる際に発生する可能性があるエラーは以下の2つです。

1. オペレーティングシステムのタイムゾーンバージョン2014fまたはそれ以降のrpmがインストールされていない。
2. /etc/localtimeリンクが無効または存在しないタイムゾーンを指している。

正しいタイムゾーンパッケージが使用できないか、または正しくセットアップされていない場合でも、インストールは続行できます。続行する場合は、インストール後にESMコンポーネントのタイムゾーン情報をアップデートできます。

正しいパッケージをダウンロードおよびインストールしていること、リンクが正しく設定されていることを確認してから、以下の手順を実行します。

1. arcsightユーザーで、すべてのarcsightサービスをシャットダウンします(これは重要です)。次のコマンドを実行します。
   ```
   /etc/init.d/arcsight_services stop all
   ```
2. rootユーザーで、以下のコマンドを実行します(実際には1行です) 。
   ```
   /opt/arcsight/manager/bin/arcsight tzupdater /opt/arcsight /opt/arcs
   ight/manager/lib/jre-tools/tzupdater
   ```
3. 次のコマンドを使用して、すべてのarcsightサービスを開始します。
   ```
   /etc/init.d/arcsight_services start all
   ```

ESMのアンインストール

以下の手順を使用して、ESMをアンインストールします。

1. rootユーザーとしてログインします。
2. 以下のコマンドを実行します。
   ```
   /opt/arcsight/manager/bin/remove_services.sh
   ```
3. arcsightユーザーでログインします。
4. 実行中のすべてのarcsightプロセスをシャットダウンします。

実行中のarcsightプロセスを確認するには、以下のコマンドを実行します。

```
ps -elf | grep "/opt/arcsight"
```

実行中のarcsightプロセスをシャットダウンするには、以下のコマンドを実行します。

```
kill -9 <process_id_number>
```

5. 本製品のインストール時にリンクを作成したディレクトリからアンインストーラープログラムを実行します。リンクを作成していない場合は、/opt/arcsight/suite/UninstallerDataディレクトリから以下のコマンドを実行します。

   ```
   ./Uninstall_ArcSight_ESM_Suite_6.11.0
   ```

   あるいは、/home/arcsight (またはショートカットリンクをインストールした) ディレクトリから以下のコマンドを実行することができます。

   ```
   ./Uninstall_ArcSight_ESM_Suite_6.11.0
   ```

6. /tmpディレクトリと/opt/arcsightディレクトリに、ESM関連のファイルが含まれていないことを確認します。含まれている場合は、以下の手順を実行します。
   a. arcsightユーザーでログインしている間に、すべてのarcsightプロセスを強制終了します。
   b. /opt/arcsight/および/tmpディレクトリ配下にあるすべてのarcsight関連の残存ファイルとディレクトリを手動で削除します。
   c. インストール時に作成されたすべてのリンクを削除します。

第4章: インストール後の考慮事項

このセクションには、インストールおよび設定ウィザードの再実行に関する情報が含まれています。

インストーラーの再実行

ソフトウェアESMの場合、「File Delivery Complete:」が表示される前に、何らかの理由によりインストールが中断されてプロセスが終了した場合は、以下の手順を実行します。

1. /tmpディレクトリからすべてのinstall.dir.xxxxをすべて削除します。
2. /opt/arcsightディレクトリにあるすべてのディレクトリとファイルを削除します。
3. インストーラーを保存した場所から、インストーラーを再実行します (./ArcSightESMSuite.bin.)。

ESM設定ウィザードの再実行

実際の構成が開始される**前**に任意の時点でウィザードを終了した場合に限り、手動でウィザードを再実行できます。構成が開始されるセクションの名前は、[About to Configure ESM] です。

構成が開始される前に何らかの理由でウィザードをキャンセルしたか、またはエラーが発生した場合は、手動でウィザードを再実行できます。

1. 設定ウィザードを再実行するには、次のコマンドを使用します。

   ```
   rm /opt/arcsight/manager/config/fbwizard*
   ```

2. First Boot Wizardを実行するには、arcsightユーザーでログインしている間に /opt/arcsight/manager/binディレクトリから以下のいずれかのコマンドを実行します。

   GUIモードの場合 (ソフトウェアESMのみ)

   ```
   ./arcsight firstbootsetup -boxster -soft
   ```

   コンソールモードの場合

   ```
   ./arcsight firstbootsetup -boxster -soft -i console
   ```

   ソフトウェアESMの場合、コンソールモードでFirst Boot Wizardを実行するときにX Windowが実行されていないことを確認してください (X Windowはアプライアンスにはインストールされていません)。

構成の段階で障害が発生した場合は、ESMをアンインストールしてから再インストールします。アプライアンスの場合、アプライアンスを工場出荷時の設定に復元してやり直します。「アプライアンスの工場出荷時設定の復元」(104ページ) を参照してください。

英語以外の環境でESMのレポートを表示するためのセットアップ

文字列ベースのイベントフィールドに含まれる国際文字をクエリで取得できるようにするには、国際文字を正しく格納する必要があります。このセクションのプロセスに従うと、ESMで国際文字を正しく格納して認識することができます。

マネージャーでのレポートのセットアップ

この手順は、国際文字を使用するレポートをPDF形式で出力する予定の場合のみ実行する必要があり、ARIALUNI.TTFフォントファイルを購入する必要があります。

1. マネージャーのホストで、ARIALUNI.TTFフォントファイルを次のようなフォルダーに格納します。例:

   ```
   /usr/share/fonts/somefolder
   ```

2. デフォルトでは/opt/arcsight/manager/reports/ディレクトリにある、ESMレポートのプロパティファイルsree.propertiesを変更します。

   以下の行を追加します。

   ```
   font.truetype.path=/usr/share/fonts/somefolder
   ```

   ファイルを保存します。
3. 以下のコマンドを実行して、マネージャーを再起動します。

   ```
   /etc/init.d/arcsight_services restart manager
   ```

4. ArcSightコンソールで、レポートテンプレートを含む、すべてのレポートエレメントでArial Unicode MSフォントを選択します。この点は次のトピックを参照してください。

コンソールでのレポートのセットアップ

コンソールとコンソールホストマシンの優先設定を設定します。

1. コンソールホストのオペレーティングシステムにArial Unicode MSフォントをインストールします (インストールされていない場合)。
2. デフォルトでは<ARCSIGHT_HOME>/current/bin/scriptsディレクトリにある以下のスクリプトを編集します。

Windowsの場合: `console.bat`を編集します。

Linuxの場合: 編集は不要です。コーディングは正しく設定されています。

`ARCSIGHT_JVM_OPTIONS`セクションを探して、以下のJVMオプションを追加します。

```
" -Dfile.encoding=UTF8"
```

3. ArcSightコンソールの [Preferences] メニューで、Arial Unicode MSをデフォルトのフォントとして設定します。

   [Edit] > [Preferences] > [Global Options] > [Font] の順に選択します。

   Windowsの場合: ドロップダウンから [`Arial Unicode MS`] を選択します。

   Linuxの場合: 「`Arial Unicode MS`」と入力します。
4. 『ArcSight Console User's Guide』の「Using Report Templates」の説明に従い、レポートに使用するフォントの優先設定を設定します。

サーバーの性能の向上

アプライアンスの場合、このトピックは無視してかまいません。アプライアンスは最高のパフォーマンスが得られるようにすでにセットアップされています。ユーザーが所有するハードウェア上のソフトウェアESMの場合、BIOSを以下のようにチューニングすることでサーバーの性能を向上できます。

- **HyperThreading** - 無効にします。この設定は、HyperThreadingをサポートしているすべてのインテルプロセッサーに存在しており、最新のサーバークラスのプロセッサーにはこの設定があります。AMDプロセッサーには同等の設定はありません。
- **Intel VT-d** - 無効にします。この設定はインテルプロセッサーに固有の設定で、最新のサーバークラスのプロセッサーに含まれている傾向にあります。AMDには、AMD-Viという名前の同等機能があります。
- **HPE Power Regulator** -「Static High Performance」に設定します。この設定にすると、システムが負荷の低下を検知した際、CPUは電力節約のために速度を落とすことなく、常に高速で動作します。ほとんどの最新のCPUには同等の設定があります。
- **Thermal Configuration** - 「Increased cooling」に設定します。この設定にすると、サーバーのファン速度が速くなり、CPUを常に高速で動作しているために上昇した温度に対応できるようになります。
- **Minimum Processor Idle Power Package State -** この設定にすると、CPUのCステート(CPUのさまざまな省電力状態)が使用されなくなります。Cステートはすべてのサーバーに存在するため、ほとんどのサーバーに同様の設定があります。
- **HPE Power Profile** - 「`Maximum Performance`」に設定します。HPE以外のサーバーには同等の設定はほとんどありませんが、いくつかの個別の設定は存在する場合があります。

  この設定は以下のように変更されます。

- QPI Link Power Management (CPUの物理ソケット間のリンク) が無効になる
- PCIeのサポートが強制的にGen 2になる
- Cステートがこのプロファイルの一環として無効になる
- この設定では、CPUの低速の設定も無効になるため、CPUは常に高速で動作する

ブラウザーのTLSプロトコルの設定

ブラウザーをFIPS Webサーバーに接続するには、TLSをサポートするようにブラウザーを設定する必要があります。SSLプロトコルはサポートされていません。ブラウザーをArcSightコンソールオンラインヘルプのために使用したり、ArcSightコマンドセンターに接続したりする前に、TLSに対応させる必要があります。

すべてのSSLプロトコルが無効にされ、TLSプロトコルが有効にされていることを確認します。たとえば、Microsoft Internet Explorer (IE) の場合:

1. **[ツール] > [インターネットオプション]** を選択します。
2. **[詳細設定]** タブを選択します。
3. 下にスクロールして **[セキュリティ]** セクションに移動します。
4. **[SSL 2.0を使用する]** および **[SSL 3.0を使用する]** の選択を解除します。
5. TLSの各オプションを選択します。詳細については、「TLSのサポート」(83ページ) を参照してください。

他のブラウザー (および他のバージョンのIE) には、この設定のためのメニュー項目やオプションが異なる場合がありますので、ブラウザーのドキュメントを参照してください。

Event BrokerとESM間のSSLクライアント側認証の設定 - 非FIPSモード

Event Brokerでクライアント側認証を設定する前に、Event Brokerのルート証明書をESMトラストストアにインポートし、Event BrokerとESM間のSSLハンドシェイクを有効にする必要があります。

Event Brokerのルート証明書をESMマシンにインポートするには:

注: 以下の手順を実行してルート証明書をESMトラストストアにインポートする前に、Event Brokerの証明書がすでにESMにインポートされているかどうかを確認してください。インポートされていない場合は、次の手順を実行します。

1. Event Brokerマシンにログオンし、次の場所から証明書をコピーし、
   `/opt/arcsight/kubernetes/ssl/ca.crt`
   ESMマシン上の場所に格納します。
2. 次のarcsight `keytool`コマンドを使用して、ルートCA証明書をESMのクライアントトラストストアにインポートします。
   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientcerts -importcert -file <absolute path to certificate file> -alias <alias for the certificate>
   ```

Event BrokerとESM間でクライアント側認証を非FIPS (デフォルト) モードで有効にするには:

重要: クライアント側認証が機能するには、この手順のすべてのステップを完了する必要があります。必ずすべてのステップを実行してください。

1. Event Brokerが機能していること、およびクライアント認証がセットアップされていることを確認します。
2. arcsightユーザーとして、以下のコマンドを実行して、マネージャーを停止します。
   `/etc/init.d/arcsight_services stop manager`
3. `/opt/arcsight/manager/config/client.properties`が存在しない場合は、任意のエディターを使用して作成します。
4. キーストア`keystore.client`のストアパスワードを変更します。このパスワードは、デフォルトでは空白になっています。パスワードが空白になっていると、証明書をインポートすることができません。
   また、キーストア内の生成されたキー`services-cn`の空白のパスワードを、キーストアと同じパスワードに更新する必要があります。これを行うには、次のコマンドを実行します。
   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientkeys -storepasswd -storepass ""
   ```
   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。
   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientkeys -keypasswd -keypass "" -alias services-cn
   ```
   プロンプトが表示されたら、上の手順で入力したストアパスワードと同じパスワードを新しいパスワードとして入力します。
5. 次のコマンドを実行して、`config / client.properties`内のパスワードを更新します。

```
/opt/arcsight/manager/bin/arcsight changepassword -f
config/client.properties -p ssl.keystore.password
```

6. キーペアと証明書署名要求 (.csr) ファイルを生成します。キーペアを生成するときは、証明書の共通名 (CN) としてマネージャーホストの完全修飾ドメイン名を入力します。以下のコマンドを実行します。

   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientkeys -genkeypair –
   dname "cn=<your host's fully qualified domain name>, ou=<your
   organization>, o=<your company>, c=<your country>" -keyalg rsa -keysize
   2048 –alias ebkey -startdate -1d -validity 366
   ```

   ```
   /opt/arcsight/manager/bin/arcsight keytool -certreq -store clientkeys -
   alias ebkey -file ebkey.csr
   ```

   ebkey.csrは、csrが格納されている出力ファイルです。

7. Event Brokerのルート証明書で.csrに署名します。Event Brokerのルート証明書は、Event Brokerマシンの/opt/arcsight/kubernetes/sslにca.crtという名前で存在します。キーはca.keyという名前です。たとえば、次のコマンドは、ca.crtおよびca.keyが存在する場合、Event Brokerマシン上でも、openssl が機能する別のマシンでも実行できます。

   ```
   openssl x509 -req -CA <full path to ca.crt> -CAkey <full path to ca.key> -
   in <full path to the esm csr> -out <full path and file name for storing
   the generated cert> -days 3650 -CAcreateserial -sha256
   ```

   例:

   ```
   openssl x509 -req -CA /tmp/ca.crt -CAkey /tmp/ca.key -in /tmp/ebkey.csr -
   out /tmp/ebkey.crt -days 3650 -CAcreateserial -sha256
   ```

   すべてのファイルの場所は、絶対パスで指定する必要があります。

8. ESMマシンで、次のコマンドを実行して、署名付き証明書 (上記のopenssl コマンドの-outパラメーター) をインポートします。

   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientkeys -alias
   /tmp/ebkey -importcert -file <path to signed cert> -trustcacerts
   ```

   例:

   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientkeys -alias
   /tmp/ebkey -importcert -file ebkey.crt -trustcacerts
   ```

9. 設定が完了し、Event Brokerへの接続が正常に確立されたことを確認するには、managersetupを実行して、設定がエラーなく伝播されていることを確認します。
10. マネージャーを起動します。

    ```
    /etc/init.d/arcsight_services start manager
    ```

インストール後の次の手順

- **ArcSightコンソールのインストール**
  ArcSightコンソールをダウンロードして、サポート対象のプラットフォームにインストールしま

す。詳細については、「コンソールのインストール」の章を参照してください。パフォーマンス上の理由から、ArcSightコンソールは、ESMをインストールしたマシンとは別のマシンにインストールしてください。

