Hewlett Packard Enterprise

HPE Security ArcSight Management Center

ソフトウェアバージョン: 2.6x

管理者ガイド

2017年7月13日

ご注意

保証

Hewlett Packard Enterprise製品およびサービスに対する保証については、当該製品およびサービスの保証規定書に記載されています。ここでの記載は、追加保証を提供するものではありません。ここに含まれる技術的、編集上の誤り、または欠如について、Hewlett Packard Enterpriseはいかなる責任も負いません。

ここに記載する情報は、予告なしに変更されることがあります。

本書の例で使用しているネットワーク情報 (IPアドレスやホスト名を含む) は、説明のみを目的としています。

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

本書は機密情報です。

権利の制限

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

著作権について

著作権と謝辞の完全な記述については、以下のリンク先をご覧ください。
https://www.protect724.hpe.com/docs/DOC-13026

サポート

連絡窓口

電話	電話番号の一覧は、HPE Security ArcSightテクニカルサポートページに掲載しています: 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: HPE ArcSight Management Centerの概要

ここでは、以下の内容について説明します。

HPE ArcSight Management Center (ArcMC) は、セキュリティポリシーの設定、展開のメンテナンス、および監視を効率的かつ経済的な方法で簡素化する一元管理ツールです。

ArcMCでは、次の重要な機能が利用できます。

• **管理および監視:** 単一の管理インターフェイスを利用して、コネクターアプライアンス、Logger、コネクター、他のArcMC、およびEvent Brokerなど、ArcSightの管理対象ノードの管理と監視を行うことができます。

• **SmartConnectorホスティング:** ハードウェアアプライアンスの場合、SmartConnectorをインスタンス化 (ホスティングおよび実行) するプラットフォームとして機能します。

ArcMCには、次の利点があります。

- 新規のセキュリティポリシーおよび更新されたセキュリティポリシーの迅速な実装。
- 管理対象ノードの設定の精度向上とエラー削減。
- 運用費用の削減。

新機能と機能強化

このバージョンのArcMCには、次の新機能と機能強化が含まれています。

- **Event Broker管理:** ArcSight Event Broker管理には、ルートおよびトピックの作成に加えて、ヘルスおよびステータスパラメーターの監視が含まれます。Event Brokerの管理対象パラメーターには、CPU使用量、メモリ、ディスク使用量、Event Brokerスループット、合計EPS入力、イベント解析エラー、ストリーム処理EPS、およびストリーム処理遅延があります。
- **ノード管理インターフェイスの改善:** ノード管理インターフェイスが、分かりやすく使いやすいものに改善されました。
- **トポロジビューの改善:** トポロジビューに、アクティブでないデバイスを期限切れにして、管理から除外するための、タイムアウト設定が追加されました。

- **ホストのインポート処理の改善:** 複数のジョブが並列して実行されるため、CSVからのホストのインポートに要する時間が以前よりも短くなります。
- **License Consumptionレポートの改善:** License Consumptionレポートを、年単位ではなく、指定された時間間隔で実行できるようになりました。
- **新しいルール:** 追加の監視ルールがいくつかデフォルトで有効になりました。これらは必要に応じて編集または削除できます。

第2章: ソフトウェアのインストール

この章では、ソフトウェアArcSight Management CenterおよびArcSight Management Centerエージェントをインストールする方法について説明します。

ここでは、以下の内容について説明します。

概要

ソフトウェアArcSight Management Centerをインストールするプロセスは、以下の手順で構成されます。

インストールモードを選択する

選択したマシンにソフトウェアArcSight Management Centerをインストールするモードを選択します。rootユーザーとしてインストールする準備をします。また、ArcMCのインストール中には、アプリケーションを起動するのに使用するユーザー名の入力を求められます。

ソフトウェアArcSight Management Centerは、次のモードでインストールできます。

- **GUI**: GUIモードでは、ウィザードが、インストールと設定のプロセスを手順ごとにガイドします。詳しい手順については、「インストールの手順」(20ページ)を参照してください。

  注: Windowsシステムを使用してソフトウェアArcSight Management Centerをインストールするマシンに接続し、GUIモードでインストールを行う場合は、**Xming for Windows**などのX Windowクライアントを使用して接続する必要があります。

- **コンソール**: コンソールモードでは、コマンドラインプロセスが、インストールと設定のプロセスを手順ごとにガイドします。詳しい手順については、「インストールの手順」(20ページ)を参照してください。
- **サイレント:** サイレントモードでは、インストールプロセスをスクリプトで記述します。インストールと設定の入力内容はファイルを通じて提供するため、インストーラーとの対話は必要ありません。詳しい手順については、「インストールの手順」(20ページ)を参照してください。

ライセンスを適用する

ソフトウェアArcSight Management Centerには、有効なライセンスが必要です。ライセンスファイルは、製品のインスタンスごとに一意に生成されます。そのため、同じライセンスファイルを使用して、製品の複数のインスタンスをインストールすることはできません。

ライセンスを取得するには、発注後にHPEから電子メールで送付されるElectronic Delivery Receiptの手順に従ってください。

ArcMCのインストール中に、ライセンスのインストールを求めるプロンプトが表示されます。ライセンスを提示しない場合は、デフォルトで「インスタントオン」ライセンスが適用されます。インスタントオンライセンスは、30日間有効です。この期間中に、HPE Software Entitlementポータルから正規のライセンスを入手して適用してください。

サービスとして起動する

rootユーザーとしてインストールを行っている場合は、システムサービスとして起動するようにソフトウェアArcSight Management Centerを設定できます。詳細については、「システムサービスとしてのArcSight Management Centerの有効化/無効化」(26ページ)を参照してください。

ホストを解決可能にする

Apache Webプロセスを起動するには、ソフトウェアArcSight Management Centerのホスト名が解決可能である必要があります。ホスト名を`/etc/hosts`またはDNSに追加します。

資格情報を保護する

初期セットアップが完了したら、アプリケーションに接続し、デフォルトのパスワードをセキュアなパスワードに変更します。デフォルトのパスワードを変更するには、「ArcMCのユーザー/グループ」(263ページ)の手順に従います。

必要に応じて、追加のセキュリティ対策として、デフォルトの管理者ユーザー名をセキュアなユーザー名に変更します。ユーザー名を変更するには、「User Management」(273ページ)の手順に従います。

ArcMCエージェントをインストールする(必要な場合)

さらに、1つ以上のソフトウェアArcMC、ソフトウェアコネクターアプライアンス、またはソフトウェアLoggerを管理することを計画している場合は、それぞれにArcSight Management Centerエージェントをインストールする必要があります。ArcSight Management Centerエージェントの

手動インストールの詳細については、「ArcSight Management Centerエージェントのインストール」(33ページ)を参照してください。

ArcMCアプライアンスまたはソフトウェアArcMCおよびソフトウェアLoggerの最新バージョンの場合、インストールの必要はありません。

ファイアウォールのポートを開く

最適な形で機能するように、ファイアウォールで必要なポートを開きます。必要なオープンポートの一覧については、「ファイアウォールルールの設定」(28ページ)を参照してください。

ArcSight Marketplaceでアカウントを作成する

ArcSight Marketplaceは、コンテンツ更新、信頼できるセキュリティコンテンツパッケージ、およびベストプラクティスを通じて、ArcSight SIEMの迅速なプロビジョニングを可能にするアプリストアです。

ArcSight Management Centerでは、一部のコンテンツ更新をダウンロードして実行するのに、ArcSight Marketplaceのグローバル管理アカウントが必要です。ArcSight Marketplace (https://marketplace.saas.hpe.com/arcsight) にアクセスして、管理アカウントをセットアップします。

ArcSight Management Centerのインストール

ここでは、ソフトウェアArcSight Management Centerをインストールする手順について説明します。

インストールの前提条件

ソフトウェアArcMCのインストールを始める前に、以下の前提条件を確認してください。

前提条件	説明

ファイル記述子数の制限	ホストでは、ファイル記述子数を10240に制限している必要があります。現状のレベルを確認するには、ホスト上で`ulimit -n`を実行します。制限が10240に等しくない場合は、以下の手順を実行します。
	1. `/etc/security/limits.conf`を開きます(または作成します)。
	2. 次の2つのパラメーターを設定します。
	`* hard nofile 10240`
	`* soft nofile 10240`
	3. ファイルを保存します。
	4. セッションを再起動します。

UTF-8サポート	ホストはUTF-8をサポートしている必要があります。
unzipパッケージ	ソフトウェアArcSight Management Centerをインストールする前に、unzipコマンドのパスを設定する必要があります。
非rootアカウント	ArcSight Management Centerをrootユーザーとしても、root以外のユーザーとしてもインストールできます。ただし、rootユーザーとしてインストールする場合は、一部の必要なプロセスを実行するのに、root以外のユーザーアカウントが必要になります。 • rootユーザーとしてArcSight Management Centerをインストールする場合は、安全なWeb接続(HTTPS)をリスンするポートを選択できます。root以外のユーザーとしてインストールする場合は、ポートを9000に設定する必要があります。この値は変更できず、外部からアクセス可能でなければなりません。 • ArcSight Management Centerをroot以外のユーザーとしてインストールし、ホストを再起動した場合、ArcMCのサービスは自動的に開始されません。この場合は、次のコマンドを使用して、手動で開始します。 `<install_dir>/current/arcsight/arcmc/bin/arcmcd start` root以外のアカウントを使用してインストールした場合は、初期化スクリプトを使用してサービスを自動的に起動します。「root以外のインストールでのサービスの自動起動」(27ページ)を参照してください。
タイムゾーンデータベース	tzdata-2016g以降が必要です。
OSのアップグレード	ArcMCをインストールする際には、事前にサポートされるオペレーティングシステムへのアップグレードを行います。サポートされるオペレーティングシステム、サポートされるブラウザー、およびその他の技術要件に関する最新情報については、HPE ArcSightソフトウェアコミュニティから入手可能なArcSight Management Centerのリリースノートを参照してください。

インストールの手順

インストールを開始するには、選択したマシンにソフトウェアArcSight Management Centerをインストールするモードを選択します。GUIモード、コンソールモード、およびサイレントインストールの3つのモードから選択できます。

GUIモードのインストール

GUIモードのインストールでは、インストーラーウィザードを使用してアプリケーションをインストールします。

GUIモードを使用してソフトウェアArcSight Management Centerをインストールするには

1. ソフトウェアArcSight Management Centerインストーラーをコピーしたディレクトリから以下の2つのコマンドを実行します。
   - `chmod +x ArcSight-ArcMC-2.6.0.<installer_build_number>.0.bin`
   - `./ArcSight-ArcMC-2.6.0.<installer_build_number>.0.bin`

     ここで、`<installer_build_number>`は最新のインストーラーのビルド番号です。

     インストールウィザードが起動します。ダイアログボックスを確認し、[**Next**] をクリックします。
2. ライセンス契約の詳細を確認し、ライセンス契約の詳細の一番下までスクロールします。[**I accept the terms of the License Agreement**] を選択します。続いて、[**Next**] をクリックします。
3. 以下に示すように、ArcSight Management Centerをインストールするフォルダーを指定または参照します。デフォルトのインストールディレクトリは、`/opt`です。ただし、ArcSight Management Centerのファイルを容易に識別できるように、`/opt`内の新しいインストールディレクトリ(`/opt/arcmc`など) を指定して、他のHPE ArcSight製品に関連するファイルと区別することをお勧めします。
4. [**Pre-Installation Summary**] ダイアログでインストール情報のサマリーを確認し、[**Install**] をクリックします。

   ArcSight Management Centerのインストーラーによるインストールが始まります。
5. インストールが完了したら、[**Next**] をクリックして設定ウィザードを開始します。
6. ArcSight Management Centerソフトウェアのインストーラーをrootユーザーとして実行している場合は、次のダイアログでroot以外の既存のユーザーを指定し、ArcSight Management Centerのユーザーが UIを介して接続するのに使用するポートを設定できます。

   たとえば、標準HTTPSポートである443や、それぞれのニーズに適したその他のポートを入力できます。443以外のポートを指定する場合、ArcSight Management Center UIにアクセスするために使用するURLにポート番号を入力する必要があります。

   root以外のユーザーのユーザー名とHTTPSポート番号を入力し、[**Next**] をクリックします(これらの値はインストールプロセスで後から変更できません)。
7. ソフトウェアがインストールされたら、[**Next**] をクリックしてArcSight Management Centerの初期化を開始します。

8. 初期化が完了したら、[**Done**] をクリックしてArcSight Management Centerの設定ウィザードを起動します。

   注: 設定ウィザードは自動的に起動します。自動的に起動しない場合は、次のコマンドを使用してウィザードを起動します。

   ```
   <install_dir>/current/arcsight/arcmc/bin/arcsight arcmcsetup
   ```

9. ArcSight Management Centerソフトウェアのインストーラーをrootユーザーとして実行している場合は、次のダイアログで、システムサービスとして実行するようにArcSight Management Centerを設定できます。デフォルトでは、ArcSight Management Centerはスタンドアロンアプリケーションとして実行されるため、手動で起動する必要があります。

   ArcSight Management Centerをrootユーザーとしてインストールする場合、`arcsight_arcmc`という名前のサービスを設定、作成し、ランレベル3と5で有効化できます。

   さらに、`ldconfig`を使用して、いくつかのライブラリが追加されます。これらのライブラリの一覧については、`/etc/ld.so.conf.d/arcsight_arcmc.conf`と`<install_dir>/current/arcsight/install/ldconfig.out`を参照してください。

10. ArcSight Management Centerのインストールが完了しました。[**Start ArcSight Management Center Now**] をクリックするか、[**Start ArcSight Management Center later**] をクリックしてから、[**Finish**] をクリックします。

    ArcSight Management Centerを後で起動するオプションを選択した場合は、「ArcSight Management Centerデーモン (arcmcd)」(31ページ) の説明を参照して、ArcSight Management Centerを後から起動する方法を確認します。

11. [**Start ArcSight Management Center Now**] を選択した場合は、[**Finish**] をクリックしてウィザードを終了します。または、次のダイアログにArcSight Management Centerのインターフェイスにアクセスするurlが表示されるのを待ちます。

    ArcSight Management Centerは引き続き、バックグラウンドでサービスとプロセスを起動します。ウィザード内で作業を続けることを選択した場合は、ダイアログの手順に従うか、「ArcSight Management Centerユーザーインターフェイスへの接続」(30ページ) の手順を使用して、ArcSight Management Centerに接続します。

コンソールモードのインストール

コンソールモードのインストールでは、コマンドラインインターフェイスを使用してアプリケーションをインストールします。

CLIの最初の数ステップ以降のインストール手順は、「コンソールモードのインストール」(22ページ) で説明したGUIモードのインストールと同じです。GUIモードのインストールで説明した手順に従って、インストールを完了します。

コンソールモードを使用してソフトウェアArcSight Management Centerをインストールするには

1. ArcSight Management Centerソフトウェアをコピーしたディレクトリから以下のコマンドを実行します。

   ```
   chmod +x ArcSight-ArcMC-2.6.0.<installer_build_number>.0.bin
   ```

   ```
   ./ArcSight-ArcMC-2.6.0.<installer_build_number>.0.bin -i console
   ```

   ここで、<installer_build_number>は最新のインストーラーのビルド番号です。

   インストールウィザードがコマンドラインモードで起動します。
2. **Enter**を押して続行します。表示されるプロンプトに従い、インストールと設定を完了します。

注: ArcSight Management Centerをコンソールモードでインストールした場合、アンインストールもコンソールモードで行われます。詳細については、「コンソールモードでのアンインストール」(33ページ)を参照してください。

サイレントモードのインストール

サイレントモードでは、インストールプロセスのスクリプトを記述できます。ArcSight Management Centerをサイレントモードでインストールする前に、サイレントモードのインストールで必要になる2つのプロパティファイルを作成する必要があります。

- インストール用プロパティを取得するためのファイル
- 設定用プロパティを取得するためのファイル

これらの2つのファイルを生成した後に、これらのファイルを1つのファイルにマージして、そのファイルをサイレントモードのインストールに使用します。

サイレントモードのインストール用ライセンス

ソフトウェアArcSight Management Centerのインストールでは、サイレントモードのインストールごとに固有のライセンスファイルが必要です。HPEカスタマーサポートからライセンスを取得し、それをサイレントモードでインストールするマシンにインストールするか、そのマシンからアクセスできる場所に置きます。

サイレントモードインストール用プロパティファイルの生成

この手順では、2つのプロパティファイルを生成した後に、これらを1つのファイルにまとめる方法について説明します。後にサイレントモードでインストールを行う際に、このファイルを使用します。

1. インストール用のプロパティファイルを生成するマシンにログインします。

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

   ```
   ./ArcSight-ArcMC-2.6.0.<installer_build_number>.0.bin -r <directory_location>
   ```

   ここで、<installer_build_number>はインストーラーファイルのビルド番号で、<directory_location>は生成されたプロパティファイルを配置するディレクトリです。これを、ArcSight Management Centerをインストールするのと同じディレクトリにすることはできません。

   プロパティファイルは、installer.propertiesという名前にする必要があります。
3. 「サイレントモードのインストール」(23ページ) の手順に従って、ArcSight Management CenterをGUIモードでインストールし、ステップ10まで進みます。

   インストール手順のステップ10で、以下を実行します。

   a. [**Done**] をクリックして先に進む代わりに、[**Previous**] をクリックします。

   b. 続いて、[**Cancel**] をクリックしてインストールを停止します。
4. 確認メッセージが表示されたら、[**Cancel**] をクリックします。[**Quit**] をクリックして、このメッセージをクリアします。
5. 以前にinstaller.propertiesファイル用に指定したディレクトリに移動します。

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

```
# Replay feature output
# ---------------------
# This file was built by the Replay feature of InstallAnywhere.
# It contains variables that were set by Panels, Consoles or Custom Code.
#Choose Install Folder
#---------------------

USER_INSTALL_DIR=/opt/<arcmc_installation_folder>/<build number>/installdir
#Install
#-------

-fileOverwrite_/opt/<arcmc_installation_folder>/<build
number>/installdir/UninstallerData/Uninstall_ArcSight_Management_Center_
2.1.lax=Yes
#Intervention Required
#---------------------
USER_AND_PORT_1=username
USER_AND_PORT_2=443
```

1. 設定プロパティを記録するオプションを指定して、設定ウィザードを起動します。

   ```
   <install_dir>/current/arcsight/arcmc/bin/arcsight arcmcsetup -i recorderui
   ```

設定プロパティを取得するためのファイル名の入力を求めるプロンプトが表示されたら、分かりやすい名前 (例: config.properties) を入力し、installer.propertiesファイルと同じディレクトリを参照して選択します。

2. 「サイレントモードのインストール」(23ページ) の**ステップ10**からの手順に従って、設定ウィザードを実行します。
3. 設定プロパティファイルが生成されたら、このファイルの内容を前の手順 (「サイレントモードインストール用プロパティファイルの生成」(23ページ)) で生成したinstaller.propertiesファイルに追加して、1つにまとめたファイルを作成します。

   たとえば、次のように、catコマンドを使用して、両方のファイルを連結できます。

   ```
   cat installer.properties config.properties > <combinedproperties.properties>
   ```

4. 次のプロパティを結合ファイルに追加します。

   ```
   ARCSIGHT_CONAPP_SETUP_PROPERTIES=<directory_location>/
   <combined_properties_file>
   ```

   ここで、<directory_location>は結合ファイルのあるディレクトリのパスで、<combined_properties_file>は前に作成した結合ファイルのファイル名です。

   以下の「生成したプロパティファイルを使用したインストール」(25ページ) の手順に従って、ArcSight Management Centerをサイレントモードでインストールする際に、この結合ファイルを使用します。

生成したプロパティファイルを使用したインストール

サイレントモードを使用してArcSight Management Centerをインストールするには、以下の手順を実行します。

1. 「ソフトウェアArcSight Management Centerのアンインストール」(32ページ) の手順に従って、ArcSight Management Centerの以前にインストールしたバージョンをアンインストールします。
2. ArcSight Management Centerをインストールするマシンが、HPE ArcSight Management Centerのリリースノートに記載されている要件と、「インストールの前提条件」(19ページ) に記載されている前提条件に適合していることを確認します。
3. 以前に生成した結合プロパティファイルを、ArcSight Management Centerソフトウェアをコピーした場所にコピーします。
4. 以下のいずれかを実行します。
   - サイレントモードプロパティファイルのlicensePanel.pathプロパティを編集し、このインストールインスタンス用のライセンスファイルの場所を設定します(各インストールインスタンスごとに固有のライセンスファイルが必要です)。または、
   - licensePanel.pathプロパティが、たとえばarcmc_license.zipを指し示すように設定します。次に、サイレントモードのインストールインスタンスごとに、関連するライセンスファイ

ルを該当の箇所にコピーしてarcmc_license.zipにファイル名を変更します。これにより、結合したプロパティファイルを各インストールごとに更新する必要が無くなります。

5. ArcSight Management Centerソフトウェアをコピーしたディレクトリから以下の2つのコマンドを実行します。
   - `chmod +x ArcSight-ArcMC-2.6.0.<installer_build_number>.0.bin`
   - `./ArcSight-ArcMC-2.6.0.<installer_build_number>.0.bin -i silent -f <combined_properties_file>`

     ここで、<installer_build_number>は、インストーラーファイルのビルド番号です。

     これ以降のインストールと設定は、サイレントに行われるため、ユーザーによる入力は必要ありません。

場合によっては、誤ったエラーメッセージが表示されることがあります。"SLF4J: Failed to load class "org.slf4j.impl.StaticLoggerBinder" これは無害なエラーなので、無視できます。

インストール後の次のステップ

ArcMCで製品の管理を始めるには、最後に、管理するホストを追加する必要があります。ホストの追加の詳細は、「ホストの追加について」(57ページ)を参照してください。

システムサービスとしてのArcSight Management Centerの有効化/無効化

システムサービスとして実行するようにArcSight Management Centerをインストールしている場合は、arcmcdを使用してArcMCのプロセスを管理できます。詳細については、「ArcSight Management Centerデーモン (arcmcd)」(31ページ)を参照してください。

ArcSight Management Centerをシステムサービスとして有効または無効にするには

1. メニューバーで、**[Adminstration] > [System Admin]** をクリックします。
2. ナビゲーションバーで、[**Startup Settings**] をクリックします。
3. [**Software Startup Options**] で、[**Start as a Service**] を選択してシステムサービスとしての起動を有効にするか、[**Do not start as a service**] を選択して無効にします。
4. [**Save**] をクリックします。

   有効にした場合は、リブートするか(サービスが自動的に再起動されます)、リブートせずにサービスを手動で起動します。

root以外のインストールでのサービスの自動起動

ArcSight Management Centerをroot以外のユーザーとしてインストールし、ホストを再起動した場合、ArcMCのサービスは自動的に開始されません。ただし、初期化スクリプトを使用すれば、サービスを自動的に起動するように設定できます。

初期化スクリプトはsuとして実行されるため、コンソールへのログ出力は行われません。

以下にスクリプトの例を示します。これはあくまでも例です。それぞれの環境に合わせた専用のスクリプトを作成する必要があります。

```
#!/bin/sh

# ArcMC               Wrapper script for the Arcsight Management Center

# processname:        arcsight_arcmc

# chkconfig:          2345 99 01

# description:        Arcsight Management Center

DAEMON=/<install_dir>/current/arcsight/arcmc/bin/arcmcd

DAEMON_USER=<NonRootUser-with-which-arcmc-was-installed>

# Exit if the package is not installed

[ -x "$DAEMON" ] || exit 0

if [ $UID -ne 0 ] ; then

echo "You must run this as root."

exit 4

fi

su $DAEMON_USER -c "$DAEMON $1 $2"

exit $?
```

DAEMON変数は、arcmcdプロセスが実行されているディレクトリを指定するのに使用します。

DAEMON_USER変数は、ArcMCを実行するroot以外のユーザーを指定するのに使用します。

最後に、suコマンドで(変数DAEMONで定義された)既存のスクリプトをラップし、$DAEMONスクリプトにパラメーターを渡します。

初期化スクリプトを設定するには

1. rootユーザーの資格情報を使用して、VMにSSH接続します。
2. `/etc/init.d`に移動します。
3. コマンド`vi arcsight_arcmc`を入力して、サービスを作成します。
4. スクリプトのテキストを入力し、ファイルを保存します。
5. コマンド`chmod +x arcsight_arcmc`を使用して、スクリプトの実行権限を付与します。
6. 次のコマンドを使用して、スクリプトを登録します。

```
chkconfig –add arcsight_arcmc
```

7. コマンド`chkconfig | grep arcsight_arcmc`を入力し、initスクリプトの追加後にchkconfigで報告される内容を確認します。次のような結果が期待されます。

```
arcsight_arcmc 0:off 1:off 2:on 3:on 4:on 5:on 6:off
```

ファイアウォールルールの設定

ArcSight Management Centerでデータを受信するには、ファイアウォールで一部のポートを開いておく必要があります。

- ソフトウェアArcSight Management Centerの場合、ユーザーの責任でファイアウォールのセットアップを行います。HPE ArcSightでは、必要なポートのみを開くように、ファイアウォールを設定することをお勧めします。
- ArcSight Management Centerアプライアンスの場合、HPE ArcSightからファイアウォールを設定するためのスクリプトを提供します。詳細については、「ファイアウォールルールの設定」(28ページ) を参照してください。

`iptables-config`を編集し、該当するポートのホワイトリストを作成することで、任意のサーバーの場合と同様に、ArcSight Management Center上でファイアウォールを設定することができます。ArcSight Management Centerアプライアンスの場合は、用意されたスクリプトを使用して、お使いのファイアウォールで該当するポート以外のすべてのポートを閉じることができます。

ヒント: FTP、SNMP、またはローカルコネクターなど、オープンポートが必要なサービスや機能を追加または削除する際には、必ずファイアウォールの設定を更新してください。

ArcMCを初めてインストールまたはアップグレードしたときには、それぞれのフォームファクターやインストールに応じて、以下のポートのみを開くようにファイアウォールを設定します。

デフォルトの着信ポート

サービス	ArcMCアプライアンス	ソフトウェアArcMC、rootインストール	ソフトウェアArcMC、非rootインストール
ArcMCエージェント	7913	7913	7913
FTP	21	該当なし	該当なし
HTTPS	443	443	9000
NTP	123	該当なし	該当なし
コネクターのリモート管理	9001-9008	該当なし	9001-9008
SSH	22	22	22

ArcSight Management Centerアプライアンスでのファイアウォールの設定

ArcSight Management Centerアプライアンスには、ファイアウォールの設定に使用できるスクリプトが含まれています。このスクリプトでは、ArcSight Management Centerの現在の設定を確認し、どのポートを開いたままにする必要があるかを判断します。あるいは、`iptables-config`を編集して該当するポートのホワイトリストを作成することで、任意のサーバーの場合と同様に、アプライアンス上でファイアウォールを設定することもできます。

引数を指定せずに呼び出した場合、`/usr/sbin/arcfirewall`スクリプトは開いたままにするポートをプレビューして表示します。ただし、ファイアウォールの設定を変更するアクションは実行されません。ファイアウォールの設定を変更するには、`-set`オプションを使用します。

スクリプトでオープンされるポートのリストをプレビューするには

1. アプライアンスにrootとしてログインします。
2. 以下のコマンドを実行します。

   ```
   /usr/sbin/arcfirewall
   ```

以下の例に示すように、このスクリプトでオープンされるポートが表示されます。

```
[root@myserver ~]# /usr/sbin/arcfirewall
PREVIEW MODE - NO FIREWALL CHANGES...
List of ports that firewall would allow inbound from any IP address:
21/tcp
22/tcp
443/tcp
7913/tcp
9001/tcp
```

```
9002/tcp
9003/tcp
9004/tcp
9005/tcp
9006/tcp
9007/tcp
9008/tcp
123/udp
```

ファイアウォールを設定するには

1. アプライアンスにrootとしてログインします。
2. 以下のコマンドを実行します。

   ```
   [root@myserver ~]# /usr/sbin/arcfirewall --set
   ```

このスクリプトでは、ファイアウォールが設定されてプレビューされたポートが開いたままになります。

ArcMCアプライアンスのローカルコンテナーを設定し、これにネットワークポートを割り当ててから、`arcfirewall`を実行すると、新しいポートを開く必要があることが検出され、そのポートがプレビューのリストに表示されます。その後、`--set`オプションを指定して`arcfirewall`を実行すると、実際にポートを開くことができます。

arcfirewallを実行せず、ポートを開いていない場合、このコネクターはイベントを受信しません。

ArcSight Management Centerの操作

ここでは、接続方法、ArcSight Management Centerがアクティブになっているときに実行されるプロセス、およびArcSight Management Centerコマンドラインユーティリティ (`arcmcd`) を使用するためのコマンドなど、ArcSight Management Centerの操作について詳しく説明します。

ArcSight Management Centerユーザーインターフェイスへの接続

次のURLを使用してArcSight Management Centerに接続します。

`https://<ホスト名またはIPアドレス>:<ポート>`

ここで、ホスト名またはIPアドレスは、ArcSight Management Centerをインストールしたシステムです。ArcSight Management Centerをrootとしてインストールし、デフォルトポートを使用した場合、<ポート>は省略可能です。

初めてログインする際には、次のデフォルトの資格情報を使用します。

ユーザー名： admin
パスワード: password

セキュリティ上の理由から、初めてログインしたらすぐにデフォルトの資格情報を変更してください。資格情報の変更の詳細については、「User Management」(273ページ)を参照してください。

ArcSight Management Centerのプロセス

以下のプロセスは、ArcSight Management Centerの一部として実行されます。

- apache
- aps
- postgresql
- web

Webサービスがダウンしている場合のArcMCへのログイン

Webサービスが停止している場合は、ArcMCに接続してWebサービスを再起動できます。

1. ArcMCホストにsshでログインします。
2. <arcmc_install_dir>/current/arcsight/arcmc/bin/arcmcd stop allを実行します。
3. <arcmc_install_dir>/current/arcsight/arcmc/bin/arcmcd statusを実行します。すべてのプロセスステータスが “Not monitored” になるまでしばらく待ちます。
4. <arcmc_install_dir>/current/arcsight/arcmc/bin/arcmcd start allを実行します。すべてのプロセスステータスが “running” になるまでしばらく待ちます。
5. 通常どおりArcMCのWeb UIにログインします。

ArcSight Management Centerデーモン (arcmcd)

arcmcdは、ソフトウェアフォームファクターのArcMCでのみ利用できます。

arcmcdユーティリティでは、起動、停止、再起動などの、ArcSight Management Centerソフトウェアプロセスの管理や制御を行うことができます。arcmcdを実行する構文は、次のとおりです。

```
<install_dir>/current/arcsight/arcmc/bin/arcmcd <command>
```

ここで、<install_dir>はArcSight Management Centerのインストールディレクトリで、<command>は以下に示すコマンドです。

システムサービスとして実行するようにArcSight Management Centerをインストールしている場合、arcmcdを使用して特定のArcMCプロセスを管理できます。

arcmcdのコマンド

コマンド	説明
start	aps、apache、postgresql、およびwebプロセスを起動します。
stop	aps、apache、postgresql、およびwebプロセスを停止します。
restart	aps、apache、postgresql、およびwebプロセスを再起動します。
status	すべてのプロセスの現在のステータスを表示します。
quit	aps、apache、postgresql、およびwebプロセスと、ArcSight Management Centerアプリケーションを停止します。
start <process_name>	指定したプロセスを起動します。例: start apache
stop <process_name>	指定したプロセスを停止します。例: stop apache
restart <process_name>	指定したプロセスを再起動します。例: restart apache

ソフトウェアArcSight Management Centerのアンインストール

ArcSight Management Centerのアンインストールは、インストールを行ったのと同じユーザーモードで行います。たとえば、rootとしてインストールを行った場合は、rootとしてアンインストールを行う必要があります。

GUIモードでのアンインストール

GUIモードでソフトウェアArcSight Management Centerをアンインストールするには

1. ArcSight Management Centerをインストールしたディレクトリで、以下を実行します。

   <install_dir>/UninstallerData/Uninstall_ArcSight_Management_Center_2.6.0

2. アンインストールウィザードが起動します。[**Uninstall**] をクリックしてArcSight Management Centerのアンインストールを開始し、ウィザードに表示されるプロンプトに従います。
3. アンインストールが済んだら、手動で/userdataディレクトリを削除します。

注: ArcSight Management Centerソフトウェアをssh接続経由で、GUIモードを使

用してアンインストールする場合、アンインストールウィザード画面を見られるように、**-X**オプションを使用してX window転送機能を有効にしていることを確認してください。

PuTTYを使用する場合は、さらに、接続元のマシンにX11クライアントが必要です。

コンソールモードでのアンインストール

ArcSight Management Centerをコンソールモードでインストールした場合は、デフォルトで、アンインストールがコンソールモードで実行されます。

コンソールモードでアンインストールするには

1. コマンドラインで、次のコマンドを実行します。`<install_dir>/UninstallerData/Uninstall_ArcSight_Management_Center_2.6.0`
2. アンインストールが済んだら、手動で`/userdata`ディレクトリを削除します。

プロンプトが表示されたら、再度**Enter**を押してアンインストールを確定します。アプリケーションがアンインストールされます。

サイレントモードでのアンインストール

ArcSight Management Centerをサイレントモードでインストールした場合は、デフォルトで、アンインストールがサイレントモードで実行されます。

サイレントモードでアンインストールするには

1. コマンドラインで、次のコマンドを実行します。`<install_dir>/UninstallerData/Uninstall_ArcSight_Management_Center_2.6.0`
   アプリケーションがアンインストールされます。アンインストール中の操作は必要ありません。
2. アンインストールが済んだら、手動で`/userdata`ディレクトリを削除します。

ArcSight Management Centerエージェントのインストール

ArcSight Management Centerエージェントは管理対象ホスト上で動作し、ArcSight Management Centerでの管理を可能にします。管理対象ホスト上にArcSight Management Centerをインストールする必要があるかはホストのフォームファクターに依存します。これについては、表にまとめられており、詳細は後述します。

ホストタイプ	ArcMCエージェントが必要?	エージェントのインストール
ArcMC、Logger、またはコネクターアプライアンスハードウェアフォームファクター (すべてのバージョン)	はい	ホストを追加する際に自動的に実行されます。
ソフトウェアコネクターアプライアンス (すべてのバージョン)	はい	手動インストールが必要です。ホストを追加する前に実行してください。
ソフトウェアLogger (バージョン6.0より前)	はい	手動インストールが必要です。ホストを追加する前に実行してください。
ソフトウェアLogger (バージョン6.0以降)	はい	ホストを追加する際に自動的に実行されます。
ソフトウェアArcMC (バージョン2.1より前)	はい	手動インストールが必要です。ホストを追加する前に実行してください。
ソフトウェアArcMC (バージョン2.1以降)	はい	ホストを追加する際に自動的に実行されます。
ソフトウェアコネクター (任意)	いいえ	なし。ArcMCエージェントは不要。
Event Broker	いいえ	なし。ArcMCエージェントは不要。

自動インストール

ArcMCに次のいずれかのホストタイプを追加すると、ArcMCエージェントが自動的にインストールされます。

- ハードウェアアプライアンス(ArcSight Management Centerアプライアンス、コネクターアプライアンス、またはLoggerアプライアンス)
- ソフトウェアLogger (バージョン6.0以降)
- ソフトウェアArcMC (バージョン2.1以降)

ホストの追加処理の一環として、ArcSight Management Centerは追加されたホストに自動的にArcSight Management Centerエージェントのインストーラーをプッシュし、エージェントをインストールした後にサービスを開始します。追加されたホストは、ArcSight Management Centerですぐに管理できます。手動でインストール手順を実行する必要はありません。ホストの追加処理の詳細については、「ホストの追加について」(57ページ)を参照してください。

ArcMCエージェントの自動インストールにはPerlが必要です。ArcMCにホストを追加する前に、Perlがホストにインストールされていることを確認してください。

手動インストール

ArcMCエージェントをArcMCに管理用に追加する前に、これらのホストタイプのいずれかでArcMCエージェントを手動でインストールする必要があります。

- ソフトウェアArcSight Management Center (バージョン2.1より前)
- ソフトウェアLogger (バージョン6.0より前)
- ソフトウェアコネクターアプライアンス (すべてのバージョン)

ArcMCを使用して製品を管理する場合は、ArcMCと同じバージョンのエージェントをインストールしておく必要があります。たとえば、ArcMC 2.1を使用して製品を管理する場合、そのArcMC上で動作するArcMCエージェントもバージョン2.1である必要があります。

手動でArcSight Management Centerエージェントをインストールするには

1. インストーラーを転送したディレクトリで、次の2つのコマンドを実行します。
   - `chmod +x ArcSight-ArcMCAgent-2.6.0.<agent_installer_build_number>.0.bin`
   - `./ArcSight-ArcMCAgent-2.6.0.<agent_installer_build_number>.0.bin LAX_VM <install_dir>/current/local/jre/bin/java`

     ここで `<agent_installer_build_number>` は、最新のインストーラーのビルド番号です。`<install_dir>` は、ソフトウェア製品のインストールディレクトリです。

インストールウィザードが起動します。

2. ダイアログボックスを確認し、[**Next**] をクリックします。必要なインストールパスは、インストールディレクトリ(つまり、ソフトウェアコネクターアプライアンスまたはソフトウェアLoggerがインストールされているディレクトリと同じディレクトリ) です。
3. プロンプトにしたがってインストールを完了します。ArcMCエージェントは、インストール処理が完了すると自動的に起動します。

   ArcMCエージェントがローカルホストにインストールされない場合、ローカルホストの管理は有効になりません。エージェントが正しくインストールされたことを確認するには、[**Issues**] の [**Host**] タブをオンにします。ツールチップに表示される指示に従って、エージェントを正しくインストールし、表示されている問題を解決してください。

ソフトウェアコネクターとEvent Broker

ソフトウェアコネクターとEvent Brokerでは、ArcMCを使用して管理するのに、ArcSight Management Centerエージェントをインストールする必要はありません。

ArcSight Management Centerエージェントの操作

インストール後、`arcmcagent`プロセスが管理対象ホスト上で実行されます。このプロセスは、自動インストールまたは手動インストール後に自動的に開始されます。ただし、エージェントが何らかの理由で停止した場合は、手動で開始することができます。

アプライアンスホスト上のエージェントを手動で起動、停止、または再起動するには

1. 管理対象ホストで、**[Setup] > [System Admin] > [Process status]** をクリックします。
2. プロセスのリストからarcmcagentを選択します。
3. 必要に応じて、**[開始]**、**[停止]**、または[**再起動**]をクリックします。

ソフトウェアArcMC、ソフトウェアコネクターアプライアンス、またはソフトウェアLogger

ソフトウェアArcMC、ソフトウェアコネクターアプライアンス、またはソフトウェアLoggerでエージェントを手動で開始または停止するには

1. `<install_dir>/current/arcsight/<conapp|logger|arcmc>/bin/<conappd|loggerd|arcmcd> <start|stop> arcmcagent`を実行します。

エージェントの検証

エージェントがホスト上で実行されていることを確認するには、次のいずれかの手順を実行します。

- 管理対象ホストのGUIで、**[Setup] > [System Admin] > [Process Status]** をクリックします。ArcSight Management Centerエージェント (`arcmcagent`) は、実行状態のプロセスとして表示されます。
- (ソフトウェアArcMC、ソフトウェアコネクターアプライアンス、またはソフトウェアLoggerのみ) エージェントをインストールした後、コマンドラインで次のコマンドを実行します。

  `<install_dir>/current/arcsight/<conapp|logger>/bin/<conappd|loggerd> status`

  エージェントが、実行状態のサービスとして表示されます。

ArcSight Management Centerエージェントのアンインストール

ArcSight Management Centerエージェントをアンインストールするには、以下のコマンドを実行します。

```
<install_dir>/arcmcagent/UninstallerData/Uninstall_ArcSight_Management_
Center_Agent_<version number>
```

ここで `<install_dir>` はインストールディレクトリの名前です。`<version number>` はArcMCエージェントのバージョンです。

アンインストールウィザードが起動します。[**Uninstall**] をクリックしてウィザードを開始します。アンインストールが完了したら、[**Done**]をクリックします。

- 新しいバージョンをインストールする際には、前もって以前のバージョンのArcSight Management Centerエージェントを停止してアンインストールします。

- ソフトウェアArcMC、ソフトウェアLogger、またはソフトウェアコネクターアプライアンスをアンインストールする場合は、管理対象製品のアンインストールを始める前に、ノードからArcSight Management Centerエージェントがアンインストールされていることを確認します。

第3章: ユーザーインターフェイス

ここでは、以下の内容について説明します。

概要

この章では、ArcSight Management Centerのインターフェイスの概要について説明します。ArcSight Management Centerでは、ブラウザーベースのユーザーインターフェイスを使用します。サポートされているブラウザーの最新情報については、ArcSight Management Centerのリリースノートを参照してください。

メニューバー

メニューバーでは、ArcSight Management Centerの主要な機能コンポーネントにアクセスできます。メニューバーには、[**Dashboard**]、**[Node Management]**、**[Configuration Management]**、**[User Management]**、および [**Administration**] メニューが含まれます。

Monitoring Summary

[Monitoring Summary] ページには、すべての監視対象製品に関する情報が表示されます。

- 各タイプの製品に対して集計されたヘルスステータスが、円グラフ形式で表示され、ノードの合計数と、各ステータスに対応する数が示されます。サマリーテーブルには、同じデータがパーセント形式で表示されます。
- 管理パネルには、[**Monitoring Summary**] テーブルが表示され、現在問題をレポートしているすべての製品が表示されます。
- ナビゲーションパネルでは、管理パネルの個々の製品タイプの監視サマリーを表示できます。製品タイプをクリックすると、その製品の監視サマリーが表示されます。

監視の表示と設定の詳細については、「ダッシュボード」(188ページ) を参照してください。

Node Management

[**Node Management**] は、次のノードタイプを管理するのに使用します。

- ソフトウェアコネクター
- ハードウェアまたはソフトウェアコネクターアプライアンス
- ハードウェアまたはソフトウェアLogger
- ハードウェアまたはソフトウェアArcSight Management Center
- Event Broker

ノードの追加と管理の詳細については、「ノードの管理」(42ページ)を参照してください。同じメニューから、管理対象のArcSight製品に対して選択した管理タスクを実行することもできます。「HPE ArcSight製品の管理」(74ページ)を参照してください。

Configuration Management

[**Configuration Management**] は、ノードの設定や複数ノード間での設定の同期 (プッシュ) を作成および管理し、Loggerの初期設定を迅速に行うのに使用します。次の設定のタイプを管理できます。

- 以下に関するサブスクライバーの設定:
  - ArcSight Management Center
  - コネクター
  - コネクターアプライアンス
  - 通知先
  - Logger
  - システム管理
- その他の設定:
  - Loggerの初期設定
  - Loggerイベントアーカイブ
  - ピアLoggerの管理
  - Event Brokerの管理

サブスクライバー設定の管理の詳細については、「設定の管理」(129ページ)を参照してください。

初期設定の詳細については、「初期設定管理」(164ページ)を参照してください。

User Management

[User Management] では、すべての管理対象ノードのユーザー管理を行うことができます。ユーザー、ユーザーリスト、関連付け、およびロールの作成と編集を行うことができます。また、各ノードが管理を行っているArcMCの許可されたユーザーのリストに適合しているかどうかを確認することができます。

ユーザー管理の詳細については、「概要」(177ページ)を参照してください。

Administration

[**Administration**] メニューには、次の項目があります。

- **Backup**: ArcSight Management Centerの現在の設定をバックアップできます。詳細については、「バックアップと復元の管理」(205ページ)を参照してください。
- **Repositories**: ログ、証明書、ドライバーなどのファイルを保存するリポジトリを管理できます。詳細については、「リポジトリの管理」(211ページ)を参照してください。
- **Snapshot**: HPE ArcSight Management Centerのスナップショットイメージを取得し、トラブルシューティングに役立つログを生成できます。詳細については、「スナップショット」(208ページ)を参照してください。
- **Restore**: 保存したバックアップから設定を復元できます。詳細については、「バックアップと復元の管理」(205ページ)を参照してください。
- **System Admin**: ユーザーとユーザーグループの作成および管理、およびシステムのセキュリティ設定を行うためのシステム管理ツールについて説明します。詳細については、「システム管理」(229ページ)を参照してください。
- **Consumption Report**: 選択した管理対象ノードのLoggerデータ消費量に関するレポートを生成します。

Stats (EPS In/Out)

[**Stats**] メニュー項目には、すべての管理対象コネクター (スタンドアロンのSmartConnectorおよび管理対象ホスト上で実行されているコネクター) で受信および送信された、1秒あたりのイベント数 (EPS) の合計が表示されます。

サイトマップ

アクセスを容易にして利便性を高めるため、サイトマップでは、ArcSight Management Center UIのすべてのページをリンクしています。

サイトマップにアクセスするには: ArcMCのメインツールバーで、[**Site Map**] をクリックします。目的のリンクを選択して移動します。

履歴管理

履歴管理を使用すると、以前に表示したページにすばやく簡単にアクセスできます。履歴管理は、[Node Management]、[Configuration Management]、[User Management] ページ、および一部の [Administration] ページで利用できます。

[Node Management] では、ナビゲーションツリーにツリーで選択した項目のフルパスが表示されます。パス内のいずれかのノードをクリックすると、対応するページに直接移動します。

また、階層リンク内の対応するリンクをクリックして、以前に表示したページに戻ることもできます。

さらに、ブラウザーの [**戻る**] および [**進む**] ボタンを使用して、以前に表示したページに移動することもできます。

第4章: ノードの管理

ここでは、以下の内容について説明します。

概要

ノードは、ArcSight Management Centerを介して一元的に管理できるネットワーク接続されたHPE ArcSight製品です。各ノードは、ネットワーク接続された1つのホストに関連付けられています。ホストには、ホスト名、IPアドレス、またはその両方が割り当てられています。

ノードタイプには、以下のHPE ArcSight製品が含まれます。

- コネクターアプライアンスまたはソフトウェアコネクターアプライアンス
- Loggerアプライアンスまたはソフトウェアlogger
- コンテナーまたはソフトウェアコネクター
- その他のArcSight Management Center (ソフトウェアまたはハードウェア)
- Event Broker

1つのホスト (展開済みの1つのEvent Brokerなど) に、管理目的で複数のノードが含まれる場合があります。また、ノードが他のノードと親または子の関係になることもあります。

以下のノード管理タスクを実行できます。

- 管理対象ノードのロケーション別、ホスト別、またはノードタイプ別の表示。
- ホストのロケーションの追加、表示、編集、および削除。
- ホストからのノードの追加、CSVファイルからのホストのインポート、ホストの表示と削除、ロケーション内のすべてのホストの表示、ホスト上のソフトウェアの更新、ホストの別のロケーションへの移動、新しいコネクターまたはコンテナーでのホストのスキャン。

ホストの追加の詳細は、「ホストの追加について」(57ページ) を参照してください。

ノード管理

ノードを管理するには、メニューバーで、**[Node Management] > [View All Nodes]** をクリックします。[Node Management] のUIが表示されます。[Node Management] のUIは、次の2つのパネルで構成されます。

- 左側には、ナビゲーションツリーが表示されます。
- 右側には、管理パネルが表示されます。管理パネルでは、ナビゲーションツリーで選択した項目に対して管理操作を行うことができます。

ナビゲーションツリー

ナビゲーションツリーでは、管理対象ノードが階層形式で表示されます。ナビゲーションツリーには、以下の内容が含まれます。

 **System**: ArcSight Management Centerで管理されているすべてのノードが表示されます。

 **Location**: [**System**] の下に個々のロケーションが表示されます。ロケーションは追加された順に表示されます。ロケーションは、ホストのリストを整理するのに使用できる論理的なグループ分けです。詳細については、「ロケーション」(55ページ) を参照してください。

 **Host**: 各ロケーションブランチには、そのロケーションに割り当てられているすべてのホストが表示されます。ホストは追加された順に、ホスト名で表示されます。詳細については、「ホスト」(57ページ) を参照してください。

<ノードタイプ>: 各ホストブランチには、そのホストに割り当てられているすべての管理対象ノードが表示されます。ノードには次のタイプがあります。

 **Connector Appliance or Software Connector Appliance:** 各コネクターアプライアンス (ハードウェアまたはソフトウェア) が、個別のノードとして表示されます。

 **Logger Appliance or Software Logger:** 各Logger (ハードウェアまたはソフトウェア) が、個別のノードとして表示されます。

 **ArcSight Management Center:** 各ArcSight Management Center (ハードウェアまたはソフトウェア) が、個別のノードとして表示されます。

 **Container:** ホストにコンテナーが含まれている場合、各コンテナーが1つのノードとして表示されます。

Connector: コンテナーノードにコネクターが含まれている場合、コンテナーノードの下に、含まれているコネクターが表示されます。

Event Broker: 管理対象のEvent Brokerがノードとして表示されます。

ツリー内の項目は階層形式で構成されるため、ツリー内の各項目には、その下に表示されるすべてのブランチが含まれます。たとえば、[**Location**] ブランチには、そのロケーションに割り当てられているすべてのホストが含まれます。くさび形アイコンをクリックすると、ブランチの表示とブランチに含まれる項目の表示が切り替わります。

管理パネル

ナビゲーションツリーで項目を選択すると、中央の管理パネルのいずれかのタブに項目の詳細情報が表示されます。たとえば、ナビゲーションツリーに表示された特定のホストの詳細情報を表示するには、ツリーでそのホストを選択します。ツリーの右側の管理パネルに、選択したホストに関連する詳細情報とコントロールが表示されます。

管理タブ

管理パネルに表示されるタブは、ナビゲーションツリーで選択した項目のタイプに依存します。表示される管理タブには、選択した項目に関連する詳細情報が、その項目の階層内の位置に応じて示されます。

ナビゲーションツリーで選択した項目のタイプ	管理パネルに表示されるタブ
System	Locations、Hosts、Containers、Connectors、ConApps、Loggers、ArcMCs、EB Nodes
Location	Hosts、Containers、Connectors、ConApps、Loggers、ArcMCs、EB Nodes
Host	Containers、Connectors、ConApps、Loggers、ArcMCs、EB Nodes
Node	Connectors、ConApps、Loggers、ArcMCs、EB Nodes

たとえば、ナビゲーションツリーでロケーションの項目を選択した場合は、**[Hosts]**、**[Containers]**、**[Connectors]**、**[ConApps]**、**[Loggers]**、**[ArcMCs]**、**[EB Nodes]** のタブが表示されます。各タブには、選択したロケーションに関連する指定されたタイプの項目が詳細情報を含めて表示されます。

管理パネルでの項目の操作

1つまたは複数の項目の選択: 管理パネルで項目のリストから項目を選択するには、項目をクリックします。隣り合った複数の項目を選択する場合はShiftキー+クリックを使用し、隣り合っていない複数の項目を選択する場合はCtrlキー+クリックを使用します。

カラムの設定: 歯車アイコンをクリックして、カラムの設定を変更します。

- **ソート:** データをカラムでソートするには、[**Sort Ascending**] または [**Sort Descending**] を選択します。
- **カラム表示:** テーブルに表示されるカラムを変更するには、[**Columns**] を選択します。次に、表示する1つ以上のカラムを切り替えます。
- **フィルター:** 項目のリストをフィルター処理するには、[**Filters**] を選択します。次に、1つ以上のフィルター条件を入力して、これらの条件と一致する項目を表示します。

リストの更新: リストのデータを更新するには、右上隅の [**Refresh**] をクリックします。

タブのコントロール

以下のコントロールは、管理パネルのすべてのタブに表示されます。

- **ツールバーボタン:** ツールバーボタンでは、タブ上の項目に関連する操作を行うことができます。
- **項目のテーブル:** タブヘッダーに対応する項目がテーブルに表示されます。たとえば、[Locations] タブでは、ロケーションが表形式でリスト表示されます。
- **一括操作ボタン:** ほとんどのタブでは、一括操作ボタンを使用して、1つ以上の項目に対して操作を行うことができます。リストから1つまたは複数の項目を選択してからボタンをクリックして、ボタンが表す操作を実行します。たとえば、ホストなどの複数の項目を削除するには、[**Hosts**] タブで1つ以上のホストを選択してから、[**Delete**] をクリックします。選択したホストが削除されます。

また、タブには、それぞれの項目タイプに固有のコントロールが含まれることもあります。たとえば、[**Connectors**] タブには、コネクターの管理に関するコントロールが含まれます (「コネクターの管理」(99ページ) を参照)。

[Locations] タブ

[**Locations**] タブには、ArcSight Management Centerで定義されたすべてのロケーションが表示されます。[**Locations**] タブには以下のボタンがあります。

Add Location	新しいロケーションを追加します。詳細については、「ロケーションの追加」(55ページ) を参照してください。
Delete	選択した1つ以上のロケーションをArcMCから削除します。詳細については、「ロケーションの削除」(56ページ) を参照してください。

[**Locations**] テーブルには、ロケーションごとに次のパラメーターが表示されます。

- **Name:** ロケーション名。
- **Number of Hosts:** ロケーションに割り当てられたホストの数。
- **Action:** ドロップダウンに、ロケーションを編集するためのコントロールが表示されます。ロケーションの編集の詳細については、「ロケーションの編集」(56ページ)を参照してください。

ロケーションの管理の詳細については、「ロケーション」(55ページ)を参照してください。

[Hosts] タブ

[**Hosts**] タブには、ナビゲーションツリーで選択したロケーションに関連付けられたすべてのホストが表示されます。[**Hosts**] タブには以下のボタンがあります。

Add Host	ホストを追加します。ナビゲーションツリーでロケーションを選択している場合に、[**Hosts**] タブで利用できます。ホストの追加の詳細は、「ホストの追加について」(57ページ)を参照してください。
Move	選択したホストを新しいロケーションに移動します。詳細については、「ホストの別のロケーションへの移動」(70ページ)を参照してください。
Update Agent	選択したホストでArcMCエージェントを更新します。エージェントがインストールされていない場合、このボタンを使用するとエージェントがインストールされます。詳細については、「ArcMCエージェントの更新 (またはインストール)」(70ページ)を参照してください。
Delete	選択したホストをArcMCから削除します。詳細については、「ホストの削除」(69ページ)を参照してください。

[**Hosts**] テーブルには、ホストごとに次のパラメーターが表示されます。

- **Hostname:** ホストの完全修飾ドメイン名 (FQDN) またはIPアドレス。このホスト名は、ホストのSSL証明書のホスト名と一致している必要があります(ホストを追加するのにIPアドレスを使用した場合、証明書は使用したIPアドレスと一致します)。
- **Path:** ホストのパス。
- **Agent Version:** ホスト上で実行されているArcSight Management Centerエージェントのバージョン番号
- **Issues:** ホストに関連する問題のステータス。可能なインジケーターは、次のとおりです。
  - ✅None: ホストに関連する問題はありません。
  - ❗Internet connection Not Present: インターネット接続によってホストに到達できなくなっています。ArcMCがMarketplaceに接続して、パーサーアップグレードバージョンを取得できない場合に表示されます。ユーザー環境でインターネット接続用のプロキシサーバーが必要な場合は、logger.propertiesファイルを設定します。ユーザー環境がアプライアンスの場合は、**[System Admin] > [Network]** ページでDNS設定を保存します。
  - ❗Valid Marketplace Certificate Not Found in ArcMC: Marketplaceの証明書がArcMCのトラストストアの証明書と一致しない場合に表示されます。
  - ❗Host Certificate Mismatch: ホスト名が、SSL証明書のホスト名と一致していません。

ホストの証明書をダウンロードおよびインポートする手順については、「ホストの証明書のダウンロードとインポート」(72ページ)を参照してください。ローカルホストでこの問題が表示され、証明書をダウンロードできない場合は、ローカルホストでWebサービスを再起動してください。

- ArcMC Agent Out of Date: 管理を行っているArcMCからホストのエージェントバージョンをアップグレードできないか、ArcSight Management Centerが管理対象ノードのArcSight Management Centerエージェントと通信できません。ArcMCエージェントの手動でのインストールが必要になる場合があります。要件と手順については、「ArcSight Management Centerエージェントのインストール」(33ページ)を参照してください。
- ArcMC Agent Stopped: ホストのエージェントプロセスが停止しています。
- ArcMC Agent Upgrade Recommended: ホストのエージェントバージョンが、管理を行っているArcMCのエージェントバージョンよりも古くなっています。エージェントをアップグレードすることをお勧めします。
- ArcMC Agent Uninstalled: ホストのエージェントがアンインストールされました。
- ArcMC Agent Down: ホストのエージェントが実行されていません。
- Update the authentication credentials on the localhost, and then install the ArcMC Agent.: リモート管理用に追加されたローカルホストでは、認証情報を更新して認証が確実に行われるようにした後に、ArcMCエージェントをインストールして管理ができるようにする必要があります。この問題を修正するには、これらの両方の手順を実行します。
- Error in REST Authentication.: Event Brokerノードに、ArcMCの証明書、ArcMCのセッションID、またはArcMCのURLとポートがありません。この問題を解決するには、以下を実行します。
  - ユーザーがEvent Brokerの操作に関する権限を持っていることを確認します。
  - 有効なArcMCの証明書 (FQDNと.crt拡張子を使用) が、Event Brokerの次の場所にあることを確認します: /opt/arcsight/k8s-hostpath-volume/eb/arcmccerts
  - [ArcSight Installer] > [Event Broker Configuration] > [ArcMC_Monitoring] フィールドで、ArcMCのURLが正しいFQDNとポートを使用して更新されていることを確認します。
  - ユーザーがArcMCの証明書をEBの上記の場所に置き直すたびに、EBのWebサービスポッドを再起動して、新しい証明書を読み込ませてトラストストアを更新する必要があります。
- **Model**: ホストがアプライアンスの場合、アプライアンスのHPE ArcSightモデル番号が表示されます。ホストがアプライアンスでない場合は、Softwareというラベルが表示されます。
- **Type**: インストールのタイプ (ArcMCアプライアンスまたはソフトウェア)。
- **Version**: ホスト上のソフトウェアのバージョン番号。
- **Action:** ドロップダウンに、以下のような、ホストの管理タスクを実行するためのコントロールが表示されます。
  - ホストのスキャン

- 証明書の詳細のダウンロード
- ホストの資格情報の更新

ホスト管理の詳細については、「ホスト」(57ページ)を参照してください。

[Containers] タブ

[**Containers**] タブには、ナビゲーションツリーで選択した項目に関連するすべてのコンテナーが表示されます。たとえば、ナビゲーションツリーでいずれかのロケーションを選択した場合、ロケーションにはホストが含まれているため、[**Containers**] タブには、選択したロケーションのすべてのホストに関連するすべてのコンテナーが表示されます。[**Containers**] タブには以下のボタンがあります。

Properties	選択したコンテナーのプロパティを設定します。詳細については、「コンテナープロパティの更新」(86ページ)を参照してください。
Certificates	選択したコンテナーの証明書を管理します。詳細については、「コンテナー上の証明書の管理」(94ページ)を参照してください。
FIPS	選択したコンテナーでFIPSモードを有効または無効にします。詳細については、「コンテナーでのFIPSの有効化」(91ページ)を参照してください。
Upgrade	選択したコンテナーのすべてのコネクターをアップグレードします。詳細については、「コンテナー内のすべてのコネクターのアップグレード」(88ページ)を参照してください。
Credentials	選択したコンテナーの資格情報を管理します。詳細については、「コンテナー資格情報の変更」(87ページ)を参照してください。
Logs	選択したコンテナーのログを管理します。詳細については、「コンテナーログの表示」(90ページ)を参照してください。
Restart	選択したコンテナーのすべてのコネクターを再起動します。詳細については、「コンテナーの再起動」(90ページ)を参照してください。
Delete	選択したコンテナーをArcSight Management Centerから削除します。詳細については、「コンテナーの削除」(86ページ)を参照してください。

[**Containers**] テーブルには、次のカラムが含まれます。

- **Name:** コンテナーの名前。
- **Path**: コンテナーのパス。
- **Issues:** コンテナーに関連する問題のステータス。
- **Port**: コンテナーが通信時に使用するポート番号。
- **Framework Ver**: コンテナーのフレームワークバージョン番号。
- **Parser Ver**: コンテナーのパーサーバージョン番号。
- **Status**: コンテナーのステータス。コンテナーのステータスの可能な値は、次のとおりです。
  - Improper configuration: 初期のデフォルト状態。
  - Initializing connection: コネクターのURLは解決可能ですが、ArcSight Management

Centerがまだコネクターにログインしていません。
- Down: ログインコマンドの実行時に例外が発生しました。
- Unauthorized: ログインコマンドが実行され、ログインに失敗しました。
- Connecting: ログインを実行中です。
- Connected: ログインに成功しました。
- Empty: ログインに成功しましたが、コンテナー内にコネクターが存在しません。
- Initialized: ログインに成功し、コンテナー内にコネクターが存在します。
- Unknown: ステータスに関する情報なし。解決するには、手動でシステムにSSH接続し、コンテナーを再起動します。

- **Last Check:** 最後のステータスチェックの日付と時刻。
- **Action:** ドロップダウンに、以下のような、コンテナーの管理タスクを実行するためのさまざまなコントロールが表示されます。
  - コンテナーの編集
  - コンテナーコマンドの送信
  - コネクターの追加
  - Logfuの実行
  - 証明書のダウンロード
  - 証明書の表示
  - (ArcExchangeへの) 展開
  - FlexConnectorウィザードの実行

コンテナー管理の詳細については、「コンテナー内のすべてのコネクターのアップグレード」(88ページ)を参照してください。

[Connectors] タブ

[**Connectors**] タブには、ナビゲーションツリーで選択した項目に関連するすべてのソフトウェアコネクターが表示されます。たとえば、ナビゲーションツリーでいずれかのコンテナーを選択した場合、[**Connectors**] タブには、そのコンテナー内のすべてのコネクターが表示されます。コネクターの管理の詳細については、「コネクターの管理」(99ページ)を参照してください。

[**Connectors**] タブには、選択した1つ以上のコネクターで操作を行うための、以下のボタンがあります。

Add Connector	(ナビゲーションツリーでコンテナーを選択している場合にのみ表示されます。)コネクターを選択したコンテナーに追加します。
Runtime Parameters	選択したコネクターの実行時パラメーターを編集します。詳細については、「コネクターパラメーターの編集」(102ページ)を参照してください。

Destinations	選択したコネクターの通知先を設定します。詳細については、「通知先の管理」(104ページ)を参照してください。
Parameters	選択したコネクターのパラメーターを設定します。詳細については、「コネクターパラメーターの編集」(102ページ)を参照してください。
Delete	ArcSight Management Centerからコネクターを削除します。詳細については、「コネクターの削除」(112ページ)を参照してください。

[**Connectors**] テーブルには、コネクターごとに次のパラメーターが表示されます。

- **Name:** コネクターの名前。
- **Path:** コネクターのパス。
- **Type:** コネクターのタイプ。
- **EPS In:** コネクターが受信した1秒あたりのイベント数。
- **EPS Out:** コネクターが通知先に送信した1秒あたりのイベント数。
- **Cache:** コネクターのキャッシュサイズ
- **Last Check:** 最後のステータスチェックの日付と時刻。
- **Action:** ドロップダウンに、ソフトウェアコネクターの管理タスクを実行するためのさまざまなコントロールが表示されます。これには、以下が含まれます。
  - コネクターコマンドの送信
  - ArcExchangeへのコネクターの共有
  - FlexConnectorの編集

コネクター管理の詳細については、「コネクターの管理」(99ページ)を参照してください。

[Connector] サマリータブ

個々のコネクターの詳細を表示するには、表示するコネクターをナビゲーションツリーでクリックします。サマリータブのツールバーには、コネクターの操作を行うための以下のボタンがあります。

Connector Command	コネクターにコマンドを送信します。詳細については、「コネクターへのコマンドの送信」(112ページ)を参照してください。
Remove Connector	コネクターを削除します。詳細については、「コネクターの削除」(112ページ)を参照してください。
Run Logfu	コネクターに対してLogfuの診断を実行します。詳細については、「コネクターに対するLogfuの実行」(113ページ)を参照してください。
Share	ArcExchangeを介してコネクターを共有します。詳細については、「ArcExchangeでのコネクターの共有」(119ページ)を参照してください。

ツールバーの下のテーブルには、基本的なコネクターデータ、パラメーター、およびコネクターの通知先などの、コネクターの詳細が表示されます。これらのテーブルには、次のカラムが含まれます。

Connector Data

- **Type:** コネクターのタイプ。
- **Status:** コネクターステータス。
- **Input Events (SLC):** 前回のチェック (通常は1分ごとに1回) 以降にコネクターが受信したイベントの合計数。
- **Input EPS (SLC):** 前回のチェック (通常は1分ごとに1回) 以降にコネクターが受信した1秒あたりのイベント数。
- また、右側のカラムには、コネクターの編集、実行時パラメーターの編集、フェイルオーバー通知先の追加、および通知先コマンドの送信を行うためのツールがあります。

Connector Parameters

[**Connector Parameters**] をクリックすると、このテーブルの表示が切り替わります。
[**Connector Parameters**] には、以下の内容が含まれます。

- : クリックしてパラメーターを編集します。
- **Parameters:** パラメーターには、コネクターのネットワークポート、IPアドレス、プロトコルなどの情報が含まれます。
- **Value:** パラメーターの値。

Table Parameters (WUCコネクターのみ)

WUCコネクター (のみ) では、次のパラメーターが表示されます。

- **Domain Name:** コネクターのドメイン名。
- **Host Name:** コネクターのホスト名。
- **User Name:** コネクターのユーザー名。
- **Security Logs:** セキュリティイベントが収集されるかどうかを示します。
- **System Logs:** システムイベントが収集されるかどうかを示します。
- **Application:** 共通アプリケーションイベントログからアプリケーションイベントが収集されるかどうかを示します。
- **Custom Log Names:** カスタムアプリケーションログ名のリスト (存在する場合)。
- **Microsoft OS Version:** コネクターのMicrosoftオペレーティングシステム。
- **Locale:** コネクターのロケール。

Destinations

[**Destinations**] をクリックすると、このテーブルの表示が切り替わります。[**Destinations**] テーブルには、次の内容が含まれます。

- ＋: クリックして通知先を追加します。
- **Name:** 通知先の名前。
- **Output Events (SLC):** 前回のチェック (通常は1分ごとに1回) 以降にコネクターが通知先に向けて出力したイベントの合計数。
- **Output EPS (SLC):** 前回のチェック (通常は1分ごとに1回) 以降にコネクターが通知先に向けて出力した1秒あたりのイベント数。
- **Cached:** 通知先に送信するためにキャッシュされたイベントの合計数。
- **Type:** 通知先タイプ。通知先タイプの説明は、『SmartConnectorユーザーガイド』に記載されています。
- **Location:** 通知先のロケーション。
- **Device Location:** 通知先が存在するデバイスのロケーション。
- **Comment:** 通知先に関するコメント。
- **Parameters:** 通知先固有のパラメーター (IPアドレス、ポート、プロトコルなど)。
- **Action Buttons:** アクションボタンでは、通知先の編集、実行時パラメーターの編集、新しいフェイルオーバー通知先の追加、通知先コマンドの送信、および通知先の削除などの、通知先管理タスクを実行できます。

コネクターの管理の詳細については、「コネクターの管理」(99ページ) を参照してください。

[ConApps] タブ

[**ConApps**] タブには、ナビゲーションツリーで選択した項目に関連するすべてのハードウェアおよびソフトウェアコネクターアプライアンスが表示されます。たとえば、ナビゲーションツリーで [**System**] を選択した場合、[**Connector Appliances**] タブには、ArcSight Management Centerのすべてのコネクターアプライアンスが表示されます。また、いずれかのロケーションを選択した場合は、そのロケーション内のすべてのコネクターアプライアンスが表示されます。

[**Connector Appliances**] タブには、選択した1つ以上のコネクターアプライアンスで操作を行うための、以下のボタンがあります。

Set Configuration	選択したコネクターアプライアンスの設定を行います。詳細については、「ConAppでの設定の実行」(76ページ) を参照してください。

[**Connector Appliances**] テーブルには、コネクターアプライアンスごとに次のパラメーターが表示されます。

- **Name:** コネクターアプライアンスの名前。
- **Path**: コネクターアプライアンスのパス。
- **Port**: コネクターアプライアンスが通信時に使用するポート番号。
- **Version**: コネクターアプライアンスのソフトウェアバージョン。
- **Status**: コネクターアプライアンスのステータス。

- **Last Check:** 最後のステータスチェックの日付と時刻。
- **Action:** ドロップダウンに、以下のような、コネクターアプライアンスの管理タスクを実行するためのさまざまなコントロールが表示されます。
  - 再起動
  - シャットダウン
  - 設定の編集または削除

コネクターアプライアンスの管理の詳細については、「コネクターアプライアンス (ConApp) の管理」(74ページ) を参照してください。

[Loggers] タブ

[**Loggers**] タブには、ナビゲーションツリーで選択した項目に関連するすべてのハードウェアおよびソフトウェアLoggerが表示されます。たとえば、ナビゲーションツリーで [**System**] を選択した場合、[**Loggers**] タブには、ArcSight Management Centerのすべてのloggerが表示されます。また、いずれかのロケーションを選択した場合は、そのロケーション内のすべてのLoggerが表示されます。

[**Loggers**] タブには、選択した1つ以上のLoggerで操作を行うための、以下のボタンがあります。

Set Configuration	選択したLoggerの設定を行います。詳細については、「Loggerの設定の実行」(84ページ) を参照してください。
Upgrade Logger	選択したLoggerをアップグレードします。詳細については、「Loggerのアップグレード」(82ページ) を参照してください。

[**Loggers**] テーブルには、Loggerごとに次のパラメーターが表示されます。

- **Name:** Loggerの名前。
- **Path**: Loggerのパス。
- **Port**: Loggerが通信時に使用するポート番号。
- **Version**: Loggerのソフトウェアバージョン。
- **Top Storage Use:** 最も使用されているストレージグループとそのストレージの割合が表示されます。
- **Status**: Loggerのステータス。
- **Last Check:** 最後のステータスチェックの日付と時刻。
- **Action:** 次のような、Loggerの管理タスクを実行するためのコントロールが表示されます。
  - 再起動
  - シャットダウン
  - 設定の編集または削除

[ArcMCs] タブ

[**ArcMCs**] タブには、ナビゲーションツリーで選択した項目に関連するすべてのソフトウェアArcSight Management CenterとArcSight Management Centerアプライアンスが表示されます。たとえば、ナビゲーションツリーで [**System**] を選択した場合、[**ArcMCs**] タブには、管理対象のすべてのArcSight Management Centerが表示されます。また、いずれかのロケーションを選択した場合は、そのロケーション内のすべてのArcMCが表示されます。

[**ArcMCs**] タブには、選択した1つ以上のArcMCで操作を実行するための、以下のボタンがあります。

Set Configuration	選択したArcMCの設定を行います。詳細については、「管理対象のArcMCでの設定の実行」(79ページ)を参照してください。
Upgrade ArcMC	選択したArcMCをアップグレードします。詳細については、「ArcMCのアップグレード」(78ページ)を参照してください。

[**ArcMCs**] テーブルには、ArcMCごとに次のパラメーターが表示されます。

- **Name:** ArcSight Management Centerの名前。
- **Path**: ArcSight Management Centerのパス。
- **Port**: ArcSight Management Centerが通信時に使用するポート番号。
- **Version**: ArcSight Management Centerのソフトウェアバージョン。
- **Status**: ArcSight Management Centerのステータス。
- **Last Check:** 最後のステータスチェックの日付と時刻。
- **Action:** 次のような、ArcMCの管理タスクを実行するためのコントロールが表示されます。
  - 再起動
  - シャットダウン
  - 設定の編集

ArcSight Management Centerでの他のArcSight Management Centerの管理の詳細については、「他のArcSight Management Centerの管理」(77ページ)を参照してください。

[EB Nodes] タブ

ArcMCで管理できるEvent Brokerは1つだけです。ただし、管理対象の1つのEvent Brokerには、任意の数のEvent Brokerノードを含めることができ、それぞれのノードをArcMCで管理および監視することができます。Event BrokerをホストとしてArcMCに追加すると、そのEvent Brokerのすべてのノードが追加されます。

[**EB Nodes**] タブには、管理対象のEvent Broker内に存在するすべてのEvent Brokerノードが表示されます。たとえば、ナビゲーションツリーで [**System**] を選択した場合、[**EB Nodes**] タブには、管理対象のすべてのEvent Brokerノードが表示されます。また、いずれかのロケーションを選択した場合は、そのロケーション内のすべてのEvent Brokerノードが表示されます。

このタブには、管理対象のEvent Brokerノードごとに、次のパラメーターが表示されます。

- **Name:** Event Brokerノードの名前。
- **Port**: Event Brokerノードが通信時に使用するポート番号。
- **Type**: Event Brokerノードのタイプ。
- **Last Check:** 最後のステータスチェックの日付と時刻。

ArcSight Management CenterでのEvent Brokerの管理の詳細については、「Event Brokerの管理」(173ページ) を参照してください。

ロケーション

ロケーションは、ホストを論理的にグループ化したものです。グループ化は、地理的な場所や所属組織など、選択した任意の条件に基づいて行うことができます。ロケーションは、一連のホストを整理するのに便利です。

たとえば、ニューヨークにあるすべてのホストを、サンフランシスコにあるホストとは別にグループ化し、それぞれを「New York」および「San Francisco」という名前のロケーションに割り当てることができます。同様に、「Sales」という名前のロケーションと「Marketing」というロケーションにホストをグループ化することもできます。

ロケーションは、**任意の数**のホストを含むことができます。ロケーションへのホストの追加の詳細は、「ホストの追加について」(57ページ) を参照してください。

注: ArcSight Management Centerにはデフォルトで (Defaultという名前の) ロケーションが1つ含まれていますが、別のロケーションをいくつでも追加することができます。Defaultロケーションの名前は変更可能です。また、このロケーションを削除することもできます。

ロケーションの追加

ロケーションはいくつでも追加できます。

ロケーションを追加するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、**[System]** をクリックします。
3. 管理パネルで **[Add Location]** をクリックします。
4. 新しいロケーションの名前を入力し、**[Next]** をクリックします。
5. **[Done]** をクリックします。新しいロケーションがSystemツリーに表示されます。

ロケーションの編集

ロケーションの名前を編集できます。

ロケーションを編集するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、[**System**] をクリックしてから、[**Locations**] タブをクリックします。
3. **[Locations]** タブで、名前を変更するロケーションを1つ以上選択します。
4. 選択したロケーションの [**Action**] ドロップダウンで、[**Edit Location**] を選択します。
5. ロケーションの新しい名前を入力し、**[Next]** をクリックします。
6. **[Done]** をクリックします。ロケーションの名前が変更されます。

すべてのロケーションの表示

ArcSight Management Centerに存在するすべてのロケーションを表示できます。

すべてのロケーションを表示するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、**[System]** をクリックし、**[Locations]** タブをクリックすると、すべてのロケーションが表示されます。

ロケーションの削除

ArcSight Management Centerからロケーションを削除すると、そのロケーション内のホスト (および関連するノード) もすべて削除されます。

ヒント: ArcSight Management Centerでロケーションを削除する一方、そのロケーション内のホストは維持する必要がある場合は、ロケーションを削除する前にホストを移動します。「ホストの別のロケーションへの移動」(70ページ) を参照してください。

ロケーションを削除するには

1. [**Node Management**] をクリックします。
2. ナビゲーションツリーで、[**System**] をクリックしてから、[**Locations**] タブをクリックします。
3. **[Locations]** タブで、削除するロケーションを1つ以上選択します。
4. [**Delete**] をクリックします。
5. [**OK**] をクリックして削除を確定します。選択したロケーションが削除されます。

ホスト

ホストとは、一意のIPアドレスまたはホスト名に関連づけられた、ネットワーク接続されたシステムです。ホストには、ArcSightアプライアンスや、ArcSightソフトウェア製品 (ソフトウェアLoggerなど) が実行されているシステムがあります。

管理するホストの追加の詳細は、「ホストの追加について」(57ページ) を参照してください。

ホストの追加について

ArcSight Management Centerにホストを追加すると、そのホスト上のArcSight製品はノードになり、管理できるようになります。たとえば、4つのコンテナーを含むコネクターアプライアンスを実行しているホストを追加した場合、コネクターアプライアンスと各コンテナーを合わせて5つのノードがArcSight Management Centerに追加されることになります。

ArcMC 2.2以降では、ArcMCローカルホストがリモート管理用に自動的に追加されます。このローカルホストは他のノードと同じように管理できます。

ホストの追加の前提条件 (ホストタイプ別)