- **ArcSightコマンドセンターへのアクセス**
  ArcSightコマンドセンターの使用に関する詳細については、『ArcSight Command Center User's Guide』を参照してください。
- **リリースノートの確認**
  このリリースのリリースノートは、Protect 724から入手できます。
- **ユースケースのダウンロード**
  すぐに設定して実行できるように、HPEでは、https://saas.hpe.com/marketplace/arcsightからダウンロード可能なセキュリティユースケースパッケージを提供しています。これらのパッケージは、ネットワークシステム(IDS/IPS、VPN、ファイアウォールなど)の基本的なセキュリティの監視を可能にし、異常なトラフィックや不審な送信トラフィックなど、セキュリティの観点で重大な懸念のあるイベントストリームの監視と分析を行うパッケージを提供します。
- **アプライアンスへのリモートアクセス**
  オプションとして、応答不能になったアプライアンスにカスタマーサポートがアクセスしてトラブルシューティングできるように、アプライアンスにアウトオブバンドリモートアクセスを設定できます。すべてのアプライアンスモデルには、HPE Integrated Lights-Out (iLO) 拡張リモート管理カードが装備されています。詳細な情報およびドキュメントについては、https://www.hpe.com/us/en/servers/integrated-lights-out-ilo.htmlにアクセスしてください。

第5章: ArcSightコンソールのインストール

ArcSightコンソールには、(ArcSightコマンドセンターのブラウザーベースのインターフェイスとは対照的に) ESMと接続するためのホストベースのインターフェイスがあります。この章では、デフォルトモードでのArcSightコンソールのインストールおよび構成方法について説明します。コンソールをFIPSモードでインストールするには、「FIPSモードでのArcSightコンソールのインストール」(85ページ)を参照してください。「FIPSモードまたはデフォルトモードの選択」(10ページ)には、モードの基本的な違いを記載しています。

ArcSightコンソールをインストールする前に、マネージャーが実行していることを確認します。一般的に、ArcSightコンソールは、ArcSightマネージャーを保護するファイアウォールの外にある複数の周辺マシンに展開されます。

コンソールサポート対象のプラットフォーム

サポート対象のプラットフォームとブラウザーの最新情報については、Protect 724サイトで入手可能な『HPE ArcSight ESM Support Matrix』ドキュメントを参照してください。

RHELおよびCentOS (64ビット) に必要なライブラリ

RHELおよびCentOS 6.x以降 (64ビット) のワークステーションの場合、コンソールには、以下のライブラリの最新バージョンがインストールされている必要があります。

```
pam-1.1.1-10.el6.x86_64.rpm
pam-1.1.1-10.el6.i686.rpm
libXtst-1.0.99.2-3.el6.x86_64.rpm
libXtst-1.0.99.2-3.el6.i686.rpm
libXp-1.0.0-15.1.el6.x86_64.rpm
libXp-1.0.0-15.1.el6.i686.rpm
libXmu-1.0.5-1.el6.x86_64.rpm
libXmu-1.0.5-1.el6.i686.rpm
libXft-2.1.13-4.1.el6.x86_64.rpm
libXft-2.1.13-4.1.el6.i686.rpm
libXext-1.1-3.el6.x86_64.rpm
libXext-1.1-3.el6.i686.rpm
libXrender-0.9.7-2.el6.i686.rpm
gtk2-engines-2.18.4-5.el6.x86_64.rpm
gtk2-2.18.9-6.el6.x86_64.rpm
```

```
compat-libstdc ++  -  33-3.2.3-69.el6.x86_64.rpm
compat-libstdc ++  -  33-3.2.3-69.el6.i686.rpm
compat-db-4.6.21-15.el6.x86_64.rpm
compat-db-4.6.21-15.el6.i686.rpm
```

コンソールのインストール

以下の注には、さまざまなオペレーションシステムにArcSightコンソールをインストールするための重要な考慮事項が含まれています。

注 : Linuxの場合

Linuxマシンではルートユーザーでコンソールをインストールしないでください。ルートユーザーでインストールすると、インストール完了後に、特定のディレクトリのオーナーシップの変更を要求されます。そのため、以下の手順はすべて非ルートユーザーで実行することを推奨します。
この問題は、Windowsマシンには該当しません。

注 : Macintoshの場合

- `keytoolgui`は、Macでは動作しません。したがって、キーストアまたは証明書を管理する必要がある場合は、『ESM Administrator's Guide』で説明されているkeytoolコマンドを使用してください。
- コンソールを起動する前に、印刷用のデフォルトプリンターを設定してください。チャネルを開き、いくつかの行を選択して右クリックし、メニューから [**選択行を印刷**] を選択した場合、デフォルトプリンターが設定されていないとコンソールがクラッシュします。

ArcSightコンソールをインストールする前に、ESMがインストールされていることを確認してください。

1. ArcSightコンソールをインストールするには、ターゲットプラットフォームに適した自己解凍アーカイブファイルを実行します。ArcSightコンソールインストーラーが格納されているディレクトリに移動します。`nnnn`はビルド番号を表します。

プラットフォーム	インストールファイル
Linux	`ArcSight-6.11.0.nnnn.0-Console-Linux.bin`
Windows	`ArcSight-6.11.0.nnnn.0-Console-Win.exe`
Macintosh	`ArcSight-6.11.0.nnnn.0-Console-MacOSX.zip`

   インストーラーのログファイルの場所は、以下のとおりです。

プラットフォーム	インストールのログファイル
Linux	/home/<user>
Windows	C:\Users\<user>
Macintosh	/Users/<user>

2. [**Installation Process Check**] 画面で [**Next**] をクリックします。
3. [**Introduction**] パネルの紹介テキストを読み、[**Next**] をクリックします。
4. [**License Agreement**] パネルの [I accept the terms of the License Agreement] チェックボックスは、契約テキストの最後までスクロールするまでは無効になっています。テキストを読み終えたら [**I accept the terms of the License Agreement**] チェックボックスを選択して、[**Next**] をクリックします。
5. [**Special Notice**] パネルのテキストを読み、[**Next**] をクリックします。
6. [**Choose ArcSight installation directory**] パネルでは、デフォルトのインストールディレクトリを受け入れるか、[**Choose**] をクリックして既存のフォルダーに移動するか、またはコンソールをインストール場所のパスを入力することができます。存在しないフォルダーを指定すると、そのフォルダーが作成されます。

   注意 : インストールパスにスペースを使用しないでください。この規則は、Linux、Macintosh、およびWindowsシステムに適用されます。コンソールインストーラーにエラーメッセージは表示されませんが、コンソールが起動しなくなります。

7. [**Choose Shortcut Folder**] パネルで、コンソールおよびアンインストールアイコンのショートカットを作成する場所を選択して、[**Next**] をクリックします。
8. [**Pre-Installation Summary**] 画面でサマリーを確認し、表示されているパスに問題がない場合は [**Install**] をクリックします。変更を加える場合は、[Previous] ボタンをクリックして変更します。

   インストールの進捗状況は、進捗状況バーで確認できます。

注 : Windowsでは、インストーラーによってコンソールが構成されている際、[**Please Wait**] パネルに、TZDataのアップデートが失敗したことを示すメッセージが表示されることがあります。このメッセージが表示された場合は、[OK] をクリックして続行します。コンソールは正常にインストールされます。通常、TZDataはこのメッセージが表示されても正しくアップデートされます。TZDataがアップデートされたことを確認するには、<ARCSIGHT_HOME\current\jre\lib\zi.tzdata_2016g_1\ディレクトリ内のファイルのタイムスタンプが、コンソールのインストール日時と一致していることを確認します。タイムスタンプが古い、またはファイルが見つからない場合は、コンソールをアンインストールしてから再インストールします。

ArcSightコンソールの構成

コンソールは、インストール後に構成する必要があります。

1. ウィザードに、既存のArcSightコンソールのインストールから構成オプションを転送するかどうかを尋ねるメッセージが表示されます。新しいクリーンなインストールを作成する場合は、[**No, I do not want to transfer the settings**] を選択して、[**Next**] をクリックします。
2. コンソールを設定するモードを、デフォルトまたはFIPSから選択します。

   マネージャーのインストールモードと同じモードを選択します。

   [**Run console in FIPS mode**] を選択すると、FIPSモードに切り替えるとデフォルトモードに戻れなくなるという警告が表示され、続行するかどうかを尋ねられます。

   (FIPSモードのみ) 暗号スイートを選択するプロンプトが表示されます。選択肢は次のとおりです。

   - FIPS 140-2
   - FIPS with Suite B 128 bits
   - FIPS with Suite B 192 bits

   Suite Bでは、2つのセキュリティレベル (128ビットと192ビット) が定義されます。この2つのセキュリティレベルは、Suite Bによって提供される全体的なセキュリティの代わりに使用されるAES (Advanced Encryption Standard) のキーサイズに基づいています。128ビットのセキュリティレベルでは、128ビットのAESキーサイズが使用されますが、192ビットのセキュリティレベルでは、256ビットのAESキーサイズが使用されます。キーサイズが大きくなるとセキュリティも強化されますが、時間とリソース (CPU) 消費の点で計算コストも高くなります。ほとんどのシナリオでは、128ビットのキーサイズで十分です。

   [Next]をクリックします。
3. このコンソールが接続するマネージャーのホスト名またはIPアドレスを [**Manager Host Name**] フィールドに入力します。

   マネージャーが使用している**IP Version** (IPv4またはIPv6) を選択します。デュアルスタックマシンでESMにホスト名で接続する必要があり、DNSまたはその他のネーミングサービスでESMがIPv4アドレスとIPv6アドレスの両方で関連付けられている場合は、ESMとの通信に優先IPプロトコルが使用されます。

   注意 : マネージャーのポート番号は変更しないでください。

   [Next] をクリックします。
4. [**Use direct connection**] オプションを選択して、[**Next**] をクリックします。マネージャーに直接接続できない場合は、プロキシサーバーをセットアップして、そのプロキシサーバーからマネージャーに接続することができます。

   [Use proxy server] オプションを選択した場合は、プロキシサーバー情報の [**Proxy Host Name**] と [**Proxy Host**] の入力を求めるプロンプトが表示されます。

   [Proxy Host Name] に名前を入力して、[**Next**] をクリックします。
5. ArcSightコンソールの設定ウィザードで、使用するクライアント認証タイプを選択するプロンプトが表示されます。選択肢は次のとおりです。

- Password Based Authentication
- Password Based and SSL Client Based Authentication
- Password Based or SSL Client Based Authentication
- SSL Client Only Authentication

注意 : PKCS#11認証を使用するためには、[**Password Based or SSL Client Based Authentication**] 方式を選択する必要があります。

注 : [**Password Based and SSL Client Based Authentication**] オプションは、現在、SSLベースの認証用のクライアントキーストアのみをサポートしています。[**Password Based and SSL Client Based Authentication**] オプションにおける、SSLクライアントベースの認証方式としてのPKCS#11トークンの使用は、現在はサポートされていません。

[**Password Based Authentication**] を選択した場合は、ユーザー名とパスワードを指定してログインします。

[**Password Based and SSL Client Based Authentication**] を選択した場合は、ユーザー名とパスワードに加えて、ログインするためのクライアント証明書が必要になります。『ESM Administrator's Guide』の手順に従い、クライアント証明書をセットアップします。

[**Password Based or SSL Client Based Authentication**] または [**SSL Client Only Authentication**] を選択した場合は、SSLクライアントベースの認証方式を選択する必要があります。選択肢は次のとおりです。

- Client Key Store
- PKCS#11 Token

PKCS#11トークンを使用する予定の場合は、トークンのソフトウェアとハードウェアを事前にセットアップしておく必要があります。まだトークンをセットアップしていない場合は、[Client Key Store] を選択して、インストールを続行することができます。コンソールのインストール完了後に、「PKCS#11プロバイダーを使用するためのセットアップ」(71ページ) を参照して、トークンのセットアップ手順を確認できます。

[**Client Key Store**] を選択した場合、インストール完了後に、クライアント証明書のセットアップを要求する次のメッセージが表示されます。

Manual setup of the client certificate will be required.
Do you wish to proceed?

設定ウィザード完了後、『ESM Administrator's Guide』の手順に従い、クライアント証明書をセットアップします。

6. ArcSightコンソールの設定ウィザードから、レポート、Knowledge Centered Supportの記事、その他のWebページのコンテンツ表示に使用するデフォルトのWebブラウザーを指定

するプロンプトが表示されます。Knowledge Centered Supportの記事、およびArcSightコンソールから起動されるその他のWebページの表示に使用するWebブラウザーの実行可能ファイルの場所を指定します。**ブラウザーの実行可能ファイル**を参照して選択し、[**Next**] をクリックします。

7. このコンソールのインストールが、単一ユーザーによって使用されるのか、または複数のユーザーによって使用されるのか選択します。

   以下のオプションから選択できます。

   - This is a single system user installation(推奨)

     このオプションは、次の場合に選択します。

     - 1人以上のコンソールユーザーがコンソールに接続するために使用する該当マシン上のシステムアカウントが1つだけの場合。たとえば、システムアカウントadminが、コンソールユーザーのJoe、Jack、Jill、およびJaneによって使用される場合。

       または

     - コンソールに接続するために該当マシンを使用するすべてのコンソールユーザーがマシン上に独自のユーザーアカウントを保有していて、それらのユーザーにArcSightコンソールの`\current`ディレクトリへの書き込みパーミッションが付与されている場合。

       利点: すべてのコンソールユーザーのログが、ArcSightコンソールの (`\current\logs` ディレクトリ) にのみ書き込まれます。すべてのコンソールユーザーのユーザー設定ファイル (`username.ast`で指定) が、ArcSightコンソールの`\current`に格納されます。

       欠点: セキュリティポリシーによって、すべてのコンソールユーザーが単一システムユーザーのアカウントを共有することや、すべてのユーザーがArcSightコンソールの`\current`ディレクトリに書き込まれることが許可されない場合、このオプションは使用できません。

   - Multiple users will use this installation

     このオプションは、次の場合に選択します。

     - コンソールに接続するために該当マシンを使用するすべてのコンソールユーザーが、そのマシン上に独自のユーザーアカウントを保有している場合。

       かつ

     - それらのユーザーに、ArcSightコンソールの`\current\logs`ディレクトリへの書き込みパーミッションが付与されていない場合。

     このオプションを選択すると、各ユーザーのログと設定ファイルが、該当マシン上のユーザーのローカルディレクトリ (Windowsの場合、`Document and Settings\username\.arcsight\console`など) に書き込まれます。

     利点: すべてのコンソールユーザーに対して、コンソールの`\current`ディレクトリへの書き込みパーミッションを有効にする必要がありません。

     欠点: ログが分散されるため、特定の時間範囲のログを確認するには、その時間帯に接続していたユーザーのローカルディレクトリからログにアクセスする必要があります。

すべてのコンソールユーザーに対して、コンソールの\currentディレクトリへの書き込みパーミッションを有効にしていない場合、ユーザーは、コンソールのコマンドラインインターフェイスから (コンソールの\bin\scriptsにある) 以下のコマンドのみを実行できます。

- sendlogs
- console
- exceptions
- portinfo
- websearch

その他のコマンドはすべて、コンソールの\currentディレクトリへの書き込みパーミッションが必要になります。

注: コンソールによるユーザー設定ファイルのアクセス場所、ログの書き込み場所は、前述のオプションの選択によって決まるため、初期構成後にオプションを切り替える場合、カスタマイズしたユーザー設定はすべて失われたように表示されます。たとえば、Windowsマシン上のコンソールが [This is a single system user installation] オプションを指定して構成されている場合、コンソールユーザーJoeのカスタマイズした設定ファイルは、コンソールの<ARCSIGHT_HOME>\currentにあります。この場合、consolesetupコマンドを実行して、設定を [Multiple system users will use this installation] に変更すると、次に、**Joe**がコンソールに接続する際、コンソールは、デフォルトの設定が含まれているDocument and Settings\joe\.arcsight\consoleからJoeの設定ファイルにアクセスすることになります。