ホストの追加に必要な接続情報

ホストタイプ	必要な情報
Appliance with Local Connectors (ArcSight Management Centerアプライアンス、コネクターアプライアンス、またはLoggerアプライアンス (L3XXX) を含む)	• ホスト名 (FQDN) またはIPアドレス。ホスト名またはIPは、ArcSight Management Centerで解決可能 (DNSを使用してホスト名を解決可能、またはIPアドレスを直接解決可能) である必要があります。ホスト名を使用する場合、入力されたホスト名がホストのSSL証明書のホスト名と一致している必要があります (FQDNが解決されない場合は、Webサービスを再起動します)。 • ホストにログインするための認証情報 (ユーザー名とパスワード)。ホストで外部認証 (LDAPやRADIUSなど) が設定されている場合、可能な場合は外部認証の資格情報を使用するか、そうでない場合はフォールバック認証の資格情報を使用します。 **注:** 認証情報の詳細については、「ホストの追加の前提条件 (ホストタイプ別)」(58ページ)を参照してください。 • ローカルコンテナー用の認証情報 (ユーザー名とパスワード)。アプライアンスに複数のコンテナーが含まれている場合、各コンテナーの資格情報が同じである必要があります。たとえば、コネクターアプライアンスで管理されている1つのコンテナーのユーザー名とパスワードがmyusernameとmypasswordである場合には、同じコネクターアプライアンスで管理されるすべてのローカルコンテナーの資格情報がmyusernameとmypasswordである必要があります。
Appliance without Local Connectors (Loggerアプライアンス (L3XXX以外) を含む)	• ホスト名 (FQDN) またはIPアドレス。ホスト名またはIPは、ArcSight Management Centerで解決可能 (DNSを使用してホスト名を解決可能、またはIPアドレスを直接解決可能) である必要があります。ホスト名を使用する場合、入力されたホスト名がホストのSSL証明書のホスト名と一致している必要があります (FQDNが解決されない場合は、Webサービスを再起動します)。 • ホストにログインするための認証情報 (ユーザー名とパスワード)。ホストで外部認証 (LDAPやRADIUSなど) が設定されている場合、可能な場合は外部認証の資格情報を使用するか、そうでない場合はフォールバック認証の資格情報を使用します。 **注:** 認証情報の詳細については、「ホストの追加の前提条件 (ホストタイプ別)」(58ページ)を参照してください。

ホストの追加に必要な接続情報 (続き)

ホストタイプ	必要な情報
Software Form Factor (ソフトウェアArcSight Management Center、ソフトウェアコネクターアプライアンス、またはソフトウェアLoggerを含む)	• ホスト名 (FQDN) またはIPアドレス。ホスト名またはIPは、ArcSight Management Centerで解決可能 (DNSを使用してホスト名を解決可能、またはIPアドレスを直接解決可能) である必要があります。ホスト名を使用する場合、入力されたホスト名がホストのSSL証明書のホスト名と一致している必要があります (FQDNが解決されない場合は、Webサービスを再起動します)。 • ホストにログインするための認証情報 (ユーザー名とパスワード)。ホストで外部認証 (LDAPやRADIUSなど) が設定されている場合、可能な場合は外部認証の資格情報を使用するか、そうでない場合はフォールバック認証の資格情報を使用します。 **注:** 認証情報の詳細については、「ホストの追加の前提条件 (ホストタイプ別)」(58ページ)を参照してください。 • 製品に割り当てられたポート番号。
Software Connector (すべてのタイプのSmartConnectorを含む)	• ホスト名 (FQDN) またはIPアドレス。ホスト名またはIPは、ArcSight Management Centerで解決可能 (DNSを使用してホスト名を解決可能、またはIPアドレスを直接解決可能) である必要があります (FQDNが解決されない場合は、Webサービスを再起動します)。 • コネクター用の認証情報 (ユーザー名とパスワード)。 **注:** 認証情報の詳細については、「ホストの追加の前提条件 (ホストタイプ別)」(58ページ)を参照してください。 • オプションで、すべてのソフトウェアコネクターに対応したポート範囲をスキャンする場合は、ハイフンで区切ったポート範囲 (9004-9008など、最初と最後の値を含む) を指定します。 **注:** ポート範囲に複数のコネクターが含まれている場合、その範囲内の各コネクターの資格情報が同じである必要があります。たとえば、範囲内の1つのコネクターのユーザー名とパスワードがmyusernameとmypasswordである場合には、ポート範囲内のすべてのコネクターの資格情報がmyusernameとmypasswordである必要があります。 ソフトウェアベースのSmartConnectorをホストとして追加する前に、ArcMCでのSmartConnectorの管理の説明に従ってSmartConnectorを準備する必要があります。

ホストの追加に必要な接続情報 (続き)

ホストタイプ	必要な情報
Event Broker	• ホスト名 (FQDN) またはIPアドレス。ホスト名またはIPは、ArcSight Management Centerで解決可能 (DNSを使用してホスト名を解決可能、またはIPアドレスを直接解決可能) である必要があります (FQDNが解決されない場合は、Webサービスを再起動します)。 • Event Brokerのポート番号 (デフォルト: 38080) • Event Brokerをホストとして追加するには、アクティブユーザーがこの操作を行う権限を持つArcMCの権限グループに属している必要があります。デフォルトで、管理者ユーザーにはこの権限が割り当てられています。 **注:** ホストの追加処理を実行する前に、完全なFQDNを使用してArcMCの証明書を生成し、その.crtファイルをダウンロードして、Kubernetesマスターノードに証明書ファイルをコピーする必要があります。この手順の詳細は、「Event Brokerのホストとしての追加の準備」を参照してください。

- **SSL証明書:** 次のホストタイプを管理する場合は、SSL証明書を生成する必要があります。
  - コネクターアプライアンスまたはソフトウェアコネクターアプライアンス
  - Loggerアプライアンスまたはソフトウェアlogger
  - Event Broker
  - ArcSight Management CenterアプライアンスまたはソフトウェアarcSight Management Center

    証明書内のホスト名は、ArcSight Management Centerに追加するホスト名と一致している必要があります。これらのホストタイプでの証明書の生成の詳細については、各製品の『HPE ArcSight Administrator's Guide』を参照してください (追加するホストにすでに証明書がインストールされている場合、証明書のホスト名が追加するホストのホスト名と一致していれば、既存の証明書を使用できます)。

    注: ホスト名がSSL証明書内のホスト名と一致しない場合は、次のいずれかの方法で、一致する証明書を生成し直すことができます。

    - ハードウェアアプライアンスの場合は、**[System Admin] > [Network]** で **[NICS]** タブをクリックします。**[Host Settings]** で、[Hostname] フィールドのエントリをメモします (ホストをArcSight Management Centerに追加するには、この値を使用する必要があります)。**[Restart Network Service]** をクリックします。続いて、ナビゲーションメニューの **[Security]** で、**[SSL Server Certificate]** を選択します。**[Generate Certificate]** をクリックします。**[NICS]** タブのホスト名と一致する新しい証明書が生成されます。
    - ソフトウェアフォームファクターの場合は、**[System Admin] > [SSL Server Certificate]** の **[Enter Certificate Settings]** で、前にメモした [NICS] タブのホスト名が **[Hostname]** フィールドに入力されていることを確認します。次に、

> [**Generate Certificate**] をクリックします。[**NICS**] タブのホスト名と一致する新しい証明書が生成されます。

- **エージェントのインストールの確認:** 「ArcSight Management Centerエージェントのインストール」(33ページ) の表を確認して、ホストをArcMCに追加する前に、ArcMCエージェントをホストにインストールする必要があるかどうかを確認します。一部のホストタイプでは、ホストの追加時にエージェントが自動的にインストールされます。

> ArcMCエージェントの自動インストールにはPerlが必要です。ArcMCにホストを追加する前に、Perlがホストにインストールされていることを確認してください。

ノードの認証情報

ArcSight Management Centerは、各管理対象ノードと通信するたびに、それぞれの認証情報 (ホストを最初に追加したときに指定したユーザー名とパスワード) を使用して、ノードに対する認証を行います。ホストにコネクターやコンテナーが含まれている場合は、コネクターやコンテナーの認証情報も指定する必要があります (ただし、Event Brokerの場合は、個別ノードごとの認証情報は必要ありません)。そのため、ホストの追加時には、各ノードの有効な資格情報が必要です。

ノードの資格情報の確認:

各管理対象ノードのシステム管理者に問い合わせて、現在のログイン資格情報を確認します。ArcSight製品は出荷時に、デフォルトの資格情報が設定されています。セキュリティ上の理由から、デフォルトの資格情報はすぐに管理者によって変更されると考えられるため、デフォルトの資格情報を認証に使用することはできません。

- HPE ArcSight製品のデフォルトの資格情報については、関連する製品の管理者ガイドを参照してください (SmartConnectorのデフォルトの資格情報については、Protect724のHPEサポートコミュニティから入手可能な『SmartConnectorユーザーガイド』を参照してください)。
- 一部の製品では、管理者が外部認証の使用を設定できます。この場合は、ArcSight Management Centerにホストを追加する際に、外部認証の資格情報またはフォールバック認証の資格情報を指定する必要があります (SmartConnectorでは、外部認証を設定することはできません)。

資格情報の変更または期限切れ

ArcSight Management Centerにノードを追加した後で、ノードのユーザー名またはパスワードが変更されると (または有効期限が切れると)、ノードは管理されなくなります。その場合でも、ノードは管理対象ノードのリストに表示されたままになります。たとえば、一部のホストで、一定期間後にパスワードが自動的に期限切れになるように設定されている場合、ノードの最初の資格情報を使用して、ArcSight Management Centerで正常に認証を行うことがで

きなくなります。この問題を回避するには、期限切れの起こらないノードの資格情報を使用します。資格情報が変更されたノードまたは期限切れになったノードの管理を継続するには、ホストの資格情報の更新機能を使用します。

動的な資格情報

認証情報が動的に変化するように設定されている場合 (RADIUSのワンタイムパスワードを使用する場合など)、外部認証の資格情報を指定する代わりに、フォールバック認証を使用することが許可された管理対象ノードのローカルユーザーの資格情報を指定することができます。この場合、ArcSight Management Centerは、最初に外部認証方式を使用して管理対象ノードに対する認証を行い、これに失敗すると、ローカルユーザーの資格情報を使用して管理対象ノードに対する認証を行います。

ArcMCでのSmartConnectorの管理

ArcMCでは、以前にインストールされたソフトウェアベースのSmartConnectorをリモートで管理できます。ただし、リモート管理機能は、ソフトウェアSmartConnectorでデフォルトで無効になっています。

ハードウェアでサポートされている場合には、1つのホストに複数のSmartConnectorをインストールできます。ArcSightでは、Windowsホストで最大4つ、Linuxホストで最大8つのSmartConnectorを利用できます。

ArcMCでソフトウェアベースのSmartConnectorを管理するには、次のように、各コネクターでリモート管理を有効にする必要があります。

1. テキストエディターを使用し、SmartConnectorのインストールディレクトリで、`/<install_dir>/user/agent/agent.properties`ファイルを開きます。
2. 次の行を追加します。`remote.management.enabled=true`
3. 必要に応じて、コネクターがリッスンするポートをカスタマイズします。デフォルト値は9001です。この値を変更するには、次の行を追加します: `remote.management.listener.port=<port_number>`。ここで、`<port_number>`は、新規のポート番号です。
4. ファイルを保存します。
5. SmartConnectorを再起動し、変更を有効にします。

Event Brokerのホストとしての追加の準備

Event Brokerを管理対象ホストとして追加する前に、完全なFQDNを使用してArcMCの証明書を生成し、その.crtファイルをダウンロードして、Kubernetesマスターノードに証明書ファイルをコピーする必要があります。

Event Brokerをホストとして追加する準備を行うには

1. ArcMCで、**[Administration] > [System Admin]** をクリックします。
2. **[Security] > [SSL Server Certificate]** で、[Hostname] に、ArcMCのFQDNを入力します。
3. [**Generate Certificate**] をクリックします。
4. 証明書をローカルに保存します。
5. Kubernetesマスターノードに接続します。
6. 生成した証明書を`/opt/arcsight/k8s-hostpath/eb/arcmccerts`にコピーします。
7. ArcSightインストーラーを起動します。
8. **[Configuration] > [ArcSight Event Broker]** をクリックします。
9. [**ArcMC Monitoring**] タブで [**ArcMC URL**] に、管理を行っているArcMCのFQDNとポート番号を入力します。

続いて、ArcMCで、「ホストの追加」で説明する手順を実行します。

ホストの追加

ホストの追加を行う前に、ホストが必要な前提条件を満たしていることを確認します。詳細については、「ホストの追加の前提条件 (ホストタイプ別)」(58ページ) を参照してください。

ホストをArcMCに追加するには

1. [**Node Management**] をクリックします。
2. ナビゲーションツリーで、ホストの追加を計画しているロケーションを選択します。
3. [**Hosts**] タブで、[**Add Host**] をクリックします。
4. [**Add a new Host**] ダイアログで、[**Hostname/IP**] に、ホストのホスト名またはIPアドレスを入力します。
5. [**Type**] で、ドロップダウンリストからノードのタイプを選択します。
6. 必要な設定項目の値を入力します (必要な情報はノードタイプによって異なります)。
   - [**Host Credentials**] または [**Connector Credentials**] に、認証に必要なユーザー名とパスワードを入力します。
   - [**Port**] に、必要に応じて、ArcSight Management Centerからホストに接続するのに使用するポートの値を入力します。
7. [**Add**] をクリックします。ホストがArcSight Management Centerに追加されます。

コンテナーを含むホストの追加

コンテナーを含むホスト (コネクターアプライアンスなど) を追加する場合、ArcSight Management Centerはホスト上に存在するすべてのコンテナーからSSL証明書を取得し、各コンテナーを別々のノードとして追加しようとします。リモートホスト上のコンテナーは、ArcSight Management Centerが証明書と提供される資格情報を使用して認証できる場合のみ管理できます。証明書を取得する際、ArcSight Management Centerにインポートするかどうかを尋ねられます。

注: ArcSight Management Centerアプライアンスでは、すべてのローカルコンテナーがSoftware Connectorタイプのホストとして自動的に追加されます。

複数のホストのインポート

複数のホストを一括してすばやく簡単に追加するには、追加するホストの名前と必要な属性を列挙したCSV (カンマ区切り値) ファイルをインポートします。

注: ArcSight Management Center 1.0では、コネクターのホストをインポートするのに若干異なるファイル形式が使用されていました。このファイル形式は、ArcSight Management Center 2.1ではサポートされません。代わりに、ここで説明するファイル形式を使用します。

複数のホストのインポートの前提条件

ホストのインポートには、次の前提条件が適用されます。

- **ホストの追加の前提条件:** ホストの追加処理の前提条件が、CSVファイルによる複数のホストのインポートにも適用されます。「ホストの追加について」(57ページ) を参照してください。
- **有効なCSVファイル:** CSVファイル内の値が有効で正しいものであることを確認します。ホストのインポートジョブは、無効な値や正しくない値を受け取るとただちに失敗します。CSVファイル形式の説明は、「CSVファイルのフォーマット」(64ページ) に記載されています。
- **エージェント 1.0のプロセスの停止:** また、インポート対象のホストの中にArcSight Management Center 1.0のエージェントを実行中のものがある場合は、インポート前にそれらのホストで実行されているエージェントプロセスを停止します (これは、1.0より後のバージョンのArcMCエージェントでは必要ありません)。

CSVファイルのフォーマット

CSV (カンマ区切り値) ファイルでは、次のヘッダー行を最初の行として使用する必要があります。

```
location,hostname,type,host username,host password,connector
username,connector password,port/port range
```

それ以降は、各行にインポートするホストを1つずつ記述します。各行には、ホストごとのカンマ区切りの以下のフィールドの値を記述します。

<ロケーション>, <ホスト名>,<ホストタイプ>,<ホストのユーザー名>,<ホストのパスワード>, <コネクターのユーザー名>,<コネクターのパスワード>,<ポート/ポート範囲>

ホストタイプによって、すべてのフィールドの値が必須である場合と、一部のフィールドが省略可能である場合があります。省略可能なフィールドで値を指定しない場合でも、そのフィールドが空であることを示すためのカンマは必要です。

ホストフィールドの値

ホストフィールドの有効な値は、以下の表で詳しく説明しています。アスタリスク (*) は、必須フィールドを示します。省略可能なフィールドで値を指定しない場合でも、そのフィールドが空であることを示すためのカンマは必要です。

フィールド	説明
Location*	ホストを割り当てるロケーション。
Hostname*	ホストのホスト名 (FQDN) またはIPアドレス。 • FQDNまたはIPは、ArcSight Management Centerで解決可能 (DNSを使用してホスト名を解決可能、またはIPアドレスを直接解決可能) である必要があります。 • ホスト名を使用する場合、入力されたホスト名がホストのSSL証明書のホスト名と一致している必要があります。 • ハードウェアアプライアンスの場合、DNSは管理を行うアプライアンスで設定する必要があります (**[System Admin] > [DNS]**)。
Host Type*	ホストタイプ。有効な値 (大文字/小文字を区別しない) は、次のとおりです。 • `appliance_with_local_connectors`: ArcSight Management Centerアプライアンス、コネクターアプライアンス、Loggerアプライアンス (L3XXX) など。 • `appliance_without_local_connectors`: Loggerアプライアンス (L3XXX以外) など。 • `software_form_factor`: ソフトウェアArcSight Management Center、ソフトウェアコネクターアプライアンス、またはソフトウェアLoggerなど。 • `software_connector`: すべてのソフトウェアコネクターおよびSmartConnectorなど。

フィールド	説明
Host Username/ Password*	ホストに対する認証に使用するユーザー名とパスワード。 **注:** 認証情報の詳細については、「ホストの追加について」(57ページ)を参照してください。
Connector Username/ Password	ソフトウェアコネクターに対する認証に使用するユーザー名とパスワード。Appliance with Local ConnectorsおよびSoftware Connectorタイプのホストの場合は必須。それ以外の場合は、オプションです。 **注:** 認証情報の詳細については、「ホストの追加について」(57ページ)を参照してください。
Port/Port Range	コネクタースキャンの開始ポートまたはポート範囲。有効な値は次のとおりです。 • ポート番号 • ポート範囲 • カンマ区切りのポート番号 (例: 9000,9004,9007) 注: • ソフトウェアフォームファクターの場合は、ポートが必要です。 • アプライアンスフォームファクターの場合、すべてのローカルコンテナーを追加するには、このフィールドを空白のままにします。ただし、いずれかのポート番号を入力した場合は、指定したポートのみに対応する証明書がダウンロードされ、該当するコンテナーのみがインポートされます。 • ソフトウェアコネクターの場合、ポートまたはポート範囲が必要です。ポート範囲を使用する場合は、開始ポートと終了ポートの間にハイフンを使用して、ポート範囲 (最初と最後の値を含む) を指定します。たとえば、9001-9003のポート範囲を指定した場合は、9001、9002、9003のポートがスキャンされます。 **注:** ポート範囲に複数のコネクターが含まれている場合、その範囲内の各コネクターの資格情報が同じである必要があります。たとえば、範囲内の1つのコネクターのユーザー名とパスワードがmyusernameとmypasswordである場合には、ポート範囲内のすべてのコネクターの資格情報がmyusernameとmypasswordである必要があります。

有効なインポートファイルの例 (2つのホストをインポート) を以下に示します。

```
location,hostname,type,host_username,password1,connector_
username,password2,port/port range

CorpHQ,hostname.example.com,software_connector,username,password,connector__
username,connector_password,9001-9010

EMEA,hostname2.example.com,appliance_without_local_connectors,
logger_user,logger_pword,,,
```

この例では、最初の行は必須のヘッダー行で、2番目の行はSoftware Connector、3番目の行はLoggerアプライアンスを表します。

ホストのインポートの手順

一度に実行できるホストのインポートジョブは1つだけです。

CSVファイルからホストをインポートするには

注: バージョン1.0のArcMCエージェントを実行中のホストがある場合は、インポートを始める前に、それらのエージェントプロセスを停止します。

1. テキストエディターでCSVファイルを作成して保存します。
2. ArcSight Management Centerにログインします。
3. **[Node Management] > [Import Hosts]** を選択します。Import Hostsウィザードが起動します。
4. [**Browse**] をクリックし、ホストのCSVファイルの場所を参照します。
5. [**Import**] をクリックします。ホストのインポートがバックグラウンドジョブとして実行されます。

   CSVファイルが有効な場合、ArcSight Management Centerがコンテナー内の各コネクターと通信できるように、コネクターの証明書が自動的に取得されます。Upload CSVウィザードにより証明書の一覧が表示されます (証明書の詳細を表示するには、証明書にマウスカーソルを合わせます)。

ArcMCエージェントの自動インストールにより、Import Hostsジョブに要する時間が増える場合があります。

- 証明書をインポートして続行するには、**[Import the certificates...]** を選択して **[Next]** をクリックします。
- 証明書をインポートしない場合は、**[Do not import the certificates...]** を選択して **[Next]** をクリックします。Upload CSVウィザードは、CSVのアップロード処理を完了しません。

  注: Import Hostsウィザードは、コンテナー内のいずれかのコネクターの証明書のアップロードが失敗した場合や、いずれかの証明書がトラストストアへのインポートに失敗した場合、アップロードを完了しません。

2. Import Hostsジョブが実行されます。

Import Hostsジョブのログ

ArcSight Management Centerには、すべてのImport Hostsジョブの結果がログとして記録されます。ジョブごとに、`import_hosts_<date>_<time>.txt`という名前のログが新規に生成されます。ここで、`<date>`と`<time>`はホストのインポートジョブの日付と時刻です。

- ソフトウェアArcSight Management Centerの場合、ログはディレクトリ`<install_dir>/userdata/logs/arcmc/importhosts`にあります。
- ArcSight Management Centerアプライアンスの場合、ログはディレクトリ`opt/arcsight/userdata/logs/arcmc/importhosts`にあります。

ログのフォーマット

ログ内の各エントリには、各ホストのインポートの成功または失敗が、次のフォーマットで示されます。

<ジョブを開始したユーザー>, <CSVファイル名>, <ホストのインポートジョブの開始時刻>,<ホスト名>,<成功/失敗の結果>

例:

```
admin, my_csv_file.csv, Tue Apr 08 14:16:58 PDT 2015, host.example.com, Host added successfully
```

CSVファイルに無効なエントリが1つ以上含まれていて、ホストのインポートジョブに失敗した場合は、行番号とエラーを含む解析エラーの詳細が結果ファイルに示されます。

例:

```
Line [1] has [connector password] field empty. [connector password] field is required for this host type.
```

ホストのエクスポート

ArcSight Management Centerからホストをエクスポートすると、そのArcSight Management Centerで管理されているホストのリストがCSV形式で作成されます (このファイルには、パスワード情報は含まれません)。

このファイルに各ホストのパスワードを追加した後に、「複数のホストのインポート」(64ページ)に記載されているホストのインポート機能を使用して、このホストのリストを別のArcSight Management Centerにインポートできます。

ホストのエクスポートは、ホストの管理を別のArcMCに割り当て直す場合に非常に便利です。

たとえば、ArcMC EastとArcMC Westという、2つのArcSight Management Centerがあるとします。現在は、ArcMC Eastで50個のホストを管理していますが、すべてのホストの管理を新しいArcMC Westに統合しようと考えています。この作業をすばやく簡単に行うには、ArcMC EastのホストをCSVファイルにエクスポートします。続いて、このCSVファイルにArcMC Eastの追加エントリを追加します。

各ホストのパスワードデータを追加した後に、CSVファイルをArcMC Westにインポートします。この処理が終了すると、ArcMC Eastのすべてのホストと ArcMC Eastそのものが、ArcMC Westによって管理されるようになります。

ArcSight Management Centerでホストをエクスポートするには

1. **[Node Management] > [Export Hosts]** を選択します。
2. ArcSight Management Centerで管理されているすべてのホストが、ローカルCSVファイル (`exporthosts.csv`) にエクスポートされます。

3. 必要に応じて、CSVエディターでファイルを開きます。各ホストのパスワード情報をCSVファイルに追加し、ファイルを保存します。

すべてのホストの表示

ArcSight Management Centerで管理されているすべてのホストを表示 (またはロケーションごとにホストを表示) することができます。

すべてのホストを表示するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、**[System]** をクリックします (ロケーションごとに表示するには、表示するロケーションをクリックします)。
3. [**Hosts**] タブをクリックします。すべての管理対象ホストが表示されます。

ホスト上の管理対象ノードの表示

ホスト上のすべての管理対象ノードを、ノードタイプ別に表示することができます。

ホスト上の管理対象ノードを表示するには

1. [**Node Management**] をクリックします。
2. ナビゲーションツリーで、ホストが割り当てられているロケーションをクリックします。続いて、ホストをクリックします。
3. 該当するタブをクリックし、管理対象ホストの該当するノードタイプを表示します: **[Containers]**、**[Connectors]**、**[Connector Appliances]**、**[Loggers]**、または **[ArcMCs]**

ホストの削除

ホストを削除すると、ホストに関連付けられているノードも削除されます。ホストを削除すると、ArcSight Management Centerからそのホストのエントリが削除されますが、それ以外にホストマシンに影響はありません。

ホストを削除する際には注意してください。ホストを削除すると、ホストに関連付けられたノードを含むノードリスト、関連付け、ピアのリスト、またはサブスクライバーのリストから、それらのノードが削除されます。

1つ以上のホストを削除するには

1. [**Node Management**] をクリックします。
2. ナビゲーションツリーで、[**System**] をクリックしてから、[**Hosts**] タブをクリックします。
3. 削除する1つ以上のホストを選択します。
4. [**Delete**] をクリックします。
5. [**Yes**] をクリックして削除を確定します。ホスト (および関連するすべてのノード) が削除されます。

ホストの別のロケーションへの移動

1つ以上のホストを新しいロケーションに割り当てることができます。ホストを移動すると、ホストに関連付けられているノードも移動されます。たとえば、コネクターアプライアンスを新しいロケーションに移動した場合、関連するコンテナーと管理対象コネクターもすべて新しいロケーションに移動されます。

1つ以上のホストを移動するには

1. [**Node Management**] をクリックします。
2. ナビゲーションツリーで、[**System**] をクリックしてから、[**Hosts**] タブをクリックします。
3. 移動する1つ以上のホストを選択します。
4. [**Move**] をクリックします。
5. **Host Move**ウィザードに表示されるプロンプトに従います。選択したホストが、新しいロケーションに割り当てられます。

ArcMCエージェントの更新 (またはインストール)

古いバージョンのArcSight Management Centerエージェントが実行されているホストは、最新バージョンにすばやくアップグレードできます。

エージェントのインストールまたはアップグレードは、すべてのバージョンのArcMCアプライアンス、コネクターアプライアンス (ハードウェア) およびLoggerアプライアンス、ソフトウェアLogger 6.0以降、およびソフトウェアArcMC 2.1以降でサポートされています。

ヒント: 各ホストのエージェントのバージョンをチェックするには、[**Hosts**] タブをクリックし、[**Agent Version**] カラムを確認します。

1つ以上のホストでエージェントをアップグレードまたはインストールするには

1. [**Node Management**] をクリックします。
2. ナビゲーションツリーで、[**System**] をクリックしてから、[**Hosts**] タブをクリックします。
3. 更新する1つ以上のホストを選択します。
4. [**Update Agent**] をクリックします。Agent Upgradeウィザードが起動します。プロンプトにしたがってAgent Upgradeウィザードを完了します。

ホストのスキャン

ホストをスキャンすると、ホスト上で現在実行中のすべてのコンテナーとそれらに関連付けられたコネクターのインベントリが作成されます。

注: コンテナーを含むホストはすべて、ArcSight Management Centerに最初に追加されたときに自動的にスキャンされます。

コンテナーのインベントリが正確で最新の状態になるようにするため、以下の場合には、新しいコンテナーを手動でスキャンする必要があります。

- リモートホストがArcSight Management Centerに追加された後に、追加のコンテナーまたはコネクターがそのホストに追加された場合。
- コンテナーまたはコネクターが、ArcSight Management Centerで管理されているリモートホストから削除された場合。
- 最初に自動スキャンが実行されたときにダウンしていたコンテナーが、その後復旧した場合。
- (別のArcSight Management Centerで管理されている) 管理対象ArcSight Management Centerのライセンスがアップグレードされ、ライセンスされたコンテナーの数が増えた場合。

コンテナーを実行できるすべてのホストタイプを手動でスキャンできます。これらのタイプには、以下が含まれます。

- コネクターアプライアンス
- Loggers (L3XXXモデルのみ)
- ArcSight Management Centerアプライアンス
- ソフトウェアコネクター

スキャンプロセス

ホストのスキャンでは、ホスト上で実行中のすべてのコンテナーから、すべてのCA証明書に関する情報が取得されます。リモートホスト上のコンテナーは、ArcSight Management Centerが証明書と提供される資格情報を使用して認証できる場合のみ管理できます。取得した証

明書をArcSight Management Centerのトラストストアにインポートするかどうかを確認するプロンプトが表示されます。

次のいずれかに当てはまる場合、手動スキャンは中断されます。

- スキャンされたコネクターアプライアンスホスト上のいずれかのコンテナーがダウンしている場合。
- 取得した証明書をインポートしないことを選択した場合。
- いずれかのコンテナーで認証に失敗した場合。

ホストを手動でスキャンするには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、ホストが割り当てられているロケーションを選択します。
3. **[Hosts]** タブをクリックします。
4. スキャンするホストの [**Action**] ドロップダウンで、[**Scan Host**] をクリックします。Host Scanウィザードが起動します。
5. Host Scanウィザードで **[Next]** をクリックします。
6. 次の表のパラメーターの値を入力し、**[Next]** をクリックします。

パラメーター	説明
Starting Port	ArcSight Management Centerがコンテナーのスキャンを開始するホスト上のポート番号。
Ending Port	ArcSight Management Centerがコンテナーのスキャンを開始するホスト上のポート番号。
User	ホストを認証するために使用するユーザー名。
Password	指定したユーザー名のパスワード。

7. ArcSight Management Centerがコンテナー内の各コネクターと通信できるように、コネクターの証明書が自動的に取得されます。Host Scanウィザードには証明書の一覧が表示されます (証明書の詳細を表示するには、証明書にマウスカーソルを合わせます)。
   - スキャンを続行するには、[**Import the certificates**] を選択し、[**Next**] をクリックして証明書をインポートして続行します。
   - それ以外の場合は、[**Do not import the certificates**] を選択し、[**Next**] をクリックします。Host Scanウィザードでスキャンが中断されます。

ホストの証明書のダウンロードとインポート

ホスト名がSSL証明書内のホスト名と一致しない場合は、ホストの現在の証明書をダウンロードしてインポートできます。

ホストの証明書をダウンロードしてインポートするには

1. [**Node Management**] をクリックします。
2. ナビゲーションツリーで、ホストが割り当てられているロケーションを選択します。
3. [**Hosts**] タブをクリックします。
4. 目的のホストの [**Action**] ドロップダウンで、[**Download Certificate**] を選択します。
5. Downloadウィザードで [**Next**] をクリックします。
6. ウィザードのプロンプトに従って処理を完了します。

ホストの資格情報の更新

ArcMCでは、管理対象ホストとの接続および認証に、ホストのログイン資格情報を使用します。これらの資格情報は、ホストをArcMCに管理用に追加する際に指定します。これらの資格情報が変更された場合、ArcMCとホストとの間の管理リンクが失われます。

ただし、ArcMCが管理対象ホストとの認証に使用する資格情報を更新して、管理リンクが失われないようにすることができます。

ArcMCでホストの資格情報を更新しても、管理対象ホスト上の実際の資格情報は変更されません。実際の資格情報は、この操作を行う直前または直後に、ホスト上で直接変更する必要があります。資格情報の更新では、ArcMCが管理対象ホストとの認証に使用する資格情報が更新されるだけです。

ホストの資格情報を更新するには

1. [**Node Management**] をクリックします。
2. ナビゲーションツリーで、ホストが割り当てられているロケーションを選択します。
3. [**Hosts**] タブをクリックします。
4. 目的のホストの [**Action**] ドロップダウンで、[**Update Credentials**] を選択します。
5. [**Username**] と [**Password**] に、ArcMCがホストとの接続に使用する新しい資格情報を入力します。
6. [**Save**] をクリックします。

第5章: HPE ArcSight製品の管理

ここでは、以下の内容について説明します。

概要

ArcSight Management Centerでは、次のようなさまざまなHPE ArcSight製品で管理タスクを実行できます。

- ハードウェアおよびソフトウェアコネクターアプライアンス
- ハードウェアおよびソフトウェアArcSight Management Center
- ハードウェアおよびソフトウェアLogger
- コンテナー
- ソフトウェアコネクター
- Event Broker

この章では、これらの製品のリモート管理について説明します。

コネクターアプライアンス (ConApp) の管理

ArcSight Management Centerを使用し、管理対象のコネクターアプライアンスまたはソフトウェアコネクターアプライアンスに対して、以下の管理タスクを実行できます。

- 再起動またはシャットダウン。
- 設定の編集または削除。
- 1つ (または複数) のコネクターアプライアンスの設定。

注: ArcSight Management Centerを使用して、コネクターアプライアンスのすべての機能を管理できる訳ではありません。コネクターアプライアンスの機能の詳細な説明については、『Connector Appliance Administrator's Guide』を参照してください。

ConAppの再起動

管理対象のコネクターアプライアンスをリモートから再起動するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、**[System]** をクリックします。
3. 管理パネルで **[ConApps]** をクリックします。
4. コネクターアプライアンスのリストで、再起動するコネクターアプライアンスを選択します。
5. コネクターアプライアンスの **[Action]** ドロップダウンで **[Reboot ConApp]** を選択します。
6. **[Next]** をクリックして再起動を確定します。
7. コネクターアプライアンスが再起動されます。**[Done]** をクリックします。

ConAppのシャットダウン

管理対象のコネクターアプライアンスをリモートからシャットダウンするには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、**[System]** をクリックします。
3. 管理パネルで **[ConApps]** をクリックします。
4. コネクターアプライアンスのリストで、シャットダウンするコネクターアプライアンスを選択します。
5. コネクターアプライアンスの **[Action]** ドロップダウンで **[Shutdown ConApp]** を選択します。
6. **[Next]** をクリックしてシャットダウンを確定します。
7. コネクターアプライアンスがシャットダウンされます。**[Done]** をクリックします。

ConAppの設定の編集または削除

管理対象のコネクターアプライアンスの設定の編集や、リスト設定のプロパティ値の削除を行うことができます。

設定を編集または削除すると、ノードの現在の設定は上書きされます。これにより、ノードが現在のサブスクリプションに準拠しなくなる可能性があります。

コネクターアプライアンスで設定を編集または削除するには

1. [**Node Management**] をクリックします。
2. ナビゲーションツリーで、[**System**] をクリックします。

3. 管理パネルで **[ConApps]** をクリックします。
4. コネクターアプライアンスのリストで、目的のコネクターアプライアンスを選択します。
5. コネクターアプライアンスの [**Action**] ドロップダウンで [**Edit/Remove Config**] を選択します。Update Configurationsウィザードが起動します。
6. ダイアログボックスを確認し、[**Next**] をクリックします。
7. プロンプトにしたがってウィザードを完了します。
8. ウィザードが完了したら、[**Done**] をクリックします。

注: コネクターアプライアンスノードのバックアップ設定を編集するには、ノードにスケジュールされたバックアップが存在している必要があります。

ConAppでの設定の実行

Set Configurationウィザードを使用して、1つまたは複数のコネクターアプライアンスで設定を行うことができます。

- リスト設定の場合は、Set Configurationウィザードを使用して、複数のコネクターアプライアンスの既存の設定にプロパティ値を追加します。新規の値のみが追加されます。リスト設定の詳細については、「リスト設定」(132ページ) を参照してください。
- リスト設定以外の設定の場合は、Set Configurationウィザードを使用して、複数のコネクターアプライアンスの設定を上書きします。

注意: 1つまたは複数のコネクターアプライアンスで設定を行うと、各コネクターアプライアンスが現在のサブスクリプションに準拠しなくなる場合があります。

1つまたは複数のコネクターアプライアンスで設定を行うには

1. [**Node Management**] をクリックします。
2. ナビゲーションツリーで、[**System**] をクリックします。
3. 管理パネルで [**Connector Appliances**] をクリックします。
4. コネクターアプライアンスのリストで、コネクターアプライアンスを1つ以上選択します。
5. [**Set Configuration**] をクリックします。Set Configurationウィザードが起動します。
6. ダイアログボックスを確認し、[**Next**] をクリックします。
7. プロンプトにしたがってウィザードを完了します。
   - 新規のプロパティをリスト設定に追加するには、[**Add Row**] をクリックし、必要な値を入力します。
8. 選択したコネクターアプライアンスで設定が行われます。[**Done**] をクリックします。

他のArcSight Management Centerの管理

管理対象のソフトウェアArcSight Management CenterまたはArcSight Management Centerアプライアンスに対して、以下の管理タスクを実行できます。

- 再起動またはシャットダウン。
- 設定の編集または削除。
- ArcMCのリモートからのアップグレード。
- 1つ(または複数)のArcSight Management Centerの設定。

ArcMCの再起動

管理対象のArcSight Management Centerをリモートから再起動するには

1. [**Node Management**] をクリックします。
2. ナビゲーションツリーで、[**System**] をクリックします。
3. 管理パネルで [**ArcMCs**] をクリックします。
4. ArcSight Management Centerのリストで、再起動するArcSight Management Centerを見つけます。
5. ArcMCの [**Action**] ドロップダウンで、[**Reboot ArcMC**] を選択します。
6. [**Next**] をクリックして再起動を確定します。
7. ArcSight Management Centerが再起動されます。[**Done**] をクリックします。

ArcMCのシャットダウン

管理対象のArcSight Management Centerをリモートからシャットダウンするには

1. [**Node Management**] をクリックします。
2. ナビゲーションツリーで、[**System**] をクリックします。
3. 管理パネルで [**ArcMCs**] をクリックします。
4. ArcSight Management Centerのリストで、シャットダウンするArcSight Management Centerを見つけます。
5. ArcMCの [**Action**] ドロップダウンで、[**Shutdown ArcMC**] を選択します。
6. [**Next**] をクリックしてシャットダウンを確定します。
7. ArcSight Management Centerがシャットダウンされます。[**Done**] をクリックします。

ArcMCの設定の編集または削除

管理対象のArcSight Management Centerで、設定の編集や、リスト設定のプロパティ値の削除を行うことができます。

設定を編集または削除すると、ノードの現在の設定は上書きされます。これにより、ノードが現在のサブスクリプションに準拠しなくなる可能性があります。

ArcSight Management Centerで設定を編集または削除するには

1. [**Node Management**] をクリックします。
2. ナビゲーションツリーで、[**System**] をクリックします。
3. 管理パネルで [**ArcMCs**] をクリックします。
4. ArcSight Management Centerのリストで、目的のArcSight Management Centerを見つけます。
5. [**Action**] ドロップダウンで [**Edit/Remove Config**] を選択します。Update Configurationsウィザードが起動します。
6. ダイアログボックスを確認し、[**Next**] をクリックします。
7. プロンプトにしたがってウィザードを完了します。
8. ウィザードが完了したら、[**Done**] をクリックします。

> **注:** ArcMCノードのバックアップ設定を編集するには、ノードにスケジュールされたバックアップが存在している必要があります。

ArcMCのアップグレード

ArcMCでは、以下のタイプの管理対象ArcMCをリモートからアップグレードできます。

フォームファクター	アップグレードファイル名	アップグレード前のバージョン	アップグレード後のバージョン	コメント
アプライアンス	`arcmc-<ビルド番号>.enc`	バージョン2.0以降	それ以降のバージョン。	
ソフトウェア	`arcmc-sw-<ビルド番号>-remote.enc`	バージョン2.1	それ以降のバージョン。	ソフトウェアArcMCでは、オペレーティングシステムのリモートアップグレードはサポートされていません。必要な場合は、手動でアップグレードする必要があります。