8. ArcSightコンソールの構成が完了したら、最後のパネルの [**Finish**] をクリックして、設定ウィザードを終了します。
9. 次の画面で [**Done**] をクリックします。
10. 最適な結果を得るため、ArcSightコンソールは、マネージャーと同じロケールに設定されているオペレーティングシステムにインストールしてください。ArcSightコンソールとマネージャーは、起動中にオペレーティングシステムからロケールを自動的に検知して使用します。

    ただし、Linuxマシンにコンソールをインストールする場合は、次の行を追加して/home/arcsight/.bash_profileファイルを編集します。

    ```
    export LANG=[language].UTF-8
    ```

    [language]は、以下のいずれかです。
    en_US (英語)
    zh_CN (簡体字中国語)
    zh_TW (繁体字中国語)
    ja_JP (日本語)
    fr_FR (フランス語)
    ko_KR (韓国語)
    ru_RU (ロシア語)

ブラウザーへのコンソールの証明書のインポート

コンソールのオンラインヘルプは、ブラウザーに表示されます。SSL Client Based Authenticationモードを使用している場合、オンラインヘルプを表示するには、以下の手順を実行します。

1. コンソールからキーペアをエクスポートします。詳細については、『ESM Administrator's Guide』の「Export a Key Pair」を参照してください。
2. コンソールのキーペアをブラウザーにインポートします。

ArcSightコンソールは、すでに正常にインストールされています。

キャラクターセットのエンコーディング

コンソールは、マネージャーと同じキャラクターセットのエンコーディングを使用するマシンにインストールします。

キャラクターのエンコーディングが一致していない場合、ユーザーIDとパスワードには、以下の文字しか使用できません。

```
a-z A-Z 0-9_@.#$%^&*+?<>{}|,()-[]
```

コンソールのエンコーディングが一致せず、ユーザー**ID**に他の文字が含まれている場合、ユーザーはカスタムショートカットキー (ホットキー) スキーマを保存できません。この場合のユーザーIDは、keymap.xmlファイルに正しくエンコードされていないため、ログイン中にユーザーのショートカットスキーマを作成することはできません。そのような状況では、コンソールに対するログインはすべて失敗します。

UTF-8以外のエンコーディングを使用する必要があり、ユーザーIDに他の文字を使用する必要がある場合、それらのユーザーがログインするコンソールではカスタムショートカットキーはサポートされません。そのような場合は、`console.properties`ファイルに次のプロパティを追加します。`console.ui.enable.shortcut.schema.persist=false`。このプロパティにより、カスタムショートカットキースキーマの変更や追加が防止されます。

コンソールのエンコーディングが一致せず、**パスワード**に他の文字が含まれている場合、パスワードハッシュがパスワードの作成時にマネージャーに作成されたものと一致しないため、該当ユーザーはそのコンソールからはログインできません。

ArcSightコンソールの起動

インストールとセットアップが完了したら、インストールされているショートカットを使用してArcSightコンソールを起動するか、またはコンソールの`bin`ディレクトリでコマンドウィンドウを開いて以下のコマンドを実行します。

Windowsの場合

```
arcsight console
```

UNIXの場合

```
./arcsight console
```

コンソールのインストール時に選択したクライアント認証方式に応じて、ログイン画面に以下のボタンが表示されます。

選択した認証方式	表示されるボタン
Password Based Authentication	Login Cancel
Password Based and SSL Client Based Authentication	Login Cancel
Password Based or SSL Client Based Authentication	クライアントキーストアを認証方式として選択した場合は、以下のボタンが表示されます。 • Login (username and password) • SSL Client Login • Cancel PKCS#11トークンを選択した場合は、以下のボタンが表示されます。 • PKCS#11 Login • Login • Cancel
SSL Client Only Authentication	クライアントキーストアを認証方式として選択した場合は、以下のボタンが表示されます。 • ログイン認証は、クライアントのキーストアによって行われるため、ユーザーIDとパスワードのフィールドはグレー表示 (無効) になっています。 • Login • Cancel PKCS#11トークンを選択した場合は、以下のボタンが表示されます。 • PKCS#11 Login (SSL client authentication) • Cancel

注 : 状況によっては、cacertsフォルダーが原因でアクセスが拒否されたというログイン失敗のメッセージが表示されることがあります。arcsightユーザーにcacertsファイルへの書き込み権限があることを確認してください。Windowsシステムを使用して、この方法で問題が解決されない場合は、cacertsファイルのファイルロックが原因である可能性があります。ファイルロックは、コンピューターを再起動するとクリアできる可能性があります。

コンソールへのログイン

注 : [Password Based or SSL Client Based Authentication] を使用するように構成されているマネージャーにログインしている間に、証明書を使用してログインしようとするとそのログインは失敗します。また、同一セッションの間は、その後のユーザー名とパスワードを使用したログインの試みもすべて失敗します。この問題を解決するには、コンソールを再起動します。

コンソールを起動するには、[**Login**] をクリックします。コンソールの初回起動時には、[Login] をクリックすると、マネージャーの証明書を信頼するかどうかを尋ねるダイアログが表示され、設定した内容に固有の詳細情報がプロンプトに表示されます。[**OK**] をクリックして、マネージャーの証明書を信頼します。証明書はコンソールのトラストストアに恒久的に格納されるため、次回ログイン時にプロンプトが再度表示されることはありません。

ArcSightマネージャーへの再接続

ArcSightコンソールとArcSightマネージャーの接続が失われた場合 (マネージャーを再起動した場合など)、ArcSightマネージャーとの接続が失われたことを示すダイアログボックスがArcSightコンソールに表示されます。[**Retry**] クリックしてArcSightマネージャーとの接続を再確立するか、または [**Relogin**] をクリックします。

ArcSightマネージャーへの接続は、ArcSightマネージャーが再起動している間、またはマネージャーにより接続が拒絶されている場合は再確立できません。また、接続が失われているか、またはArcSightマネージャーが再起動している間は、再試行プロセス中に接続の例外が表示されることがあります。

ArcSightコンソールの再構成

ArcSightコンソールは、コマンドウィンドウで、コンソールの`bin`ディレクトリにある以下のコマンドを実行することで、いつでも再構成できます。

Windowsの場合 : `arcsight consolesetup`

Linuxの場合 : `./arcsight consolesetup`

その後、表示されるプロンプトに従います。

ArcSightコンソールのアンインストール

ArcSightコンソールをアンインストールする前に、現在のセッションを終了します。

Windowsでアンインストールする場合は、**スタートボタン > [すべてのプログラム] > [ArcSight ESM 6.11.0 Console] > [Uninstall ArcSight ESM Console]** プログラムを選択して実行します。[スタート] メニューにコンソールのショートカットが組み込まれていない場合は、コンソールのUninstallerDataフォルダーを見つけて、以下のコマンドを実行します。

```
Uninstall ArcSight ESM Console Installation.exe
```

UNIXホストでアンインストールする場合は、本製品のインストール時にリンクを作成したディレクトリからアンインストーラープログラムを実行します。リンクを作成していない場合は、/opt/arcsight/console/current/UninstallerDataディレクトリから以下のコマンドを実行します。

```
./Uninstall ArcSight ESM Console Installation
```

あるいは、/home/arcsight (またはショートカットリンクをインストールした) ディレクトリから以下のコマンドを実行することができます。

```
./Uninstall ArcSight_ESM_Console_6.11.0
```

注 : UninstallerDataディレクトリには、すべてのユーザーに対する読み取り、書き込み、および実行パーミッションが記録されている.com.zerog.registry.xmlファイルが含まれています。Windowsホストの場合、アンインストーラーが機能するためにはこれらのパーミッションが必要ですが、UNIXホストの場合は、全員のパーミッションを読み取りと書き込み (つまり、666) に変更することができます。

付録A: トラブルシューティング

以下の情報は、ESMのインストールまたは使用時に発生する可能性がある問題の解決に役立ちます。ケースによっては、本書またはESMの他のドキュメントでソリューションを見つけることができますが、必要な場合は、HPEカスタマーサポートを利用することができます。

HPEカスタマーサポートに診断プロセスの支援を依頼する場合は、具体的な症状と設定に関する情報を提供できるように準備してください。

コンポーネントのログファイルの場所

各ログファイルは以下の場所にあります。

ログファイル名	場所	説明
First Boot Wizardのログ		
fbwizard.log	/opt/arcsight/manager/logs/default/	「設定ウィザードの使用」(37ページ)の手順の実行中に記録された詳細なトラブルシューティング情報が含まれています。
firstbootsetup.log	/opt/arcsight/manager/logs/	「設定ウィザードの使用」(37ページ)の手順で実行したコマンドに関する簡単なトラブルシューティング情報が含まれています。
CORR-Engine のログファイル		
logger_server.log	/opt/arcsight/logger/current/arcsight/logger/logs	CORR-Engineに関するトラブルシューティング情報が含まれています。
logger_server.out.log	/opt/arcsight/logger/current/arcsight/logger/logs	CORR-Engineのstdoutログファイル
arcsight_logger.log	/opt/arcsight/logger/current/arcsight/logger/logs	CORR-Engineのセットアップに関するログ
logger_init_driver.log	/opt/arcsight/logger/current/arcsight/logger/logs	CORR-Engineのセットアップに関するログ
logger_init.sh.log	/opt/arcsight/logger/current/arcsight/logger/logs	CORR-Engineのセットアップに関するログ

ログファイル名	場所	説明
logger_ wizard.log	/opt/arcsight/logger/current/arcsight/logger/logs	CORR-Engineのセットアップに関するログ
logger_ wizard.out.log	/opt/arcsight/logger/current/arcsight/logger/logs	CORR-Engineのセットアップに関するログ
マネージャーのログファイル		
server.log	/opt/arcsight/manager/logs/default	マネージャーに関するトラブルシューティング情報が含まれています。
server.std.log	/opt/arcsight/manager/logs/default	マネージャーのstdout出力が含まれています。
server.status.log	/opt/arcsight/manager/logs/default	すべてのMBeanのダンプ、メモリステータス、スレッドステータスなどが含まれています。
サービスのログファイル		
arcsight_ services.log	/opt/arcsight/services/logs/	ArcSightサービスプロセスを管理するコマンドからの情報が含まれています。
monit.log	/opt/arcsight/services/monit/data/	ArcSightサービスプロセスの起動およびシャットダウンのタイミングの情報が含まれています。

インストールが失敗した場合の対応

インストールが失敗した場合、またはインストールが破損している場合の対処方法は次のとおりです。

アプライアンスの場合は、工場出荷時の設定に戻します。「アプライアンスの工場出荷時設定の復元」(104ページ) を参照してください。

ソフトウェアESMの場合、2つのケースがあります。

ケース1: `setup_services.sh`の実行後にインストールが壊れてしまった場合は、ルートユーザーで以下のスクリプトを実行します。

```
remove_services.sh
```

次に、以下のリカバリ手順を実行します。

ケース2: `setup_services.sh`の実行前にインストールが壊れてしまった場合は、リカバリ手順を実行します。

リカバリ手順: 前述のケース1またはケース2の場合に実行します。

1. インストールプロセスを終了したら、現在実行中のArcSightサービスをすべて停止します。または
   a. rootユーザーとしてログインします。
   b. 以下のコマンドを実行します。

      ```
      /opt/arcsight/manager/bin/remove_services.sh
      ```

2. `/opt/arcsight and /tmp`ディレクトリ配下にあるArcSight関連のすべてのファイルとディレクトリを削除します。
3. インストール時に作成されたすべてのショートカットを削除します (デフォルトでは、arcsightユーザーのホームディレクトリにあります)。
4. ソフトウェアESMの場合は、製品を再インストールしてください。

マネージャーのカスタマイズ

First Boot Wizardを実行すると、マネージャーとCORR-Engineストレージを構成できます。コンポーネントを詳細にカスタマイズするには、以下の手順に従いコンポーネントのセットアッププログラムを起動します。

arcsightユーザーでログインしている間に、以下の手順を実行します。

1. 以下のコマンドを実行して、マネージャーを停止します (実行している場合)。

   ```
   /etc/init.d/arcsight_services stop manager
   ```

2. `/opt/arcsight/manager/bin`ディレクトリから以下のコマンドを実行します。

   ```
   ./arcsight managersetup
   ```

3. ウィザードの画面に表示されるプロンプトに従います。具体的な画面の情報については、『Administrator's Guide』を参照してください。
4. ウィザードが完了したら、以下のコマンドを実行してマネージャーを再起動します。

   ```
   /etc/init.d/arcsight_services start manager
   ```

First Boot Wizard実行時の致命的なエラー - アプライアンスのインストール

このセクションの内容は、アプライアンスのインストールのみに適用されます。

First Boot Wizardの実行時に致命的なエラーが発生すると、ウィザードはエラーメッセージを表示して終了します。該当コンポーネントのログファイルでエラーメッセージを確認します。ログファイルの一覧は、「コンポーネントのログファイルの場所」(62ページ)に記載されています。

この問題を解決する場合は、以下の手順を試してください。

1. /opt/arcsight/manager/logs/default/fbwizard.logファイルを確認して、エラーの発生箇所を探します。
2. 「開いたままにしておくTCPポート」(31ページ)で説明されている必要なTCPポートがすべて開いている。
3. コンポーネントを構成する前にエラーが発生した場合は、rootユーザーとしてログインし、次の操作を行います。

   /opt/arcsightディレクトリの内容をクリア(削除)します。

   以下のコマンドを使用してセットアップを再実行します。

   ```
   cd
   /home/arcsight/install.esm/ESMComponents/service/opt/arcsight/services/bin
   /scripts
   ```
   (すべて1行です)

   ```
   ./esm_setup.sh
   ```

上記の手順がうまくいかない場合、たとえば、セットアップがすでにマネージャーの設定を開始している場合やインストールが破損している場合は、工場出荷時の設定に戻してください。「アプライアンスの工場出荷時設定の復元」(104ページ)を参照してください。

マシンのホスト名の変更

「hostname」と表示されている場合は、「ホスト名またはIPアドレス」を意味しています。ピアを構成している場合は、ピアの関係を必ず再構築してください。

注: ホスト名としてIPv6アドレスを使用することはできません。IPv4アドレスは、ホスト名として使用できます。

高可用性モジュールを使用している場合の手順は異なります。正しい手順については、『ArcSight High Availability Module User's Guide』を参照してください。

First Boot Wizardを正常に実行した後で、マシンのサービスIPアドレスを変更する場合は、以下の手順を実行します。

注: マネージャーのセットアップコマンドは、arcsightユーザーでログインしているときに実行します。

1. arcsightユーザーで以下のコマンドを実行して、すべてのArcSightサービスを停止します。

   ```
   /etc/init.d/arcsight_services stop all
   ```

2. マシンのホスト名を変更します。
3. マシンを再起動します。
4. arcsightユーザーで以下のコマンドを実行して、マネージャーを停止します。

   ```
   /etc/init.d/arcsight_services stop manager
   ```

5. arcsightユーザーで、/opt/arcsight/manager/binディレクトリからマネージャーのセットアッププログラムを実行します。

   ```
   ./arcsight managersetup
   ```

   a. ウィザードからプロンプトが表示されたら、[Manager Host Name] フィールド、および古いホスト名が表示されているその他すべてのフィールドに、(前述の手順で使用マシンに設定した) 新しいホスト名を入力します。
   b. プロンプトが表示されたら自己署名キーペアのオプションを選択し、必要な情報を入力して、新しいホスト名を含んでいる自己署名証明書を生成します。

      FIPSモードの場合、キーペアを再生成するオプションはありません。この場合、キーペアを手動で削除して再生成し、次の手順に進んでマネージャーを再起動します。
6. arcsightユーザーで以下のコマンドを実行して、マネージャーを起動します。

   ```
   /etc/init.d/arcsight_services start manager
   ```

7. arcsightユーザーで以下のコマンドを実行して、マネージャーが実行しているかどうかを確認します。

   ```
   /etc/init.d/arcsight_services status manager
   ```

   「manager service is available」という行が表示されるまで、このコマンドを1分間に一度実行します。表示されたら、次のステップに進みます。
8. マネージャーの新たに生成された証明書を、そのマネージャーにアクセスするすべてのクライアント (コンソールおよびコネクター) にインポートします。『ESM Administrator's Guide』で「SSL Authentication」の章の「Import a Certificate」を参照してください。
9. テストを行い、以下のことを確認します。
   - クライアントがマネージャーに接続できる。
   - ピア構成が想定どおりに機能している。機能していない場合は、ピア構成をやり直します。

検索クエリの結果グラフがSafariブラウザーに表示されない

Safariでクエリ結果をグラフとして表示できるようにするには、Mac OS用の最新バージョンのAdobe Flash Player Webプラグインがインストールされている必要があります。

ダッシュボードにホスト名 がIPv6アドレスとして表示 される

これは、システムのホスト名 、ネットワークの設 定 、およびユーザーの環 境 の名 前 解 決 が一 致 していないために発 生 します。システムのホストファイルとDNS設 定 、およびDNS内 でシステムホスト名 対 応 するアドレスを確 認 します。

IPv6システムからインターネット にアクセスできない

システムがIPv6のみで構 成 されている場 合 、システムの構 成 とインターネット アクセスによっては、コンソールまたはArcSightコマンド センター内 のリンクからインターネット にアクセスできないことがあります。リンクにアクセスするには、IPv4のみまたはデュアルスタックのシステムにリンクをコピーします。

付 録B: コンポーネントのデフォルトの設 定

この付 録には、ESMの各 ソフトウェアコンポーネントのデフォルトの設 定 が記 載 されています。

各 コンポーネントは、そのセットアッププログラムを実 行 することでいつでもカスタマイズできます。

一 般 的な設 定

設 定	
トラストストアのデフォルトパスワード	changeit
cacertsのデフォルトパスワード	changeit
キーストアのデフォルトパスワード	password

CORR-Engineの設 定

以 下 の表 に示 されているのは、CORR-Engineに事 前 に構 成 されているデフォルト値 の一 部 です。

設 定	デフォルト値
ロガーの場 所	/opt/arcsight/logger
データベースのユーザー名	arcsight
データベースのポート	3306

マネージャーの設 定

注 : マネージャーでは、First Boot Wizardを使 用してシステムを構 成したときに生 成 される自 己 署 名 証 明 書 が使 用されます。コンソールの初 回 ログイン時 に、マネージャーの証 明 書 を受 け入 れるためのプロンプトが表 示 されます。ダイアログ上 の [Yes] をクリックするか、またはマネージャーの証 明 書 を後 から手 動 でインポートすることができます。

以下の表に示されているのは、マネージャーに事前に構成されているデフォルト値の一部です。

設定	デフォルト値
マネージャーの場所	`/opt/arcsight/manager`
マネージャーのホスト名	ESMのホスト名またはIPアドレス
マネージャーのポート	`8443`
マネージャーのJavaヒープメモリ	16 GB
認証タイプ	Password Based
使用される証明書のタイプ	自己署名証明書
キーストアのデフォルトパスワード	`password`
cacertsのデフォルトパスワード	`changeit`
トラストストアのデフォルトパスワード	`changeit`

メール通知	内部SMTPサーバー。外部SMTPサーバーを使用する場合は、以下の手順を実行します。
	1. arcsightユーザーで以下のコマンドを実行して、マネージャーを停止します。
	`/etc/init.d/arcsight_services stop manager`
	2. プロンプトが表示されたら、`/opt/arcsight/manager/bin`ディレクトリから以下のコマンドを実行して、外部SMTPサーバーをセットアップします。
	`./arcsight managersetup`
	3. arcsightユーザーで以下のコマンドを実行して、マネージャーを起動します。
	`/etc/init.d/arcsight_services start manager`

センサーアセットの自動作成	`true`
インストール済みのパッケージ/デフォルトコンテンツ	デフォルトのシステムコンテンツ

付録C: PKCSの使用

PKCS (Public-Key Cryptography Standard) は、信頼性の高いセキュアな公開キー暗号法に使用される標準で構成されています。公開キー暗号法は、送信者側でデータを暗号化して、受信者側で解読することで機能します。

ArcSight ESMでは、ID確認やアクセス制御のために、CAC (Common Access Card) または90MeterなどのPKCS#11トークンの使用がサポートされています。PKCS#11トークンは、ユーザーインターフェイスからマネージャーにログインするために使用されます。PKCS#11は、RSA Laboratoriesによって公開されているPKCS (Public-Key Cryptography Standard) であり、「Cryptokiと呼ばれる、テクノロジーに依存しない、スマートカードやPCMCIAカードなどの暗号化デバイス用プログラミングインターフェイス」であると説明されています。

PKCS#11トークンは、ArcSightコンソールの実行モードが、FIPS 140-2モードであるか、デフォルトモードであるかに関係なく、ログインに使用できます。

PKCS#11認証は、RADIUS、LDAP、およびActive Directoryの認証方式ではサポートされていません。

PKCS#11

PKCS標準の1つであるPKCS#11は、ハードウェアセキュリティモジュールやスマートカードなどの暗号トークン、ソフトウェアトークン、およびハードウェアトークンの汎用インターフェイスを定義しているAPIです。暗号トークンは、スマートカードやCAC (Common Access Card)、90Meterなどの、ソフトウェアまたはハードウェアの使用を許可するために使用されるセキュリティデバイスです。許可されたユーザーの認証情報はハードウェア自体に格納されます。ESMは、NSS (Network Security Services) 暗号モジュールによって提供されているPKCS#11インターフェイスを使用して、NSS暗号モジュールと通信します。PKCS#11の使用は、クライアント側の認証の一例です。

ESMにおけるPKCS#11トークンのサポート

ESMは、PKCS#11 2.0以上をサポートしているPKCS#11トークンベンダーに対応しています。PKCS#11トークンを使用する予定のマシンに、使用するベンダーのドライバーとPKCS#11ドライバーのDLLがインストールされていることを確認してください。

PKCS#11トークンを使用する前に、PKCS#11トークンを使用する予定のArcSightコンソールシステムにプロバイダーのソフトウェアがインストールされていることを確認します。暗号化デバイスのインストールおよび構成方法については、使用しているPKCS#11トークンプロバイダーのドキュメントを参照してください。

PKCS#11トークンは、ESMクライアントの動作モード (FIPS 140-2モードまたはデフォルトモード) に関係なく使用できます。ただし、ESMマネージャーがクライアントと通信するときに「パスワードまたはSSL認証」を使用するように設定する必要があります。この設定は、『Administrator Guide』の「Running the Manager Configuration Wizard」の章に記載されているように、マネージャー設定ウィザードを実行して設定します。

PKCS＃11トークンを使用するには、トークンのCAのルート証明書と証明書自体がArcSightマネージャーのトラストストアにインポートされていることを確認します。ArcSightコマンドセンターで、外部IDを編集して [Admin] タブの共通名と一致させることができます。

PKCS#11プロバイダーを使用するためのセットアップ

ESMでは、任意のPKCS#11トークンを介した認証がサポートされていますが、この付録では、ActivClientのCAC (Common Access Card) の使用方法を例として取り上げます。CACカードのセットアップ手順は以下のとおりです。

1. 各クライアントマシンで「PKCS#11プロバイダーのソフトウェアのインストール」(71ページ) を実行します。対象には、ArcSightコンソール、およびブラウザーを使用してArcSightコマンドセンターにアクセスするすべてのマシンが含まれます。
2. 「ユーザーの外部IDとサブジェクトCNのマッピング」(72ページ)
3. 「CAC/90Meterの発行者の証明書の取得」(73ページ)
4. 「CAC/90Meter証明書からのルートCA証明書の抽出」(75ページ)
5. 「ArcSightマネージャーへのCAC/90Meterルート CA証明書のインポート」(77ページ)
6. 「ArcSightコンソールセットアップ時の認証オプションの選択」(78ページ)

PKCS#11プロバイダーのソフトウェアのインストール

PKCS#11トークンの使用を開始する前に、各クライアントシステムにPKCS#11のソフトウェアをインストールしていることを確認します。対象となるクライアントシステムは、ArcSightコンソール、およびWebベースのインターフェイスに使用するブラウザーがインストールされているすべてのマシンです。インストールおよび構成方法については、使用しているPKCS#11プロバイダーのドキュメントを参照してください。

注: 64ビットシステムを使用している場合は、ActivClientソフトウェアの32ビットバージョンと64ビットバージョンの両方をインストールします。特定のプラットフォームでは、`.msi`ファイルの代わりに、`setup.exe`リンクをダブルクリックしてインストールすることができます。

90MeterやActivClientなどの適切なPKCS#11プロバイダーをインストールします。個別のdllをコピーするだけでは十分ではない場合があります。場合によっては、`arcsight consolesetup` で指定されたライブラリが他のプロバイダーモジュールを必要とすることがあります。

90Meterの場合は、SCM_1.2.27_64Bit_S.msiをインストールします。インストールの一部として32ビットライブラリが付属していますが、これは必須です。

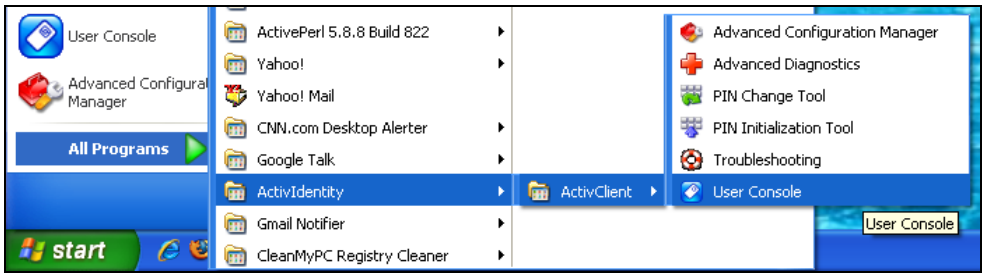
ユーザーの外部IDとサブジェクトCNのマッピング

CAC/90Meterカードには、署名証明書、暗号化証明書、およびID証明書の3種類の証明書が含まれています。次の手順は、ID証明書に関連しています。ID証明書は、PKCS＃11を使用したログインのSSLハンドシェイクに使用されます。

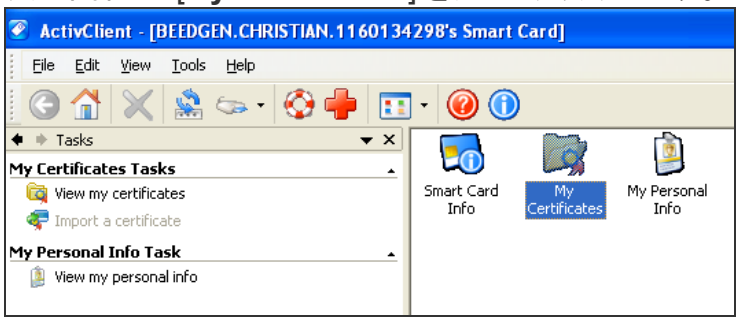
PKCS#11トークンのCN (共通名) をArcSightマネージャー上のユーザーの外部IDにマッピングします。外部ユーザーIDは、PKCS#11トークンのID証明書に表示される共通名と同じである (共通名に含まれるスペースやピリオドを含む) 必要があります(例: **john.smith.9691998563**)。その結果、ArcSightマネージャーは、PKCS#11トークンに格納されているIDによって表されているユーザーを認識することができます。

次のスクリーンショットは、CNを見つけてActivClientのユーザーの外部IDにマップする方法を示しています。これは一例です。他のPKCS＃11プロバイダーの場合、プロバイダー固有の異なるUIを使用して同様の手順を実行することになります。手順については、プロバイダーのドキュメントを参照してください。

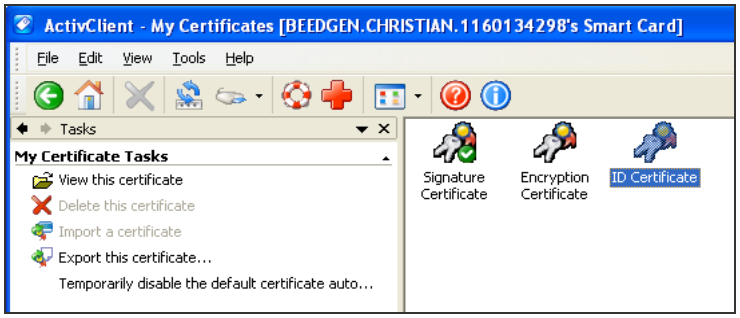
1. CAC/90Meterカードからサブジェクト CNを取得します。
   a. CAC/90Meterカードをリーダーに挿入します (未挿入の場合)。
   b. **[Start] > [ActivIdentity] > [ActivClient] > [User Console]** の順にクリックして、ActivClientソフトウェアを起動します。



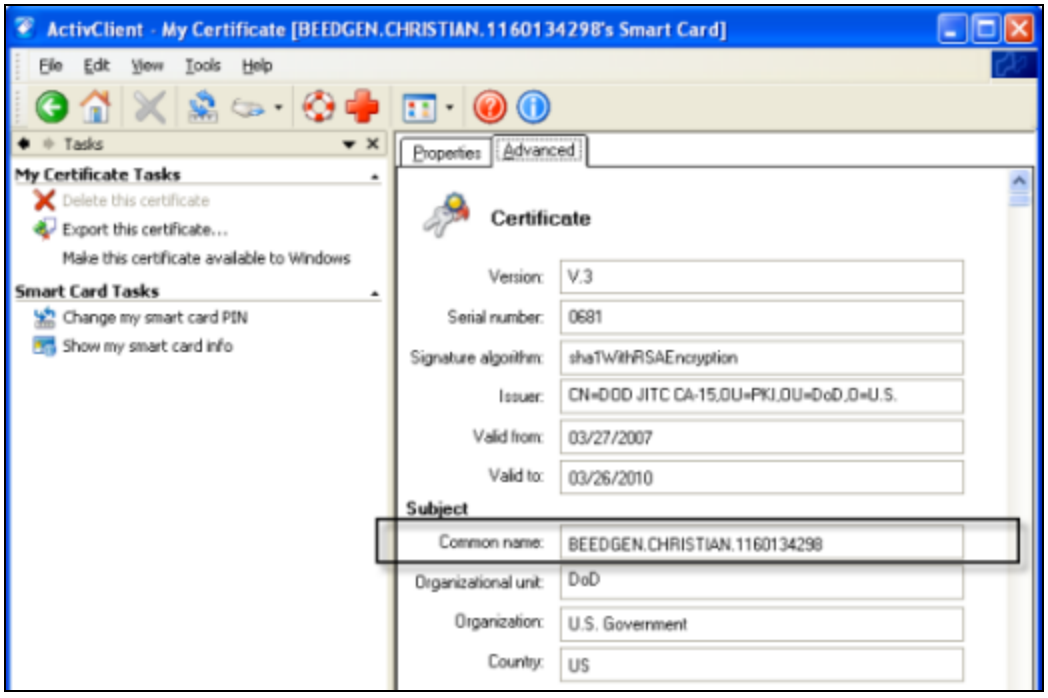
   c. 次の画面で [**My Certificates**] をダブルクリックします。



   d. 次の画面で [**ID Certificate**] をダブルクリックします。



e. [**Advanced**] タブをクリックして、[Common name] テキストボックスの内 容 をコピーしま す。この内 容 は用 紙 に手 書 きでコピーする必 要 があります。コンテキストメニューを使 用したコピーはサポートされていません。