アップグレードでは、最初にArcMCのリポジトリに関連するファイルをアップロードする必要があります。その後、アップグレードファイルを管理対象のArcMCに適用します。

アップグレードファイルをリポジトリにアップロードするには

1. 上記の表の説明に従って、アップグレードバージョンに対応したArcMCアップグレードファイルをダウンロードし、ネットワークの安全な場所に保管します。
2. **[Administration] > [Repositories]** をクリックします。
3. ナビゲーションツリーで、**[Upgrade Files]** を選択します。
4. 管理パネルで **[Upload]** をクリックします。
5. **[Choose File]** をクリックしてアップグレードファイルを選択し、**[Submit]** をクリックします。ファイルがアップロードされます。

管理対象のArcMCをリモートからアップグレードするには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、**[System]** をクリックします。
3. 管理パネルで **[ArcMCs]** をクリックします。
4. ArcMCのリストで、ArcMCを1つ以上選択します (アップグレードファイルタイプに関連するフォームファクターのみを選択できます。上記の説明を参照してください)。
5. **[Upgrade ArcMC]** をクリックします。Upgradeウィザードが起動します。
6. ダイアログボックスを確認し、[**Next**] をクリックします。
7. プロンプトにしたがってウィザードを完了します。
8. ウィザードが完了したら、**[Done]** をクリックします。

.encファイルによるローカルホストのアップグレードが完了したときに、空のページが表示される場合があります。このページが表示されても特に問題はありません。

管理対象のArcMCでの設定の実行

Set Configurationウィザードを使用して、1つまたは複数のArcSight Management Centerで設定を行うことができます。

- リスト設定の場合は、Set Configurationウィザードを使用して、複数のArcSight Management Centerの既存の設定にプロパティ値を追加します。新規の値のみが追加されます (リスト設定の詳細については、「[Configurations] テーブル」(130ページ) を参照してください)。
- リスト設定以外の設定の場合は、Set Configurationウィザードを使用して、複数のArcSight Management Centerの設定を上書きします。

注意: 1つまたは複数のArcSight Management Centerで設定を行うと、各ArcSight Management Centerが現在のサブスクリプションに準拠しなくなる場合があります。

1つまたは複数のArcSight Management Centerで設定を行うには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、**[System]** をクリックします。
3. 管理パネルで **[ArcMCs]** をクリックします。
4. ArcSight Management Centerのリストで、設定を行うArcSight Management Centerを1つ以上選択します。
5. **[Set Configuration]** をクリックします。Set Configurationウィザードが起動します。
6. ダイアログボックスを確認し、[**Next**] をクリックします。
7. プロンプトにしたがってウィザードを完了します。
   - 新規のプロパティをリスト設定に追加するには、[**Add Row**] をクリックし、必要な値を入力します。
8. 選択したArcSight Management Centerで設定が行われます。**[Done]** をクリックします。

ArcMCでのSmartConnectorの管理

ArcMCでは、以前にインストールされたソフトウェアベースのSmartConnectorをリモートで管理できます。ただし、リモート管理機能は、ソフトウェアSmartConnectorでデフォルトで無効になっています。

ハードウェアでサポートされている場合には、1つのホストに複数のSmartConnectorをインストールできます。ArcSightでは、Windowsホストで最大4つ、Linuxホストで最大8つのSmartConnectorを利用できます。

ArcMCでソフトウェアベースのSmartConnectorを管理するには、次のように、各コネクターでリモート管理を有効にする必要があります。

1. テキストエディターを使用し、SmartConnectorのインストールディレクトリで、`/<install_dir>/user/agent/agent.properties`ファイルを開きます。
2. 次の行を追加します。`remote.management.enabled=true`
3. 必要に応じて、コネクターがリッスンするポートをカスタマイズします。デフォルト値は9001です。この値を変更するには、次の行を追加します: `remote.management.listener.port=<port_number>`。ここで、`<port_number>` は、新規のポート番号です。
4. ファイルを保存します。
5. SmartConnectorを再起動し、変更を有効にします。

Loggerの管理

ArcSight Management Centerを使用し、管理対象のLoggerアプライアンスまたはソフトウェアLoggerアプライアンスに対して、以下の管理タスクを実行できます。

- 再起動またはシャットダウン。
- 設定の編集または削除。
- 1つ(または複数)のLoggerの設定。
- Loggerのリモートからのアップグレード。

注: ArcSight Management Centerを使用して、Loggerのすべての機能を管理できる訳ではありません。Loggerの機能の詳細な説明については、『Logger管理者ガイド』を参照してください。

Loggerの再起動

管理対象のLoggerをリモートから再起動するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、**[System]** をクリックします。
3. 管理パネルで **[Loggers]** をクリックします。
4. Loggerのリストで、再起動するLoggerを選択します。
5. そのLoggerの **[Action]** ドロップダウンで、**[Reboot Logger]** を選択します。
6. **[Next]** をクリックして再起動を確定します。
7. Loggerが再起動されます。**[Done]** をクリックします。

Loggerのシャットダウン

管理対象のLoggerをリモートからシャットダウンするには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、**[System]** をクリックします。
3. 管理パネルで **[Loggers]** をクリックします。
4. Loggerのリストで、シャットダウンするLoggerを選択します。
5. そのLoggerの **[Action]** ドロップダウンで、**[Shut Down Logger]** を選択します。
6. **[Next]** をクリックしてシャットダウンを確定します。
7. Loggerがシャットダウンされます。**[Done]** をクリックします。

Loggerの設定の編集または削除

管理対象のLoggerの設定の編集や、リスト設定のプロパティ値の削除を行うことができます。

設定を編集または削除すると、ノードの現在の設定は上書きされます。これにより、ノードが現在のサブスクリプションに準拠しなくなる可能性があります。

管理対象Loggerの設定を編集または削除するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、**[System]** をクリックします。
3. 管理パネルで **[Loggers]** をクリックします。
4. Loggerのリストで、目的のLoggerを選択します。
5. そのLoggerの **[Action]** ドロップダウンで **[Edit/Remove Config]** を選択します。Update Configurationsウィザードが起動します。
6. ダイアログボックスを確認し、[**Next**] をクリックします。
7. プロンプトにしたがってウィザードを完了します。
8. ウィザードが完了したら、**[Done]** をクリックします。

注: Loggerノードのバックアップ設定を編集するには、ノードにスケジュールされたバックアップが存在している必要があります。

Loggerのアップグレード

ArcMCでは、以下のタイプの管理対象Loggerをリモートからアップグレードできます。

フォームファクター	アップグレードファイル名	アップグレード前のバージョン	アップグレード後のバージョン	コメント
アプライアンス	logger-<ビルド番号>.enc	6.0以降	6.1以降	Loggerアプライアンスのリモートアップグレードファイルのファイル名の形式は、logger-<ビルド番号>.encです。
ソフトウェア	logger-sw-<ビルド番号>-remote.enc	6.0以降	6.1以降	• ソフトウェアLoggerのリモートアップグレードファイルのファイル名の形式は、logger-sw-<ビルド番号>-remote.encです。 • ソフトウェアLoggerでは、オペレーティングシステムのリモートアップグレードはサポートされていません。必要な場合は、手動でアップグレードする必要があります。

Loggerバージョン6.0にアップグレードするには、管理対象LoggerでArcMCエージェント1167.1以降が実行されている必要があります。管理対象Loggerでエージェントをアップグレードした後に、Logger 6.0へのアップグレードを行います。

アップグレードファイルをリポジトリにアップロードするには

1. 上記の表の説明に従って、アップグレードバージョンに対応したLoggerアップグレードファイルをダウンロードし、ネットワークの安全な場所に保管します。
2. **[Administration] > [Repositories]** をクリックします。
3. ナビゲーションツリーで、**[Upgrade Files]** を選択します。
4. 管理パネルで **[Upload]** をクリックします。
5. **[Choose File]** をクリックしてアップグレードファイルを選択し、**[Submit]** をクリックします。ファイルがアップロードされます。

管理対象のLoggerをリモートからアップグレードするには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、**[System]** をクリックします。
3. 管理パネルで **[Loggers]** をクリックします。
4. Loggerのリストで、Loggerを1つ以上選択します(選択できるアップグレード対象のフォームファクタータイプは1つだけです)。
5. **[Upgrade Logger]** をクリックします。Upgradeウィザードが起動します。

6. ダイアログボックスを確認し、[**Next**] をクリックします。
7. プロンプトにしたがってウィザードを完了します。
8. ウィザードが完了したら、**[Done]** をクリックします。

.encファイルによるローカルホストのアップグレードが完了したときに、空のページが表示される場合があります。このページが表示されても特に問題はありません。

Loggerの設定の実行

Set Configurationウィザードを使用して、1つまたは複数のLoggerで設定を行うことができます。

- リスト設定の場合は、Set Configurationウィザードを使用して、複数のLoggerの既存の設定にプロパティ値を追加します。新規の値のみが追加されます。たとえば、3つのLoggerに共通のユーザーグループが存在する場合、Set Configurationウィザードを使用して、1回のアクションで、3つのLoggerすべてに同じ新規ユーザーを追加することができます(リスト設定の詳細については、「[Configurations] テーブル」(130ページ) を参照してください)。
- リスト設定以外の設定の場合は、Set Configurationウィザードを使用して、複数のLoggerの設定を上書きします。

注意: 1つまたは複数のLoggerで設定を行うと、各Loggerが現在のサブスクリプションに準拠しなくなる場合があります。

1つまたは複数のLoggerで設定を行うには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、**[System]** をクリックします。
3. 管理パネルで **[Loggers]** をクリックします。
4. Loggerのリストで、設定を行うLoggerを1つ以上選択します。
5. **[Set Configuration]** をクリックします。Set Configurationウィザードが起動します。
6. ダイアログボックスを確認し、[**Next**] をクリックします。
7. プロンプトにしたがってウィザードを完了します。
   - 新規のプロパティをリスト設定に追加するには、[**Add Row**] をクリックし、必要な値を入力します。
8. 選択したLoggerで設定が行われます。**[Done]** をクリックします。

コンテナーの管理

コンテナーは、コネクターを4つまで実行できる単一のJVM (Java Virtual Machine) です。コネクターの正確な数は、現在のサービス契約とコネクターのタイプに依存します。

コンテナーは、ArcMC、コネクターアプライアンス、およびL3XXXモデルのLogger上で実行できます。一度に実行可能なコンテナーの数は、製品のライセンスに基づいています。これについては、**[System Admin] > [License & Update]** を確認してください。

管理対象のホストをスキャンすると、ホスト上で現在実行中のすべてのコンテナー (および、それらに関連付けられたコネクター) の正確なインベントリが作成されます。詳細については、「ホストのスキャン」(71ページ) を参照してください。

注: 以下のタイプのコネクターは、それぞれのコンテナー内で実行されるただ1つのコネクターである必要があります。

- Trend Micro Control Manager (TMCM)
- Syslog
- Windows Unified Connector (WUC)

すべてのコンテナーの表示

ArcSight Management Centerで管理されているすべてのコンテナーを表示できます。

すべてのコンテナーを表示するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、**[System]** をクリックします(特定のホスト上のコンテナーを表示する場合は、ナビゲーションツリーでホストを選択します)。
3. **[Containers]** タブをクリックして、コンテナーを表示します。

コンテナー内のコネクターの表示

コンテナー内のすべてのコネクターを表示できます。

コンテナー内のコネクターを表示するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、表示するコネクターがあるコンテナーを選択します。

3. そのコンテナーに対応するツリーのブランチをクリックします。
4. [**Connectors**] タブをクリックします。コンテナー内のコネクターが表示されます。

コンテナーの編集

コンテナーのデフォルトの名前は、Container Nです。ここで、Nはコンテナーが追加された順序を示す続き番号です。ただし、コンテナーのデフォルトの名前は編集できます。

コンテナーを編集するには

1. [**Node Management**] をクリックします。
2. ナビゲーションツリーで、名前を変更するコンテナーがあるホストを選択します。
3. コンテナーのリストで、編集するコンテナーを選択します。
4. そのコンテナーの [**Action**] ドロップダウンで [**Edit Container**] をクリックします。
5. [**Name**] に新しいコンテナー名を入力し、[**Next**] をクリックします。
6. [**Done**] をクリックします。コンテナーの名前が変更されます。

コンテナーの削除

コンテナーを削除すると、それに含まれているコネクターも削除されます。

コンテナーを削除するには

1. [**Node Management**] をクリックします。
2. ナビゲーションツリーで、コンテナーがあるホストを選択します。
3. [**Containers**] タブをクリックします。
4. [**Containers**] タブで、削除するコンテナーを1つ以上選択します。
5. [**Delete**] をクリックします。
6. [**OK**] をクリックして削除を確定します。選択したコンテナーが削除されます。

コンテナープロパティの更新

既存のコンテナープロパティの更新、削除、新しいプロパティの追加を行うことができます。

コンテナープロパティを更新するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、コンテナーがあるホストを選択します。
3. **[Containers]** タブをクリックします。

4. **[Containers]** タブで、更新するコンテナーを1つ以上選択します。
5. **[Properties]**をクリックします。
6. ウィザードの指示に従ってコンテナープロパティを更新します。

> **注:** プロパティを削除しても、コンテナーを再起動するまでは表示されたままになります。

コンテナー資格情報の変更

各コンテナーに関連付けられたユーザー名とパスワードを変更できます。

> **注意:** コンテナーのデフォルトのユーザー名はconnector_userであり、デフォルトのパスワードはchange_meです。HPE ArcSightでは、セキュリティ上の理由から、本番環境に展開する前に、各コンテナーの資格情報をデフォルト以外の値に変更することを強く推奨します。

コンテナー資格情報を変更するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、コンテナーがあるホストを選択します。
3. **[Containers]** タブをクリックします。
4. **[Containers]** タブで、資格情報を変更するコンテナーを1つ以上選択します。
5. **[Credentials]** をクリックします。
6. ウィザードの指示に従って、選択したコンテナーの資格情報を更新します。

コンテナーへのコマンドの送信

コンテナーに対してコマンドを実行し、メモリ設定、OPSEC証明書の取得、キーの生成、コンテナーの再起動を行うことができます。

コンテナーに対してコマンドを実行するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、コンテナーがあるホストを選択します。
3. **[Containers]** タブをクリックします。
4. そのコンテナーの **[Action]** ドロップダウンで **[Send Container Command]** をクリックします。Send Commandウィザードが起動します。
5. ドロップダウンリストから、送信するコマンドを選択し、**[Next]** をクリックします。
6. パラメーターの適切な値を入力し、[**Done**] をクリックします。

コンテナー内のすべてのコネクターのアップグレード

コンテナー内のすべてのコネクターを、特定のパーサーまたはフレームワークのバージョン番号にアップグレードできます。

アップグレードを行う前に

コンテナーのアップグレードを行う前に、次のいずれかが必要になります。

- ArcMCのリポジトリ内のパーサーまたはフレームワークの新しいバージョンのコネクターAUPファイルを使用できます。この方法を使用する場合は、次のように、バージョンファイルをリポジトリにアップロードする必要があります。

バージョンファイルをリポジトリにアップロードするには

1. **[Administration] > [Repositories]** をクリックします。
2. ナビゲーションツリーで、[**Upgrade Files**] を選択します。
3. 管理パネルで **[Upload]** をクリックします。
4. **[Choose File]** をクリックしてコネクターAUPファイルを選択し、**[Submit]** をクリックします。ファイルがアップロードされます。

- あるいは、リポジトリのパーサーAUPファイルを使用する代わりに、ArcSight Marketplaceからパーサーファイルをダウンロードして使用することもできます (フレームワークファイルはMarketplaceでは入手できません)。ArcSight Marketplaceで管理アカウントを作成します。Marketplaceのアカウントをまだ作成していない場合は、パーサーのアップグレード中にアカウントを登録できます。

コンテナー内のすべてのコネクターでパーサーまたはフレームワークのアップグレードを行うには

1. [**Node Management**] をクリックします。
2. ナビゲーションツリーで、コンテナーがあるホストを選択します。
3. [**Containers**] タブをクリックします。
4. **[Containers]** タブで、アップグレードするコンテナーを1つ以上選択します。
5. **[Upgrade]** をクリックします。
6. アップグレードページの [**Select Upgrade Type**] で、[**Parser upgrade**] または [**Framework upgrade**] を選択します。
7. [**Select Upgrade Version**] で、ドロップダウンリストから、選択したコンテナーのアップグレード後のバージョンを選択します(「logger.propertiesの変更」の説明に従って、ドロップダウンに表示されるパーサーアップグレードバージョンの数を制御できます)。

a. パーサーのアップグレードで、選択したパーサーバージョンがMarketplaceのもので、ローカルリポジトリのものでない場合は、お使いのMarketplaceの資格情報をArcMCに保存します。これらの資格情報を更新しない限り、これは1回限りの作業になります。

8. **[Upgrade]** をクリックします。すべてのコンテナーでアップグレードが行われます。

プロキシサーバー経由でパーサーのアップグレードを行う場合は、追加の設定が必要です。詳細については、「logger.propertiesの変更」を参照してください。

logger.propertiesの変更

実行などの一部の機能を有効化または変更する場合は、任意のテキストエディターで、<install_dir>/userdata/arcmc/logger.propertiesファイルを編集して、パラメーターを追加する必要があります。

一般的な編集の手順

<install_dir>/userdata/arcmc/logger.propertiesが存在しない場合は、テキストエディターでファイルを作成します。このファイルは、root以外のユーザーが所有者である必要があります。ArcMCアプライアンスの場合は、'arcsight' ユーザーを使用し、ソフトウェアArcMCの場合は、ArcMCをインストールするのに使用したroot以外のアカウントを使用します。

logger.propertiesファイルは、すべてのユーザーが読み取りおよび書き込み可能であるとは限りません。以下のコマンドをこのファイルに適用します。

```
chown <非rootユーザー>:<非rootユーザー> logger.properties

chmod 660 logger.properties
```

最後に、logger.propertiesを編集して、Webプロセスを再起動します。

プロキシサーバー経由でのパーサーアップグレード

パーサーのアップグレードを行う場合に、プロキシサーバー経由でMarketplaceに接続する必要がある場合は、プロキシの詳細情報を使用して、<install_dir>/userdata/arcmc/logger.propertiesファイルを変更する必要があります。

```
proxy.server=<サーバーアドレス>

proxy.port=<サーバーポート>

#プロキシサーバーで認証が必要な場合は、プロキシサーバーの資格情報を指定

proxy.username=<ユーザー名>

proxy.password=<パスワード>
```

表示されるパーサーアップグレードバージョンの数

パーサーアップグレードのドロップダウンリストに表示されるパーサーアップグレードバージョンの数を制御できます。logger.propertiesで、次のパラメーターを設定します。

marketplace.parser.update.latest.versions.count = <Marketplaceから取得するパーサーアップグレードバージョンの数>

Marketplace接続の無効化

ArcMCのMarketplace接続を無効にするには、logger.propertiesで、次のパラメーターを設定します。

marketplace.enable=false

falseに設定した場合、Marketplaceからのパーサーアップグレードバージョンはドロップダウンリストに表示されません。また、Parser Out of Dateステータス (**[Node Management] > [Containers]** タブの [**Parser Version**] カラム) も利用できなくなります。

コンテナーの再起動

コンテナーを再起動すると、コンテナー内のすべてのコネクターが再起動します。複数のコンテナーを一括して再起動できます。

1つ以上のコンテナーを再起動するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、コンテナーがあるホストを選択します。
3. **[Containers]** タブをクリックします。
4. **[Containers]** タブで、再起動するコンテナーを1つ以上選択します。
5. **[Restart]** をクリックします。
6. **[Yes]** をクリックして再起動を確定します。選択したコンテナーが再起動します。

コンテナーログの表示

1つ以上のコンテナーのログファイルを取得して表示できます。ログファイルは.zip形式になっています。

コンテナーログを表示するには、その前にコンテナーログをLogsリポジトリにアップロードする必要があります。ログをアップロードする手順については、「Logsリポジトリへのファイルのロード」(212ページ) を参照してください。

コンテナーログを取得して表示するには

1. [**Node Management**] をクリックします。
2. ナビゲーションツリーで、コンテナーがあるホストを選択します。
3. [**Containers**] タブをクリックします。
4. [**Containers**] タブで、ログを表示するコンテナーを1つ以上選択します。
5. [**Logs**] をクリックします。
6. [**Next**] をクリックして、[**Retrieve Container Logs**] プロセスを開始します。完了したら [**Done**] をクリックします。
7. [**Administration**] > [**Repositories**] をクリックします。
8. 左パネルで [**Logs**] をクリックします。
9. 管理パネルで をクリックして、表示するログファイルを (`.zip`形式で) 取得します。

コンテナーログの削除

不要なコンテナーログを必要に応じて削除できます。

コンテナーログファイルを削除するには

1. **[Administration] > [Repositories]** をクリックします。
2. 左パネルで **[Logs]** をクリックします。
3. 管理パネルのログのリストで、削除するログファイルの横の をクリックします。
4. **[OK]** をクリックして削除を確定します。

コンテナーでのFIPSの有効化

FIPSモードは、バージョン4.7.5以降が動作するローカル、リモート、およびソフトウェアコネクターでサポートされています。ただし、一部のコネクターではFIPSモードはサポートされていません。FIPSモードがサポートされていないコネクターについては、Protect 724で提供されている『Installing FIPS-Compliant SmartConnectors』ドキュメントを参照してください。サービスとして動作しているソフトウェアコネクターを含むコンテナーでFIPSを有効にする前に、そのドキュメントに記載されている注意事項を確認してください。

ArcSight Management Centerでは、FIPSはデフォルトで無効になっていますが、「FIPS 140-2」(262ページ) の説明に従って有効にすることができます。アプライアンスでFIPSを有効にすると、コンテナーでFIPSを有効にできます。FIPSを有効にしたコンテナー内のFIPS準拠のコネクター (または、FIPSを有効にした後に追加されるコネクター) は、自動的にFIPSモードで通信します。

- コネクター通知先がArcSight Managerである場合は、コネクター管理によってArcSight Managerの証明書がトラストストアに自動的にインポートされ、コンテナーに適用されます。
- ただし、コネクター通知先がLoggerである場合は、Loggerの証明書を手動でアップロードして、コンテナーに適用する必要があります。

FIPS Suite Bの証明書は、以下の「コンテナーでのFIPS Suite Bの有効化」の説明に従って、コネクター通知先に関係なく、手動でアップロードする必要があります。

FIPSを有効または無効にする手順は同じです。

コンテナーでFIPSモードを有効または無効にするには

1. [**Node Management**] をクリックします。
2. ナビゲーションツリーで、コンテナーがあるホストを選択します。
3. [**Containers**] タブをクリックします。
4. [**Containers**] タブで、FIPSを有効にするコンテナーを1つ以上選択します。
5. [**FIPS**] をクリックします。
6. ウィザードの指示に従ってFIPSステータスを更新します。

適切なCA証明書がトラストストアに格納されており、コンテナー内のコネクターが設定されている通知先を正常に検証できるようになっていることを確認します。必要に応じて、適切な証明書をコンテナーに追加します。

> 有効な32ビットのFIPSコネクターが64ビットLinuxシステムにインストールされている場合、リモートから管理することはできません。

コンテナーでのFIPS Suite Bの有効化

管理対象のコネクターは、FIPS Suite Bモードで通知先と通信できます。FIPS Suite Bの証明書は、コネクター通知先に関係なく、手動でインポートしてコンテナーに適用する必要があります。

以下の手順を実行する前に、「FIPS 140-2」(262ページ) の説明に従って、ArcSight Management CenterでFIPSモードが有効になっていることを確認します。

コンテナーでFIPS Suite Bを有効化するには

1. コネクター通知先 (ArcSight ManagerまたはLogger) の証明書を、一時ディレクトリにエクスポートします。たとえば、ArcSight Managerで、$ARCSIGHT_HOME/current/binから、次のコマンドを入力します。`./arcsight runcertutil -L -n mykey -r -d /opt/arcsight/manager/config/jetty/nssdb -o /tmp/managercert.cer`
2. 「CA Certsリポジトリ」(212ページ) の説明に従って、証明書を一時ディレクトリからCA Certsリポジトリにアップロードします。

3. 上記の手順に従って、コンテナーでFIPSを有効にします。
4. 「コンテナー上の証明書の管理」(94ページ) の説明に従って、コンテナー上の証明書を追加します。
5. [**Node Management**] をクリックします。
6. ナビゲーションツリーで、コンテナーがあるホストを選択します。
7. [**Containers**] タブをクリックします。
8. [**Containers**] タブで、FIPS Suite Bを有効にするコンテナーを1つ以上選択します。
9. [**FIPS**] をクリックします。
10. ウィザードの指示に従ってFIPS Suite Bステータスを更新します。

コンテナーへのコネクターの追加

各コンテナーでは、最大4つのコネクターを保持できます。

コネクターをコンテナーに追加するには

1. [**Node Management**] をクリックします。
2. ナビゲーションツリーで、コネクターを追加するコンテナーを選択します。
3. [**Connectors**] タブで、[**Add Connector**] をクリックします。**Connector Setup**ウィザードが起動します。
4. [**Next**] をクリックし、プロンプトに従って新しいコネクターをセットアップします。

注: 新しいコネクターのデフォルトの資格情報は、必ずデフォルト以外の値に変更します。詳細については、「コンテナー資格情報の変更」(87ページ) を参照してください。

コンテナーに対するLogfuの実行

Logfuユーティリティは、ArcSightログを分析して、ログに格納されている情報の対話型のビジュアルな表現を生成する診断ツールです。イベントフローの問題が発生した場合、時間とともに発生した事象を視覚的に表現できると便利です。

コンテナーに対してLogfuを実行するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、コンテナーがあるホストを選択します。
3. **[Containers]** タブをクリックします。
4. **[Containers]** タブで、Logfuを実行するコンテナーを1つ選択します。
5. そのコンテナーの **[Action]** ドロップダウンで **[Run Logfu]** をクリックします。

6. Logfuの進行状況ウィンドウが表示され、システムデータログの取得と分析が行われます。その後データは、**Group**、**Field**、および**Chart**別に表示されます。
   - **[Group]** ボックスで、表示するデータの種類を選択します。**[Group]** ボックスには、選択したコンテナー内のすべてのコネクターに加えて、メモリ使用量、伝送速度などの他の多くのデータタイプがリストされます。
   - 次に、いずれかの [Group] ボックスの**データポイント**を選択します。選択したデータポイントに応じて、フィールドのリストが下の [Field] ボックスに表示されます。
   - 表示する**フィールド**を選択します。[Chart] ボックスにグラフが表示され、速度と時間の情報が表示されます。[Chart] ボックスの下部にあるキーは、グラフ内でマップされたデータポイントを定義します。
   - 分析用に別のデータポイントを選択するには、**[Reset Data]** をクリックします。
7. 完了したら表示ウィンドウを閉じます。

コンテナー上の証明書の管理

コネクターには、通知先と安全に通信するために、CA (認証局) から発行されるか自己署名されたSSL証明書が必要です。**[Containers]** タブから使用できるCertificate Managementウィザードを使用すると、コンテナー上の証明書を追加または削除することができます。ウィザードを使用して以下のことが可能です。

- 証明書をコンテナーに追加する。
- 複数の証明書を一括して追加し、複数のコンテナーをまとめて有効化する。
- 非FIPSモードのコンテナーでのみ、デモ証明書を有効化または無効化する。
- 非FIPSモードのコンテナーにのみ、CA証明書ファイルを追加する。
- 証明書をコンテナーから削除する。

[Containers] タブおよび **[Connectors]** タブから、コンテナーに適用されている証明書の詳細を表示できます。「コンテナー上の証明書の表示」(97ページ) を参照してください。

無効な証明書の解決については、「無効な証明書に関するエラーの解決」(98ページ) を参照してください。

CA証明書のコンテナーへの追加

単一のCA証明書は、FIPSモードまたは非FIPSモードのコンテナーに追加できます。

注: コンテナーでFIPSモードを有効または無効にするときには、必ず必要な証明書がトラストストアに格納されていることを確認し、必要に応じて追加してください。

マウスカーソルをコンテナー名に合わせると、適用されている証明書の種類が表示されます。アイコンをクリックすると、コンテナー上で使用できる証明書の一覧が表示されます。

以下の手順を実行する前に、追加する証明書がCA Certsリポジトリにロードされていることを確認してください。

単一のCA証明書をコンテナーに追加するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、**[System]** をクリックします。
3. **[Containers]** タブをクリックします。
4. **[Containers]** タブで、証明書を追加するコンテナーを1つ以上選択します。
5. **[Certificates]** をクリックします。Certificate Managementウィザードが起動します。
6. ダイアログボックスを確認し、[**Next**] をクリックします。
7. [**Choose an Action**] で、[**Add Certificate**] を選択し、[**Next**] をクリックします。
8. ウィザードの指示に従って証明書を追加します。
   コンテナーが停止しているか、コネクターで古いビルドが動作している場合、ウィザードの進行状況バーと [Summary] ページにエラーが表示されます。

CA証明書のコンテナーからの削除

不要になったCA証明書はコンテナーから削除できます。CA証明書を削除すると、証明書がコンテナーのトラストストアから削除されますが、リポジトリからは削除され**ません**。

注意: 証明書を削除する際には注意してください。コンテナーから証明書を削除し、コネクターの通知先がまだその証明書を使用している場合、コネクターはその通知先と通信できなくなります。

CA証明書をコンテナーから削除するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、**[System]** をクリックします。
3. **[Containers]** タブをクリックします。
4. **[Containers]** タブで、証明書を削除するコンテナーを1つ以上選択します。
5. **[Certificates]** をクリックします。**Certificate Management**ウィザードが起動します。
6. ダイアログボックスを確認し、[**Next**] をクリックします。
7. [**Choose an Action**] で、[**Remove certificate**] を選択し、[**Next**] をクリックします。
8. 1つ以上の証明書を証明書リストから選択し、**[Next]** をクリックします。証明書が証明書リストから削除され、使用できなくなります。FIPSモードのコンテナーから証明書を削除すると、コンテナーが自動的に再起動します。
9. Certificate Managementウィザードには、正常に削除された証明書の一覧が、カンマ区切りリストで表示されます。削除できない証明書は、カンマ区切りのリストに、証明書の削除に失敗した理由とともに表示されます。

CA証明書ファイルのコンテナーへの追加

CA証明書ファイルは、非FIPSモードの任意のコンテナーに追加できます。

注意: CA証明書ファイルを適用すると、コンテナー上のトラストストア全体が上書きされます。以前追加したすべての証明書が上書きされます。

以下の手順に従う前に、追加するCA証明書ファイルがCA Certsリポジトリにロードされていることを確認してください。

CA証明書ファイルを非FIPSモードのコンテナーに追加するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、**[System]** をクリックします。
3. **[Containers]** タブをクリックします。
4. **[Containers]** タブで、CA証明書を追加する非FIPSモードのコンテナーを1つ以上選択します。
5. **[Certificates]** をクリックします。**Certificate Management** ウィザードが起動します。
6. ダイアログボックスを確認し、[**Next**] をクリックします。
7. [**Choose an Action**] で、[**CA Cert (Legacy)**] を選択します。
8. ウィザードの指示に従います。
   CA証明書ファイルがコンテナーに追加された後、コンテナーが自動的に再起動します。

コンテナー上でデモ証明書を有効または無効にする

デモ証明書は、コンテナー上でテスト目的で使用できます。デフォルトでは、コンテナー上のデモ証明書は無効になっています。デモ証明書のテスト目的での一時的な有効化は、非FIPSモードのコンテナーで実行できます。

注: デモ証明書は、非FIPSモードのコンテナーでデモ目的でのみ有効にしてください。デモ証明書は固有のものでないため、実稼働環境でデモ証明書を使用すると、セキュリティ上の重大な問題が発生します。

コンテナー上でデモ証明書を有効または無効にするには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、**[System]** をクリックします。
3. **[Containers]** タブをクリックします。
4. **[Containers]** タブで、CA証明書を有効または無効にする非FIPSモードのコンテナーを1つ以上選択します。

5. **[Certificates]** をクリックします。**Certificate Management** ウィザードが起動します。
6. ダイアログボックスを確認し、[**Next**] をクリックします。
7. [**Choose an Action**] で、[**Demo CA (Legacy)**] を選択し、[**Next**] をクリックします。
8. Certificate Managementウィザードの指示に従います。
   デモ証明書をコンテナーに追加した後、コンテナーは自動的に再起動します。

複数の通知先証明書のコンテナーへの追加

FIPSモードであるかどうかに関係なく、複数の通知先証明書をコンテナーに追加できます。

注: コンテナーでFIPSモードを有効または無効にするときには、必ず必要な証明書がトラストストアに格納されていることを確認し、必要に応じて追加してください。

アイコンをクリックすると、コンテナー上で使用できる証明書の一覧が表示されます。

複数の通知先証明書をコンテナーに適用するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、**[System]** をクリックします。
3. **[Containers]** タブをクリックします。
4. [**Containers**] タブで、複数の通知先証明書を追加するコンテナーを1つ以上選択します。
5. **[Certificates]** をクリックします。**Certificate Management** ウィザードが起動します。
6. ダイアログボックスを確認し、[**Next**] をクリックします。
7. [**Choose an Action**] で、[**Import destination certificates**] を選択して証明書を追加します。
8. ウィザードの指示に従って処理を完了します。

コンテナー上の証明書の表示

コンテナーに適用されているCA証明書の一覧を表示したり、リスト内の特定の証明書の詳細を表示できます。コンテナー上の証明書を表示するには

- [**Containers**] タブで、証明書を表示するコンテナーの [**Action**] ドロップダウンから、[**Display Certificates**] を選択します。
- **[Connectors]**タブで、ページ上部にある **[Certificates]** をクリックします。

Certificate Listウィザードに、コンテナーに適用されている証明書が表示されます。証明書の詳細を表示するには、証明書を選択し、ページ下部の **[Next]** をクリックします。

無効な証明書に関するエラーの解決

コンテナー内のコネクターに対する有効なCA証明書が存在しない場合は、以下の手順で、無効な証明書に関するエラーを解決します。

無効な証明書に関するエラーを解決するには

1. ナビゲーションツリーでコンテナーを選択します。
2. **[Containers]** タブをクリックします。エラーメッセージが表示されます。
3. 問題のあるコンテナーの [**Action**] ドロップダウンで、[**Download Certificates**] を選択します。
4. ウィザードの指示に従って有効な証明書をダウンロードしてインポートします。

コンテナーに対する診断の実行

コンテナーに対して診断を実行できます。

注: 診断ツールは、**[Administration] > [System Admin]** でも利用できます。

コンテナーに対して診断を実行するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、コンテナーがあるホストを選択します。
3. **[Containers]** タブをクリックします。
4. **[Containers]** タブで、診断を実行するコンテナーを1つ以上選択します。
5. **[Action]** ドロップダウンで **[Run Logfu]** をクリックします。Diagnosticsウィザードが起動します。
6. 選択したコンテナーに対して実行するアクションを選択します。
   - コンテナーの`user/agent`フォルダーにある、拡張子が`.properties`、`.csv`、または`.conf`のファイルを編集するには、**[Edit a configuration file]** を選択します。
   - コンテナーの`user/agent`フォルダーにある任意のファイル(`.zip`、`.jar`、`.exe`などのバイナリファイルを除く)を編集するには、**[Edit a user file]**を選択します。
7. 使用可能なファイルの一覧から、編集するファイル選択します。ファイルが [Edit File] パネルに表示されます。編集を行い、**[Next]** をクリックして編集内容を保存し、コンテナーを再起動します。

   注: **[Next]** をクリックしたときに、ArcSight Management Centerによって更新されたファイルがコンテナーの`user/agent`フォルダーに保存されます。元のファイルは上書きさ

れます。

8. **[Done]** をクリックしてDiagnosticsウィザードを閉じます。

コネクターの管理

コネクター (SmartConnectorとも呼びます) は、イベントとログをネットワーク上の各種のソースから収集するHPE ArcSightソフトウェアコンポーネントです。コネクターは、ArcSight Management Centerや、コネクターアプライアンスが組み込まれたLoggerプラットフォーム上で設定できます。また、ネットワーク内のコンピューターにインストールしてリモートから管理することもできます。サポートされているコネクターの一覧については、HPE ArcSightカスタマーサポートサイトを参照してください。

以下では、コネクターを管理する手順について説明します。

すべてのコネクターの表示

現在管理されているすべてのコネクターを表示できます。

すべてのコネクターを表示するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで **[System]** をクリックします。
3. 管理パネルで、**[Connectors]** タブをクリックします。管理パネルの **[Connectors]** タブにすべてのコネクターが表示されます。

コネクターの追加

前提条件

コネクターを追加する前に、以下の重要な情報を確認してください。

- コネクターの追加先のコンテナー、ホスト、ロケーションがArcSight Management Centerに存在することを確認してください。これらの要素の中に存在しないものがある場合は、作成してください。
- 「各コネクタータイプの設定に関する注意事項」(124ページ) に記載されている、設定のベストプラクティスに従います。

  Check Point OPSEC NGコネクターを設定する場合は、「Check Point OPSEC NGコネクターの設定」(125ページ) 、および『SmartConnector Configuration Guide for Check Point OPSEC NG』を参照してください。

JDBC対応のMS SQL Serverドライバーが必要なデータベースコネクターを設定する場合は、「MS SQL Server JDBCドライバーの追加」(127ページ)の手順に従ってください。

注意: このコネクタータイプには、JDBCと認証設定に関する特別な要件があります。コネクターをインストールする前に、『SmartConnector Configuration Guide for Microsoft SQL Server Multiple Instance Audit DB』でこの重要な情報を参照してください。

- ソフトウェアベースのコネクターを追加する場合は、コネクターのユーザー名とパスワードが、コネクターの追加先のコンテナーのユーザー名とパスワードに一致していることを確認してください。必要に応じて、「コンテナー資格情報の変更」(87ページ)を参照してください。

  注意: 各コネクターのデフォルトのユーザー名は`connector_user`であり、デフォルトのパスワードは`change_me`です。これらのデフォルト値を変更せずに使用しているコネクターは、安全でないとみなす必要があります。HPE ArcSightでは、セキュリティ上の理由から、本番環境に展開する前に、各コネクターの資格情報をデフォルト以外の値に変更することを強く推奨します。

- ファイルベースのコネクターは、CIFS (Common Internet File System) またはNFS (Network File System) を使用します。ArcMCの一部として動作するローカルのソフトウェアコネクターを作成する場合は、次の条件が適用されます。
  - Windowsシステムでは、CIFS共有を設定してからファイルベースのコネクターを追加する必要があります。
  - その他のすべてのコネクターでは、NFSマウントを確立してからファイルベースのコネクターを追加する必要があります。また、コネクターのパラメーターを入力する場合は、[**Configuration File**] フィールドに設定ファイル名を拡張子を付けずに入力します。拡張子`.sdkrfilereader.properties`が自動的に追加されます。
- 個々のコネクターパラメーターの詳細については、選択したコネクターのタイプに対応する専用のHPE ArcSight SmartConnector構成ガイドを参照してください。構成ガイドでは、コネクターとともに使用するソースデバイスを設定する方法も説明されています。