2. 代 わりに、外 部 IDとArcSightコンソール内 のCNを一 致 させることもできます。
   a. ArcSightコンソールで、**[Resources] > [Users] > [user group]** に移 動 して、CAC/90Meterカード の共 通 名 にマッピングするユーザーの外 部 IDをダブルクリックしま す。該 当 ユーザーの [Inspect/Edit] ペインが開 きます。
   b. ステップ1で取 得 したCNを **[External User ID]** フィールド に入 力 して、**[Apply]** をクリッ クします。

CAC/90Meterの発 行 者 の証 明 書 の取 得

PKCS#11トークン認 証 は、SSLのクライアント側 の認 証 に基 づいています。Common Access Cardを使 用 している場 合 、クライアント (CAC/90Meterデバイス) のキーペアはカード 自 体 に格 納 されています。CAC/90Meterの証 明 書 をCACのキーストアからエクスポートして、

CACの証明書からルートCAおよびすべての中間証明書を抽出できるようにする必要があります。

使用する証明書が中間のCAによって発行されている場合は、発行者 (中間のルートCA) の証明書だけではなく、そのトップのルートCA証明書もエクスポートします。

オプション1

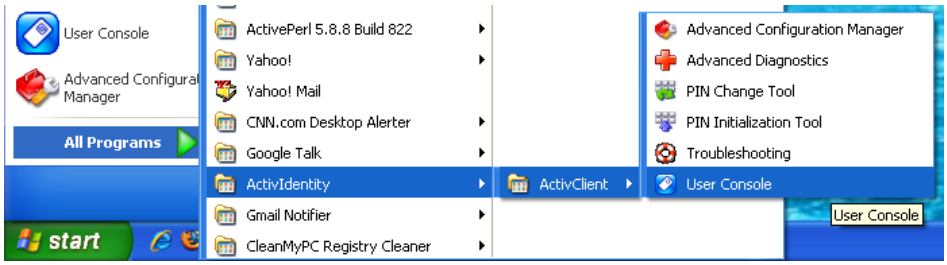
CAC/90Meterカードの証明書署名者のルートCA証明書および中間のすべての署名者の証明書は、PKI管理者から取得できます。

オプション2

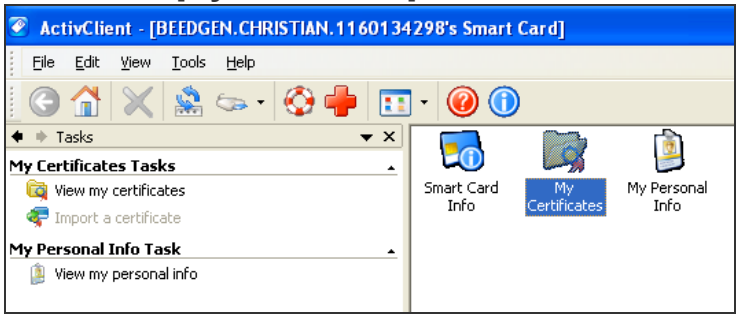
CAC/90Meterカードの証明書および中間のすべての署名者の証明書をCACのキーストアからエクスポートして、その証明書からルートCA証明書を抽出できます。

カードからCAC/90Meterカードの証明書を抽出する手順は、以下のとおりです。

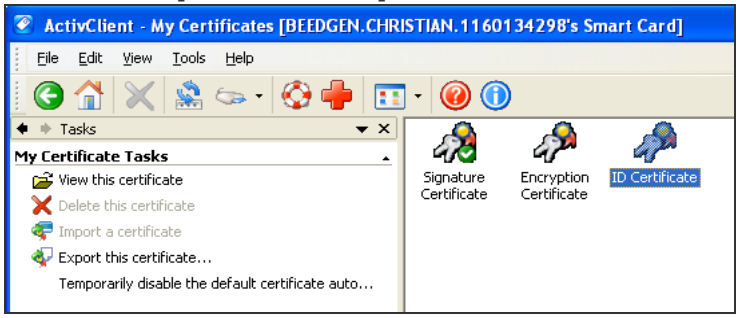
1. CAC/90Meterカードをリーダーに挿入します (未挿入の場合)。
2. **[Start] > [ActivIdentity] > [ActivClient] > [User Console]** の順にクリックして、ActivClientソフトウェアを起動します。



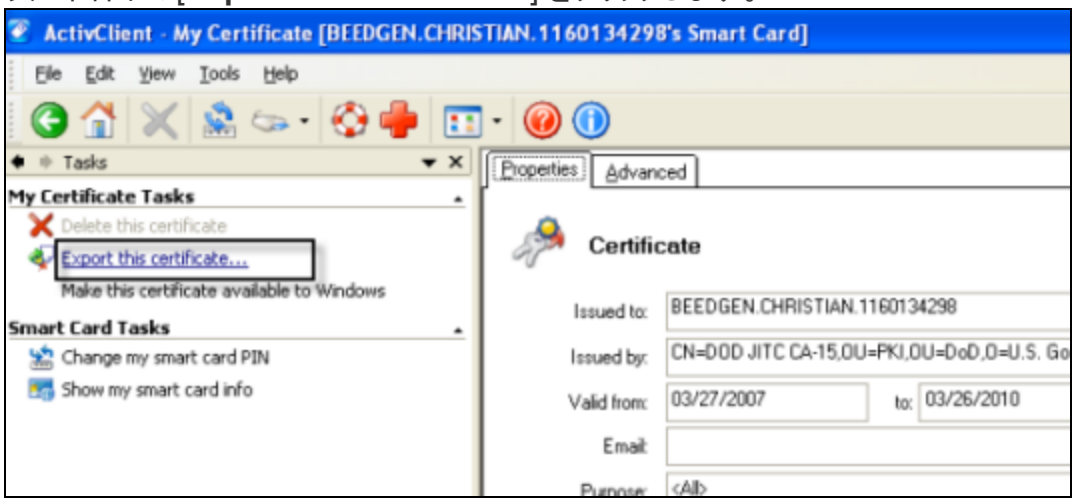
3. 次の画面で **[My Certificates]** をダブルクリックします。



4. 次の画面で **[ID Certificate]** をダブルクリックします。



5. 次の画面で [**Export this certificate...**] をクリックします。



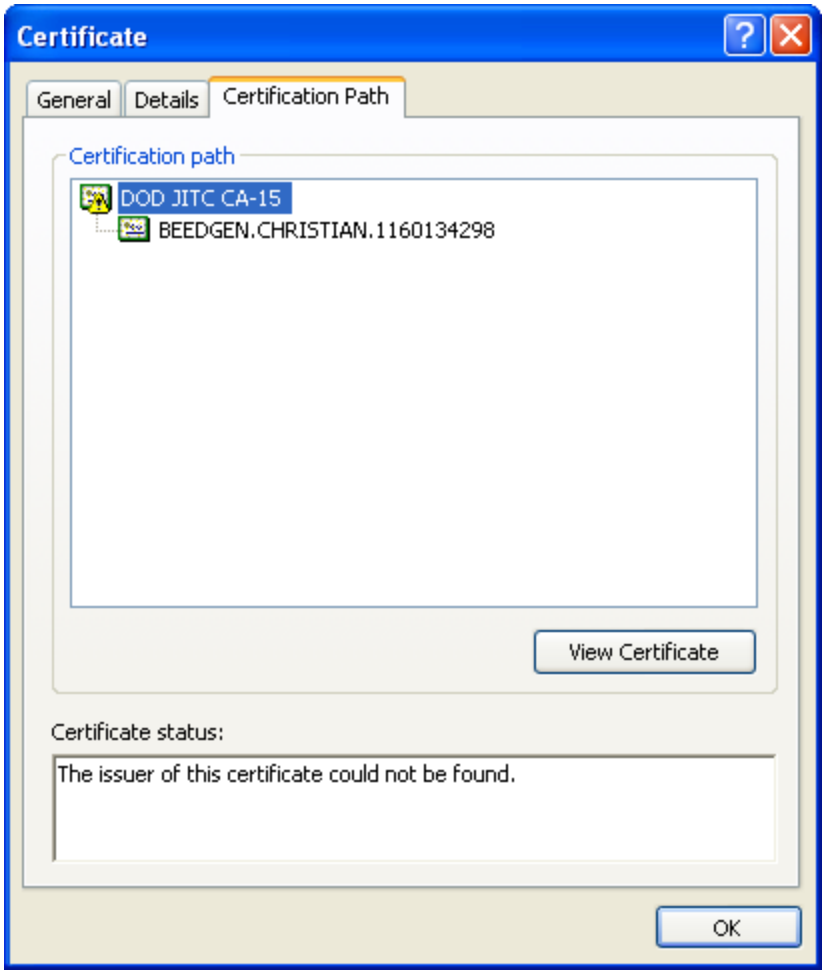
6. [**File name**] ボックスに証明書の名前を入力し、使用マシン上の証明書のエクスポート先にナビゲートして [**Save**] をクリックします。
7. 成功のメッセージが表示されたら [OK] をクリックします。
8. [ActivClient] ウィンドウを閉じます。

CAC/90Meter証明書からのルートCA証明書の抽出

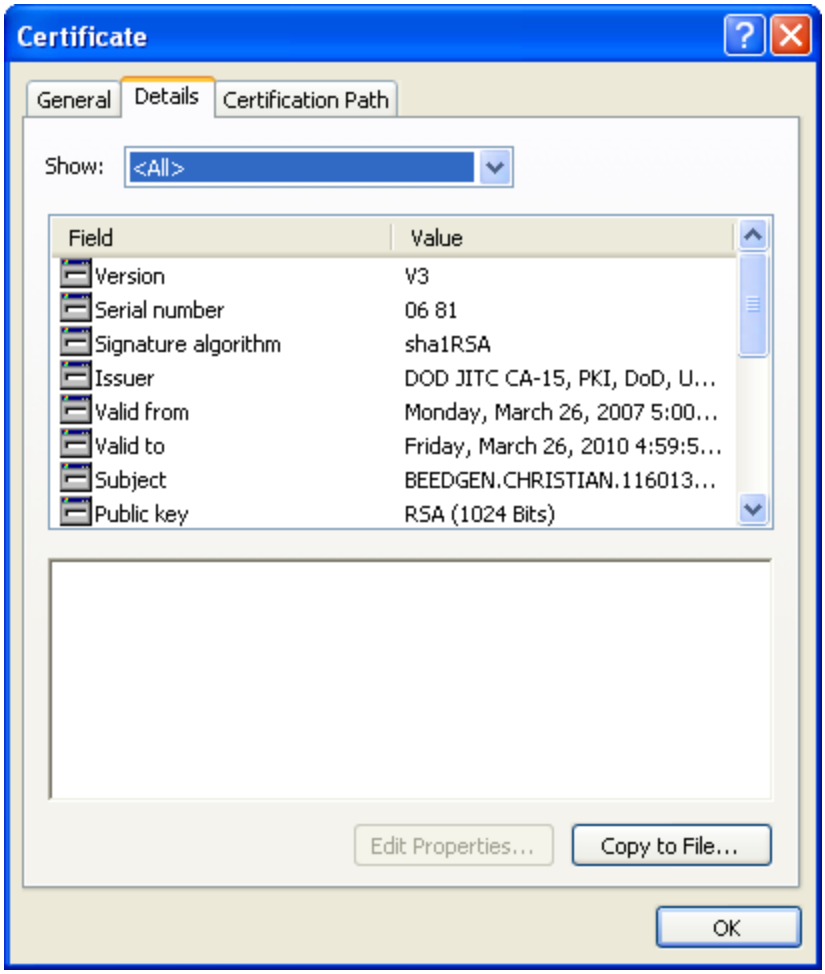
CAC/90Meter証明書の署名者のCAルート証明書と中間署名者の証明書は、ArcSightマネージャーのキーストアにインポートする必要があります。

以下の手順を実行して、中間の証明書もすべて抽出します (存在する場合)。

1. エクスポートした証明書をダブルクリックします。[Certificate] インターフェイスが開きます。
2. [**Certification Path**] タブをダブルクリックして、ルート証明書を選択します (以下の図を参照)。



3. [**View Certificate**] をクリックします。
4. [**Details**] タブをクリックして、[**Copy to File...**] をクリックします。



5. Certificate Export Wizardが開きます。ウィザードの画面に表示されるプロンプトに従い、デフォルト値をすべて受け入れます。
6. プロンプトが表示されたら、CAC/90MeterルートCA証明書ファイルの名前を入力して、デフォルト値をすべて受け入れてウィザードを続行します。証明書は、抽出元のCAC/90Meter証明書と同じ場所にエクスポートされます。
7. [Certificate] ダイアログを終了します。

ArcSightマネージャーへのCAC/90MeterルートCA証明書のインポート

ArcSightマネージャーのトラストストアへのインポート

証明書をArcSightマネージャーのトラストストアにインポートするには:

1. ArcSightマネージャーが動作している場合は、arcsightユーザーとしてログインし、次のコマンドを使用します。

```
/etc/init.d/arcsight_services stop manager
```

2. 次 のコマンドを実 行して、PKCS#11トークン署 名 者 のCAルート証 明 書をインポートしま す。

   ```
   cd <ARCSIGHT_HOME>
   ```

   bin/arcsight keytool -store managercerts -importcert -alias admin -file admin.cer
3. arcsightユーザーとしてログインした状 態 で次 のコマンドを実 行して、ArcSightマネー ジャーを再 起 動します。

   ```
   /etc/init.d/arcsight_services start manager
   ```

ArcSightコンソールセット アップ時 の認 証 オプションの選 択

ArcSightコンソールの認 証 オプションは、ArcSightマネージャーに設 定している認 証 オプション とー 致している必 要 があります。ArcSightコンソールセット アッププログラムを実 行して、 ArcSightコンソールとArcSightマネージャーの認 証 のー 致 を確 認 するか、またはー 致 するよう に変 更します。そのためには、以 下 の手 順 を実 行します。

1. ArcSightコンソールを停 止します (実 行している場 合)。
2. ArcSightコンソールのbinディレクトリからArcSightコンソールのセット アッププログラムを実 行 します。

   ```
   ./arcsight consolesetup
   ```
3. ウィザード画 面 に表 示されるプロンプトに従 い、認 証 オプションの画 面 が表 示されるまで、 すべてのデフォルト値 を受 け入 れます。選 択 肢 は次 のとおりです。
   - Password Based Authentication
   - Password Based and SSL Client Based Authentication
   - Password Based or SSL Client Based Authentication
   - SSL Client Only Authentication
4. [**Password Based or SSL Client Based Authentication]** のオプションを選 択します。 ArcSightマネージャーをセット アップしたときにも、このオプションを選 択しているはずです。
5. 後 続 の数 画 面 では、表 示されるプロンプトに従 いすべてのデフォルト値 を受 け入 れます。
6. [**Select client keystore type**] 画 面 で、[**PKCS#11 Token]** オプションを選 択します。
7. プロンプトが表 示されたら、PKCS#11ライブラリのパスを入 力 するか、またはPKCS#11ラ イブラリを参 照します。

   ActivClient以 外 のベンダーを使 用している場 合 は、そのインストールライブラリの場 所 を 指 す必 要 があります。

ActivClientを使 用している場 合 、デフォルトでは、PKCS#11ライブラリは次 の場 所 にあります。

32ビット版Windowsの場 合
`C:\Program Files\ActivIdentity\ActivClient\acpkcs211.dll`

64ビット版Windowsの場 合
`C:\Program Files (x86)\ActivIdentity\ActivClient\acpkcs211.dll`
(これは、ActivClientライブラリの32ビット版 です)

または、ActivClient 7.1以 降 の場 合 は、次 のパスを指 定します。

`C:\Program Files (x86)\HID Global\ActivIdentity\ActivClient\acpkcs211.dll`

90Meterの場 合 は、常 に次 の場 所 にある32ビットライブラリを使 用します。
`C:\Program Files\90meter\CACPIVMD\pkcs11\x86\LitPKCS11.dll`

8. デフォルト値 をすべて受 け入 れてセットアッププログラムを終 了します。
9. 実 行 中 のすべてのArcSightコンソールを再 起 動します。

PKCS#11トークンを使 用したArcSightコンソールへのログイン

ArcSightコンソールを起 動 すると、[PKCS#11] ログインボタンがある画 面 が表 示 されます。

以 下 のいずれかのオプションを使 用してログインできます。

- [Username and password combination] (このオプションの場 合 は、CAC/90Meterカードを外します)
- [PKCS#11 Login]

PKCS#11トークンを使 用してログインするには、[PKCS#11 Login] ログインオプションを選 択します。[**ActivClient Login**] ダイアログの [**PIN**] テキストボックスに、ActivClientカードのPIN番 号を入 力します。

PKCS#11トークンを使 用したESM Web UIへのログイン

ArcSightコマンドセンターに接 続 するためには、サポートされているWebブラウザーを使 用します。

1. PKCS#11トークンがカードリーダーに確 実 に挿 入 されていることを確 認します。
2. 次 のウェブサイトに移 動します。`https://<hostname>:8443/`

   Firefoxの場 合 の注 意 : Firefoxを使 用している場 合 は、ActivClientモジュールをロードして、ActivClientと連 動 するようにFirefoxを構 成してください。Webブラウザーを使 用して

接 続 する場 合 、一 部 のPKCS＃11プロバイダーに合 わせてブラウザーを設 定 する必 要 があります。

a. **[ツール]> [オプション]** を開き、**[詳 細] > [証 明 書]** タブに移 動 します。
b. **[セキュリティデバイス]** で、**[新 しいモジュールの追 加]** を選 択 します。
c. "ActiveIdentity"の場 合 は、次 のパスで32ビットdllを指 定 します。
   ```
   C:\Program Files (x86)\ActivIdentity\ActivClient\acpkcs211.dll
   ```
   または、ActivClient 7.1以 降 の場 合 は、次 のパスを指 定 します。
   ```
   C:\Program Files (x86)\HID
   Global\ActivIdentity\ActivClient\acpkcs211.dll
   ```
   90Meterの場 合 、すべてが自 動 的 に設 定 されます。
d. **[ログイン]** ボタンを使 用 してモジュールにログインし、指 示 に従 ってPINを入 力 します。自 動 認 証 を防 ぐために、必 ず [**ログアウト**]ボタンを使 用 してください。
e. Firefoxを再 起 動 すると、資 格 情 報 なしでArcSightコマンドセンターにログインできます。

3. PINの入 力 を求 められます。

   例 外 がある場 合 は、[**Add exception**] をクリックし、証 明 書 キーを生 成 して確 認 します。[**User Identification Request**] ダイアログが表 示 されたら、[**OK**] をクリックします。
4. ArcSightコマンドセンターのログイン時 には、ユーザーIDやパスワードを入 力 しないでください。両 方 をブランクのままにして、[**Login**] をクリックします。ユーザー認 証 は、次 に表 示 されるダイアログでPKCS＃11のPINを入 力 した後 に解 決 されます。
5. 確 認 用 のダイアログにPINを入 力 します。ダイアログのタイトルと外 観 は、PKCS＃11トークンの設 定 によって異 なります。

付録D: FIPSモードでのESMのインストール

ESMは、連邦情報処理規格 (FIPS) 140-2およびSuite Bをサポートします。一度、特定のFIPSモード用にESMシステムを設定すると、そのシステムを再構成して別のFIPSモードを有効にすることはできません。たとえば、FIPS 140-2が有効になるように構成されたシステムを再構成してFIPS Suite Bを有効にすることはできません。

注: マネージャーをFIPSモードでインストールする場合は、他のすべてのコンポーネントもFIPSモードでインストールする必要があります。

FIPSモードを使用している場合は、Mac上でArcSightコンソールを使用することはできません。

FIPSの概要

FIPSは、NIST (National Institute of Standards and Technology) によって発行された規格であり、ソフトウェアコンポーネントの暗号化モジュールを認可するために使用されます。暗号モジュールは、暗号ロジックを実装するために使用されるハードウェアまたはソフトウェア、またはその2つを組み合わせたものです。米国連邦政府は、SBU (取扱注意ではあるが機密扱いでない) 情報を扱うすべてのIT製品がFIPS 140-2規格に準拠していることを義務付けています。FIPSに準拠するため、ESMはBouncy Castle Java暗号を暗号モジュールとして使用します。

注: FIPS 140-2に準拠するには、すべてのコンポーネントをFIPS 140-2モードで構成する必要があります。FIPSモードで実行されているArcSightマネージャーが非FIPSモードのコンポーネントからの接続を受け入れることができるとしても、このような混在構成はFIPS 140-2に準拠するとみなされません。完全にFIPS 140-2に準拠するには、すべてのコンポーネントをFIPSモードで実行することをお勧めします。

FIPSに準拠するため、ESMは、Mozilla Network Security Services (NSS) の代わりに、Bouncy Castle Java暗号を使用します。Bouncy Castleは、デフォルトモードだけでなくFIPSモードでも、TLS 1.2のサポートを可能にします。

Suite Bの概要

Suite Bは、国家安全保障局 (NSA) が国の暗号技術の一部として推進する一連の暗号アルゴリズムです。FIPS 140-2がサポートするのは取扱注意ではあるが機密扱いでない情報

ですが、FIPS with Suite Bは非機密情報と最も機密性の高い極秘情報の両方をサポートします。AESに加えて、Suite Bには、ハッシュ、デジタル署名、および鍵交換のための暗号化アルゴリズムが含まれています。

注:

- ESMのすべてのバージョンが、FIPS with Suite Bモードをサポートしているわけではありません。FIPS with Suite Bモードをサポートするプラットフォームについては、Protect 724 Webサイトで入手可能なESM HPE ESM Support Matrixドキュメントを参照してください。
- マネージャーがFIPS with Suite B準拠モードでインストールされている場合、すべてのコンポーネント (ArcSightコンソール、SmartConnector、およびLogger、該当する場合) をFIPS with Suite B準拠モードでインストールし、ESMへのアクセスに使用するブラウザーのTLSを有効にする必要があります (SSLプロトコルはサポートされていません)。詳細については、「ブラウザーのTLSプロトコルの設定」(47ページ)を参照してください。
- ESMをFIPS with Suite Bモードでインストールする前に、バージョン4.0より前のLoggerはFIPS対応のArcSightマネージャーと通信できなくなることに注意してください。

FIPS暗号スイートの情報については、「FIPSモードまたはデフォルトモードの選択」(10ページ)を参照してください。

トランスポートレイヤーセキュリティ (TLS) 設定の概念

TLSの設定には、サーバー側認証のみの場合、またはサーバー側とクライアント側の認証の両方が含まれる場合があります。クライアント側認証の設定はオプションです。

TLSバージョンのサポート情報とFIPSモードでのESMの設定については、「TLSのサポート」(83ページ)を参照してください。

TLSはSSL 3.0に基づいているため、SSLの仕組みをよく理解しておくことをお勧めします。SSLの仕組みの詳細については、『ESM Administrator's Guide』の「Understanding SSL Authentication」を参照してください。

TLSでは、パブリックキーとプライベートキーのペア、およびパブリックキーとサーバーのIDをリンクする暗号化証明書がサーバーに必要です。証明書には、クライアントが信頼するエンティティの署名が必要です。一方、クライアントは、このエンティティを「信頼する」ように構成する必要があります。サーバーとクライアントが同じ機関によって管理されている場合は、証明書をローカルに作成できます (自己署名証明書)。もう1つの安全な方法は、クライアントが信頼するように事前に設定された組織が署名した証明書を取得することです。この方法では、数ある商用証明機関 (CA) のいずれかと取引する必要があります。

既存のデフォルトモードのインストールをFIPSモードにアップグレードする方法については、『ESM Administrator's Guide』を参照してください。

TLSのサポート

実装する必要があるTLSのバージョンは、ESM/Loggerのピアリング、FIPSまたは非FIPSの実装、またはスタンドアロン型のESM構成の使用によって異なります。

注:

- PCI DSS (Payment Card Industry Data Security Standard) 3.2に準拠するには、TLS 1.2を使用します。この場合、ESMピアもESM 6.11.0以降を実行する必要があり、LoggerピアはLogger 6.4以降を実行する必要があります
- スタンドアロン型のESM実装を実行している場合は(他のマネージャーまたはLoggerとのピアリングなし)、FIPSまたは非FIPS設定に関わらずTLS 1.2を使用します。
- ESM 6.11.0より前のESMリリースでは、ピアリングしているESM/Loggerのインスタンスは、TLS 1.0またはTLS 1.1を使用する必要があります。TLS 1.0を使用する場合、そのシステムはPCI DSS 3.2に準拠していないということに注意してください。
- ESM 6.11.0より前のESMリリースでは、スタンドアロン型 (ピアリングなし) のESM/Loggerのインスタンスは、TLS 1.1を使用する必要があります。
- ESM 6.11.0以降、TLS 1.0、1.1および1.2はすべて、FIPSモードおよびデフォルト (非FIPS) モードのESMでサポートされています。SSLプロトコルはサポートされなくなりました。

また、次の表は、ESMまたはLoggerとピアリングしているESM 6.11.0システムでサポートされるTLSを表しています。

ESM 6.11.0からのピアリング先		
	非FIPS	**FIPS**
ESM 6.11.0	TLS 1.2	TLS 1.2
ESM 6.11.0より前のESMリリース	TLS 1.0 *、TLS 1.1	TLS 1.0 *、TLS 1.1
Logger 6.4	TLS 1.2	TLS 1.2
Logger 6.4より前のLoggerリリース	TLS 1.0 *、TLS 1.1、TLS 1.2	TLS 1.0 *、TLS 1.1
* TLS 1.0の使用は、PCI DSS 3.2に準拠していないことに注意してください。		

サーバー側認証

SSLハンドシェイクの最初のステップでは、サーバー(ArcSightマネージャー)が自分自身をArcSightコンソールに対して認証します。これをサーバー側認証といいます。

ArcSightマネージャーでサーバー側認証のためにTLS構成を設定するには、以下のものが必要です。

- ArcSightマネージャーのキーストア内のキーペア。
- ArcSightマネージャーのキーストアに格納されているキーペアの公開鍵が組み込まれたArcSightマネージャーの証明書。デフォルトでは、自己署名証明書です。

次に、ArcSightマネージャーの証明書をキーストアからエクスポートし、最後にこの証明書を、このArcSightマネージャーに接続するクライアントのキーストアにインポートします。

クライアント側認証

SSL 3.0は、クライアント側認証をサポートしています。これは、オプションで追加のセキュリティ対策として設定できます。クライアント側認証では、クライアント自身がサーバーに対して認証を行います。SSLハンドシェイクでは、クライアント側認証が設定されている場合、サーバー(ArcSightマネージャー)がクライアントに対する認証を行った後で、クライアント側認証が行われます。この時点で、サーバーはクライアントが自分自身を認証するように要求します。

クライアントがArcSightマネージャーに対して自分自身を認証するには、クライアントのキーストアに以下のものが必要です。

- キーペア。
- クライアントの公開鍵を組み込んだクライアントの証明書。

Common Access CardなどのPKCS＃11トークンを使用する場合は、トークンはArcSightマネージャーに対するクライアントであるため、トークンの証明書をArcSightマネージャーのFIPSトラストストアにインポートする必要があります。

上記の各手順の詳細手順については、『ESM Administrator's Guide』の「Establising SSL Client Authentication」を参照してください。

マネージャーの証明書のクライアントへのエクスポート

このトピックは、証明書を自動的にインポートするArcSightコンソールには適用されません。コネクターなど、マネージャーに接続するクライアントをインストールするときは、このエクスポートされた証明書を使用可能にする必要があります。証明書をインストールするときに、証明書をクライアントのキーストアにインポートします。ArcSightマネージャーの証明書をインポートすると、クライアントがArcSightマネージャーを信頼できるようになります。

マネージャーの証明書をインポートするには、ArcSightマネージャーの`/opt/arcsight/manager/bin`ディレクトリから次のコマンドを実行します。

```
./arcsight keytool -exportcert -store managerkeys -alias mykey -file <path_
to_manager_certificate.cer>
```

注: `-file`には、エクスポートしたArcSightマネージャーの証明書を格納する場所への絶対パスを指定します。絶対パスを指定しない場合、ファイルはデフォルトで`/opt/arcsight/manager`ディレクトリにエクスポートされます。

たとえば、ArcSightマネージャーの証明書を`/opt/arcsight/manager`ディレクトリにエクスポートし、次のコマンドを実行します。

```
./arcsight keytool -exportcert -store managerkeys -alias mykey -file
manager.cer
```

これにより、`ManagerCert.cer`ファイル、ArcSightマネージャーの証明書が`/opt/arcsight/manager`ディレクトリにエクスポートされます。

マネージャーの多くのユーティリティ機能 (`arcsight archive`や`arcsight managerinventory`など) は、マネージャー用のクライアントです。FIPSモードでは、マネージャーの証明書は自動的にインポートされません。ユーティリティを使用するには、次のコマンドを実行して証明書をインポートします。

```
./arcsight keytool -importcert -store clientcerts -alias <hostname> -file
<path_to_manager_certificate.cer>
```

FIPSモード設定でのPKCS#11トークンの使用

ActivClientのCommon Access Card (CAC) または90MeterなどのPKCS＃11トークンを使用するには、「PKCS#11プロバイダーを使用するためのセットアップ」(71ページ)に記載された手順に従います。

FIPSモードでのArcSightコンソールのインストール

注: ArcSightコンソールでクライアント側認証をセットアップする場合の詳細な手順については、『Administrator's Guide』を参照してください。

FIPSモードを使用している場合は、Mac上でArcSightコンソールを使用することはできません。

一般的に、ArcSightコンソールは、ArcSightマネージャーを保護するファイアウォールの外にある複数の周辺マシンに展開されます。

ArcSightコンソールをサポートするプラットフォームの詳細については、Protect 724サイト (https://www.protect724.hpe.com) で入手可能な『ESM Product Lifecycle』ドキュメントを参照してください。

このセクションでは、ArcSightコンソールをFIPSモードのみでインストールする方法について説明します。ArcSightコンソールをデフォルトモードでインストールする方法の詳細については、このガイドの「ArcSightコンソールのインストール」の章を参照してください。

ArcSightコンソールをFIPS対応のArcSightマネージャーと通信させるには、ArcSightコンソールがArcSightマネージャーを信頼する必要があります。この信頼を確立するには、ArcSightマネージャーの証明書をArcSightコンソールキーストアにインポートします。ArcSightコンソールをFIPS用に設定すると、最初に起動するときに自動的にArcSightマネージャーの証明書がインポートされます。キーストアに証明書が存在している場合、インポートは行われません。

ArcSightコンソールをFIPSモードでインストールするには:

1. ターゲットプラットフォームに適した自己解凍アーカイブファイルを実行します。
2. ウィザードの画面に表示されるプロンプトに従います。各画面の詳細については、「ArcSightコンソールのインストール」の章を参照してください。
3. 次の画面で [**No, I do not want to transfer the settings**] を選択し、[**Next**] をクリックします。
4. 次の画面が表示されます。