コネクターを追加するには

ヒント: Check Point FW-1/VPN-1システム用のコネクターを追加する場合は、「Check Point OPSEC NGコネクターの設定」(125ページ)で詳しい手順を参照してください。

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、コネクターを追加するホストを選択します。
3. 管理パネルで、**[Containers]** タブをクリックします。
4. **[Containers]** タブでコネクターに割り当てるコンテナーを選択します。
5. **[Action]** ドロップダウンで **[Add Connector]** をクリックします。Connector Setupウィザードが起動します。
6. ダイアログボックスを確認し、[**Next**] をクリックします。

7. コネクタータイプを使用可能なタイプのプルダウンリストから選択し、**[Next]** をクリックします。
8. コネクターの基本的なパラメーターを入力します。パラメーターは、コネクターの種類によって変わります (フィールド上にカーソルを置くと、フィールドの詳細情報が表示されます)。すべてのフィールドを入力したら、**[Next]**をクリックします。

   注: ファイルパスを含むパラメーターを入力する場合は、パスをPOSIX形式 (たとえば `/folder/filename`) で入力します。

   Windowsシステム上のファイルベースのコネクターの場合は、コネクター用に作成したCIFSマウントポイントの名前を指定します(`/opt/mnt/<CIFS_share_name>`を指定する必要があります)。

   一部のコネクターにはテーブルパラメーターが含まれています。たとえば、Microsoft Windows Event Logには、ドメイン内の各ホストのパラメーターと、1つ以上のログタイプ (セキュリティ、アプリケーション、システム、ディレクトリサービス、DNS、ファイルレプリケーションなど) が含まれています。テーブルパラメーターはCSVファイルからインポートできます。別のコネクターからエクスポートしたCSVファイルをインポートできますが、同じコンテナーからCSVファイルをエクスポートしてインポートする場合に限られます。CSVファイルが、異なるコンテナーからエクスポートされた場合は、CSVファイル中で難読化されているパスワードなどのシークレットパラメーターをプレーンテキストに変更してからCSVファイルをインポートする必要があります。

   注: Microsoft Active Directoryにクエリを実行してデバイスを検出するコネクターでは (たとえば、Microsoft Windows Event Log - Unified)、「Network Security: LDAP Server Signing Requirements」ポリシーがドメインコントローラー上で「Signing Required」に設定されている場合、ArcSight Management Centerは、Active Directoryに接続したりデバイスをブラウズしたりすることができなくなります。コネクターデバイスのブラウザータイプとして**[Windows Host Browser]**を選択すると、エラーが表示されます。

9. コネクターの一次通知先を選択し、通知先固有のパラメーターを以降のページで入力した後、**[Next]** をクリックします。通知先としては以下のものがあります。
   - ArcSight Logger SmartMessage (暗号化)
   - ArcSightマネージャー (暗号化)
   - CEF syslog (平文、つまり暗号化なし)

   注: FIPS Suite Bの証明書は自動的に取得されないため、手動でアップロードする必要があります。

   証明書の詳細を表示するには、証明書にマウスカーソルを合わせます。
   - 証明書をインポートして続行するには、**[Import the certificate to the connector from the destination]** を選択して**[Next]** をクリックします。

- 証明書をインポートしない場合は、**[Do not import the certificate to the connector from the destination]** を選択して **[Next]** をクリックします。通知先は追加されません。

10. コネクターの詳細を入力します。

パラメーター	説明
Name	このコネクターのわかりやすい名前。
Location	コネクターロケーション (ホスト名など)。
Device Location	コネクターにイベントを送信するデバイスのロケーション。
Comment	追加のコメント。

11. 完了したら **[Done]** をクリックします。

コネクターパラメーターの編集

HPE ArcSightは、各種のソースからセキュリティイベントを収集するための多数の種類のコネクターをサポートしています。これには、syslog、ログファイル、リレーショナルデータベース、専用のデバイスが含まれます。そのため、設定のパラメーターは、設定するコネクターのタイプによってさまざまです。

特定のコネクターまたは同じタイプの複数のコネクターのパラメーター (単純なパラメーターとテーブルパラメーター) を一度に編集できます。

1つのコネクターの単純なパラメーターの更新

以下の手順では、特定のコネクターの単純なパラメーターの更新方法について説明します。

特定のコネクターのパラメーターを更新するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、更新するコネクターを選択します。
3. 管理パネルに、**[Connector]** サマリータブが表示されます。
4. [**Connector**] タブで、[**Connector Parameters**] の横の をクリックします。
5. 必要に応じてパラメーターを変更し、**[Next]** をクリックします。

注: ファイルパスを含むパラメーターを編集する場合は、パスをPOSIX形式 (たとえば `/folder/filename`) で入力します。

6. 完了したら **[Done]** をクリックします。更新後のパラメーターが [Connector] サマリータブの **[Connector Parameters]** テーブルに表示されます。

1つのコネクターのテーブルパラメーターの更新

Microsoft Windows Eventコネクターなどの特定のコネクターのパラメーターはテーブルになっています。特定のコネクターのテーブルパラメーターを必要に応じて更新できます。

特定のコネクターのテーブルパラメーターを更新するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、更新するコネクターを選択します。管理パネルに、**[Connector]** サマリータブが表示されます。
3. [**Connector**] サマリータブで、[**Table Parameters**] の横の  をクリックします。
4. 必要に応じてパラメーターを変更し、**[Next]**をクリックします。
   - パラメーター行を追加するには、**[Add Row]**リンクをクリックします。
   - Excelと互換性のあるプログラムを使用して、情報が格納されたCSVテキストファイルを作成し、**[Import File]**ボタンをクリックしてテーブル全体を一度にロードできます。ファイルは、[Update Table Parameters] ページに示される行と同じ形式になっており、そのページに示す順序でパラメーターラベルを含むヘッダー行が含まれている必要があります。チェックボックス値が必要なフィールドについては、値としてTrueまたはFalseを入力します。以下に例を示します。

	A	B	C	D	E	F
1	Domain Name	Host Name	User Name	Password	Security Logs	System Logs
2	test	1.1.1.1	admin	password	TRUE	FALSE
3	test2	1.1.1.1.1	admin	password	TRUE	FALSE

5. 完了したら **[Done]** をクリックします。更新後のテーブルパラメーターが [Connector] ページの [Table Parameters] セクションに表示されます。

注: 別のコネクターからエクスポートしたCSVファイルをインポートできますが、同じコンテナーからCSVファイルをエクスポートしてインポートする場合に限られます。CSVファイルが、異なるコンテナーからエクスポートされた場合は、CSVファイル中で難読化されているパスワードなどのシークレットパラメーターをプレーンテキストに変更してからCSVファイルをインポートする必要があります。

複数のコネクターに対する単純なパラメーターとテーブルパラメーターの更新

同じ種類のコネクターが複数ある場合は、すべてのコネクターの単純なパラメーターとテーブルパラメーターを同時に変更できます。

同じタイプの複数のコネクターのパラメーターを編集するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、コネクターがあるホストを選択します。
3. 管理パネルで、パラメーターを更新するコネクターを選択します。
4. **[Parameters]** をクリックします。Update Connect Parametersウィザードが起動します。
5. ダイアログボックスを確認し、[**Next**] をクリックします。
6. ウィザードの指示に従います。
   - 選択したすべてのコネクターの単純なパラメーターを一度に変更するか、コネクターごとに単純なパラメーターを変更するかを選択できます。
   - コネクターにテーブルパラメーターがある場合、変更できるようにテーブルパラメーターが表示されます。複数のコネクターの多数のテーブルパラメーターを変更する必要がある場合は、CSVファイルからパラメーターをインポートできます。また、テーブルパラメーターをCSVファイルにエクスポートして、バックアップとして使用したり、別のコネクターアプライアンスでインポートすることもできます。

     注: 異なるバージョンの複数のコネクターのパラメーターを更新する場合は、新しいコネクターにパラメーターが追加されている可能性があります。その場合は、すべてのコネクターで共有されるパラメーターのみが、更新用に表示されます。
7. 完了したら **[Done]** をクリックします。

通知先の管理

コネクターは、ArcSightマネージャーやArcSight Loggerなどの複数の通知先にイベントを転送できます。1つのコネクターに1つ以上の通知先を割り当てることができます。複数の通知先を1つのコネクターに割り当て、プライマリ通知先が障害になった場合のフェイルオーバー(代替)通知先を指定できます。

次の手順では、以下のアクションを特定のコネクターまたは複数のコネクターで同時に実行する方法について説明します。

- プライマリ通知先またはフェイルオーバー通知先の追加
- 通知先パラメーターと通知先実行時パラメーターの編集
- 通知先の削除
- 通知先の再登録
- 通知先の代替設定の管理
- 通知先へのコマンド送信

プライマリ通知先のコネクターへの追加

プライマリ通知先をコネクターに追加する場合は、通知先のホスト名や使用するポートなど、通知先の詳細を入力する必要があります。

プライマリ通知先をコネクターに追加するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、通知先を追加するコネクターを選択します。管理パネルに、**[Connector]** サマリータブが表示されます。
3. [**Connector**] サマリータブで、[**Destinations**] の横の ＋ をクリックします。Add Destination ウィザードが起動します。
4. ウィザードの手順に従います。既存の通知先を選択するか、新しい通知先を追加することができます。新しい通知先を追加する場合は、通知先の種類を選択し、通知先のパラメーターを入力します。通知先タイプの説明は、『SmartConnectorユーザーガイド』に記載されています。

   注: 5.1.2.5823以降が動作するコンテナーでは、ArcSight Management CenterはArcSightマネージャー通知先の証明書を自動的に取得し、証明書のサマリーを表示します。

   5.1.2以前が動作するコンテナーの場合は、証明書をコンテナーにアップロードしてから通知先を追加します。

   FIPS Suite Bの証明書は自動的に取得されないため、手動でアップロードする必要があります。

   証明書の詳細を表示するには、証明書にマウスカーソルを合わせます。

   - 証明書をインポートして続行するには、**[Import the certificate to the connector from the destination]** を選択して**[Next]** をクリックします。
   - 証明書をインポートしない場合は、**[Do not import the certificate to the connector from the destination]** を選択して **[Next]** をクリックします。通知先は追加されません。
5. 完了したら **[Done]** をクリックします。

フェイルオーバー通知先のコネクターへの追加

各通知先には、プライマリ通知先との接続が障害になった場合に使用されるフェイルオーバー通知先を設定できます。

ヒント: UDP接続は転送エラーを検出できません。CEF Syslog通知先にはRaw TCPを使用してください。

フェイルオーバー通知先をコネクターに追加するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、通知先を追加するコネクターを選択します。管理パネルに、**[Connector]** サマリータブが表示されます。
3. [**Connector**] サマリータブの [**Destinations**] テーブルで、  をクリックします。Add Destinationウィザードが起動します。
4. ウィザードの手順に従って、使用可能な通知先から選択し、通知先の詳細を入力します。

   注: FIPS Suite Bの証明書は自動的に取得されないため、手動でアップロードする必要があります。

   証明書の詳細を表示するには、証明書にマウスカーソルを合わせます。
   - 証明書をインポートして続行するには、**[Import the certificate to the connector from the destination]** を選択して**[Next]** をクリックします。
   - 証明書をインポートしない場合は、**[Do not import the certificate to the connector from the destination]** を選択して**[Next]**をクリックします。通知先は追加されません。
5. 完了したら **[Done]** をクリックします。

プライマリ通知先またはフェイルオーバー通知先の複数のコネクターへの追加

プライマリ通知先またはフェイルオーバー通知先を複数のコネクターに同時に追加できます。

プライマリ通知先またはフェイルオーバー通知先を複数のコネクターに追加するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、コネクターがあるコンテナーを選択します。
3. 管理パネルで、**[Connectors]** タブをクリックします。
4. コネクターのリストから、通知先を割り当てるコネクターをすべて選択します。
5. ＋ [**Destinations**] をクリックします。**Manage Destinationsウィザードが起動します。**
6. ダイアログを確認し、[**Next**] をクリックします。
7. [**Choose an Option**] で、[**Add a destination] を選択し、**[**Next**] をクリックします。
8. 新しい通知先の作成か、既存の通知先の選択を選択し、**[Next]** をクリックします。
   - **新しい通知先の作成**を選択した場合は、通知先の種類を選択し、通知先のパラメーターを入力します。通知先タイプの説明は、『SmartConnectorユーザーガイド』に

記載されています。

- **既存の通知先の選択**を選択した場合は、リストから通知先を選択します。

  注: ArcSight Management Centerは通知先のArcSightマネージャー証明書を自動的に取得し、証明書のサマリーを表示します。

  FIPS Suite Bの証明書は自動的に取得されないため、手動でアップロードする必要があります。

  証明書の詳細を表示するには、証明書にマウスカーソルを合わせます。

  - 証明書をインポートして続行するには、**[Import the certificate to the connector from the destination]** を選択して**[Next]** をクリックします。
  - 証明書をインポートしない場合は、**[Do not import the certificate to the connector from the destination]** を選択して **[Next]** をクリックします。通知先は追加されません。

9. プライマリ通知先またはフェイルオーバー通知先を選択し、通知先の機能を定義します。
   - **[Primary destination]** を選択する場合は、**[Next]** をクリックして、設定を更新します。
   - **[Failover destination]** を選択する場合は、以下の手順を実行します。
     a. フェイルオーバーに適用されるプライマリ通知先を選択します。
     b. 表示されているすべてのコネクターを変更するには、表見出しのボックスをチェックします。
     c. **[Next]** をクリックして、設定を更新します。
10. 完了したら **[Done]** をクリックします。

通知先の削除

通知先はいつでもコネクターから削除できます。各コネクターには、少なくとも1つの通知先が必要です。そのため、コネクターからすべての通知先を削除することはできません。

コネクターから単一の通知先を削除するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、通知先を削除するコネクターを選択します。管理パネルに、**[Connector]** サマリータブが表示されます。
3. [**Connector**] サマリータブの [**Destinations**] テーブルで、削除する通知先の✕をクリックします。
4. **[OK]** をクリックして削除を確定します。

複数の 通知先を1つ以上のコネクターから削除するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、コネクターがあるコンテナーを選択します。
3. 管理パネルで、**[Connectors]** タブをクリックします。
4. コネクターのリストから、通知先を削除するコネクターをすべて選択します。
5. [**Destinations**] をクリックします。**Manage Destinationsウィザードが起動します。**
6. ダイアログを確認し、[**Next**] をクリックします。
7. [**Choose an Option**] で、[**Remove a destination] を選択し、**[**Next**] をクリックします。
8. ウィザードの指示に従い、完了したら **[Done]** をクリックします。

通知先の再登録

場合によっては、1つ以上のコネクターに対して通知先の再登録が必要になることがあります。たとえば、ESMをアップグレードした後や、LoggerアプライアンスまたはESMアプライアンスが応答不能になった場合などです。

1つ以上のコネクターについて通知先を再登録するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、コネクターがあるコンテナーを選択します。
3. 管理パネルで、**[Connectors]** タブをクリックします。
4. コネクターのリストから、通知先を割り当てるコネクターをすべて選択します。
5. **[Destinations]** をクリックします。**Manage Destinationsウィザードが起動します。**
6. ダイアログを確認し、[**Next**] をクリックします。
7. [**Choose an Option**] で、[**Re-register destinations**] を選択し、[**Next**] をクリックします。
8. ウィザードの指示に従い、完了したら **[Done]** をクリックします。

通知先パラメーターの編集

次の手順では、特定のコネクターの通知先パラメーターを編集する方法と、複数のコネクターの通知先パラメーターを編集する方法について説明します。

コネクターの通知先パラメーターを編集するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、通知先パラメーターを編集するコネクターを選択します。管理パネルに、**[Connector]** サマリータブが表示されます。

3. [**Destinations**] テーブルで、編集する通知先の横の  をクリックし、**[Edit Destination Parameters]** ページを表示します。
4. 変更を行い **[Next]** をクリックします。
5. 完了したら **[Done]** をクリックします。

複数のコネクターの通知先パラメーターを編集するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、コネクターがあるコンテナーを選択します。
3. 管理パネルで、**[Connectors]** タブをクリックします。
4. コネクターのリストから、通知先パラメーターを編集するコネクターをすべて選択します。
5. **[Destinations]** をクリックします。**Manage Destinationsウィザードが開きます。**
6. ダイアログを確認し、[**Next**] をクリックします。
7. [**Choose an Option**] で、[**Edit a destination**] を選択し、[**Next**] をクリックします。
8. ウィザードの指示に従い、完了したら **[Done]** をクリックします。

通知先実行時パラメーターの編集

通知先実行時パラメーターを使用すると、バッチ化、時間補正、帯域幅制御など、詳細な処理オプションを指定できます。設定可能なパラメーターは、「通知先実行時パラメーター」(299ページ)に記載されています。ユーザーインターフェイスには、通知先で有効なパラメーターが自動的に表示されます。

次の手順では、特定のコネクターの実行時パラメーターを編集する方法と、複数のコネクターの実行時パラメーターを同時に編集する方法について説明します。

1つのコネクターの通知先実行時パラメーターを編集するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、通知先実行時パラメーターを編集するコネクターを選択します。管理パネルに、**[Connector]** サマリータブが表示されます。
3. [**Connector**] サマリータブの [**Destinations**] テーブルで、実行時パラメーターを編集する通知先の横の  をクリックします。
4. [**Add Alternate Configurations**] で、編集する代替設定の横の  をクリックします。

   代替設定を行っていない場合は、**[Default]**の横の  をクリックします。代替設定の詳細については、「代替設定の管理」(110ページ)を参照してください。
5. 表示されるパラメーターの値を指定または更新し、**[Save]** をクリックします。

複数のコネクターの通知先実行時パラメーターを同時に編集するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、コネクターがあるコンテナーを選択します。
3. 管理パネルで、**[Connectors]** タブをクリックします。
4. コネクターのリストから、通知先実行時パラメーターを編集するコネクターをすべて選択します。
5. **[Runtime Parameters]**をクリックしてウィザードを開きます。
6. ウィザードの以下の手順に従って、実行時パラメーターを編集します。
   a. 実行時パラメーターを変更する通知先を選択します。
   b. 影響を受ける設定を選択します (デフォルト設定または代替設定)。
   c. 変更するパラメーターグループ (たとえば、バッチ化、キャッシュ、ネットワーク、処理) を選択します。
   d. パラメーターを変更します。

代替設定の管理

代替設定は、毎日指定された時間にデフォルト設定の代わりに使用されるランタイムパラメーターのセットです。たとえば、異なるバッチ化方式 (緊急度またはサイズによる) を、異なる時間帯に対して指定することができます。1つの送信先に対して複数の代替設定を定義して、1日の異なる時間範囲でそれらを送信先に適用できます。たとえば、午前8時から午後5時までの時間範囲に対してある設定を定義し、午後5時から午前8時までの時間範囲には別の設定を定義できます。

デフォルトでは、**Default**というラベルの設定が通知先に適用されます。その後定義した設定には、**Alternate#1**、**Alternate#2**などのラベルが付きます。デフォルト設定は、他の代替設定で指定された時間範囲でカバーされない時間帯がある場合に使用されます。たとえば、午前7時から午後8時の間に有効な**Alternate#1**という代替設定を指定した場合、午後8時から午前7時の間はデフォルト設定 (**Default**) が使用されます。

複数の通知先に対して同じ代替設定を適用する場合は、これらの通知先ごとに (同じ設定内容の) 代替設定を定義する必要があります。

新しい代替設定の定義

新しい代替設定を定義する場合は、最初に設定を定義した後に、その設定を編集して設定が有効になる時間範囲を指定します。

代替設定を定義するには

1. [**Node Management**] をクリックします。
2. ナビゲーションツリーで、通知先実行時パラメーターを編集するコネクターを選択します。管理パネルに、**[Connector]** サマリータブが表示されます。
3. [**Connector**] サマリータブの [**Destinations**] テーブルで、 をクリックします。
4. [**Add Alternate Configurations**] で、[**Add**] をクリックします。
5. 表示されるパラメーターの値を指定または更新します。
6. [**Save**] をクリックします。最初に定義した代替設定は、Alternate#1という名前で保存されます。その後の代替設定は、Alternate#2、Alternate#3などの名前で保存されます。

   定義した設定が有効になる時間範囲を指定するには、以下の手順 (「代替設定の編集」(111ページ)) を使用して、定義した設定を編集します。

代替設定の編集

代替設定の編集では、パラメーター値を変更するだけでなく、設定が有効になる時間範囲を指定することもできます。

代替設定を編集するには

1. [**Node Management**] をクリックします。
2. ナビゲーションツリーで、通知先実行時パラメーターを編集するコネクターを選択します。管理パネルに、**[Connector]** サマリータブが表示されます。
3. [**Connector**] サマリータブの [**Destinations**] テーブルで、 をクリックします。
4. 代替設定のリストから編集する代替設定を選択し、 をクリックします。
5. [From Hour]/[To Hour] の時間範囲を含め、表示されるパラメーターの値を指定または更新します。
6. ページの下部にスクロールし、**[Save]** をクリックします。

代替設定の一括編集

複数の代替設定で同じパラメーターを更新する必要がある場合は、「通知先実行時パラメーターの編集」(109ページ) に記載されている手順に従います。

通知先へのコマンドの送信

コネクターの通知先にコマンドを送信できます。

コネクター上で通知先にコマンドを送信するには

1. [**Node Management**] をクリックします。
2. ナビゲーションツリーで、コマンドを送信するコネクターを選択します。管理パネルに、[**Connector**] サマリータブが表示されます。
3. [**Connector**] サマリータブの [**Destinations**] テーブルで、をクリックします。
4. 実行するコマンドを選択し、**[Next]**をクリックします。
5. ユーザーインターフェイスに表示されるパラメーターの値を入力し、**[Finish]** をクリックします。

コネクターの削除

1つ以上のコネクターを削除するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、コネクターがあるコンテナーを選択します。
3. 管理パネルで、**[Connectors]** タブをクリックします。
4. コネクターのリストから、削除するコネクターをすべて選択します。
5. **[Delete]** をクリックします。
6. **[OK]** をクリックして削除を確定します。
7. 各コネクターが関連付けられていたコネクターアプライアンスまたはLoggerシステムを再起動します。

注: 特定のコネクターを [**Connector**] サマリータブから削除することもできます。タブの上部のをクリックして、コネクターを削除します。

コネクターへのコマンドの送信

コネクターにコマンドを送信できます。

コネクターにコマンドを送信するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、コマンドの送信先となるコネクターを選択します。管理パネルに、**[Connector]** サマリータブが表示されます。
3. [**Connector**] サマリータブで、[**Connector Command**] をクリックします。
4. **[Command Type]** ドロップダウンリストから、コネクターに送信するコマンドを選択し、**[Next]** をクリックします。

コネクターに対するLogfuの実行

コネクターに対してLogfuを実行すると、ArcSightログを分析して、ログに格納されている情報の対話型でビジュアルな表現を生成できます。

コネクターに対してLogfuを実行するには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、Logfuを実行するコネクターを選択します。管理パネルに、**[Connector]** サマリータブが表示されます。
3. [**Connector**] サマリータブで、[**Run Logfu**] をクリックします。
4. Logfuの進行状況ウィンドウが表示され、システムデータログの取得と分析が行われます。その後データは、**Group**、**Field**、および**Chart**別に表示されます。
   - [**Group**] ボックスで、表示するデータタイプを選択します。**[Group]** ボックスには、選択したコンテナー内のすべてのコネクターに加えて、メモリ使用量、伝送速度などの他の多くのデータタイプがリストされます。
   - 次に、いずれかの **[Group]** ボックスの**データポイント**を選択します。選択したデータポイントに応じて、フィールドのリストが下の **[Field]** ボックスに表示されます。
   - 表示する**フィールド**を選択します。**[Chart]** ボックスにグラフが表示され、速度と時間の情報が表示されます。**[Chart]** ボックスの下部にあるキーは、グラフ内でマップされたデータポイントを定義します。
   - 分析用に別のデータポイントを選択するには、**[Reset Data]** をクリックします。
5. 完了したら、Logfu表示ウィンドウを閉じます。

リモートファイルシステム

システムは、NFS (Network File System、バージョン3.0のみ) およびCIFS (Windows) 共有をマウントできます。そのため、UNIX、Linux、Windowsリモートホスト、およびこれらのOSに基づいた任意のNAS (Network Attached Storage) ソリューションから、ログファイルやイベントデータを読み取ることができます。Windowsシステムでは、ArcSight Management Centerにファイルベースのコネクターを追加する前に、CIFSマウントを確立する必要があります。

リモートファイルシステムの管理

共有をマウントする前に、以下の要件が満たされていることを確認してください。

ファイルシステムタイプ	要件
CIFS (Windows)	• 共有ドライブにアクセス可能なユーザーアカウントがWindowsシステムに存在すること。 • マウントポイントを確立しようとしているフォルダーが、共有用に設定されていること。 • **注:** NTLMv2およびNTLMv2i認証がサポートされます。Windows 2008 R2でNTLMv2iをサポートするには、Microsoft修正プログラムKB957441をインストールする必要があります。
NFS	• NFSシステムに対する読み書きがArcSightシステムに許可されていること。 • マウントに使用するアカウントが、`uid`として数値ID 1500、`gid`として750を使用していること。

リモートファイルシステムマウントを追加するには

1. 上部のメニューバーから **[Setup] > [System Admin]** をクリックします。
2. 左パネルの**[Storage]**セクションにある**[Remote File Systems]**をクリックします。[Remote File Systems] フォームが表示されます。
3. ページ左上の**[Add]**をクリックし、表示されるフォームの以下のフィールドに値を入力します。

パラメーター	説明
Select File System Type	NFSとCIFSのどちらの共有をマウントするのか。
NFSの設定	
Name	マウントポイントの意味のある名前。名前にスペースを含めることはできません。この名前は、マウントポイントを参照するのにシステム上でローカルに使用されるため、共有に保存されるデータのアーカイブ設定を設定する場合に指定する必要があります。
Hostname / IP Address	マウントを作成するホストの名前またはIPアドレス。
Remote Path (for NFS)	ネットワークファイルシステムマウントのルートとなる、リモートホスト上のフォルダー。たとえば/public/system_logsを指定します。 このフィールドに指定する場所に書き込むことができるのがこのシステムのみであることを確認してください。複数のシステム (または他のシステム) がこの場所をマウントして書き込むと、この場所のデータが破壊されます。

パラメーター	説明
Mount Options	AutoFSオプション。たとえば、リモートホストから読み取り専用の場合はro、読み書きを許可する場合はrw、リモートホストが応答するまで再試行し続ける場合はhardを指定します。 **注:** マウントポイントでrw許可を設定しても、ホストが読み取り専用アクセスを許可するように設定されている場合は、リモートホストにrwアクセスは許可されません。 **注:** NTLMv2およびNTLMv2i認証がサポートされます。
説明	マウントポイントの意味のある説明。
CIFSの設定	
Name	マウントポイントの意味のある名前。名前にスペースを含めることはできません。この名前は、マウントポイントを参照するのにシステム上でローカルに使用されるため、共有に保存されるデータのアーカイブ設定を設定する場合に指定する必要があります。
Location	以下のいずれかの方法で共有名を入力します。 • 次の形式の共有名 <IPアドレス>または<ホスト名>:<共有名> 例: 198.0.2.160:myshare このフォルダーは共有用に設定されている必要があります (通常、Windowsのフォルダーを共有用に設定するには、フォルダー名を右クリックして、**[プロパティ] > [共有]** を選択します)。 **注意:** クラスター内のWindows Server 2008からマウントする場合には、IPアドレス**ではなく**ホスト名を使用しないと、正常にマウントできません。 • UNCパス 例: //198.0.2.160/myshare
Mount Options	AutoFSオプション。たとえば、リモートホストから読み取り専用の場合はro、読み書きを許可する場合はrw、リモートホストが応答するまで再試行し続ける場合はhardを指定します。 **注:** マウントポイントでrw許可を設定しても、ホストが読み取り専用アクセスを許可するように設定されている場合は、リモートホストにrwアクセスは許可されません。 **重要:** ログファイルコネクター (たとえば、Symantec AntiVirusコネクター) の場合は、ArcSight Management Centerで新しいイベントを処理できるように、**directio**オプションを有効にする必要があります。[**File System Mount Options**] フィールドで、rw,directioを入力します。
Description	マウントポイントの意味のある説明。
CIFSの資格情報	
Username	Windows共有への読み書き権限を持つユーザーアカウントの名前。 ユーザー名の前には、必ずドメイン情報を追加してください。例: tahoe\arcsight
Password	上で指定したユーザー名のパスワード。

4. **[Add]** をクリックします。

すべてのマウントポイントは/opt/mntの下に作成されます。作成されるマウントポイントの名前に注意してください。この共有を使用するコネクターをArcSight Management Centerに追加するときには、この名前を指定する必要があります。

リモートファイルシステムマウントを編集するには

注: 使用中のマウントポイントは編集できません。**[Edit]** リンクは、マウントポイントを編集できる場合のみ表示されます。

1. 上部のメニューバーから **[Setup] > [System Admin]** をクリックします。
2. 左パネルの**[Storage]**セクションにある**[Remote File Systems]**をクリックします。
3. 編集するマウントポイントを選択し、ページの左上にから**[Edit]**をクリックします。
4. フィールドの値を変更します。
5. **[Save]**をクリックします。

リモートファイルシステムマウントを削除するには

注: 使用中のマウントポイントは削除できません。**[Delete]**リンクは、マウントポイントを削除できる場合のみ表示されます。停止した後、マウントを編集または削除できるようになるまでに最大2分かかります。

1. 上部のメニューバーから **[Setup] > [System Admin]** をクリックします。
2. 左パネルの**[Storage]**セクションにある**[Remote File Systems]**をクリックします。
3. 削除するマウントポイントを選択し、ページの左上にある**[Delete]**をクリックします。

イベントのネットワークインターフェイスアドレスの変更

ArcSight Management Centerには複数のネットワークインターフェイスがあります。デフォルトでは、コネクターはArcSightコンソールまたはLoggerに表示されるイベント用に使用するネットワークインターフェイスアドレスを決定しますが、一般にはeth0を使用します。

イベントに特定のネットワークインターフェイスアドレスを使用するには、パラメーター connector.network.interface.name をコネクターのagent.propertiesファイルに追加します。たとえば、eth1のIPアドレスを使用するには、以下のパラメーターを指定します。

```
connector.network.interface.name=eth1
```

FlexConnectorの開発

FlexConnectorは、サードパーティデバイスからの情報を読み込んで分析し、その情報をArcSightのイベントスキーマにマッピングできる、ユーザー定義のカスタムSmartConnectorで

す。

ArcSight Management Centerには、FlexConnector Developmentウィザードが用意されています。これを使用すると、パーサーファイルを作成することでFlexConnectorを素早く容易に開発でき、新しいFlexConnectorを展開前にテストしてパッケージ化することができます。ウィザードは、正規表現を生成し、イベントフィールドマッピングの推奨を自動的に提供するため、ユーザーが正規表現の作成、パーサー構文、ArcSightのイベントスキーマの専門家である必要はありません。

単純なログファイル用のFlexConnectorを作成するには、FlexConnector Developmentウィザードを使用します。複雑なログファイルについては、FlexConnector SDKを使用します(HPE ArcSightカスタマーサポートサイトから入手できます)。

FlexConnector Developmentウィザードは、Regex Files、Folder Follower、およびSyslog (Daemon、File、Pipe) FlexConnectorのみをサポートしています。

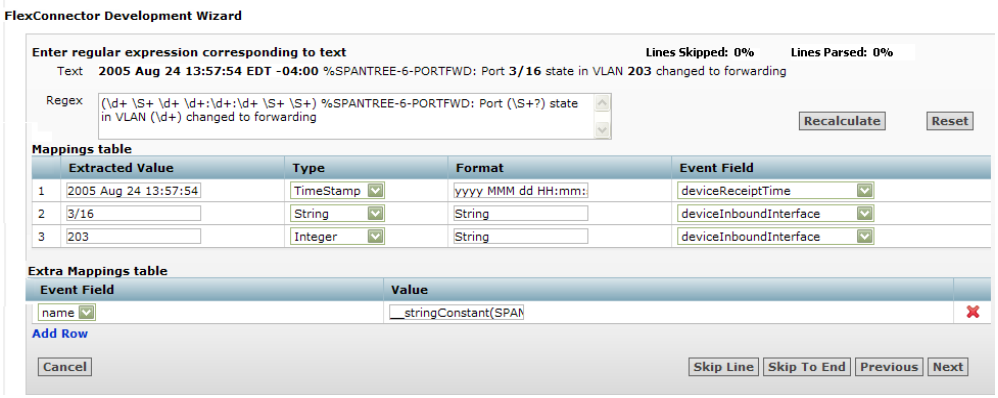
FlexConnector Developmentウィザードは、追加のプロセッサープロパティや複数のサブメッセージをサポートしていません。これらの機能が必要な場合は、FlexConnector SDKを使用してFlexConnectorを作成してください。

注意: FlexConnector Developmentウィザードで作成したFlexConnectorの動作は、HPE ArcSight SmartConnector SmartConnectorよりも遅い可能性があります。

FlexConnectorを開発するには

1. [**Node Management**] をクリックします。
2. ナビゲーションツリーで、コネクターを開発するコンテナーを選択します。
3. 管理パネルで、[**Connectors**] タブをクリックします。
4. [**Connectors**] タブの [Action] ドロップダウンで、[**Edit FlexConnector**] をクリックします。FlexConnector Developmentウィザードが起動します。
5. FlexConnectorを作成するデバイスのベンダーと製品名を入力し、**[Next]** をクリックします。
6. データソースのタイプを選択し、**[Next]** をクリックします。
   - syslogメッセージからイベントを読み込むSyslog FlexConnectorを作成するには、**[Syslog]** を選択します。
   - 正規表現を使用して可変フォーマットのログファイルを分析するFlexConnectorを作成する場合や (ArcSight FlexConnector Regex File)、バッチモードで可変形式のログファイルを分析するには (ArcSight FlexConnector Folder Follower)、**[File]** を選択します。
7. 前のステップで選択したデータソースタイプのサンプルログファイルをアップロードし、**[Next]** をクリックします。
8. ウィザードはログファイル中の最初の未分析の行を探し、その行を照合してトークンを抽

出する正規表現を生成し、抽出された各トークンについて提案されるフィールドマッピングを [Mappings] テーブルに表示します。



注: マッピングは、可能性の高いものから順番に表示されます (HPE ArcSightのトレーニングデータに基づきます)。リストから選択することでマッピングを変更できます。

ファイル内の分析された行のパーセンテージが、パネルの右上に表示されます。このパーセンテージを使用して、ログファイル中の現在の場所を推定できます。ファイル内でスキップされ分析されていない行のパーセンテージも、パネルの右上に表示されます。

- [**Regex**] ボックスで正規表現を変更し、マッピングを再計算するには、正規表現を編集して [**Recalculate**] ボタンをクリックします。正規表現を提案された値に戻すには、[**Reset**] ボタンをクリックします。
- ログファイルの未分析の行の中の抽出されたトークンに直接対応しないフィールドマッピングは、[Extra Mappings] テーブルに表示されます。イベントフィールドを変更し、トークン処理を指定できます。新しいフィールドイベントを追加するには、**[Add Row]**をクリックします。

  追加のマッピングを使用して、以下のことが可能です。

  - 既存のマッピングに加えて、抽出したトークンを異なるイベントフィールドに再マッピングします。たとえば、値が$3のイベントフィールドを追加できます ($3は提案されるマッピングのリスト内の3番目のトークン)。
  - 変更したトークンまたはトークンの組み合わせをイベントフィールドにマッピングします。たとえば、値が*__operation*($1,$3)のイベントフィールドを追加できます。
  - イベントフィールドを制約文字列または整数にマッピングします。たとえば、値が*__stringConstant*(constant)のイベントフィールドを追加できます。

    トークンがArcSightのイベントフィールドにマッピングされるときに使用されるトークン操作の一覧については、『FlexConnector Developer's Guide』(ArcSightカスタマーサポートサイトから入手可能) を参照してください。

9. マッピングをパーサーファイルに保存し、ログファイル中の次の分析されていない行を表示するには、**[Next]**をクリックします。

ログファイル中の分析されていないすべての行に対応する正規表現とマッピングが作成されると、確認のためにパーサーファイルが表示されます。

10. パーサーファイルを確認し、必要に応じて直接 [Review Parser File] パネルで変更します。
11. **[Next]**をクリックしてパーサーファイルを保存しパッケージ化します。
12. FlexConnectorを展開する方法を選択します。
    - 既存のコネクターを使用してパーサーファイルを使用するには、**[Deploy parser to existing connector in container]** を選択し、**[Next]** をクリックします。FlexConnectorウィザードを閉じて **[Container]** タブを再表示するには **[Done]** をクリックします。

      注: [Deploy parser to existing connector in container]オプションは、コンテナーにすでに同じ種類のコネクターが含まれている場合のみ表示されます。

    - パーサーを新しいコネクターとして追加するには、**[Add new connector to container]** を選択し **[Next]** をクリックします。手順に従ってコネクターをコンテナーに追加します。

FlexConnectorは他のユーザーと共有できます。「ArcExchangeでのコネクターの共有」(119ページ) を参照してください。

FlexConnectorの編集

FlexConnectorウィザードを使用してFlexConnectorを開発し、コンテナーに展開した後、必要に応じてFlexConnectorを編集し、パーサーファイルに変更を加えることができます。

FlexConnector Editウィザードは、**[Connectors]** タブの **[Action]** ドロップダウンで使用できます。

FlexConnectorの [**Action**] ドロップダウンで [**Edit Connector**] をクリックしてウィザードを開き、パーサーファイルを編集します。

注意: FlexConnectorウィザードで作成したFlexConnectorのみを編集してください。手動で作成したFlexConnectorを編集すると、予測不能な結果が生じる可能性があります。

ArcExchangeでのコネクターの共有

FlexConnectorとパーサーオーバーライドを他のユーザーと共有できます。

FlexConnectorは、ログファイル、データベース、その他のソフトウェアやデバイスからセキュリティイベントを収集するために定義するカスタムコネクターです。以下のタイプのFlexConnectorを共有できます。

- Syslog FlexConnectors (syslogメッセージからイベントを読み取ります)
- Log File FlexConnectors (固定形式のログファイルを読み取ります)

- Regular Expression Log File FlexConnectors (可変形式のログファイルを読み取ります)
- Regular Expression Folder Follower FlexConnectors (可変形式のログファイルを、フォルダー内で再帰的に読み取ります)
- Regular Expression Multiple Folder Follower FlexConnectors (複数のフォルダーからリアルタイムまたはバッチモードでイベントを読み取ります)
- XML FlexConnectors (フォルダー内のXMLベースのファイルから再帰的にイベントを読み取ります)

パーサーオーバーライドは、HPE ArcSightによって提供されるファイルであり、特定のコネクターでのパーサーの問題を解決したり、ログファイルの形式がわずかに変更されるか、新たなイベントタイプが追加された、サポートされているデバイスの新バージョンをサポートするために使用されます。パーサーオーバーライドは、パーサーを使用するすべてのコネクタータイプで共有できます。

FlexConnectorまたはパーサーオーバーライドを共有するには、これらをパッケージ化してHPE ArcSightのオンラインコミュニティ (Protect 724) 上のArcExchangeかローカルマシンにアップロードする必要があります。また、必要なFlexConnectorまたはパーサーオーバーライドをArcExchangeまたはローカルマシンからダウンロードし、コンテナーに追加することもできます。

注: プロキシサーバー経由でアクセスが行われる場合、ArcExchangeはHPE ArcSightのProtect 724コミュニティに到達できません。

コネクターのパッケージ化とアップロード

FlexConnectorまたはパーサーオーバーライドをProtect 724またはローカルコンピューターにアップロードする前に、アップロードウィザードを使用してzipファイル (AUPパッケージと呼びます) にパッケージ化する必要があります。

FlexConnector AUPパッケージには、コネクタープロパティファイル、分類ファイル、コネクターパラメーター、正常に展開するために必要なパッケージに対するすべてのメタデータが格納されたマニフェストファイルが含まれています。メタデータには、パッケージタイプ、コネクタータイプ、コネクターの説明など、AUPパッケージに関する情報が含まれています。1つのデバイスタイプとコネクターについて、AUPパッケージは1つしか作成できません。FlexConnectorは、Basicモードまたは Advancedモードでパッケージ化できます。

Basicモード:

- FlexConnectorプロパティファイルがウィザードによって自動的にパッケージ化されます。複数のプロパティファイルが見つかると、パッケージ化するファイルを選択するよう求められます。
- プロパティファイル中のデバイスベンダーと製品情報に基づいて分類ファイルを決定できる場合のみ、分類ファイルが自動的にパッケージ化されます。
- コネクターパラメーターはパッケージ化されません。コネクターをダウンロードして展開したときに、コネクターを設定するように求められます。

Advancedモード:

- FlexConnectorプロパティファイルがウィザードによって自動的にパッケージ化されます。複数のプロパティファイルが見つかると、パッケージ化するファイルを選択するよう求められます(これはBasicモードと同じです)。
- プロパティファイル中のデバイスベンダーと製品情報に基づいて決定できる場合、分類ファイルが自動的にパッケージ化されます。分類ファイルを決定できない場合は、コンテナー内に見つかったファイルのリストから、パッケージ化する分類ファイルを選択するよう求められます。
- ウィザードにコネクターのパラメーターが表示されるため、コネクターの展開(ダウンロード)時に表示するパラメーターを設定し、デフォルト値を指定することができます。表示するように設定しないパラメーターは現在の値を使用して事前設定され、コネクターの展開時には表示されません。

パーサーオーバーライドパッケージには、パーサーオーバーライドプロパティファイルとマニフェストファイルのみが含まれています。

FlexConnectorまたはパーサーオーバーライドをパッケージ化してアップロードするには、以下の手順に従います。

- ArcExchangeにアップロードするには、Protect 724の有効なユーザー名とパスワードを持っている必要があります。
- ネットワーク設定を、**[Administration]** > **[System Admin]** > **[Network]** で設定してあることと、ArcSight Management CenterがProtect 724サーバーと通信できることを確認してください。

FlexConnectorまたはパーサーオーバーライドをパッケージ化してアップロードするには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、パッケージをアップロードするコネクターを選択します。管理パネルに、[**Connector**] サマリータブが表示されます。
3. [**Connector**] 詳細ページで、をクリックします。アップロードウィザードが起動します。
4. **[Next]**をクリックしてウィザードの手順に従い、以下の操作を行います。
   a. 選択したコネクターに対して作成するAUPパッケージの種類を選択します。ArcSight Management Centerはコンテナーをスキャンして、パッケージ化が可能な関連ファイルを表示します。
   b. FlexConnectorでは、デフォルトパッケージを作成するには **[Basic]** を選択し、要件に合わせてパッケージをカスタマイズするには **[Advanced]** を選択します。
   c. コネクターに複数のプロパティファイルが含まれている場合は、パッケージ化するプロパティファイルを選択するよう求められます。syslogコネクターなど、特定のコネクターでは、複数のパーサーオーバーライドフォルダーを作成できます。その場合は、パッケージ

化するフォルダーを選択するよう求められます。

d. 以前FlexConnectorに対してAdvancedモードを選択し、分類ファイルを決定できない場合は、コンテナー内に見つかったファイルのリストから、パッケージ化する分類ファイルを選択するよう求められます。

注: 分類ファイルは、パーサーオーバーライドではパッケージ化されません。

e. 以前FlexConnectorに対してAdvancedモードを選択した場合は、コネクターの展開時に表示する設定のパラメーターを選択し、これらのパラメーターのデフォルト値を指定します。選択しないパラメーターは、現在の値を使用して事前設定されます。

以前に詳細なコネクターのパラメーターをデフォルトから変更している場合は、どちらを展開時に自動的に設定するかを選択できるように、ウィザードにこれらのパラメーターが表示されます。

注: パーサーオーバーライドでは、設定のパラメーターは表示されません。

コネクターにテーブルパラメーターがある場合は、パッケージ化の際に表示されません。しかし、コネクターをコンテナーにダウンロードするときに、すべてのテーブルパラメーターの値を入力するよう求められます。

f. AUPパッケージの説明とコネクターが使用するデバイスの設定方法を入力します。

g. コネクターが使用するデバイスのベンダー、製品、バージョンを指定します。

ウィザードがデバイスのベンダー、製品、バージョンを決定できる場合は、この情報がフィールドに表示されます。要件に合わせて情報を変更できます。

h. 作成したAUPパッケージをArcExchangeまたはローカルマシンにアップロードします。Protect 724のユーザー名とパスワードが必要になります。

コネクターのダウンロード

Protect 724のArcExchangeか、ローカルコンピューターにあるFlexConnectorまたはパーサーオーバーライドをダウンロードできます。FlexConnectorまたはパーサーオーバーライドは、直接コンテナーにダウンロードします。

ダウンロードウィザードを使用して、コンテナーあたり1つのFlexConnectorのみをダウンロードできます。ただし、コンテナーにダウンロードできるパーサーオーバーライドの数に制限はありません。

- パーサーオーバーライドをコンテナーにダウンロードすると、ダウンロードウィザードはコンテナー内の同じ名前の既存のオーバーライドを、確認なしで上書きします。既存のパーサーオーバーライドの上書きを避けるには、既存のパーサーオーバーライドに**Get Status**コマンドを送信して、パーサー情報を確認してから新しいパーサーオーバーライドをダウンロードしてください。Get Statusコマンドの送信については、「コネクターへのコマンドの送信」(112ページ)を参照してください。

- ダウンロードによって予期しない結果が発生した場合でも、設定を元に戻せるように、コネクターまたはパーサーオーバーライドをダウンロードする前に、必ずBackup Filesリポジトリにコンテナーをバックアップしておきます。

FlexConnectorまたはパーサーオーバーライドをコンテナーにダウンロードするには、以下の手順に従います。

ArcExchangeからダウンロードするには、Protect 724の有効なユーザー名とパスワードを持っている必要があります。また、ネットワーク設定を、**[Administration]** > **[System Admin]** > **[Network]** で設定してあることと、アプライアンスがProtect 724サーバーと通信できることを確認してください。

FlexConnectorまたはパーサーオーバーライドをダウンロードするには

1. **[Node Management]** をクリックします。
2. ナビゲーションツリーで、コンテナーがあるホストを選択します。
3. 管理パネルで、**[Containers]** タブをクリックします。
4. コンテナーのリストから、コネクターをダウンロードするコンテナーを選択します。**[Action]** ドロップダウンで **[Run FlexConnector Wizard]** を選択します。
5. **[Next]**をクリックしてウィザードの手順に従い、以下の操作を行います。
   a. コネクターを、Protect 724のArcExchangeからダウンロードするのか、ローカルコンピューターからダウンロードするのかを選択します。
   b. ダウンロードするAUPパッケージを選択します。

      Protect 724では、キーワードまたはその組み合わせを使用して、パーサーオーバーライドまたはFlexConnector AUPパッケージを検索できます。

      注: パーサーオーバーライドパッケージは、パッケージと同じ種類のコネクターがあるコンテナーのみにダウンロードできます。

      ダウンロードウィザードを使用して、コンテナーあたり1つのFlexConnectorのみをダウンロードできます。コンテナーにダウンロードしようとしているのと同じ種類のFlexConnectorがすでに含まれている場合、既存のFlexConnectorをダウンロードしようとしているもので置き換えることができますが、新規作成することはできません。

   c. FlexConnectorの場合は、必要に応じてコネクター設定パラメーターを指定します。

      事前設定されたパラメーターと詳細なパラメーターは、以前にパッケージ化された値を使用して自動的に展開されます。そのため、これらのパラメーターは設定を求められません。設定可能なパラメーターは、推奨されるデフォルト値と共に表示されます。これらの値は必要に応じて変更できます。テーブルパラメーターは設定値なしで表示されるため、必要に応じて、値を手動で指定する必要があります。
   d. コネクターの通知先を追加または選択します。

コネクターを、同じ種類の既存のコネクターがあるコンテナーにダウンロードする場合は、通知先の入力を求められません。

ウィザードによりプロパティと分類ファイルが適切な場所にコピーされ、AUPパッケージのzipファイルがArcSight Management Centerの`user/agent/deployedaups`フォルダーにインストールされ、展開履歴の記録が作成されます。

ダウンロードに成功すると、コンテナーが自動的に再起動されます。

各コネクタータイプの設定に関する注意事項

次の表に、各種コネクターの設定に関する注意事項を示します。

コネクタータイプ	制限された使用の影響
syslogコネクター	UDP (Syslogで通常使用される送信プロトコル) の性質上、設定可能なイベント速度を超えた場合に、これらのコネクターはイベントを失う可能性があります。これは、設定されたイベント速度に一致させるためにコネクターの処理が遅延している状態のときに、UDPキャッシュがいっぱいになり、オペレーティングシステムがUDPメッセージをドロップするためです。 **注**: イベント喪失の可能性があるので、これらのコネクターで **[Limit CPU Usage]**オプションを使用しないでください。
SNMPコネクター	syslogコネクターと同様に、SNMPコネクターでイベントレートが制限されている場合、イベントが失われる可能性があります。SNMPも一般にはUDPに基づいており、syslogと同じ問題があります。
データベースコネクター	コネクターはデータベーステーブルに従うため、データベースコネクターでイベントレートを制限すると、他のコネクターの動作が遅くなる可能性があります。その結果、イベントバックログが増え、アラートの報告が数分から数時間遅れる可能性があります。ただし、データベーステーブルが切り詰められない限り、イベントは失われません。イベントバーストが終わると、イベントレートが設定された制限を超えなければ、コネクターは最終的にデータベースの速度に対応できるようになります。
ファイルコネクター	ファイルベースのコネクターは、データベースコネクターと同様に、ファイルを追跡し、イベントレートを制限するとイベントバックログが増えます。これにより、実際のイベントレートに応じて、最終的にコネクターが数分または数時間遅れます。イベントレートが設定された速度を超えない場合は、コネクターが追いつく可能性があります。
アセットスキャナーコネクター	ArcSight Management Center上のすべてのコネクターは、アプリケーションとしてではなくサービスとして動作します。そのため、ArcSight Management Center上で動作するアセットスキャナーコネクターは、対話型モードではサポートされません。 アセットスキャナーコネクターを対話型モードで実行するには、コネクターをスタンドアロンシステムにインストールし、ソフトウェアベースのコネクターとして管理します。
専用APIコネクター	これらのコネクターの動作は特定のAPIに依存します (たとえば、OPSECの動作は、PostOfficeやRDEPとは異なります)。しかしほとんどの場合、API実装の内部バッファーとキューが一杯にならない限り、イベントは失われません。これらのコネクターは、データベースコネクターやファイルコネクターと同様に動作します。

付属のFlexConnector

HPE ArcSight Management Center コネクターアプライアンスには、次のプロトタイプFlexConnectorが含まれています。

- ArcSight FlexConnector File
- ArcSight FlexConnector ID-based Database
- ArcSight FlexConnector Multiple Database
- ArcSight FlexConnector Regular Expression File
- ArcSight FlexConnector Regular Expression Folder File
- ArcSight FlexConnector Simple Network Management Protocol (SNMP)
- ArcSight FlexConnector Time-based Database
- ArcSight FlexConnector XML File

これらのプロトタイプを使用して独自のFlexConnectorを開発し、これらを他のユーザーと共有することができます。「ArcExchangeでのコネクターの共有」(119ページ) を参照してください。

詳細については、HPE ArcSightカスタマーサポートから入手可能な『FlexConnector Developer's Guide』を参照してください。

Check Point OPSEC NGコネクターの設定

Check Point FW-1/VPN-1 OPSEC NGコネクターは、クリアチャネルモードまたはsslcaモードで動作できます。

注: Check Point OPSEC NGコネクターの設定には、次の条件が適用されます。

- この手順は、HPE ArcSightコネクターリリース4.6.2以降でのみサポートされています。
- ホスト名は、Check Pointではアプリケーションオブジェクト名 (Application Object Name) と呼ばれます。パスワードは、Check Pointではコミュニケーションアクティベーションキー (Communication Activation Key) と呼ばれます。

sslcaモードで動作するようにコネクターを設定するには

Check Point SmartDashboardで以下の手順を実行します。

1. Check Point SmartDashboardを使用してOPSECアプリケーションオブジェクトを作成します。アプリケーションオブジェクトを作成する際には、以下のパラメーターを指定する必要があります。

パラメーター	説明
Name	作成するアプリケーションオブジェクトの意味のある名前 (例: ArcSightLea-1)。 この名前は、システム内でOPSEC証明書を取得するために使用されます。
Host	コネクターを管理するHPE ArcSight Management Centerシステムのホスト名。

パラメーター	説明
Client Entities	LEAを選択します。
Secure Internal Communication	DN文字列が存在しない場合は、アクティベーションキーを指定して通信を初期化します。アクティベーションキーは、証明書を取得するときに使用されます。これはSIC名です。 [**Communication**] > [**Initialize**] をクリックします。

オブジェクトが作成されたら、以下の内容をメモします。これらは、設定を続行する場合に指定する必要があります。

- SIC名: 以下で説明するように、通信を初期化した後で取得するDN文字列です。
- SICエンティティ名: SmartDashboardでCheck Pointゲートウェイ名をダブルクリックして、その一般プロパティを表示します。SICエンティティ名は、一般プロパティウィンドウで設定されたSIC文字列です。
- Check Point IPアドレスまたはホスト名。

2. Check Point証明書を取得します。

そのためには、コネクターを追加するコンテナー上で`Pull OPSEC Certificate`コマンドを実行します。コンテナー上でコマンドを実行する方法の詳細については、「コンテナーへのコマンドの送信」(87ページ)を参照してください。コマンドを実行する際には、以下の情報を指定する必要があります。

パラメーター	説明
Server hostname or IP address	Check Pointサーバーの名前またはIPアドレス。
Application object name	前のステップで指定したOPSECアプリケーションオブジェクト名。このパラメーターでは、大文字と小文字が区別されます。
Password	前のステップでOPSECアプリケーションオブジェクトを作成するときに入力したアクティベーションキー。

証明書が正常に取得されると、以下のようなメッセージが表示されます。

```
OPSEC SIC name (CN=ArcSightLea-1,0=cpfw1.5ad8cn) was retrieved and stored
in /opt/arcsight/connectors/<container
name>/current/user/agent/checkpoint/<name>.Certificate was created
successfully and written to "/opt/arcsight/connectors/<container
name>/current/user/agent/checkpoint/ArcSightLea-1.opsec.p12".
```

OPSEC SIC名 (上の例ではCN=ArcSightLea-1,0=cpfw1.5ad8cn) とファイル名 (上の例ではArcSightLea-1.opsec.p12) をメモします。

ヒント: 証明書が正常に取得されなかった場合は、指定したアプリケーションオブジェクト名が正しいこと(大文字と小文字の区別を含む)と、コマンドを実行しているコン

テナーが動作していることを確認してください。

3. SmartDashboardを使用して、Check Pointゲートウェイ用にLEAクライアント上にポリシーをインストールします。

コネクターアプライアンスで以下の手順を実行します。

1. Check Pointコネクターを追加するため、「コネクターの追加」(99ページ)で説明されている手順に従います。以下の情報を入力する必要があります。

パラメーター	入力する値
Type	Check Point FW-1/VPN-1 OPSEC NG
Connection Type	SSLCA
Connector Table Parameters	Server IP: Check Pointサーバーの IPアドレス。 Server Port: サーバー上のSSLCAの接続を待つポート。デフォルト値 18184を使用してください。 OPSEC SIC Name: 「Check Point SmartDashboardを使用してOPSECアプリケーションオブジェクトを作成します。アプリケーションオブジェクトを作成する際には、以下のパラメーターを指定する必要があります。」(125ページ)でメモした名前。 OPSEC SSLCA File: 「Check Point証明書を取得します。」(126ページ)で証明書を取得した後でメモした名前。 OPSEC Entity SIC Name: 「Check Point SmartDashboardを使用してOPSECアプリケーションオブジェクトを作成します。アプリケーションオブジェクトを作成する際には、以下のパラメーターを指定する必要があります。」(125ページ)でメモした名前。

2. 以下のようなエラーが表示されます。

```
-1:[X] Unable to connect to the Lea Server[10.0.101.185] -1:1 connection test failed!
```

[Ignore warnings] チェックボックスを選択して **[Next]** をクリックします。

3. 続けて、「コネクターの追加」(99ページ)の説明に従ってコネクターの残りの設定を行います。

MS SQL Server JDBCドライバーの追加

Microsoft SQL Serverをデータベースとして使用するデータベースコネクターのインストールと設定を行う場合は、JDBCドライバーが必要です。このドライバーはプリインストールされていません。アプライアンス上でデータベースコネクターを設定する前にインストールする必要があります。

JDBCドライバーをインストールするには

1. MicrosoftのWebサイトから、MS SQL Server JDBCドライバーを、ArcSight Management Centerにアクセスできるコンピューターにダウンロードします。
2. セットアッププログラムを実行してドライバーをインストールします。
3. 「リポジトリへのファイルのアップロード」(220ページ) の手順に従って、sqljdbc.jarファイルを追加します。

   ヒント: jarファイルの名前は、一部のJDBCドライバーバージョンのものと違っている可能性があります。SQL Serverデータベースのバージョンごとに異なるバージョンのJDBCドライバーが必要です。必ず使用しているデータベースに対応した正しいドライバーを使用してください。

   以下の例に示すように、新しいドライバーファイルがリポジトリに追加されます。

   JDBCドライバーをインストールした後、SQL Serverデータベースコネクターが含まれているコンテナーにドライバーファイルをアップロードする必要があります。「リポジトリへのファイルのアップロード」(220ページ) の手順に従ってください。

   ドライバーファイルをコンテナーにアップロードした後、「コネクターの追加」(99ページ) の手順に従って、JDBCドライバーを必要とするコネクターを追加します。

MySQL JDBCドライバーの追加

MySQLをデータベースとして使用するデータベースコネクターのインストールと設定を行う場合は、JDBCドライバーが必要です。このドライバーはプリインストールされていません。アプライアンス上でデータベースコネクターを設定する前にインストールしてください。

JDBCドライバーをインストールするには

1. MicrosoftのWebサイトから、MySQL JDBCドライバーを、ArcSight Management Centerにアクセスできるコンピューターにダウンロードします。

   http://dev.mysql.com/downloads/connector/j/5.0.html
2. ドライバーを展開します。
3. 「リポジトリへのファイルのアップロード」(220ページ) の指示に従い、mysql-connector-java-x.x.x-bin.jarファイルを追加します。新しいドライバーファイルがリポジトリに追加されます。

   JDBCドライバーをインストールした後、MySQLデータベースコネクターが含まれているコンテナーにドライバーファイルをアップロードする必要があります。「リポジトリへのファイルのアップロード」(220ページ) の手順に従ってください。

   ドライバーファイルをコンテナーにアップロードした後、「コネクターの追加」(99ページ) の手順に従って、JDBCドライバーを必要とするコネクターを追加します。

第6章: 設定の管理

ここでは、以下の内容について説明します。

概要

設定は、関連するアプライアンスやソフトウェアの設定とそれぞれに関連付けられた値のグループで、1つ以上のノードタイプに適用されます。1つのノード用に作成した設定をArcSight Management Centerで管理される同じタイプのノードにプッシュすることができます。このため、ノードのグループ全体で一貫性を保証することができます。

設定には、次の種類があります。

- サブスクライバー設定は、複数のHPE ArcSight管理対象製品で定型的な管理を行うためのものです。コネクター、コネクターアプライアンス、Logger、または他のArcMCなどの同じタイプの複数のノードに対して、容易に値の割り当てを行い、同じ設定を適用・維持することができます。
- 初期設定は、複数のHPE ArcSight Logger (のみ) で同じセットアップをすばやく行うためのものです。初期設定は、HPE ArcSight Loggerの本番環境への初期展開をすばやく行うのに使用します。

設定管理タスクには、以下の内容が含まれます。

- 設定の作成: ノードタイプに対する設定は、ArcSight Management Centerで作成 (および編集または削除) できます。
- 設定のインポート: 設定は管理対象ノードで直接作成し、エクスポートした後に、ArcSight Management Centerにインポートして、同じタイプのノードで共有することができ

ます。

- 設定のプッシュ: 設定はArcMCから管理対象ノードにプッシュできます。この操作では、ArcMCから設定をコピーして、プッシュ先の各ノードの設定を変更します。
- サブスクリプション: 管理対象ノードではサブスクライバーの設定をサブスクライブできるため、ArcSight Management Centerからプッシュされた新しい設定や更新された設定を受信できます。
- 準拠状況のチェック: 管理対象ノードの設定とその値がArcSight Management Centerで指定された設定タイプのものと一致しているかどうかを確認します。一致している場合、そのノードは設定に準拠しているといいます。
- 比較: 各設定のフィールドごとの内訳、それぞれの値、および相違点を用いて、同じタイプの2つの設定をすばやく比較します。サブスクライバーノードの設定の値を、そのノードを管理するArcMCのベースライン設定または基準設定の値と比較することができます。また、1つのArcMCの同じタイプの2つの設定を比較することもできます。

たとえば、サブスクライバー設定の一般的なワークフローは、次のように動作します: アプライアンスに適したDNS設定を作成し、そのアプライアンスのプライマリDNSサーバー、セカンダリDNSサーバー、および検索ドメインを指定できます(「通知先設定のタイプ」(150ページ) を参照)。そのDNS設定をサブスクライブしているアプライアンスにプッシュし、1回のアクションでサブスクライブ中のすべてのノードのDNS設定を同じ設定にすることができます。

後で新しいプライマリDNSサーバーを使用するように設定を更新した場合は、新しい設定をすべてのサブスクライバーにプッシュできます。こうすると、1回のアクションですべての設定が新しいDNSサーバーに更新されます。

いつでも、管理対象ノードの設定への準拠を確認して、設定に目的の値が割り当てられているかどうかを確認することができます。

設定管理

設定を作成または管理するには、メニューバーで、[**Configuration Management**] をクリックします。特定の設定タイプを管理するには、サブメニューから該当する設定タイプを選択します。

たとえば、Loggerのサブスクライバー設定にアクセスするには、**[Configuration Management] > [Subscriber Configurations] > [Logger Configurations]** をクリックします。

[Configurations] テーブル

[**Configurations**] テーブルには、ArcSight Management Centerで現在利用可能なすべてのサブスクライバー設定のリストが表示されます。リスト表示される各設定は、ArcSight Management Centerで作成したものか、既存のノードからインポートしたものかに関係なく、

管理対象ノードへプッシュするための、ベースラインの設定とみなされます。このテーブルには、次のカラムが含まれます。

- **Name:** 設定の名前。
- **Type:** 設定のタイプ。
- **Last Edited By:** 設定を最後に編集したユーザー。
- **Compliance:** 個々のサブスクライバーの設定に対するステータスをまとめたもの。
  - Compliant: すべてのサブスクライバーが準拠していることを示します。
  - Non-Compliant: 少なくとも1つのサブスクライバーが準拠していないことを示します。
  - Unknown: 1つ以上のサブスクライバーの準拠ステータスを特定できない (たとえば、1つ以上のサブスクライバーとの接続が利用できない) ことを示します。

  ヒント: 各サブスクライバーの個々の準拠状況は、[**Subscribers**] タブで確認できます。

カラムのヘッダーをクリックすると、そのカラムで [**Configurations**] テーブルがソートされます。

個別の設定の詳細を表示するには、リストに表示された設定名をクリックします。[**Details**] タブと [**Subscribers**] タブに、追加情報が表示されます。

ヒント: リストで複数の項目を選択する場合は、項目を選択した状態で、Shiftキー+クリックまたはCtrlキー+クリックを使用します。

[Details] タブ

[**Details**] タブには、設定された属性や設定値などの、設定の詳細が表示されます。

設定名

各設定には一意の名前が付けられます。使用できる文字数は最大255文字です。

一般

一般説明には、以下のような、設定に関する基本事項が表示されます。

- **Configuration Type:** 設定のタイプ。設定タイプの詳細については、「サブスクライバー設定のタイプ」(143ページ) を参照してください。
- **Last Edited By:** 設定を最後に編集したユーザー。

プロパティ

プロパティは、1つ以上の設定項目のグループです。たとえば、NTPサーバーの設定に関するプロパティには、[Enable as NTP Server] (製品をNTPサーバーとして有効にするかどうかを示

す論理値)、[NTP Servers] (NTPサーバーのリスト) の2つの設定項目が含まれます。

各プロパティに含まれるパラメーター項目は、設定タイプごとに事前定義されています。ArcSight Management Centerでプロパティが選択されると、各設定項目の値の入力を求めるプロンプトが表示されます。各パラメーターには、データ型に応じて有効な値を割り当てる必要があります。たとえば、データ型が整数の場合は、整数値を指定する必要があります。赤いアスタリスク (*) は、必須パラメーターを示します。

リスト設定

複数のプロパティを含めることができる設定のタイプは、リスト設定と呼ばれます。リスト設定は、同じ種類のデータ値のインスタンスを複数含む設定です。各インスタンスはプロパティと呼ばれます。

たとえば、コネクターマップファイルの設定には、複数のマップファイルに関する情報を含めることができます。この場合、各プロパティは、(ファイルパスやコンテンツに関して異なる値を持つ) 別のマップファイルを表します。

注: リスト設定をプッシュすると、管理対象ノードの同じタイプの既存の設定がオーバーライドされます。既存の設定にデータを追加するには、一括管理ツール ([**Set Configuration**]) を使用します。

サポートされる設定タイプ、各タイプに関連するパラメーター、およびそれぞれのデータ型については、「[Configurations] テーブル」(130ページ) を参照してください。

[Subscribers] タブ

[**Subscribers**] のリストには、設定を受信する対象となっているすべての管理対象ノードが表示されます(ホストがまだ追加されていない場合、リストには何も表示されません)。

このタブには、次の操作ボタンが含まれます。

Add Subscribers	既存の設定にサブスクライバーを追加します。
Push	選択した1つ以上のサブスクライバーに設定をプッシュします。
Check Compliance	すべてのサブスクライバーのベースライン設定に対する準拠状況を確認します。
Unsubscribe	サブスクライバーのリストから、選択した1つ以上のサブスクライバーを削除します。

リストには、次のカラムが含まれます。

- **Path:** ロケーション/ホスト名/ノードタイプで構成される、サブスクライブしているノードのパス
- **Type:** サブスクライブしているノードのタイプ。
- **Last Pushed At:** サブスクライバーに対して最後にプッシュが行われた日時。
- **Last Push Status:** サブスクライバーに対する最後のプッシュのステータス。

- Succeeded: 設定のプッシュが成功しました。
- Failed: プッシュが失敗した理由を確認するには、リンクの上にカーソルを置きます。問題の修復に役立つように、エラーメッセージが表示されます。詳細については、「プッシュの修復」(140ページ)を参照してください。
- Unknown: サブスクライバーがプッシュを受け取る前の初期ステータス。

- **Last Compliance Check:** 最後に準拠状況のチェックが行われた日時。
- **Compliance:** ノードが設定に準拠しているかどうかを示します。
  - Compliant: ノードが準拠していることを示します。設定のタイプに関連付けられているすべての設定項目の値が、設定の値と一致しています。
  - Non-Compliant: ノードが準拠していないことを示します。設定タイプに関連付けられている1つ以上の設定項目の値が、設定の値と一致していません。[No] の上にカーソルを置くと、ノードが非準拠になっている理由が表示されます。
  - Unknown: 最後に準拠状況のチェックが行われたときにノードの準拠状況を特定できなかったか、またはノードでまだ準拠状況のチェックが行われていないことを示します。

非準拠レポート

準拠ステータスがNon-Compliant (非準拠) である理由を確認できます。

準拠ステータスがNon-Compliantの場合、ステータスをクリックすると、ArcMCと管理対象ノードの設定のすべての設定項目の値を比較した [**Configuration Comparison**] ダイアログが表示されます。

ステータスをCompliant (準拠) にするには、[**Push Configuration**] をクリックして設定を管理対象ノードにプッシュします。

サブスクライバー設定の作成

サブスクライブ中のノードに対してプッシュするためのサブスクライバー設定を作成できます。

注: 以下のサブスクライバー設定のタイプは、ArcSight Management Centerでは作成できません。管理対象ノードからインポートする必要があります。

- Loggerストレージグループ
- Loggerフィルター
- Logger ESMフォワーダー、コネクターフォワーダー、TCPフォワーダー、UDPフォワーダー
- 外部認証

管理対象ノードからの設定のインポートの詳細については、「サブスクライバー設定のインポート」(135ページ)を参照してください。

設定を作成するには

1. **[Configuration Management] > [Subscriber Configurations] > [All Configurations]** をクリックします。

   ヒント: フィルターで特定のサブスクライバー設定タイプを抽出するには、**[Subscriber Configurations]** サブメニューから目的の設定タイプを選択します。

2. **[Configurations]** で、**[New]** をクリックします。
3. **[Details]** タブで、**[Configuration Type]** ドロップダウンリストから設定タイプを選択します(関連する設定タイプのみがドロップダウンリストに表示されます)。
4. **[Configuration Name]** に設定の名前を入力します(設定名は一意である必要があり、使用できる文字数は最大255文字です)。
5. 必須パラメーターの値を入力します。必須パラメーターは赤いアスタリスク (*) で示されます。

   注: 各設定タイプに対して有効なパラメーター、およびそれぞれに関連付けられたデータ型については、「サブスクライバー設定のタイプ」(143ページ) を参照してください。

6. オプションで、オプションパラメーターの値を追加します。
7. オプションで、リスト設定用の追加プロパティを追加するには、**[Add Property]** をクリックしてから、要求されたパラメーターの値を入力します。必要に応じてプロパティの追加を繰り返して、設定の定義を完成させます。
8. **[Save]** をクリックします。

サブスクライバー設定の編集

サブスクライバー設定の値を変更または削除することができます(現在プッシュ中の設定を編集することはできません)。

設定を編集するには

1. **[Configuration Management] > [Subscriber Configurations] > [All Configurations]** をクリックします。

   ヒント: フィルターで特定のサブスクライバー設定タイプを抽出するには、**[Subscriber Configurations]** サブメニューから目的の設定タイプを選択します。

2. **[Configurations]** テーブルで、編集する設定の名前をクリックします。
3. **[Details]** タブで、**[Edit]** をクリックします。

- 必要に応じて一般設定を編集します。
- オプションで、リストプロパティ用の追加プロパティを追加するには、[**Add Property**] をクリックしてから、要求されたパラメーターの値を入力します。必要に応じてプロパティの追加を繰り返して、設定の定義を完成させます。
- オプションで、設定からプロパティを削除するには、[**Delete Property**] をクリックします。

4. 完了したら [**Save**] をクリックします。保存後、設定にサブスクライバーが存在する場合は、更新した設定をサブスクライバーにプッシュするように求めるプロンプトが表示されます。

サブスクライバー設定の削除

削除したサブスクライバー設定は、サブスクライバーへのプッシュには使用できなくなります。現在プッシュ中の設定を削除することはできません。

サブスクライバー設定を削除するには

1. **[Configuration Management] > [Subscriber Configurations] > [All Configurations]** をクリックします。

   ヒント: フィルターで特定のサブスクライバー設定タイプを抽出するには、[**Subscriber Configurations**] サブメニューから目的の設定タイプを選択します。

2. [**Configurations**] テーブルで、削除する設定を1つ以上選択します。
3. [**Delete**] をクリックします。
4. [**Yes**] をクリックして削除を確定します。

サブスクライバー設定のインポート

管理対象ノードで作成したサブスクライバー設定は、ArcSight Management Centerにインポートして、編集を行ったり、同じタイプの他のノードにプッシュしたりすることができます。

たとえば、管理対象コネクターアプライアンスで設定を定義し、その設定をArcSight Management Centerにインポートできます。インポートした設定は、ArcSight Management Centerで作成した設定の場合と同様に、編集を行ったり、別の管理対象コネクターアプライアンスにプッシュしたりできます。

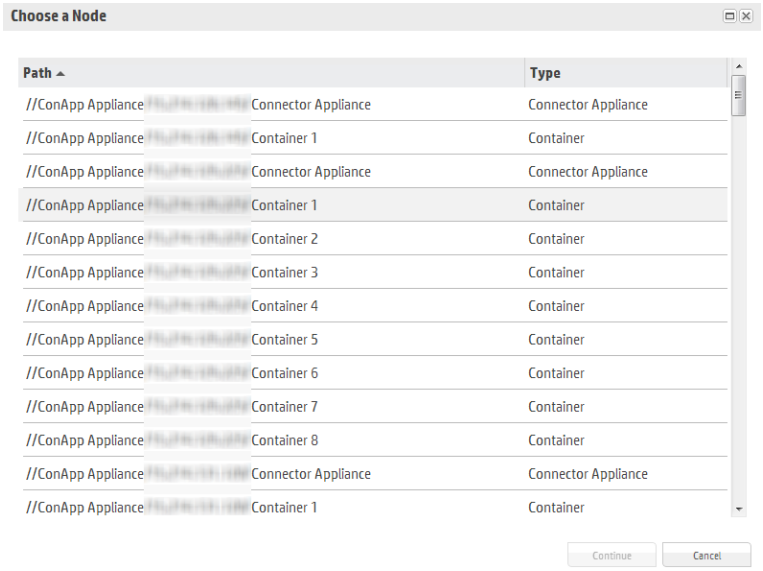
ローカルホストへの設定のインポートに失敗した場合は、ローカルホストでWebサービスを再起動します。

管理対象ノードからサブスクライバーの設定をインポートするには

1. **[Configuration Management] > [Subscriber Configurations] > [All Configurations]** をクリックします。

   ヒント: フィルターで特定のサブスクライバー設定タイプを抽出するには、**[Subscriber Configurations]** サブメニューから目的の設定タイプを選択します。

2. **[Configurations]** で、**[Import]** をクリックします。
3. **[Choose a Node]** ダイアログで、設定のインポート元のノードを選択します。



4. **[Continue]** をクリックします。
5. **[Import Configuration]** ダイアログで、次の操作を実行します。
   a. **[Type]** ドロップダウンリストから、インポートする設定の設定タイプを選択します(リストのエントリは、ステップ3で選択したノードに適用される設定タイプに依存します)。
   b. **[Name]** にインポートする設定の名前を入力します。
6. **[Import]** をクリックします。設定がArcSight Management Centerにインポートされ、**[Configurations]** テーブルに表示されます。

   注: コネクターアプライアンス、Logger、またはArcMCノードからバックアップ設定をインポートするには、ノードにスケジュールされたバックアップが存在している必要があります。

サブスクライバーの管理

サブスクライバーは、設定のプッシュ先となる管理対象ノードです。設定のプッシュ先であるサブスクライバーは、管理対象ノードの設定内容が設定で指定されたものと同じになるように、

プッシュされた設定を受け取って処理し、それを管理対象ノードに適用します。

各ノードは、設定タイプごとに設定を1つだけサブスクライブできます。

たとえば、Loggerアプライアンスでは、1つのLoggerストレージグループの設定をサブスクライブでき、同時に同じアプライアンスで、Loggerフィルター設定とLoggerトランスポートレシーバー設定を1つずつサブスクライブできます。

サブスクライバーの表示

特定の設定のサブスクライバーを表示するには

1. **[Configuration Management] > [All Configurations]** をクリックします。
2. 設定のリストから、サブスクライバーを表示する設定を選択します。
3. 設定の名前をクリックします。
4. [**Subscribers**] タブをクリックします。現在のサブスクライバーが表示されます。

サブスクライバーの追加

サブスクライバー (つまり、サブスクライブ中のノード) は、プッシュされた設定を受け取ることができます。

ノードを設定にサブスクライバーとして追加するには

1. **[Configuration Management] > [Subscriber Configurations] > [All Configurations]** をクリックします。

   ヒント: フィルターで特定のサブスクライバー設定タイプを抽出するには、[**Subscriber Configurations**] サブメニューから目的の設定タイプを選択します。

2. [**Configurations**] テーブルで、サブスクライバーを追加する設定の名前をクリックします。
3. [**Subscribers**] タブをクリックします。
4. [**Add Subscribers**] をクリックします。
5. [**Add Subscribers**] ダイアログで、サブスクライバーとして追加するノードを選択します。選択可能なサブスクライバーのリストの内容は、選択した設定タイプによって決まります。サブスクライブ用に複数のノードを選択する場合は、Ctrlキー+クリックを使用してノードを1つずつ選択します。

   注: 1つのノードでサブスクライブできるのは、設定タイプごとに1つの設定 (たとえば、1つのDNS設定) のみです。

追加しようとしたサブスクライバーが、同じタイプの設定をすでにサブスクライブ中の場合、次のメッセージが表示されます: No available subscribers have been found for the selected configuration. (選択した設定で利用可能なサブスクライバーが見つかりませんでした。)

6. [**Add Subscribers**] をクリックします。
7. [**OK**] をクリックして完了を確定します。サブスクライバーが設定の受信者に追加されます。

サブスクライバーのサブスクライブ解除

サブスクライブを解除すると、ノードはプッシュされた設定を受け取ることができなくなります。

設定からサブスクライバーを削除するには

1. **[Configuration Management] > [Subscriber Configurations] > [All Configurations]** をクリックします。

   ヒント: フィルターで特定のサブスクライバー設定タイプを抽出するには、[**Subscriber Configurations**] サブメニューから目的の設定タイプを選択します。

2. [**Configurations**] テーブルで、サブスクライバーを削除する設定の名前をクリックします。
3. [**Subscribers**] タブをクリックします。
4. サブスクライバーのリストから、1つ以上のサブスクライバーを選択します。
5. [**Unsubscribe**] をクリックします。
6. [**OK**] をクリックして確定します。選択したサブスクライバーのサブスクライブが解除されます。