   [**Run console in FIPS mode**] を選択し、[**Next**] をクリックします。
5. FIPSモードを選択すると、デフォルトモードに戻すことができなくなることに注意してください。[**Yes**] をクリックします。
6. 暗号スイートを選択するプロンプトが表示されます。ArcSightマネージャーが使用するFIPSのタイプを選択し、[**Next**] をクリックします。
7. 次に、ArcSightマネージャーのホスト名とポートを指定するプロンプトが表示されます。ArcSightマネージャーのホスト名は、ArcSightマネージャーキーペアの作成時に使用した共通名 (CN) と同じ (短い名前、完全修飾ドメイン名、またはIPアドレス) でなければなりません。
8. 認証オプションを選択する画面が表示されるまで、画面のプロンプトに従ってウィザードを進めます。(各画面の詳細については、このガイドの「ArcSightコンソールのインストール」の章を参照してください)。

   [**Password Based or SSL Client Based Authentication**] を選択します。これは、ArcSightマネージャーをインストールしたときに設定したオプションと同じである必要があります。
9. SSLクライアントベースの認証を使用していて、PKCS#11トークンをArcSightコンソールで使用する場合は、次の画面で [**PKCS#11 Token**] オプションを選択します。別の認証を使用している場合は、この画面は表示されないため、この手順はスキップできます。

   PKCS＃11ライブラリまでのパスを入力するか、PKCS＃11ライブラリを参照します。

   デフォルトでは、PKCS＃11ライブラリは次のディレクトリにあります。

   64ビット版Windowsの場合:

   ```
   C:\Program Files (x86)\ActivIdentity\ActivClient\acpkcs211.dll
   ```

   または、64ビット版WindowsでActivClient 7.1以降の場合:

```
C:\Program Files (x86)\HID Global\ActivIdentity\ActivClient\acpkcs211.dll
```

これらは、両方ともActivClientライブラリの32ビット版です。

ArcSightコンソールでPKCS#11トークンを使用しない場合は、[**Client Key Store**] を選択すると、インストール完了後に、クライアント証明書のセットアップを要求するメッセージが表示されます。

また、90Meterは次の場所から入手できます。

```
C:\Program Files\90meter\CACPIVMD\pkcs11\x86\litpkcs11.dll
```

設定ウィザードを完了したら、『ESM Administrator's Guide』の付録「Configuration Changes Related to FIPS」にある「Setting up Client-Side Authentication」の手順に従います。

10. 画面のプロンプトに従ってウィザードを進め、ArcSightコンソールのインストールを完了します。各画面の詳細については、「ArcSightコンソールのインストール」の章を参照してください。

ArcSightコンソールを起動すると、FIPSモードでArcSightコンソールの実行を開始するというメッセージが表示されます

デフォルトモードArcSightコンソールからFIPS 140-2 ArcSightマネージャーへの接続

追加の設定なしで、デフォルトモードのコンソールをFIPS 140-2マネージャーに接続できます。

注: デフォルトモードのArcSightコンソールFIPS Suite Bを使用してArcSightマネージャーに接続することはできません。

FIPSArcSightコンソールからFIPS対応のArcSightマネージャーへの接続

この手順は、複数のArcSightマネージャーに対して自動的に行います。証明書のコモンネーム(CN)がArcSightコンソールキーストア内の既存の証明書のCNと競合しないように、それぞれのArcSightマネージャーの証明書に一意のCNが指定されていることを確認してください。

ArcSightマネージャーの証明書をArcSightコンソールキーストアに手動でインポートする必要がある場合は、『ESM Administrator's Guide』で手順の詳細を確認してください。

FIPSモードでのSmartConnectorのインストール

ArcSightマネージャーをFIPSモードでインストールする場合は、SmartConnectorもFIPSモードでインストールする必要があります。SmartConnectorのインストールを実行し(SmartConnectorのドキュメントを参照)、[**Enable FIPS Mode**]を選択します。続行または終了を選択する画面が表示されるまで続行します。[**Exit**]を選択し、[**Next**]をクリックします。次の画面で、[**Done**]をクリックします。新しいコネクターを追加する前に、ArcSightマネージャーの証明書をインポートし、コネクターがArcSightマネージャーを信頼できるようにする必要があります。インストールする特定のSmartConnectorの詳細については、SmartConnectorのドキュメントを参照してください。また、SmartConnector用のFIPSモード設定の詳細については、Protect 724 (https://www.protect724.hpe.com/docs/DOC-14956) でESMおよびSmartConnector用のFIPSおよび非FIPS準拠モードの設定を参照してください。

マネージャーの証明書をインポートするには、コネクターの`<ARCSIGHT_HOME>/current/bin`ディレクトリから次のコマンドを実行します。

- Linuxの場合: `cd <CONNECTOR_HOME>/current/jre/bin`を実行し、以下のコマンドを実行します。

  ```
  ./keytool -J-Djava.security.egd=file:/dev/urandom -importcert -file
  <certificate path> -keystore <CONNECTOR_
  HOME>/current/user/agent/fips/bcfips_ks -storepass changeit -storetype
  BCFKS -providername BCFIPS -providerclass
  org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
  <CONNECTOR_HOME>/current/lib/agent/fips/bc-fips-1.0.0.jar -alias "myalias"
  ```

- Windows 64ビットの場合: `cd <CONNECTOR_HOME>\current\jre\bin`を実行し、以下のコマンドを実行します。

  ```
  keytool -importcert -file <CONNECTOR_HOME>\current\manager.cert -keystore
  <CONNECTOR_HOME>\current\user\agent\fips\bcfips_ks -storepass changeit -
  storetype BCFKS -providername BCFIPS -providerclass
  org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
  <CONNECTOR_HOME>\current\lib\agent\fips\bc-fips-1.0.0.jar -alias "myalias"
  ```

プロンプトが表示されたらパスワードとしてchangeitを入力します。これはデフォルトのパスワードです。パスワードを変更した場合は、そのパスワードを入力します。

`<ARCSIGHT_HOME>/current/bin/runagentsetup -i console`を実行して、コネクターの設定を再開します。`-i console`をスキップしてこの設定をGUIモードで実行することもできますが、このドキュメントではコンソール(コマンドライン)モードで実行する手順について説明します。

1. [**Add a Connector**]を選択し、**Enter**キーを押します。
2. 設定するコネクターを選択し、**Enter**キーを押して続行します。
3. 次に表示される各パラメーターで、値を変更するか、デフォルト値を使用することができます。Type of Destinationパラメーターが表示されるまで続けます。

4. 通知先のタイプとして**ArcSight Manager (encrypted)**を選択し、**Enter**キーを押します。
5. [**Destination Parameters**]の下、または次に表示される各パラメーターで、値を変更するか、デフォルト値を使用します。各パラメーターに、マネージャーのホスト名とログイン資格情報を入力します。
6. [**FIPS Cipher Suites parameter**] の値として、次から選択します。
   - **FIPS Default**
   - **FIPS with Suite B 128 bits**
   - **FIPS with Suite B 192 bits**

   Enterキーを押して続行します。
7. 名前や場所などのコネクターの詳細を入力します。任意の値を入力できます。
8. コネクターをサービスとしてインストールするか、スタンドアロンアプリケーションのままにしておくかを決定し、**Enter**キーを押して続行します。
9. コネクター設定ウィザードを終了します。

FIPSモードでSmartConnectorをインストールする方法の詳細については、「FIPSモードでのSmartConnectorのインストール」を参照してください。これは、個々のデバイスのSmartConnector設定ガイドと合わせて使用されます。

Event Brokerへのアクセスの設定 - FIPSモード (サーバー認証のみ) (オプション)

ESMのインストール中にもEvent Brokerへのアクセスを設定できますが、FIPSモード固有のEvent Brokerの設定は、インストールが完了した後でのみ実行できます。この設定は、ESMおよびEvent BrokerがFIPSモードの場合にのみ必要です。ESMとEvent Brokerの統合でサポートされる唯一のFIPSモードは、FIPS 140-2です。

FIPSモードでEvent BrokerへのESMのアクセスを設定するには:

1. arcsightユーザーとして、以下のコマンドを実行して、マネージャーを停止します。

   ```
   /etc/init.d/arcsight_services stop manager
   ```
2. Event Brokerマシンにログオンし、次の場所から証明書をコピーし、

   ```
   /opt/arcsight/kubernetes/ssl/ca.crt
   ```

   ESMマシン上の場所に格納します。
3. 次のarcsight `keytool`コマンドを使用して、ルートCA証明書をESMのクライアントトラストストアにインポートします。

   ```
   bin/arcsight keytool -store clientcerts -importcert -file <absolute path
   to certificate file> -alias <alias for the certificate>
   ```

4. ユーザーarcsightとして/opt/arcsight/manager/binディレクトリから次のコマンドを実行し、managersetupウィザードを起動します。

   ```
   ./arcsight managersetup -i console
   ```

   マネージャー設定ウィザード (managersetup) の実行の詳細については、『ESM Administrator's Guide』の「Using the Configuration Wizard」を参照してください。
5. Event Brokerの設定の箇所までウィザードを進めます。[**Yes**] を選択して接続を設定し、以下の項目を指定します。
   a. **Host: Port(s)**: Event Broker内のノードのホスト (ホスト名またはIPアドレス) とポートの情報を入力します。マスターノードだけでなく、複数のノード環境内のすべてのノードのホストとポートの情報を含めます。入力する内容は、カンマ区切りのリストです (例: <host>:<port>,<host>:<port>)。Event Brokerが受け入れることができるのは、ESMからのIPv4接続だけであることに注意してください。
   b. **Topic to read from**: Event Brokerから購読するトピックを指定します。これにより、データソースが決定されます。『Event Broker管理者ガイド』の「Event Brokerのトピックの管理」の章を参照してください。
   c. **Path to the Event Broker root cert**: このフィールドには値を入力しないでください。ステップ3ですでに証明書をインポートしています。
6. 設定が完了したことを確認するには、[**Next**] をクリックし、設定がエラーなく伝播されていることを確認します。
7. ウィザードを進めて設定を完了します。
8. 設定が完了したら、arcsightユーザーとして次のコマンドを実行し、マネージャーを再起動します。

   ```
   /etc/init.d/arcsight_services start manager
   ```

9. Event Brokerへの接続が機能していることを確認するには、server.std.logでEvent Broker service is initializedという文字列を探します。

Event BrokerとESMの間のSSLクライアント側認証の設定 - FIPSモード

Event Brokerでクライアント側認証を設定する前に、Event Brokerのルート証明書をESMトラストストアにインポートし、Event BrokerとESM間のSSLハンドシェイクを有効にする必要があります。

ESMとEvent Brokerの統合でサポートされる唯一のFIPSモードは、FIPS 140-2です。

Event Brokerのルート証明書をESMマシンにインポートするには:

注: 以下の手順を実行してルート証明書をESMトラストストアにインポートする前に、Event Brokerの証明書がすでにESMにインポートされているかどうかを確認してください。インポートされていない場合は、次の手順を実行します。

1. Event Brokerマシンにログオンし、次の場所から証明書をコピーし、
   `/opt/arcsight/kubernetes/ssl/ca.crt`
   ESMマシン上の場所に格納します。
2. 次のarcsight `keytool`コマンドを使用して、ルートCA証明書をESMのクライアントトラストストアにインポートします。
   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientcerts -importcert -file <absolute path to certificate file> -alias <alias for the certificate>
   ```

Event BrokerとESM間でクライアント側認証をFIPSモードで有効にするには:

重要: クライアント側認証が機能するには、この手順のすべてのステップを完了する必要があります。必ずすべてのステップを実行してください。

1. Event Brokerが機能していること、およびクライアント認証がセットアップされていることを確認します。
2. arcsightユーザーとして、以下のコマンドを実行して、マネージャーを停止します。
   `/etc/init.d/arcsight_services stop manager`
3. `/opt/arcsight/manager/config/client.properties`が存在しない場合は、任意のエディターを使用して作成します。
4. キーペアと証明書署名要求 (.csr) ファイルを生成します。キーペアを生成するときは、証明書の共通名 (CN) としてマネージャーホストの完全修飾ドメイン名を入力します。以下のコマンドを実行します。
   ```
   /opt/arcsight/manager/bin/arcsight keytool -store clientkeys -genkeypair –dname "cn=<your host's fully qualified domain name>, ou=<your organization>, o=<your company>, c=<your country>" -keyalg rsa -keysize 2048 –alias ebkey -startdate -1d -validity 366
   ```
   ```
   /opt/arcsight/manager/bin/arcsight keytool -certreq -store clientkeys -alias ebkey -file ebkey.csr
   ```
   `ebkey.csr`は、`csr`が格納されている出力ファイルです。
5. Event Brokerのルート証明書で.csrに署名します。Event Brokerのルート証明書は、Event Brokerマシンの`/opt/arcsight/kubernetes/ssl`に`ca.crt`という名前で存在します。キーは`ca.key`という名前です。たとえば、次のコマンドは、`ca.crt`および`ca.key`が存

在する場合、Event Brokerマシン上でも、opensslが機能する別のマシンでも実行できます。

```
openssl x509 -req -CA <full path to ca.crt> -CAkey <full path to ca.key> -in <full path to the esm csr> -out <full path and file name for storing the generated cert> -days 3650 -CAcreateserial -sha256
```

例:

```
openssl x509 -req -CA /tmp/ca.crt -CAkey /tmp/ca.key -in /tmp/ebkey.csr -out /tmp/ebkey.crt -days 3650 -CAcreateserial -sha256
```

6. ESMマシンで、次のコマンドを実行して、署名付き証明書 (上記のopensslコマンドの-outパラメーター) をインポートします。

```
/opt/arcsight/manager/bin/arcsight keytool -store clientkeys -alias /tmp/ebkey -importcert -file <path to signed cert>
 -trustcacerts
```

例:

```
/opt/arcsight/manager/bin/arcsight keytool -store clientkeys -alias /tmp/ebkey -importcert -file ebkey.crt -trustcacerts
```

7. 設定が完了し、Event Brokerへの接続が正常に確立されたことを確認するには、managersetupを実行して、設定がエラーなく伝播されていることを確認します。
8. マネージャーを起動します。