サブスクライバー設定のプッシュ

サブスクライバー設定をプッシュすると、ArcSight Management Centerから設定のすべてのサブスクライバーまたは選択したサブスクライバーに設定が同期されます。プッシュは手動で行う必要があります。

サブスクライバーを選択する際には、設定に関連する選択可能なサブスクライバーのみが表示されます。たとえば、Loggerのみに適用されるLoggerの設定をプッシュする場合は、管理対象のLoggerのみが選択可能なサブスクライバーとして表示され、コネクターアプライアンスやArcMCは表示されません。

ローカルホストへの設定のプッシュに失敗した場合は、ローカルホストでWebサービスを再起動します。

サブスクライバー設定をすべてのサブスクライバーにプッシュするには

1. **[Configuration Management] > [Subscriber Configurations] > [All Configurations]** を選択します。

   ヒント: フィルターで特定のサブスクライバー設定タイプを抽出するには、[**Subscriber Configurations**] サブメニューから目的の設定タイプを選択します。

2. [**Configurations**] テーブルで、プッシュする設定を選択します。
3. [**Push**] をクリックします。
4. [**Yes**] をクリックして、プッシュを確認します。設定が、選択した設定のすべてのサブスクライバーにプッシュされます。準拠状況のチェックは各サブスクライバーで自動的に実行されます。

サブスクライバー設定を選択したサブスクライバーにプッシュするには

1. **[Configuration Management] > [Subscriber Configurations] > [All Configurations]** を選択します。

   ヒント: フィルターで特定のサブスクライバー設定タイプを抽出するには、[**Subscriber Configurations**] サブメニューから目的の設定タイプを選択します。

2. [**Configurations**] テーブルで、プッシュする設定を選択し、設定の名前をクリックします。
3. [**Configuration Details and Subscribers**] ページで、[**Subscribers**] タブをクリックします。
4. [**Subscribers**] タブで、設定をプッシュするサブスクライバーを1つ以上選択します。
5. [**Push**] をクリックします。
6. [**Yes**] をクリックして、プッシュを確認します。設定が、選択したサブスクライバーにプッシュされます。準拠状況のチェックは各受信者で自動的に実行されます。

プッシュの検証

サブスクライバーに対してプッシュを行う際には、ArcSight Management Centerによって設定が自動的に検証されます。検証を行うことで、プッシュされる設定のすべての設定項目に意味のある適切な値が含まれていることを確認します。設定値の中に無効な値が見つかった場合、プッシュは失敗し、エラーメッセージが返されます。[**Subscribers**] タブの [**Push Status**] カラムで、サブスクライバーのエントリ上にカーソルを置くと、プッシュが失敗した理由が表示されます。さらに、準拠状況のチェックがプッシュ後に自動的に実行されます。

プッシュの失敗の一般的な原因

サブスクライバーへのプッシュが失敗する原因はさまざまです。失敗する原因には、以下のようなものがあります。

- **検証の失敗:** 無効なコンテンツを含むプッシュは失敗します。設定に設定タイプに応じた有効な設定値が含まれていることを確認します。
- **接続できない:** ネットワークやシステムの問題が原因で、サブスクライバーとの接続が損なわれることがあります。サブスクライバーとの接続を確認します。
- **ホスト上でエージェントが実行されていない:** サブスクライブしているノードでArcMCエージェントのプロセスがアクティブになっていることを確認します(これは、エージェントを必要としないソフトウェアコネクターには当てはまりません)。
- **サブスクライブしているホストに対する権限**: サブスクリプションをプッシュするには、(ユーザーの資格情報によって指定される) ArcSight Management Centerユーザーに、サブスクライバーノード上の設定の各設定項目を表示、編集、または削除する権限が必要になります。
- **ライセンスの期限切れ:** ホストのライセンスが期限切れになっている場合、ホストへのプッシュは失敗します。

プッシュの修復

サブスクライバーへのプッシュに失敗した場合は、失敗を修復できます。プッシュの失敗を修復するには、以下の手順を実行します。

1. [**Configurations**] テーブルから設定を選択します。
2. [**Subscribers**] タブをクリックし、プッシュが失敗したサブスクライバーを選択します。
3. [**Last Push Status**] に「Failed」と表示されます。このリンク上にカーソルを置くと、プッシュの失敗に関連するエラーメッセージが表示されます。

エラーメッセージを確認した後、管理対象ノードで適切な手順を実行して問題を解決します。問題を解決するのに、ArcSight Management Center外のノードへの直接アクセスやリモートアクセスが必要になる場合があります。

問題が解決されたら、失敗した設定のプッシュを再度実行します。

サブスクライバーの準拠状況のチェック

ノードの設定内容がArcSight Management Centerの設定に割り当てられた内容と一致している場合、サブスクライブ中のノードは設定に準拠しています。

管理を行うArcSight Management Centerにリスト表示される設定は、ベースラインの設定とみなされます。

たとえば、ArcSight Management Centerで、「Sample SMTP Configuration」という名前のSMTP設定を作成し、次の値を割り当てます。

- Primary SMTP Server: Mailserver1
- Secondary SMTP Server: Mailserver2
- Outgoing Email Address: admin@example.com

プライマリおよびセカンダリSMTPサーバーと、送信メールアドレスがSample SMTP Configurationの値と一致していれば、ノードはこの設定に準拠していることになります。

これらの値にいずれか1つでも異なるものがあれば (たとえば、ノードのプライマリSMTPサーバーがCorporateMail1であれば)、ノードは準拠していないことになります。

特定の設定に対するすべてのサブスクライバーの準拠状況は、手動でチェックすることができます。

特定の設定に対するサブスクライバーの準拠状況を手動でチェックするには

1. **[Configuration Management] > [Subscriber Configurations] > [All Configurations]** をクリックします。

   ヒント: フィルターで特定のサブスクライバー設定タイプを抽出するには、[**Subscriber Configurations**] サブメニューから目的の設定タイプを選択します。

2. [**Configurations**] テーブルで、準拠状況をチェックする設定を選択します。
3. [**Check Compliance**] をクリックします。選択した設定に対するすべてのサブスクライバーの準拠状況がチェックされます。
   - [**Configurations**] テーブルの [**Compliance**] カラムには、すべてのサブスクライバーの準拠状況をまとめたものが表示されます。
   - 設定の [**Subscribers**] タブでは、
     - [**Last Compliance Check**] カラムが更新され、最後に行われたチェックが表示されます。

       準拠状況の自動チェックは、12時間おきに実行されます。そのため、これは最後に行われた自動チェックの日時になります。

     - [**Compliance**] カラムに、各ノードの個々の準拠状況が示されます。

設定の比較

同じタイプの2つの設定を比較し、それぞれの設定の設定値が同じであるかどうかを確認できます。以下の2種類の比較が可能です。

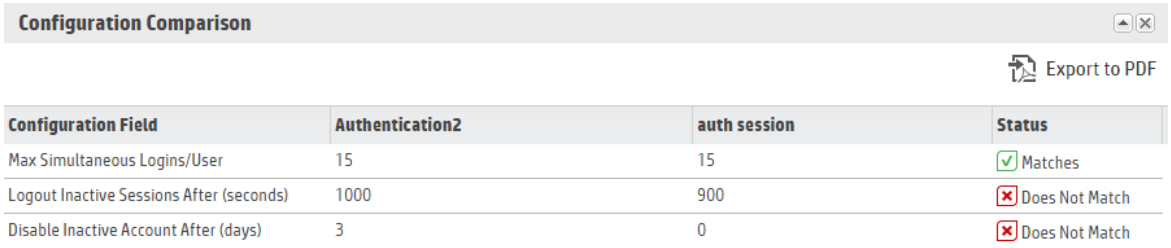
- **1つのArcMC上の2つの設定の比較:** 1つのArcMC上の同じタイプの2つの設定を比較できます。たとえば、2つの異なるSMTP設定の設定値を比較できます。
- **サブスクライバー上の設定とそれを管理しているArcMC上の同じ設定の比較:** サブスクライブしているノードの設定とそれを管理しているArcMCの同じ設定の設定値の違いを、すばやくチェックして表示することができます。

1つのArcMC上の同じタイプの2つの設定を比較するには

1. [**Configuration Management**] をクリックします。
2. [**All Configurations**] を選択します。
3. 設定のリストで、2つの設定を選択します。
4. [**Compare**] をクリックします。

[**Configuration Comparison**] ダイアログに、設定のそれぞれの設定値が表示され、[**Status**] カラムに比較項目ごとの現在値が表示されます。

比較内容をPDFレポートとして出力する場合は、[**Export to PDF**] をクリックします。



サブスクライバー上の設定とそれを管理しているArcMC上の同じ設定を比較するには

1. [**Configuration Management**] をクリックします。
2. [**All Configurations**] を選択します。
3. 設定のリストで、ArcMCとサブスクライバーの間で比較を行う設定を選択します。
4. [**Configuration Details & Subscribers**] で、[**Subscribers**] タブをクリックします。
5. [**Compliance**] カラムで、ステータスのリンクをクリックします。

[**Configuration Comparison**] ダイアログに、設定のそれぞれの設定値が表示され、比較項目ごとの現在値が表示されます。

オプションで、サブスクライバーがそれを管理しているArcMCの設定に対して非準拠 (Non-compliant) 状態である場合、[**Push Configuration**] をクリックして、設定をサブスクライバーにプッシュします (これにより、準拠 (Compliant) 状態になります)。

比較内容をPDFレポートとしてエクスポートする場合は、[**Export to PDF**] をクリックします。

設定管理のベストプラクティス

設定管理は、HPE ArcSight製品を一括して管理するための優れたツールです。わずかな操作で、複数のアプライアンスに対して設定を簡単に実装することができます。

- **ノード管理と設定管理:** 個々のノードの管理と日常の運用には、ArcSight Management Centerのノード管理ツールを使用します。ただし、管理対象ノードのデータや設定値に広範囲にわたる一貫性のある変更を加える必要があり、適切な設定が存在する場合は、設定管理を使用します。たとえば、複数の管理対象ノードでDNSの設定値を変更するには、ArcMCで設定を作成し、それを管理対象ノードにプッシュする方が、複数のデバイスの設定値を個別に変更するよりもすばやく簡単です。
- **複数のアプライアンスまたは製品でのデータ設定の一括実行:** 複数のアプライアンスまたは製品でデータ設定を実行する場合には、一括管理 ([**Set Configuration**]) ツールを使用します。たとえば、管理対象ノードに単一プラットフォーム (この場合はSMTP) の設定を適用して、同じハードウェア設定 (SMTPサーバーなど) を使用するように、すべてのアプライアンスをすばやく設定することができます(プッシュすると、既存データはすべて上書きされます)。
- **準拠と非準拠:** 設定管理で設定の準拠が問題とならない場合は、ノード管理で一括管理ツールを使用してノードの設定値を管理します。また、設定管理で一括プッシュを実行することもできます。

サブスクライバー設定のタイプ

次のセクションでは、利用可能なサブスクライバー設定のタイプ、それぞれに関連するパラメーター、データ型、およびパラメーターに関する簡単な説明を示します。パラメーターに値を割り当てる場合、次の点に注意する必要があります。

- 各パラメーターの値には、指示されたデータ型を使用する必要があります (たとえば、文字列データ型では、値として文字列を入力する必要があります)。
- 必須パラメーターにはアスタリスク (*) マークが付いており、必ず値を割り当てる必要があります。必須パラメーターの値が欠落している設定は、保存またはプッシュできません。
- 読み取り専用のパラメーターは、ArcSight Management Centerで編集できません。
- セキュリティ上の理由から、パスワードのパラメーターはすべて難読化された状態で表示されます。

ヒント: 各入力フィールドの詳細は、編集モードで、フィールドラベル上にカーソルを置くと、そのフィールドに関するツールヒントが表示されます。

コネクター設定のタイプ

コネクター設定では、コンテナーまたはソフトウェアコネクターの設定項目の値を設定します。ここでは、利用可能なコネクター設定のタイプを示します。

BlueCoatコネクター設定

BlueCoatコネクター設定では、1つ以上のBlueCoatコネクターの設定値を定義します。この設定がターゲットにプッシュされるのは、BlueCoatコネクターが存在する場合のみです。

BlueCoatコネクター設定をArcMCから、ここに示すすべてのフィールドの値がすでに定義されている管理対象ノードに対してプッシュするには、プッシュされる設定のすべてのフィールドの値を指定します。必要に応じて、デフォルト値を使用できます。

BlueCoatコネクター設定のパラメーター

パラメーター	データ型	説明
Row Number*	整数	設定のプッシュ先のテーブルパラメーターの行番号。
Log File Wildcard*	文字列	ログファイルのワイルドカード。
Log File Type*	文字列	ログファイルのタイプ。有効な値は次のとおりです。 • `main` • `im` • `ssl` • `streaming`
Processing Mode	文字列	処理モード。有効な値は、BatchおよびReal timeです。
Post-Processing Mode	文字列	後処理モード。有効な値は次のとおりです。 • `RenameFileInTheSame Directory` • `PersistFile` • `DeleteFile`
Mode Options	文字列	モードオプション。Post-Processing Modeで次を選択した場合に必要です: `RenameFileInTheSame Directory`
Processing Threshold	整数	ログファイルに処理済みとマークされるまでの間隔 (時間単位)。
Processing Limit	整数	ディレクトリで同時に読み取り可能なファイル数。

FIPS設定

FIPS設定では、コンテナーでFIPSモードを有効または無効にします。

FIPS設定をプッシュすると、プッシュ先のコンテナーが再起動されます。

FIPS設定のパラメーター

パラメーター	データ型	説明
Enabled*	論理型	[**Yes**] の場合、コンテナーでFIPSが有効になっています。

マップファイル設定

マップファイル設定では、1つ以上のコンテナーマップファイルのパスおよびコンテンツを定義します。Path/Contentの各ペアが、1つのマップファイルを表します。複数のファイルを含めるには、複数のプロパティを設定に追加します。

- プッシュすると、設定によってターゲット上の`\map`ディレクトリ内のすべての`*.properties`ファイルが削除された後、マップファイルのリストがターゲットに追加され、既存のマップファイルが置き換えられます。
- 設定に空のリストが含まれている場合は、すべての`*.properties`ファイルが削除されます。

マップ設定ファイルをインポートしてアップロードする場合は、ダウンロードしたCSVファイルをアップロード前に*.propertiesファイルに変換します。

マップファイル設定のパラメーター

パラメーター	データ型	説明
Path*	文字列	マップファイルへのパス。
Content*	文字列	マップファイルのコンテンツ。

パーサーオーバーライド設定

パーサーオーバーライド設定では、1つ以上のコンテナーパーサーオーバーライドファイルのパスおよびコンテンツを定義します。

Path/Contentの各ペアが、1つのパーサーオーバーライドファイルを表します。複数のファイルを含めるには、複数のプロパティを設定に追加します。

- プッシュすると、設定によってターゲット上の`\fcp`ディレクトリ内のすべての`*.properties`ファイルが削除された後、パーサーオーバーライドファイルのリストがターゲットに追加され、既存のパーサーオーバーライドファイルが置き換えられます。
- 設定に空のリストが含まれている場合は、すべての`*.properties`ファイルが削除されます。

パーサーオーバーライド設定のパラメーター

パラメーター	データ型	説明
Path*	文字列	パーサーオーバーライドファイルへのパス。
Content*	文字列	パーサーファイルのコンテンツ。

Syslogコネクター設定

Syslogコネクター設定では、1つ以上のSyslogコネクターの値を定義します。この設定がターゲットノードにプッシュされるのは、Syslogコネクターが存在する場合のみです。

Syslogコネクター設定のパラメーター

パラメーター	データ型	説明
Port*	整数	Syslogコネクターポート。
Protocol*	列挙型	Syslogコネクターのプロトコル(UDPまたはRaw TCPのいずれか)。

Windows Unified Connector (WUC) 外部パラメーター設定

WUC外部パラメーターコネクター設定では、1つ以上のWUCコネクターの外部パラメーターを定義します。この設定がターゲットノードにプッシュされるのは、WUCコネクターが存在する場合のみです。

WUC外部パラメーター設定の制限事項

WUC外部パラメーター設定には、次の制限事項があります。

- ドメインユーザーパスワードは、WUC設定パラメーターとしてサポートされません。ドメインユーザーパスワードは、WUCホストごとに個別に管理する必要があります。
- WUCコネクターはFIPS準拠ではありません。
- WUC設定をArcMCから、ここに示すすべてのフィールドの値がすでに定義されている管理対象ノードに対してプッシュする場合は、プッシュされる設定のすべてのフィールドの値を指定する必要があります。必要に応じて、デフォルト値を使用できます。

WUC外部パラメーター設定のパラメーター

パラメーター	データ型	説明
Domain Name*	文字列	Windowsドメイン名。
Domain User*	文字列	Windowsドメインユーザー名。

WUC外部パラメーター設定のパラメーター(続き)

パラメーター	データ型	説明
Active Directory Host	文字列	Active Directoryサーバーのホスト名 (使用されている場合)。 ◦ 指定する場合は、後続のエントリで、User、User Password、Base DN、Protocol、およびPortの値を指定する必要があります。
Active Directory Use	文字列	ADサーバーのユーザー名。 ◦ Active Directory Hostの値を指定する場合は必須。
Active Directory User Password	文字列	ADサーバーのパスワード。 ◦ Active Directory Hostの値を指定する場合は必須。
Active Directory Base DN	文字列	Active DirectoryのBase DN。 ◦ Active Directory Hostの値を指定する場合は必須。
Active Directory Protocol	文字列	Active Directoryのプロトコル。 ◦ Active Directory Hostの値を指定する場合は必須。
Active Directory Port	文字列	Active Directoryのポート。 ◦ Active Directory Hostの値を指定する場合は必須。
Global Catalog Server	文字列	グローバルカタログサーバーのホスト名 (使用されている場合)。 ◦ 指定する場合は、後続のエントリで、User Name、User Password、およびBase DNの値を指定する必要があります。
Global Catalog User Name	文字列	GCサーバーのユーザー名。 ◦ グローバルカタログサーバーの値を指定する場合は必須。
Global Catalog User Password	文字列	GCサーバーのパスワード。 ◦ グローバルカタログサーバーの値を指定する場合は必須。
Global Catalog Base DN	文字列	GCサーバーのBase DN。 ◦ グローバルカタログサーバーの値を指定する場合は必須。
WEF Collection*	文字列	Windowsイベントフォーマットの収集が有効になっているかどうかを示します。有効な値は次のとおりです。 ◦ Disabled ◦ Enabled (ソースにActive Directoryを使用) ◦ Enabled (ソースにActive Directoryを使用しない) **注:** WEF収集は、コネクターバージョン6.0.6以降でのみサポートされています。それ以外の場合、WUC外部パラメーター設定の準拠状況チェックは常に失敗します。

Windows Unified Connector (WUC) 内部パラメーター設定

WUC内部パラメーターコネクター設定では、1つ以上のWUCコネクターの内部パラメーターを定義します。この設定がターゲットにプッシュされるのは、WUCコネクターが存在する場合のみです。

WUC内部パラメーター設定の制限事項

WUC内部パラメーター設定には、次の制限事項があります。

- ドメインユーザーパスワードは、WUC設定パラメーターとしてサポートされません。ドメインユーザーパスワードは、WUCホストごとに個別に管理する必要があります。
- WUCコネクターはFIPS準拠ではありません。
- WUC設定をArcMCから、ここに示すすべてのフィールドの値がすでに定義されている管理対象ノードに対してプッシュする場合は、プッシュされる設定のすべてのフィールドの値を指定する必要があります。必要に応じて、デフォルト値を使用できます。

WUC内部パラメーター設定のパラメーター

パラメーター	データ型	説明
Enable GUID Translation*	論理型	Trueの場合、グローバルー意識別子の変換が有効になっています。
Enable SID Translation*	論理型	Trueの場合、セキュリティ識別子の変換が有効になっています。
Enable SID Translation Always*	論理型	Trueの場合、Windowsで変換されないイベントにもSID変換が使用されます。
FCP Version	整数	ファイルコントロールプロトコルのバージョン番号。
Global Catalog Port	整数	グローバルカタログサーバーで使用されるポート。
Global Catalog Security Protocol	列挙型	グローバルカタログサーバーで使用されるセキュリティプロトコル。
Host Browsing Threads Sleep Time	整数	ホスト参照クエリ間の時間 (ミリ秒単位)。
Inactivity Sleep Time	整数	設定されたホストから取得されるイベントがない場合にスリープ状態になる時間 (ミリ秒単位)。
Log Rotation Check Interval	整数	ログローテーションのチェックを行う時間間隔 (ミリ秒単位)。
Reconnect Interval	整数	ダウンしていたホストへの接続を再試行する時間間隔 (ミリ秒単位)。

WUC内部パラメーター設定のパラメーター(続き)

パラメーター	データ型	説明
Rotation Retry Count	整数	ログがローテーションされたことをチェックする回数。
Rotation Retry Interval	整数	ローテーションの再試行を行う時間間隔 (ミリ秒単位)。
Sleep Time	整数	ホストから追加イベントの収集を行う前にスリープ状態になる時間 (ミリ秒単位、-1の場合、Sleep Timeは無効)。
Thread Count	整数	コネクターで使用するスレッド数。

ArcMC/コネクターアプライアンス設定のタイプ

ArcMC/コネクターアプライアンス設定では、ソフトウェアArcSight Management Center、ArcSight Management Centerアプライアンス、およびハードウェアまたはソフトウェアのコネクターアプライアンスの設定項目の値を設定します。ここでは、現在利用可能なArcMC/コネクターアプライアンス設定のタイプを示します。

ArcMC/コネクターアプライアンス設定バックアップ設定

ArcMC/コネクターアプライアンス設定バックアップ設定では、ArcSight Management Centerまたはコネクターアプライアンスのスケジュールされた設定バックアップの値を設定します。バックアップコンテンツには、すべてのバックアップデータが含まれます。

プッシュ後に、サブスクライバーでWebプロセスが自動的に再起動されます。

この設定タイプでは、準拠状況の自動チェックは実行されません。準拠状況は手動でチェックする必要があります。

注: 1回限りの設定バックアップに関連する設定値の作成やインポートを行うことはできません。

ArcMC/コネクターアプライアンス設定バックアップのパラメーター

パラメーター	データ型	説明
Backup Server IP Address*	文字列	バックアップが保存されるリモートシステムのIPアドレス。
Port*	整数	リモートシステムのポート。デフォルト値は22です。

ArcMC/コネクターアプライアンス設定バックアップのパラメーター (続き)

パラメーター	データ型	説明
Base Remote Directory*	文字列	リモートシステム上の宛先ディレクトリ。プッシュ前にリモートシステム上に手動で作成する必要があります。プッシュ後、宛先ホスト名がこれに追加され、すべてのノードで一意の値になります。
User*	文字列	宛先のユーザー名。
Password*	文字列	宛先のパスワード(難読化されます)。
Days of the Week*	カンマ区切りの文字列のリスト	バックアップが実行される曜日のカンマ区切りのリスト。有効な値は、Su、M、T、W、Th、F、Saです。
Hours of Day*	カンマ区切りの整数のリスト	バックアップが実行される時間のカンマ区切りのリスト。有効な値は0～23です。ここで、0は深夜12:00です。たとえば、14という値は午後2時に対応します。

通知先設定のタイプ

通知先設定では、コネクター上のESM通知先の設定内容の値を設定します。ここでは、利用可能な通知先設定のタイプを示します。

通知先設定パラメーター

通知先設定パラメーター設定では、通知先設定パラメーターの値と動作を定義します。

注: 通知先設定パラメーター設定は、管理対象コネクターからインポートする必要があります。ArcSight Management Centerでは作成できません。詳細については、「サブスクライバー設定のインポート」(135ページ)を参照してください。

この設定タイプのパラメーターについては、「通知先実行時パラメーター」(299ページ)を参照してください。

ネットワークとゾーン

ネットワークとゾーン設定では、ArcSight ESMのネットワークとゾーンの値と動作を定義します。ESMのネットワークとゾーンの詳細については、ArcSightコンソールのドキュメントを参照してください。

ネットワークとゾーン設定のパラメーター

パラメーター	データ型	説明
Configuration Name*	文字列	設定の名前。

Networks CSV Content*	CSV	CSV (Comma-Separated Values) ファイル。[**Upload**] をクリックして有効なCSVファイルをアップロードするか、[**Download**] をクリックして既存のファイルをダウンロードします。
		CSVファイルの作成
		CSVファイルには、次のリテラルヘッダー行を含める必要があります。
		`#Type,Name,Parent Group URI,Customer URI`
		続いて、各行に1つのネットワークを記述します。各行は次のフィールドの値で構成し、改行コードで終了します。
		`<Type>,<Name>,<Parent Group URI>,<Customer URI>`

Zones CSV Content*	CSV	CSV (Comma-Separated Values) ファイル。[**Upload**] をクリックして有効なCSVファイルをアップロードするか、[**Download**] をクリックして既存のファイルをダウンロードします。
		CSVファイルの作成
		CSVファイルには、次のリテラルヘッダー行を含める必要があります。
		`Name,Start Address,End Address,Parent Group URI,Network URI`
		続いて、各行に1つのゾーンを記述します。各行は次のフィールドの値で構成し、改行コードで終了します。
		`<Name>,<Start Address>,<End Address>,<Parent Group URI>,<Network URI>`

Logger設定のタイプ

Logger設定では、ハードウェアおよびソフトウェアLoggerの設定項目の値を設定します。ここでは、利用可能なLogger設定のタイプを示します。

Logger設定バックアップ設定

Logger設定バックアップ設定では、ハードウェアおよびソフトウェアLoggerのリモートシステムに対するスケジュールされた設定バックアップの値を設定します。

注: 1回限りの設定バックアップに関連する設定値の作成やインポートを行うことはできません。

Logger設定バックアップ設定のパラメーター

パラメーター	データ型	説明
SCP Port*	文字列	リモートシステムのポート。デフォルト値は22です。
Backup Server IP Address*	文字列	バックアップが保存されるリモートシステムのIPアドレス。
Username*	文字列	宛先のユーザー名。
Password*	文字列	宛先のパスワード(難読化されます)。
Base Remote Directory*	文字列	リモートシステム上の宛先ディレクトリ。プッシュ後、宛先ホスト名がこれに追加され、すべてのノードで一意の値になります。
Days of the Week*	カンマ区切りの文字列のリスト	バックアップが実行される曜日のカンマ区切りのリスト。有効な値は、Su、M、T、W、Th、F、Saです。
Hours of Day*	カンマ区切りの整数のリスト	バックアップが実行される時間のカンマ区切りのリスト。有効な値は0～23です。ここで、0は深夜12:00です。たとえば、14という値は午後2時に対応します。
Backup Content*	文字列	バックアップに含めるコンテンツのタイプ。有効な値は次のとおりです。 • All: すべてのバックアップデータが含まれます。 • Report_Content_Only: レポートデータのみが含まれます。

Loggerコネクターフォワーダー設定

Loggerコネクターフォワーダー設定では、1つのLogger (バージョン6.1以降) で1つ以上のコネクターフォワーダーの値を設定します。設定内の各フォワーダーは、それぞれ異なるプロパティで表されます。

注: Loggerコネクターフォワーダー設定は、管理対象Loggerからインポートする必要があります。ArcSight Management Centerでは作成できません。詳細については、「サブスクライバー設定のインポート」(135ページ)を参照してください。

Loggerコネクターフォワーダー設定のパラメーター

パラメーター	データ型	説明
Forwarder Name*	文字列	フォワーダーの表示名。
Filter Type*	列挙型	Loggerでフォワーダーを作成する際に選択されたフィルタータイプ。有効な値は、UnifiedまたはRegexです。
Query	文字列	フォワーダーが転送するイベントをフィルター処理するのに使用します。

Loggerコネクターフォワーダー設定のパラメーター (続き)

パラメーター	データ型	説明
Unified Query Filters	文字列	ソースLoggerのデフォルトおよびユーザー定義のUnifiedフィルターから選択します。フィルタータイプがUnifiedの場合にのみ表示されます。
Regular Expression Filters	文字列	ソースLoggerのデフォルトおよびユーザー定義のRegexフィルターから選択します。フィルタータイプがRegexの場合にのみ表示されます。
Start Time	日付と時刻	時間範囲を指定する場合の開始時刻 (オプション)。
End Time	日付と時刻	時間範囲を指定する場合の終了時刻 (オプション)。
IP/Host*	文字列	転送されたイベントを受信する通知先のIPアドレスまたはホスト名。
Port*	整数	転送されたイベントを受信する通知先のポート番号。通知先でこのポートを開いておく必要があります。
Enable*	論理型	[**Yes**] の場合、フォワーダーが有効になっています。
Connection Retry Timeout*	整数	接続を再試行するまでの待機時間 (秒単位)。
Source Type*	整数	ソースタイプ。有効な値は次のとおりです。 • Apache HTTP Server Access • Apache HTTP Server Error • IBM DB2 Audit • Juniper Steel-Belted Radius • Microsoft DHCP Log • Other

Logger ESMフォワーダー設定

Logger ESMフォワーダー設定では、1つのLogger (バージョン6.1以降) で1つ以上のESM通知先の値を設定します。設定内の各通知先は、それぞれ異なるプロパティで表されます。

注: Logger ESMフォワーダー設定は、管理対象Loggerからインポートする必要があります。ArcSight Management Centerでは作成できません。詳細については、「サブスクライバー設定のインポート」(135ページ)を参照してください。

Logger ESMフォワーダーのパラメーター

パラメーター	データ型	説明
Forwarder Name*	文字列	フォワーダーの表示名。
Filter Type*	列挙型	Loggerでフォワーダーを作成する際に選択されたフィルタータイプ。有効な値は、UnifiedまたはRegexです。

Logger ESMフォワーダーのパラメーター (続き)

パラメーター	データ型	説明
Query	文字列	フォワーダーが転送するイベントをフィルター処理するのに使用します。
Unified Query Filters	文字列	ソースLoggerのデフォルトおよびユーザー定義のUnifiedフィルターから選択します。フィルタータイプがUnifiedの場合にのみ表示されます。
Regular Expression Filters	文字列	ソースLoggerのデフォルトおよびユーザー定義のRegexフィルターから選択します。フィルタータイプがRegexの場合にのみ表示されます。
Start Time	日付と時刻	時間範囲を指定する場合の開始時刻。
End Time	日付と時刻	時間範囲を指定する場合の終了時刻。
IP/Host*	文字列	転送されたイベントを受信する通知先のIPアドレスまたはホスト名。
Port*	整数	転送されたイベントを受信する通知先のポート番号。通知先でこのポートを開いておく必要があります。
Enable	論理型	[**Yes**] の場合、フォワーダーが有効になっています。

Loggerフィルター設定

Loggerフィルター設定では、1つのLoggerで1つ以上の保存された検索の値を設定します。

設定内の各フィルターは、それぞれ異なるプロパティで表されます。

注: Loggerフィルター設定は、管理対象Loggerからインポートする必要があります。ArcSight Management Centerでは作成できません。詳細については、「サブスクライバー設定のインポート」(135ページ) を参照してください。

Loggerフィルター設定のパラメーター

パラメーター	データ型	説明
Filter Name*	文字列 (読み取り専用)	フィルターの名前。
Filter Category	文字列	フィルターのカテゴリ。有効な値は、Shared、System、およびSearchGroupです。

Loggerフィルター設定のパラメーター (続き)

パラメーター	データ型	説明
Filter Type*	文字列	フィルターのタイプ。有効な値は、RegexQueryまたはUnifiedQueryです。
Query*	文字列	クエリ文字列。
Permission Group	文字列	Loggerフィルターが関連付けられている権限グループ。設定をプッシュすると、次の処理が行われます。 • 権限グループがターゲットLogger上に存在しない場合、プッシュ中に権限グループが作成されます。 • ターゲット上に同じ名前の権限グループがすでに存在しているが、所有している権限が異なる場合、ターゲットLogger上の権限グループの権限は上書きされず、フィルターと権限グループの間の関連付けが削除されます。

Logger SmartMessageレシーバー設定

Logger SmartMessageレシーバー設定では、1つ以上のSmartMessageレシーバーの値を設定します。

SmartMessageレシーバー設定をターゲットにプッシュすると、ターゲット上の既存のSmartMessageレシーバーが上書きされます。UDPやTCPなどの他の種類のレシーバーは影響を受けません。

Logger SmartMessageレシーバー設定のパラメーター

パラメーター	データ型	説明
Receiver Name*	文字列	レシーバーの名前。
Enabled*	論理型	**[Yes]** の場合、SmartMessageの受信が有効になっています。
Encoding*	文字列	エンコーディングのタイプ。有効な値は次のとおりです。 • `UTF-8` • `US-ASCII`

Loggerストレージグループ設定

Loggerストレージグループ設定では、1つ以上のLoggerストレージグループの値を設定します。

注: Loggerストレージグループ設定は、管理対象Loggerからインポートする必要があります。ArcSight Management Centerでは作成できません。詳細については、「サブスクライ

バー設定のインポート」(135ページ)を参照してください。

Loggerストレージグループ設定のパラメーター

パラメーター	データ型	説明
Storage Group Name*	文字列 (読み取り専用)	ストレージグループの名前。 • プッシュされる設定には、Loggerで設定されているのと同じ数のストレージグループが含まれている必要があります。 • プッシュされる設定内のストレージグループの名前は、Logger上のストレージグループの名前と一致している必要があります。
Maximum Age (Days)*	整数	ストレージ内のイベントの最大経過日数。
Maximum Size (GB)*	整数	ストレージグループの最大サイズ (ギガバイト)。 • すべてのストレージグループの累計サイズが、Loggerのストレージボリュームサイズを上回ることはできません。

Logger TCPフォワーダー設定

Logger TCPフォワーダー設定では、1つのLogger (バージョン6.1以降) で1つ以上のTCPフォワーダーの値を設定します。設定内の各フォワーダーは、それぞれ異なるプロパティで表されます。

注: Logger TCPフォワーダー設定は、管理対象Loggerからインポートする必要があります。ArcSight Management Centerでは作成できません。詳細については、「サブスクライバー設定のインポート」(135ページ)を参照してください。

Logger TCPフォワーダー設定のパラメーター

パラメーター	データ型	説明
Forwarder Name*	文字列	フォワーダーの表示名。
Filter Type*	列挙型	Loggerでフォワーダーを作成する際に選択されたフィルタータイプ。有効な値は、UnifiedまたはRegexです。
Query	文字列	フォワーダーが転送するイベントをフィルター処理するのに使用します。
Unified Query Filters	文字列	ソースLoggerのデフォルトおよびユーザー定義のUnifiedフィルターから選択します。フィルタータイプがUnifiedの場合にのみ表示されます。
Regular Expression Filters	文字列	ソースLoggerのデフォルトおよびユーザー定義のRegexフィルターから選択します。フィルタータイプがRegexの場合にのみ表示されます。
Start Time	日付と時刻	時間範囲を指定する場合の開始時刻 (オプション)。

Logger TCPフォワーダー設定のパラメーター (続き)

パラメーター	データ型	説明
End Time	日付と時刻	時間範囲を指定する場合の終了時刻 (オプション)。
IP/Host*	文字列	転送されたイベントを受信する通知先のIPアドレスまたはホスト名。
Port*	整数	転送されたイベントを受信する通知先のポート番号。通知先でこのポートを開いておく必要があります。
Enable*	論理型	[**Yes**] の場合、フォワーダーが有効になっています。
Preserve System Timestamp*	論理型	[**Yes**] の場合、元のイベント受信時刻を示すタイムスタンプが保持されます。
Preserve Original Syslog Sender*	論理型	[**Yes**] の場合、syslogイベントのホスト名 (またはそれに相当する) フィールドにLoggerのIPアドレスを挿入せずに、イベントがそのまま送信されます。
Connection Retry Timeout*	整数	接続を再試行するまでの待機時間 (秒単位)。

Loggerトランスポートレシーバー設定

Loggerトランスポートレシーバー設定では、1つ以上のUDP、TCP、CEF UDP、またはCEF TCPレシーバーの値を設定します。

注: Loggerのドキュメントでは、トランスポートレシーバーを単に「レシーバー」と呼んでいます。

トランスポートレシーバータイプの設定をプッシュすると、既存のUDP、TCP、CEF UDP、またはCEF TCPレシーバーはすべて上書きされます。SmartMessageレシーバーなど、その他の種類のレシーバーは影響を受けません。

Loggerトランスポートレシーバー設定のパラメーター

パラメーター	データ型	説明
Receiver Name*	文字列	レシーバーの名前。
Receiver Type*	文字列	レシーバーのタイプ。有効な値は次のとおりです。 • UDP • TCP • CEF UDP • CEF TCP
Receiver Name*	文字列	レシーバーの名前。

Loggerトランスポートレシーバー設定のパラメーター(続き)

パラメーター	データ型	説明
Port*	整数	ポート番号。ゼロ以外の正の数値である必要があります。通知先でこのポートを開いておく必要があります。
Enabled*	論理型	[**Yes**] の場合、トランスポートの受信が有効になっています。
Encoding*	文字列	エンコーディングのタイプ。有効な値は次のとおりです。 • UTF-8 • Shift_JIS • EUC-JP • EUC-KR • US-ASCII • GB2312 • UTF-16BE • Big5 • GB18030 • ISO-8859-1 • Windows-1252 CEF UDPおよびCEF TCPレシーバーの場合は、UTF-8とUS-ASCIIのみが適用されます。 **注意:** CEFレシーバーで正しくないエンコーディングを選択すると、プッシュが失敗する原因になります。

Logger UDPフォワーダー設定

Logger UDPフォワーダー設定では、1つのLoggerで1つ以上のUDPフォワーダーの値を設定します。設定内の各フォワーダーは、それぞれ異なるプロパティで表されます。

注: Logger UDPフォワーダー設定は、管理対象のLoggerからインポートする必要があります。ArcSight Management Centerでは作成できません。詳細については、「サブスクライバー設定のインポート」(135ページ)を参照してください。

Logger UDPフォワーダー設定のパラメーター

パラメーター	データ型	説明
Forwarder Name*	文字列	フォワーダーの表示名。
Filter Type*	列挙型	Loggerでフォワーダーを作成する際に選択されたフィルタータイプ。有効な値は、UnifiedまたはRegexです。

Logger UDPフォワーダー設定のパラメーター (続き)

パラメーター	データ型	説明
Query	文字列	フォワーダーが転送するイベントをフィルター処理するのに使用します。
Unified Query Filters	文字列	ソースLoggerのデフォルトおよびユーザー定義のUnifiedフィルターから選択します。フィルタータイプがUnifiedの場合にのみ表示されます。
Regular Expression Filters	文字列	ソースLoggerのデフォルトおよびユーザー定義のRegexフィルターから選択します。フィルタータイプがRegexの場合にのみ表示されます。
Start Time	日付と時刻	時間範囲を指定する場合の開始時刻 (オプション)。
End Time	日付と時刻	時間範囲を指定する場合の終了時刻 (オプション)。
IP/Host*	文字列	転送されたイベントを受信する通知先のIPアドレスまたはホスト名。
Port*	整数	転送されたイベントを受信する通知先のポート番号。通知先でこのポートを開いておく必要があります。
Enable*	論理型	[**Yes**] の場合、フォワーダーが有効になっています。
Preserve System Timestamp*	論理型	[**Yes**] の場合、元のイベント受信時刻を示すタイムスタンプが保持されます。
Preserve Original Syslog Sender*	論理型	[**Yes**] の場合、syslogイベントのホスト名 (またはそれに相当する) フィールドにLoggerのIPアドレスを挿入せずに、イベントがそのまま送信されます。