```
/etc/init.d/arcsight_services start manager
```

インストールがFIPS対応かどうかを確認する方法

既存のインストールがFIPSモードとデフォルトモードのどちらでインストールされているかを確認するには、次の場所にあるコンポーネントのプロパティファイルでfips.enabledプロパティを確認します。

- /opt/arcsight/manager/config/server.properties (ArcSightマネージャー)
- <ARCSIGHT_HOME> /current/config/console.properties (ArcSightコンソール)

FIPSモードが有効な場合、プロパティはfips.enabled = trueに設定されているはずです。コンポーネントがデフォルトモードで実行されている場合、プロパティはfalseに設定されます。

また、コンソールがFIPSモードで起動すると、console.logにそのことを示すメッセージが記録されます。マネージャーがFIPSモードで起動すると、server.std.logにそのことを示すメッセージが記録されます。

付 録E: Event Brokerのベストプラクティス

この付 録には、ESMで動 作 するEvent Brokerに関 連 するベストプラクティス情 報 が記 載 されています。Event Brokerの設 定 とプロパティの設 定 の詳 細 については、『Event Broker管 理 者 ガイド』を参 照 してください。

- バイナリイベントをEvent Brokerに書 き込 むコネクターおよびそのイベントを消 費 するESMについて、Event Brokerで別 々 のトピックを作 成 します。このトピックには最 低 5つのパーティションが必 要 です。ESMは、ESM側 からコンシューマーの数 を自 動 的 に調 整 してパーティションの数 に合 わせます。『Event Broker管 理 者 ガイド』の「Event Brokerのトピックの管 理 」の章 を参 照 してください。
- バイナリイベントとCEFイベントの両 方 を同 じトピックに送 信 しないでください。Event Brokerでは、常 にイベントの種 類 ごとに専 用 のトピックを使 用 してください。
- ESMが消 費 するデータの予 想 量 を考 慮 した上 で、Event Broker上 の時 間 とスペースの保 有 に関 する保 有 ポリシー設 定 を構 成 してください。この予 想 が重 要 なのは、Event Brokerの保 有 ポリシーがアクティブになる前 に、トピック内 のデータ量 がESMが消 費 可 能 な量 より多 くなると、ESMがまだ読 み取 っていないトピックの一 部 が削 除 される可 能 性 があるためです。Event Brokerの保 有 ポリシーの構 成 については、『Event Broker管 理 者 ガイド』を参 照 してください。
- Event Brokerで使 用 される証 明 書 は、TLSおよびクライアント認 証 の両 方 とも、ESMの起 動 時 に1回 読 み込 まれます。ESMの起 動 後 に証 明 書 を追 加 または変 更 するには、変 更 を加 えてからESMを再 起 動 します。
- ESMを起 動 する前 またはESMの起 動 直 後 に、Event Brokerを起 動 してESMのバイナリトピックを構 成 します。Event Brokerを使 用 するようにESMを構 成 した後 でESMを起 動 すると、ESMは、起 動 時 に読 み取 った構 成 と証 明 書 を使 用 できるまで、数 分 ごとにEvent Brokerに接 続 しようとします。4時 間 が経 過 すると、ESMは間 もなくEvent Brokerが利 用 できなくなると想 定 し、ESMは2時 間 ごとにEvent Brokerに接 続 しようとします。

付録F: ロケールとエンコーディング

ESMは、英語、日本語、中国語 (繁体字)、中国語 (簡体字)、フランス語、ロシア語、および韓国語をサポートしています。これらの言語に対してロケールを設定することにより、国または言語に対する、言語設定、数の書式、日付/時間の書式、タイムゾーンの設定、および夏時間の設定に関して、最適な環境を用意できます。ここでは、サポートされている言語に対してESMを構成したときに考慮すべき変更部分について説明します。

ロケールとエンコーディングの用語

キャラクターセット

キャラクターセットとは、特定の目的に合うようにまとめられた文字の集合です。英語のアルファベットは、その一例です。

コードポイント

コードセット内の各文字の値をコードポイントといいます。

コードセット

キャラクターセットの各文字には固有の値が割り当てられています。これらの値を総称してコードセットといいます。

エンコーディング

エンコーディングは、各文字のコードがメモリやディスクファイルにどのように格納されるかを指定します。

国際化

国際化とは、アプリケーションに対して、技術的な変更を加えずに多種多様な言語や地域に適合できるように設計するプロセスのことです。

ロケール

ロケールは、ArcSight ESMを実行している地域を指します。ロケールには、言語、数の書式、日付/時刻の書式などが含まれます。

ローカリゼーション

ローカリゼーションとは、国際化されたアプリケーションに対して、ある言語をサポートするようにその言語特有のファイルを追加するプロセスのことです。

地域コード

現在、使用されている地域コードの標準は**ISO 3166-2**です。ESMの以前のバージョンでは、地域コードの標準として**FIPS 10-4**が使用されていましたが、これはサポートされなくなりました。このため、地域をIPアドレスをもとに地理情報で表す方法が変わっています。たとえば、ESMの6.9.1以前のバージョンでは、IPアドレス176.62.127.255に対する地域コードとして54が報告されます。これ以降のリリースでは、OMSとして報告されます。

Unicode

Unicodeとは、世界の主要な言語すべての文字に固有のコードポイントを割り当てた大規模な汎用キャラクターセットです。

UTF-8

ESMでサポートされているUnicodeのバージョンです。

ESMのローカライズバージョンをインストールする前に

注: ArcSightマネージャーとコンソールは同じロケールで構成する必要があります。

デフォルトでは、ArcSightコンポーネント間のすべての通信にはUTF-8文字エンコーディングが使用されます。ESM内部でサポートされているのはUTF-8のみですが、コネクターがたとえばUTF-16でイベントを受信した場合でも、イベントは正しく格納されます。これは、イベントが、マネージャーに渡される前にコネクターによりUTF-8に変換されるためです。

ArcSightコンソールとマネージャー

最 適 な結 果 を得 るため、ArcSightコンソールは、マネージャーと同 じロケールに設 定 されているオペレーティングシステムにインストールしてください。ArcSightコンソールとマネージャーは、起 動 中 にオペレーティングシステムからロケールを自 動 的 に検 知 して使 用 します。

ArcSight SmartConnectors

デバイスがある言 語 固 有 のエンコーディング (Unicode以 外) に構 成 されている場 合 、このデバイスからイベントを受 信 するコネクターも同 じエンコーディングを使 用 するように構 成 する必 要 があります。

選 択 したSmartConnectorに対 するエンコーディングの設 定

コネクターによっては、使 用 するロケールに応 じてキャラクターセットにエンコーディングを設 定 することができます。エンコーディングを構 成 する手 順 については、『SmartConnector Configuration Guide』を参 照 してください。そのようなコネクターは、Javaがサポートするキャラクターセットをすべてサポートしています。

> ログファイルがデフォルト 以 外 のエンコーディングを使 用 している場 合 のみ、ログファイルの設 定 に合 うようにエンコーディングを変 更 してください。

特 定 のエンコーディング設 定 をサポートしていないコネクターは、実 行 しているオペレーティングシステムのデフォルトのエンコーディングを使 用 しています。

日 付 形 式 のローカライズ

コネクターが受 信 したログに、英 語 以 外 の言 語 またはロケールのタイムスタンプや日 付 の書 式 が含 まれる場 合 (例 :「mai 24, 2015 12:56:07.615」ここで、「mai」は「May」のドイツ語) は、`agent.properties`ファイルで`agent.parser.locale.name`プロパティを構 成 してください。このファイルは、`<ARCSIGHT_HOME>/current/user/agent` ディレクトリにあります。

`agent.parser.locale.name`プロパティの値 をコネクターのロケールに一 致 するように設 定 してください。デフォルトでは、このプロパティはen_USに設 定 されています。このプロパティに設 定 可 能 な値 については、「設 定 可 能 な値 のリスト」(97ページ) の表 を参 照 してください。

設定可能な値のリスト

agent.parser.locale.nameの値

以下の表には、このプロパティに設定可能な値が記載されています。

値	言語	国	変化形
ar	アラブ語		
ar_AE	アラブ語	アラブ首長国連邦	
ar_BH	アラブ語	バーレーン	
ar_DZ	アラブ語	アルジェリア	
ar_EG	アラブ語	エジプト	
ar_IQ	アラブ語	イラク	
ar_JO	アラブ語	ヨルダン	
ar_KW	アラブ語	クエート	
ar_LB	アラブ語	レバノン	
ar_LY	アラブ語	リビア	
ar_MA	アラブ語	モロッコ	
ar_OM	アラブ語	オマーン	
ar_QA	アラブ語	カタール	
ar_SA	アラブ語	サウジアラビア	
ar_SD	アラブ語	スーダン	
ar_SY	アラブ語	シリア	
ar_TN	アラブ語	チュニジア	
ar_YE	アラブ語	イエメン	
be	ベラルーシ語		
be_BY	ベラルーシ語	ベラルーシ	

値	言 語	国	変 化 形
bg	ブルガリア語		
bg_BG	ブルガリア語	ブルガリア	
ca	カタロニア語		
ca_ES	カタロニア語	スペイン	
cs	チェコ語		
cs_CZ	チェコ語	チェコ共 和 国	
da	デンマーク語		
da_DK	デンマーク語	デンマーク	
de	ドイツ語		
de_AT	ドイツ語	オーストリア	
de_CH	ドイツ語	スイス	
de_DE	ドイツ語	ドイツ	
de_LU	ドイツ語	ルクセンブルク	
el	ギリシャ語		
el_GR	ギリシャ語	ギリシャ	
en	英 語		
en_AU	英 語	オーストラリア	
en_CA	英 語	カナダ	
en_GB	英 語	イギリス	
en_IE	英 語	アイルランド	
en_IN	英 語	インド	
en_NZ	英 語	ニュージーランド	
en_US	英 語	アメリカ合 衆 国	
en_ZA	英 語	南 アフリカ	
es	スペイン語		

値	言語	国	変化形
es_AR	スペイン語	アルゼンチン	
es_BO	スペイン語	ボリビア	
es_CL	スペイン語	チリ	
es_CO	スペイン語	コロンビア	
es_CR	スペイン語	コスタリカ	
es_DO	スペイン語	ドミニカ共和国	
es_EC	スペイン語	エクアドル	
es_ES	スペイン語	スペイン	
es_GT	スペイン語	グアテマラ	
es_HN	スペイン語	ホンジュラス	
es_MX	スペイン語	メキシコ	
es_NI	スペイン語	ニカラグア	
es_PA	スペイン語	パナマ	
es_PE	スペイン語	ペルー	
es_PR	スペイン語	プエルトリコ	
es_PY	スペイン語	パラグアイ	
es_SV	スペイン語	エルサルバドル	
es_UY	スペイン語	ウルグアイ	
es_VE	スペイン語	ベネズエラ	
et	エストニア語		
et_EE	エストニア語	エストニア	
fi	フィンランド語		
fi_FI	フィンランド語	フィンランド	
fr	フランス語		
fr_BE	フランス語	ベルギー	

値	言 語	国	変 化 形
fr_CA	フランス語	カナダ	
fr_CH	フランス語	スイス	
fr_FR	フランス語	フランス	
fr_LU	フランス語	ルクセンブルク	
hi_IN	ヒンディー語	インド	
hr	クロアチア語		
hr_HR	クロアチア語	クロアチア	
hu	ハンガリー語		
hu_HU	ハンガリー語	ハンガリー	
is	アイスランド語		
is_IS	アイスランド語	アイスランド	
it	イタリア語		
it_CH	イタリア語	スイス	
it_IT	イタリア語	イタリア	
iw	ヘブライ語		
iw_IL	ヘブライ語	イスラエル	
ja	日 本 語		
ja_JP	日 本 語	日 本	
ko	韓 国 語		
ko_KR	韓 国 語	韓 国	
lt	リトアニア語		
lt_LT	リトアニア語	リトアニア	
lv	ラトビア語		
lv_LV	ラトビア語	ラトビア	
mk	マケドニア語		

値	言 語	国	変 化 形
mk_MK	マケドニア語	マケドニア	
nl	オランダ語		
nl_BE	オランダ語	ベルギー	
nl_NL	オランダ語	オランダ	
no	ノルウェー語		
no_NO	ノルウェー語	ノルウェー	
no_NO_NY	ノルウェー語	ノルウェー	Nynorsk
pl	ポーランド語		
pl_PL	ポーランド語	ポーランド	
pt	ポルトガル語		
pt_BR	ポルトガル語	ブラジル	
pt_PT	ポルトガル語	ポルトガル	
ro	ルーマニア語		
ro_RO	ルーマニア語	ルーマニア	
ru	ロシア語		
ru_RU	ロシア語	ロシア	
sk	スロバキア語		
sk_SK	スロバキア語	スロバキア	
sl	スロベニア語		
sl_SI	スロベニア語	スロベニア	
sq	アルバニア語		
sq_AL	アルバニア語	アルバニア	
sv	スウェーデン語		
sv_SE	スウェーデン語	スウェーデン	
th	タイ語		

値	言 語	国	変 化 形
th_TH	タイ語	タイ	
th_TH_TH	タイ語	タイ	TH (数 字 は、アラビア数 字 ではなく、タイ語 の数 字 です)
tr	トルコ語		
tr_TR	トルコ語	トルコ	
uk	ウクライナ語		
uk_UA	ウクライナ語	ウクライナ	
vi	ベトナム語		
vi_VN	ベトナム語	ベトナム	
zh	中 国 語		
zh_CN	中 国 語	中 国	
zh_HK	中 国 語	香 港	
zh_TW	中 国 語	台 湾	

ローカライズされたデバイスに対 するキー/値 パーサー

ローカライズされたデバイスの中 には、イベントメッセージにローカライズされた値 だけではなくローカライズされたキーも送 信 するものがあります。このような場 合 、イベントメッセージが正 しく解 析 されるためには、キーを英 語 に変 換 するための処 理 が追 加 で必 要 となります。たとえば、キー/値 パーサーの内 容 が以 下 のようになっているときに、

event.destinationUserName=User

以 下 のイベントメッセージを受 信 したとします。

User=김

김 は「KIM」を韓 国 語 で表 記 したものです。

この場 合 は、ダブルバイトはすでにサポートされているため、パーサーはそのままで問 題 なく動作します。

受 信 したイベントメッセージが以 下 のようになっていたとします。

우새르

우새르 は「User」を韓 国 語 で表 記したものです。この場 合 は、김を「User」に変 換 するマッピングが追 加 で必 要 となります。

ローカライズされたデバイスに上 記 のような処 理 が必 要 になる場 合 は、HPE SSO Webサイトからカスタマーサポートにお問い合 わせください。

付録G: アプライアンスの工場出荷時設定の復元

アプライアンスを元の工場出荷時設定に戻すには、組み込みのSystem Restoreユーティリティを使用します。

注意: 工場出荷時設定にリセットすると、すべてのイベントおよび設定データが削除され、元に戻すことはできません。
アプライアンスを工場出荷時の設定に復元するには、次の手順を実行します。

1. キーボード、モニター、およびマウスをアプライアンスに直接接続し、オペレーティングシステムのコンソールセッションを開きます。
2. アプライアンスを再起動します。
3. 数分後、Linuxのブートメニューが表示されたら、下矢印キーを使用してメニューから[**System Restore <build_num>**] を選択し、**Enter**キーを押します。

   System Restoreによって自動的にアーカイブイメージが検出され、表示されます。

   イメージは、次の形式で名前が付けられます。

   ```
   YYYY-MM-DD_ <model> _ <build_num> .ari
   ```

   YYYY-MM-DDは日付、<model>はアプライアンスのモデル、<build_num>は復元されるイメージのビルド番号です。イメージに問題がある場合は、カスタマーサポートに連絡してください。
4. **F10** (VERIFY) を押して、復元を行う前にアーカイブが損傷していないことを確認します。
5. **F1** (AUTOSELECT) を押すと、元のイメージが自動的にマップされます。
6. **F2** (RESTORE) を押して復元処理を開始します。

   注意: 復元処理の間は、中断したりアプライアンスの電源をオフにしないでください。復元処理を中断すると、システムが回復不能な状態に陥る可能性があります。
7. 復元処理が完了したら、**F12**を押してアプライアンスを再起動します。

ドキュメントに関するご意見、ご指摘

本書に関するコメントは、ドキュメントチーム窓口宛てに電子メールでお寄せください。システムに電子メールクライアントが構成されていない場合は、上記のリンクをクリックすると電子メールのウィンドウが開きます。件名は、以下のようになっています。

ESMインストールガイド(ESM 6.11.0)に関するフィードバック

フィードバックをご記入のうえ、送信ボタンを押してください。

電子メールクライアントが使用できない場合は、上記のフィードバック内容をWebメールクライアントに貼り付けてarc-doc@hpe.com宛てに送信していただくことも可能です。

頂いたフィードバックは、ドキュメント改善のための貴重なご意見として活用させていただきます。