システム管理設定のタイプ

システム管理設定では、システム管理用設定項目の値を設定します。ここでは、利用可能なシステム管理設定のタイプを示します。

外部認証

外部認証設定では、LDAPやRADIUSなどの、外部サーバーとの認証を必要とするハードウェアまたはソフトウェアシステムの値と動作を定義します。

ホスト上で認証メソッドを変更した場合は、ArcSight Management Centerからホストを削除してから、ノード管理を使用して再度追加する必要があります。

注: 外部認証設定は、管理対象Loggerからインポートする必要があります。ArcSight Management Centerでは作成できません。詳細については、「サブスクライバー設定のインポート」(135ページ) を参照してください。

外部認証設定のパラメーター

パラメーター	データ型	説明
Authentication Method*	文字列	システムの認証メソッド。
Allow Local Password Fallback for Default Admin Only*	論理型	[**Yes**] の場合、管理者の認証で認証サーバーがローカルパスワードにフォールバックします。
Allow Local Password Fallback for All Users*	論理型	[**Yes**] の場合、すべてのユーザーの認証で認証サーバーがローカルパスワードにフォールバックします。
LDAP Server Hostname[port]*	文字列	LDAPサーバーのホスト名とポート。
LDAP Backup Server Hostname [port]	文字列	LDAPバックアップサーバーのホスト名とポート。
LDAP Server Request Timeout (seconds)	整数	LDAPサーバーの要求タイムアウト (秒)。
RADIUS Server Hostname [port]	文字列	RADIUSサーバーのホスト名とポート。
RADIUS Backup Server Hostname[port]	文字列	RADIUSバックアップサーバーのホスト名とポート。
RADIUS Shared Authentication Secret	文字列	RADIUS認証の共有シークレット。
RADIUS Server NAS IP Address	文字列	RADIUSサーバーのNAS (Network Access Server) のIPアドレス。
RADIUS Request Timeout (seconds)	整数	RADIUSサーバーの要求タイムアウト (秒)。
RADIUS Retry Request	整数	RADIUSサーバーの要求を再試行する回数。
RADIUS Protocol	文字列	RADIUSプロトコルのタイプ。

認証ローカルパスワード

認証ローカルパスワード設定では、ハードウェアまたはソフトウェアシステムのローカルパスワードのオプションと動作を定義します。

認証ローカルパスワード設定のパラメーター

パラメーター	データ型	説明
Enable Account Lockout*	論理型	[**Yes**] の場合、間違ったパスワードを入力すると、アカウントロックアウトが有効になります。
Lock Out Account after N Failed Attempts*	整数	ロックアウト前の認証失敗回数。

認証ローカルパスワード設定のパラメーター (続き)

パラメーター	データ型	説明
Remember Failed Attempts For (seconds)*	整数	ロックアウトをトリガーする認証失敗の時間間隔 (秒)。
Lockout Account for (minutes)*	整数	アカウントをロックアウト状態にする時間 (分)。
Enable Password Expiration*	論理型	[**Yes**] の場合、パスワードの有効期限が有効です。
Password Expires in (days)*	整数	パスワードが期限切れになる間隔 (日数)。
Notify User (Days Before Expiration)*	整数	ユーザーに通知するパスワード有効期限前の日数。
Users Exempted from Password Expiration Policy	カンマ区切りの文字列のリスト	パスワードが期限切れにならないユーザーのカンマ区切りのリスト。
Enforce Password Strength*	論理型	[**Yes**] の場合、強いパスワードが強制されます。
Minimum Length (characters)*	整数	パスワードの最小文字数。
Maximum Length (characters)*	整数	パスワードの最大文字数。
Numeric [0-9]*	整数	パスワード内の数字の最小文字数。
Upper Case [A-Z]*	整数	パスワード内の大文字の最小文字数。
Lower Case [a-z]*	整数	パスワード内の小文字の最小文字数。
Special [1$^*...]*	整数	パスワード内の特殊文字の最小文字数。
Password Must Be At Least*	整数	新しいパスワードと前のパスワードで異なっている必要のある最小文字数。
Include “Forgot Password” link on Login Screen*	論理型	[**Yes**] の場合、ユーザーがパスワードを回復するためのリンクを提供します。

認証セッション

認証セッション設定では、ハードウェアまたはソフトウェアシステムの認証セッションの値を定義します。

認証セッション設定のパラメーター

パラメーター	データ型	説明
Max Simultaneous Logins Per User*	整数	ユーザーあたりの同時ログインの最大数。
Logout Inactive Session After (seconds)*	整数	非アクティブなセッションのタイムアウト (秒)。
Disable Inactive Account After (days)*	整数	アカウントが無効になるまでの非アクティブな日数。

DNS設定

DNS設定では、ハードウェアアプライアンスのドメインネームサービスの値を定義します。

DNS設定のパラメーター

パラメーター	データ型	説明
Primary DNS*	文字列	プライマリDNSサーバー。
Secondary DNS	文字列	セカンダリDNSサーバー。
DNS Search Domains	カンマ区切りの文字列のリスト	DNS検索ドメインのカンマ区切りのリスト。

FIPS設定

FIPS設定では、管理対象ノードでFIPSモードを有効または無効にします。

FIPS設定をプッシュすると、プッシュ先のノードが再起動されます。

FIPS設定のパラメーター

パラメーター	データ型	説明
Enabled*	論理型	[**Yes**] の場合、ノードでFIPSが有効になっています。

ネットワーク設定

ネットワーク設定では、ハードウェアアプライアンスのデフォルトゲートウェイ設定の値を定義します。

注: ArcSight Management Centerを使用して、次のネットワーク設定の値を変更することはできません: ホスト名、ネットワークインターフェイスのIPアドレス、静的ルート、/etc/hostsファイル、時間設定

ネットワーク設定のパラメーター

パラメーター	データ型	説明
Default Gateway*	文字列	ネットワークのデフォルトゲートウェイ。

NTP設定

NTP設定では、ハードウェアアプライアンスのNTP (ネットワークタイムプロトコル) の値を定義します。

NTP設定のパラメーター

パラメーター	データ型	説明
Enable as NTP Server*	論理型	[**Yes**] の場合、システムはNTPサーバーとして有効です。
NTP Servers*	カンマ区切りの文字列のリスト	カンマ区切りのNTPサーバーのリスト。[**Enable as NTP Server**] がFalseの場合でも必要です。

SMTP設定

SMTP設定では、ハードウェアまたはソフトウェアシステムのSMTP (Simple Mail Transfer Protocol) の値を定義します。

SMTP設定のパラメーター

パラメーター	データ型	説明
Primary SMTP Server*	文字列	プライマリSMTPサーバー。
Secondary SMTP Server	文字列	セカンダリSMTPサーバー。
Outgoing Email Address*	文字列	送信メールアドレス。

SNMPポーリング設定

SNMPポーリング設定では、ハードウェアアプライアンスのSNMP (Simple Network Management Protocol) 監視の値を定義します。ArcMCは、SNMPのv2cおよびv3をサポートしています。

SNMPポーリング設定のパラメーター

パラメーター	データ型	説明
Status	論理型	[**Yes**] の場合、SNMPポーリングが有効です。
Port*	整数	SNMPポート。
SNMP Version*	文字列	サポートされるSNMPのバージョン。有効な値は、v2cおよびv3です。
Community String	文字列	SNMPコミュニティ文字列。v2cの場合のみ必要。
Username	文字列	認証ユーザー名。v3の場合のみ必要。
Authentication Protocol*	文字列	認証プロトコル。有効な値は、MD5およびSHAです。v3の場合のみ必要。
Authentication Passphrase	文字列	認証パスフレーズ。v3の場合のみ必要。
Privacy Protocol	文字列	プライバシープロトコル。有効な値は、DESおよびAES128です。v3の場合のみ必要。

SNMPポーリング設定のパラメーター (続き)

パラメーター	データ型	説明
Privacy Passphrase	文字列	プライバシーパスフレーズ。v3の場合のみ必要。
System Name	文字列	SNMPシステムの名前。
Point of Contact	文字列	コンタクトポイント。
Location	文字列	システムロケーション。

SNMPトラップ設定

SNMPトラップ設定では、ハードウェアアプライアンスのSNMP (Simple Network Management Protocol) 通知の値を定義します。ArcMCは、SNMPのv2cおよびv3をサポートしています。

以前のバージョンのArcMCでは、SNMPトラップ設定はSNMP設定と呼ばれていました。

SNMPトラップ設定のパラメーター

パラメーター	データ型	説明
Status	論理型	[**Yes**] の場合、SNMPポーリングが有効です。
NMS IP Address	文字列	ネットワーク管理サーバーのIPアドレス。
Port*	整数	SNMPポート。
SNMP Version*	文字列	サポートされるSNMPのバージョン。有効な値は、v2cおよびv3です。
Community String	文字列	SNMPコミュニティ文字列。v2cの場合のみ必要。
Username	文字列	認証ユーザー名。v3の場合のみ必要。
Authentication Protocol*	文字列	認証プロトコル。有効な値は、MD5およびSHAです。v3の場合のみ必要。
Authentication Passphrase	文字列	認証パスフレーズ。v3の場合のみ必要。
Privacy Protocol	文字列	プライバシープロトコル。有効な値は、DESおよびAES128です。v3の場合のみ必要。
Privacy Passphrase	文字列	プライバシーパスフレーズ。v3の場合のみ必要。

初期設定管理

初期設定は、同じモデル番号およびソフトウェアバージョンの複数のHPE ArcSight Loggerで、同じセットアップをすばやく行うためのものです。初期設定は、Loggerの本番環境への初

期展開をすばやく行うのに使用します。初期設定管理は、Loggerバージョン6.1以降でサポートされます。

初期設定の作成は、ArcMCでは行いません。管理対象Loggerで適切な初期設定を作成し、それをArcMCにインポートします。その後、インポートした設定を、モデルとソフトウェアバージョン番号が同じ他の管理対象Loggerにプッシュすることができます。

初期設定ごとに以下の属性が表示されます。

属性	説明
Imported Init-Config Name	インポートされた初期設定の名前。
Product Type	設定をプッシュできるLoggerのタイプ: Logger (アプライアンス) またはSWLogger (ソフトウェア)
Source Host	設定のインポート元のホストのIPアドレス。
Imported On	インポートの日付。
Imported By	設定をインポートしたユーザー。
SW Version	設定のソフトウェアバージョン。
Source Model	アプライアンスの場合、ソースホストLoggerのモデル番号 (ソフトウェアLoggerの場合は、ここに「Software」と表示される)。

以下の初期設定管理タスクを実行できます。

- 初期設定をインポートする
- 初期設定をプッシュする
- 初期設定のイベント履歴を表示する
- 初期設定を削除する

初期設定のインポート

管理対象Logger (バージョン6.1以降) で作成した初期設定は、ArcSight Management Centerにインポートして、編集を行ったり、他のLoggerにプッシュしたりすることができます。

ArcMCでは、最大30個の初期設定を保存できます。

バージョン6.1以降のLoggerから初期設定をインポートするには

1. **[Configuration Management] > [Other Configurations] > [Logger Configurations]** をクリックします。
2. [**Configurations**] で、[**Import**] をクリックします。

3. [**Import Initial Configuration**] ダイアログの [**Name**] に、インポートする設定の名前を入力します。
4. [**Source Host URI**] で、設定のインポート元のノードを選択します。
5. [**Import**] をクリックします。設定がArcSight Management Centerにインポートされ、[**Configurations**] テーブルに表示されます。
6. オプションで、インポートした設定を管理対象ノードにプッシュする場合は、プッシュするかどうかを確認するプロンプトが表示されたときに、[**Yes**] をクリックします。

初期設定の作成は、ArcMCでは行いません。代わりに、管理対象Loggerで初期設定を作成し、それをArcMCにインポートして別の管理対象Loggerにプッシュします。

初期設定のプッシュ

バージョン6.1以降の選択した管理対象Loggerに、初期設定をプッシュすることができます。プッシュ先のLoggerは、初期設定を作成したLoggerと同じソフトウェアバージョン (ハードウェアアプライアンスの場合は、モデル番号も同じ) である必要があります。

プッシュを行うと、プッシュ先のLoggerの設定内容が上書きされます。

初期設定のプッシュは、手動で行う必要があります。

プッシュを行う前に、プッシュ先のLoggerのストレージボリュームがセットアップされ、ソースLoggerのストレージボリュームを上回っていることを確認します。

バージョン6.1以降の1つ以上の管理対象Loggerに初期設定をプッシュするには

1. **[Configuration Management] > [Other Configurations] > [Logger Configurations]** をクリックします。
2. [**Configurations**] テーブルで、プッシュする設定を選択します。
3. [**Push**] をクリックします。
4. [**Make Selections for Push**] ダイアログの、[**Available Nodes**] に、プッシュを受け取る対象となっているノードがロケーション別に表示されます。プッシュを受信するノードを参照し、[**Add**] をクリックします。選択したノードは、[**Selected Nodes**] に表示されます。(プッシュを受信する複数のノードを選択する場合は、Ctrlキー+クリックを使用して各ノードを選択します。)
5. [**Push**] をクリックします。
6. [**Yes**] をクリックして、プッシュを確認し、プッシュ先の設定内容を変更します。設定が、選択したプッシュ先ノードにプッシュされます。

プッシュステータスを正しく表示するため、ステータスが [In Progress] と表示されている場合でも、[**Refresh**] をクリックしてください。

プッシュ先Loggerのプッシュ結果

プッシュ先Loggerの設定に初期設定をプッシュした結果は、次の表に示すように、設定項目によって異なります。

プッシュ先の設定	プッシュ後の結果
• アーカイブストレージの設定 • 監査ログ • ESM通知先 • イベントアーカイブ • 完了したタスク • フォワーダー • ピアLogger	**空白:** プッシュされた初期設定に含まれている場合でも、これらの設定項目は空白になります。また、これらの設定項目に関連するプッシュ先Loggerのすべての設定も空白になります。
• アラート • ユーザーが作成したレシーバー(RFSファイルレシーバー、ファイル転送、フォルダーフォロワーレシーバー)	**無効:** これらの設定項目は、プッシュ先Loggerで無効になりますが、プッシュ先LoggerのUIで編集可能です。
• hostsファイル • グループ • ユーザー	**ソースからコピー:** これらの値は、初期設定からコピーされ、ターゲット上で上書きされます。 これには、LoggerがArcMCに対する認証に使用するユーザー資格情報が含まれることがあります。この場合、ArcMCと(これらの資格情報を必要とする)プッシュ先Loggerとの間の管理リンクが失われる可能性があります。これらの資格情報が上書きされた場合、管理を有効にするには、ArcMCからそのホストを削除した後に、(新しい資格情報を使用して)Loggerをホストとして追加し直します。
• 他のすべての設定	**ソースからコピー:** 値は初期設定からコピーされ、ターゲット上で上書きされます。

初期設定の削除

削除した初期設定は、プッシュには使用できなくなります。現在プッシュ中の設定を削除することはできません。

初期設定を削除するには

1. **[Configuration Management] > [Other Configurations] > [Logger Configurations]** をクリックします。
2. [**Logger Configurations**] テーブルで、削除する設定を1つ以上選択します。
3. [**Delete**] をクリックします。
4. [**Yes**] をクリックして削除を確定します。

イベント履歴

[**Event History**] リストには、初期設定のプッシュに関連するすべてのインポート、プッシュ、および削除トランザクションが記録されます。履歴のイベントごとに、以下の情報が表示されます。

カラム	説明
Init-Config Name	初期設定の名前。
Author	アクションを実行したユーザー。
Event Type	初期設定に関して記録されたイベントのタイプ。イベントのタイプには、Push、Import、およびDeleteがあります。
Event Occurrence	イベントのローカル日付と時刻。
Source Host	初期設定が作成されたホストのURI。
Destination URI for Push	イベントタイプがPushの場合、これは初期設定がプッシュされたプッシュ先ノードのURIになります。
Event Status	イベントのステータス。ステータスのタイプには、以下が含まれます。 • In-progress: トランザクションが進行中です。 • Successful: トランザクションが成功しました。 • Failed: トランザクションが失敗しました。失敗したステータスをクリックすると、失敗の理由を示す内容が表示されます。

これらの条件のいずれかを基準に特定のイベントを検索するには、対応するカラムヘッダーのドロップダウンをクリックします。続いて、[**Filters**] で、イベントを表示する条件を選択または入力します。フィルターと一致するイベントのみが、[**Event History**] リストに表示されます。

たとえば、すべてのプッシュを表示するには、[**Event Type**] カラムで、ヘッダーのドロップダウンをクリックします。続いて、[**Filters**] で、「Push」を選択します。

Loggerイベントアーカイブの管理

Loggerイベントアーカイブを使用すると、現在の日を含まない過去の任意の日のイベントを保存できます。ArcMCでは、管理対象LoggerでLoggerイベントアーカイブを表示し、アーカイブのロード、アンロード、およびインデックス作成などの管理タスクを実行できます。

Loggerイベントアーカイブの管理は、バージョン6.2以降の管理対象Loggerでのみ使用できます。

Loggerイベントアーカイブの管理の詳細については、『Logger管理者ガイド』を参照してください。

以下のパラメーターが、Loggerイベントアーカイブのリストに表示されます。

パラメーター	説明
Peers	Loggerに対して、Loggerのピアの数。Loggerのピアを詳しく表示するには、表示された数値をクリックします。
Event Status	現在のアーカイブジョブのステータス。ステータスは次のいずれかの値になります。 • Loading: 管理対象のLoggerでアーカイブをロード中です。 • Loaded: 管理対象のLoggerでアーカイブが現在ロードされています。 • Unloading: アーカイブジョブが現在実行中です。 • Archived: アーカイブジョブが完了しました。 • Failed: アーカイブジョブが失敗しました。
Index Status	現在のインデックス作成ジョブのステータス。ステータスは次のいずれかの値になります。 • None: インデックス作成ステータスが利用できません。 • Pending: インデックス作成ジョブが間もなく開始されます。テーブルの [**Cancel**] カラムをクリックすると、保留中のジョブをキャンセルできます。 • Indexing: インデックス作成ジョブが進行中です。 • Indexed: インデックス作成ジョブが完了しました。 • Failed: インデックス作成ジョブが失敗しました。
Cancel	保留中のインデックス作成ジョブを開始せずにキャンセルする場合は、[**X**] をクリックします。

Loggerイベントアーカイブを表示するには

1. [**Configuration Management**] で、**[Other Configurations] > [Logger Event Archive]** を選択します。
2. [**Event Archive List**] タブで、管理対象LoggerでのLoggerイベントアーカイブの検索に使用する条件を選択します。
3. 開始日と終了日を選択し、検索する1つ以上のLoggerを選択します。

4. **[Search]** をクリックします。検索条件と一致するすべてのLoggerイベントアーカイブが、管理対象Logger別、ストレージグループ別、およびイベントアーカイブ別の順に、階層形式で表示されます。

表示を開く/閉じるには、[**Expand**] または [**Collapse**] をクリックします。

イベントアーカイブの管理

管理対象のLoggerで、アーカイブのロード (またはアンロード) およびアーカイブのインデックス作成という、イベントアーカイブに関連する2つの管理タスクを実行できます。

イベントアーカイブをロードするには

1. イベントアーカイブリストで、ロードするアーカイブを選択します。
2. [**Load Archive**] をクリックします。選択した操作が実行されます。ジョブのステータスが [**Event Status**] カラムに表示されます。

イベントアーカイブのインデックスを作成するには

1. イベントアーカイブリストで、インデックスを作成するアーカイブを選択します。
2. [**Index Archive**] をクリックします。選択したアーカイブのインデックスが作成されます。インデックス作成ジョブのステータスが [**Index Status**] カラムに表示されます。

ロード/アンロード履歴の表示

Loggerイベントアーカイブのロード、アンロード、およびインデックス作成の履歴を表示することもできます。履歴の表示では、Loggerイベントアーカイブを表示するのにArcMCで実行されたアクションが表示されます。

Loggerイベントアーカイブのロード/アンロード履歴を表示するには

1. [**Configuration Management**] で、**[Initial Configurations] > [Logger Event Archive]** を選択します。
2. [**Archive Load/Unload History**] タブをクリックします。アクティビティの履歴が表示されます。

Loggerピアの管理

管理対象のLoggerは、任意の数の他のLoggerとピアリングできます。Logger間のピア関係はArcMCで管理できます。HPE ArcSightでは、可能な場合はすべてのピアLoggerをArcMCで管理することを推奨しています。

ピアの表示、Loggerに対するピアの追加または削除、ピアグループのインポート、編集、プッシュ、および削除を行うことができます。ピアグループは、複数のLoggerをまとめて管理しやすいように一連のLoggerに名前を付けたものです。

Loggerピアリングの詳細については、『HPE ArcSight Logger管理者ガイド』を参照してください。

ピアまたはピアグループの表示

Loggerがバージョン6.1以降である場合、ArcMCで管理されているLoggerのピアを表示できます。

ピアリングされたLoggerをArcMCで表示するには

1. **[Configuration Management] > [Manage Logger Peers]** を選択します。[**Manage Peer Loggers**] テーブルに、バージョン6.1以降のすべての管理対象のLoggerが表示されます。
2. リスト内の特定のLoggerとピアリングされているLoggerを表示するには、[**Peer Loggers**] カラムで、ピア数を示すリンクをクリックします。フィルタリング可能な [**Peer Loggers**] ダイアログに、Loggerのすべてのピアが表示されます。
3. ArcMCでピアグループを表示するには、[**View Peer Groups**] をクリックします。

ピアの追加または削除

管理対象のLoggerがバージョン6.1以降である場合、ArcMCで管理されているLoggerに対して、ピアの追加または削除を行うことができます。

ArcMCによってピアとして管理されていないLoggerを削除した場合、そのLoggerを含むピアグループをArcMCにインポートするか、削除したLoggerをArcMCの管理に追加しない限り、そのLoggerを再度グループに追加することはできません。

Loggerに対して、ピアの追加または削除を行うには

1. [**Manage Logger Peers**] テーブルから、ピアを編集するLoggerを選択します。
2. [**Edit Peers**] をクリックします。
3. 現在ピアリングされているすべてのLoggerが表示されます。
   a. 1つ以上のピアを追加するには、[**Add Peers**] をクリックします。次に、[**Add Peers**] ダイアログで、ピアとして追加するLoggerを選択します。オプションで、ArcMCで新しいピアグループを作成するには、[**Peer Group Name**] にピアグループの名前を入力します。続いて、[**Add**] をクリックします。

b. ピアである1つ以上のLoggerを削除するには、削除するLoggerを選択し、[**Remove Peers**] をクリックします。[**Yes**] をクリックしてピアの削除を確定します。

このリリースでは、認証コードではなく、ユーザー名とパスワードを使用してLoggerのピアリングがサポートされます。

ピアグループのインポート

LoggerのピアグループをArcMCにインポートできます。ピアグループのインポートは、バージョン6.1以降のLoggerでのみサポートされます。

Logger (バージョン6.1以降) からピアグループをインポートするには

1. **[Configuration Management] > [Manage Logger Peers]** を選択します。
2. [**View Peer Groups**] をクリックします。
3. [**Import Peers**] をクリックします。
4. [**Select Peer**] ダイアログで、管理対象のLoggerを選択します (選択したLoggerもインポートしたピアグループの一部になります)。次に、[**Next**] をクリックします。
5. [**Select Peer (of the Target)**] ダイアログで、ArcMCにインポートする1つ以上のピアを選択します。
6. [**Peer Group Name**] に、選択したピアグループの名前を入力します。
7. [**Import**] をクリックします。選択したピアグループがArcMCにインポートされます。

ピアグループの編集

名前、ピアリングされたLoggerホスト名、およびグループのメンバーなど、ピアグループの編集を行うことができます。

ピアグループを編集するには

1. **[Configuration Management] > [Manage Logger Peers]** を選択します。
2. [**View Peer Groups**] をクリックします。
3. 編集するピアグループの名前をクリックします。
4. [**Edit Peer Group**] ダイアログで、必要に応じてピアグループを編集します。ピアグループ名の編集や、グループに対するピアの追加や削除を行うことができます。
5. [**Save**] をクリックします。あるいは、[**Save As...**] をクリックして、ピアグループに別の名前を付けて保存します。

ピアグループのプッシュ

バージョン6.1以降の1つまたは複数の管理対象Loggerに対して、ピアグループをプッシュすることができます。ピアグループ内のLoggerは、ピアグループのプッシュ先の管理対象のLoggerとピアリングされます。

ピアグループをプッシュするには

1. **[Configuration Management] > [Manage Logger Peers]** をクリックします。
2. [**View Peer Groups**] をクリックします。
3. テーブルから、プッシュするピアグループを選択します。
4. [**Push**] をクリックします。
5. [**Destination Loggers**] ダイアログで、ピアグループをプッシュするプッシュ先のLoggerを1つ以上選択します。
6. [**Push**] をクリックします。ピアグループがプッシュ先のLoggerに対してプッシュされます。

ピアグループの削除

ピアグループをArcMCから削除できます。

ピアグループを削除するには

1. **[Configuration Management] > [Manage Logger Peers]** をクリックします。
2. [**View Peer Groups**] をクリックします。
3. ピアグループのリストから、削除するグループを1つ選択します。
4. [**OK**] をクリックして削除を確定します。

Event Brokerの管理

ArcMCを使用すると、Event Brokerの管理と監視を行うことができます。これらの機能には、トピックの追加、ルートの管理、およびステータス監視などが含まれます。

トピックについて

トピックとは、イベントを分類するためにイベントに適用できるメタデータタグです。Event Brokerには、あらかじめ設定された複数のトピックが付属しています。また、追加のトピックを必要な数だけ定義できます。

トピックには、次の構成要素が含まれます。

- **Name:** トピックの名前。
- **Partition:** トピックのセグメント。各トピックに対して1つ以上のパーティションを使用できます。パーティションの数によって、1つのコンシューマーグループのコンシューマーの最大数が制限されます。
- **Replication Factor:** 1つのトピック内の各パーティションのコピーの数。1つのEvent Brokerノードに対し、レプリカが1つ作成されます。たとえば、Replication Factorが3のトピックの場合、3つのEvent Brokerノードに対し、各パーティションのコピーが3つ存在することになります。

現在は、ArcMCを使用してトピックの追加のみを行うことができます。トピックの編集や削除を行うことはできません。

トピックのパーティションおよび複製の管理の詳細については、『Event Broker管理者ガイド』を参照してください。

トピックの追加

トピックを追加するには

1. **[Configuration Management] > [Other Configurations] > [Manage Event Broker]** をクリックします。
2. [Event Broker Configurations] ページで、[**Add Topic**] をクリックします。
3. [Add New Topic] ダイアログの、[**Topic Name**] に、新しいトピックの名前を入力します。
4. [**# of Partitions**] に、そのトピックのパーティション数を入力します。
5. [**Replication Factor**] に、パーティションごとに作成されるコピーの数を入力します。
6. [**Save**] をクリックします。

ベストプラクティス: トピックを作成する際には、Replication Factorに2以上の値を使用します。また、パーティションの数を、(現在および将来において)トピックをサブスクライブするコンシューマーの数と同じにします。Verticaがコンシューマーになる場合は、パーティションの数をVerticaノードの数の倍数にします。

ルートについて

ルートとは、一定の条件を満たすトピック内のイベントを取得し、それらを新しいトピックにコピーするための方法です。ルートは、さらに詳細な調査が必要なイベントのグループを選択する場合など、独自の要件に合わせてイベントをトピックにフィルター処理するのに使用します。

ルートは、次の構成要素で構成されます。

- **Name:** ルートの名前。
- **Routing Rule:** イベントをトピックにカテゴライズする条件を定義する論理フィルター。これらの条件は、CEFフィールドに対して定義されます。

- **Source Topic:** ルーティングルールと一致するイベントを取りたすためにフィルター処理されるトピック。
- **Destination Topic:** ルーティングルールと一致するイベントのコピー先となるトピック(イベントのコピーはソーストピック内に残ります)。
- **Description:** ルートの短い説明。

ArcMCでは、ルートの作成、編集、または削除を行うことができます。ルートはCEFトピックにのみ適用されます。バイナリトピック (eb-esmなど) に対して作成されたルートは、機能しません。

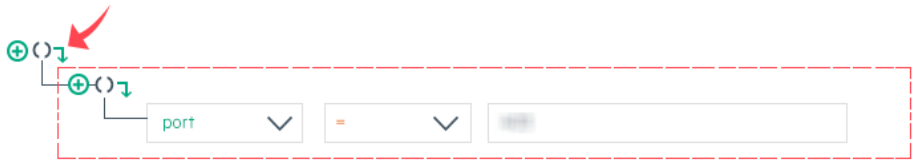
ルートの作成

ルートを作成する前に、ソースのトピックとコピー先のトピックがすでに存在していることを確認します。存在しない場合は、トピックを作成してから、そのトピックを使用するルートを作成します。

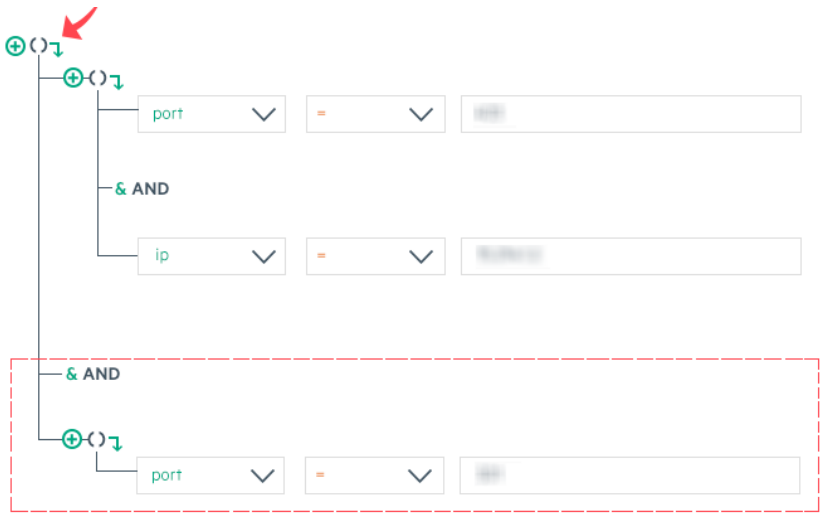
ルートを作成するには

1. **[Configuration Management] > [Other Configurations] > [Manage Event Broker]** をクリックします。
2. [Event Broker Configurations] ページで、**[Add]** をクリックします。
3. **[Route Name]** にルートの名前を入力します。
4. **[Source Topic]** ドロップダウンリストから、イベントをフィルター処理するトピックを選択します。
5. **[Destination Topic]** ドロップダウンリストから、イベントのコピー先のトピックを選択します。
6. **[Description]** に、ルートの短い説明を入力します。
7. **[Add Routing Rule]** で、ルールエディターを使用してルーティングルールの条件を定義します。

- ドロップダウンを使用し、**[Field]**、**[Operator]**、**[Value]** をフィルターで選択して、条件を定義します。フィールドは、Event Brokerのスーパースキーマから取得されます。スーパースキーマについては、「スーパースキーマ」(323ページ) で詳しく説明します。
- [+] をクリックして新しい結合 (& AND、|| OR) を追加するか、右矢印をクリックして従属する結合を追加します。続いて、必要な条件を必要な数だけ定義します。



- ネストされた結合を作成するには、現在の結合と同じレベルで右矢印をクリックします。



- 結合を変更するには、結合を右クリックして、ドロップダウンメニューから目的の選択肢を選択します。
- 結合を削除するには、結合を右クリックして、[Delete] を選択します。結合を削除すると、その結合に関連付けられた条件はすべて削除されます。

作成したルールは、ルールフィールドに表示されます。ルールが完成したら、**[Save]** をクリックします。

ルートの編集

ルートを編集するには

1. **[Configuration Management] > [Other Configurations] > [Manage Event Broker]** をクリックします。
2. [Event Broker Configurations] ページで、編集するルートを選択し、**[Edit]** をクリックします。
3. 必要に応じてルートを編集してから、**[Save]** をクリックします。

ルートの削除

ルートを削除するには

1. **[Configuration Management] > [Other Configurations] > [Manage Event Broker]** をクリックします。
2. [Event Broker Configurations] ページで、削除するルートを1つ以上選択し、**[Delete]** をクリックします。
3. **[Yes]** をクリックして削除を確定します。

第7章: 管理対象製品でのユーザーの管理

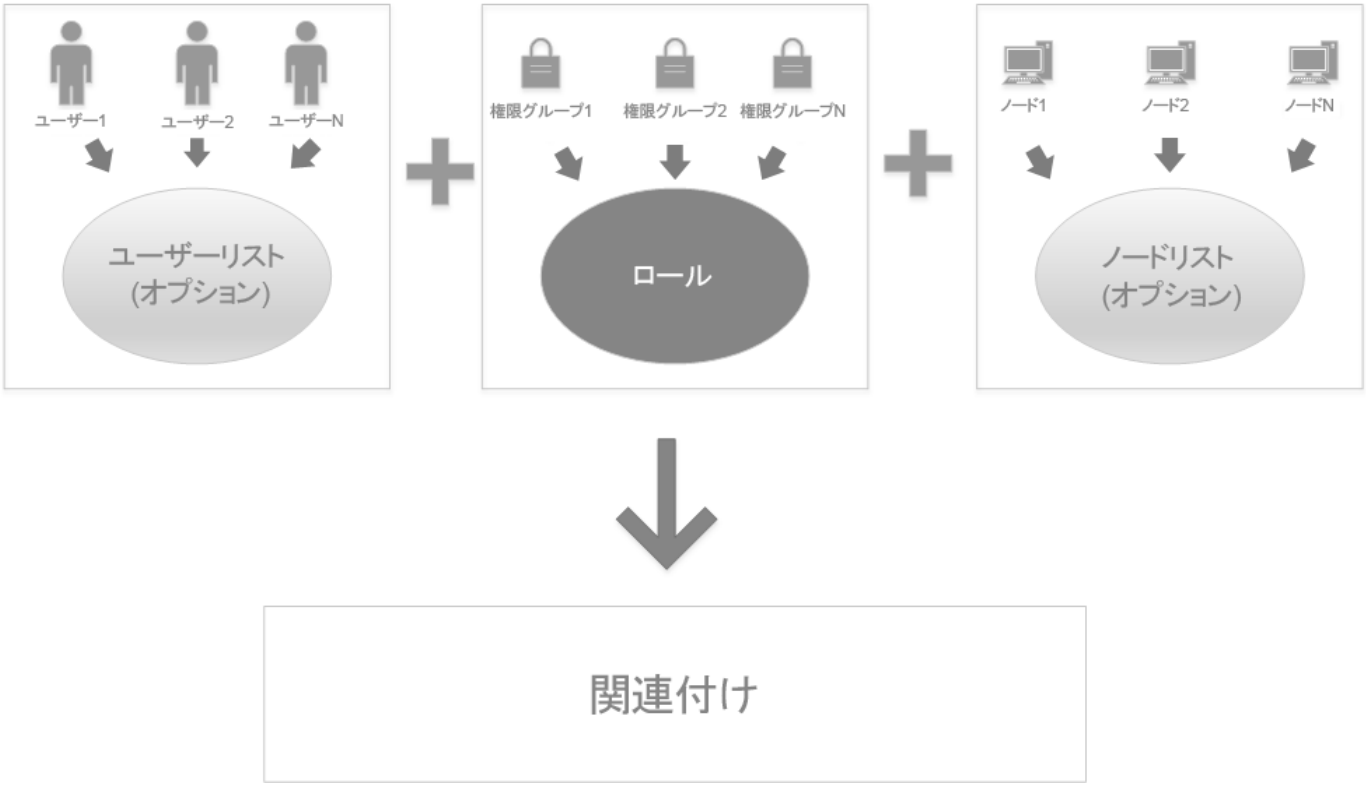
ここでは、以下の内容について説明します。

概要

ロールベースのアクセス制御 (RBAC) のユーザー管理では、指定したノードに対してカスタムロールを使用して製品のユーザーアクセスを管理できます。

以前のバージョンのArcMCでは、ノードでのユーザー管理が設定管理の一部に含まれていました (ユーザー設定でユーザー情報を定義していました)。ArcMC 2.1では、ノードでのユーザー管理が独立したRBAC (ロールベースのアクセス制御) 機能となり、大幅に改良されています。

ユーザー管理のワークフロー



ArcSight Management Centerでのユーザー管理は、次のワークフローに従います。

1. ArcSight Management Centerでユーザーを作成するか、管理対象ノードからユーザーをインポートします。
2. オプションで、構成や管理が容易になるように、ユーザーをユーザーリストにグループ化します。
3. 権限グループを作成 (またはインポート) し、管理者特権を有効にします。
4. 権限グループを割り当ててロールを作成し、製品への機能アクセスを許可します。
5. オプションで、複数のノードの構成が容易になるように、ノードリストを作成します。
6. 関連付けを作成し、ユーザー (またはユーザーリスト)、ノード (またはノードリスト)、およびロールを関連付けます。
7. 関連付けをノードにプッシュし、ロールに適した特権と目的のノードのみへのアクセスを使用して、関連付けに含まれるユーザーに対してアクセスを有効にします。
8. 管理元のArcMCで管理対象ノードのユーザーの準拠状況をチェックします。

ユーザーとユーザーリスト

ユーザーは、個人の資格情報や、氏名、電子メール、および電話番号などの識別情報に関する値を用いて定義します。ArcMCで管理されているノードでは、ノードのユーザーと各ユーザーの権限をすべてArcMCで管理できます。

ユーザーは名前付きのユーザーリストにグループ化できます。ユーザーリストには、個別ユーザーと同じようにアクセス権限を割り当てることもできます。

また、管理対象ノードからユーザーをインポートすることもできます。

ユーザーは次のパラメーターで定義します。

パラメーター	説明
User Name*	ログイン資格情報で使用される名前。
First Name*	ユーザーの名。
Last Name*	ユーザーの姓。
Distinguished Name	ユーザーのディレクトリ識別名 (ある場合)。
Email*	ユーザーのメールアドレス。関連付けの一部としてノードにプッシュされたユーザーには、ランダムに生成されたパスワードと共に、ノードに対する新規アクセスに関する確認メールがこのアドレス宛に送信されます。(これが正しいメールアドレスであることを確認してください。プッシュ後に、修正したメールアドレス宛にパスワードが再送信されることはありません。) **注:** 電子メールアラートが送信されるようにするには、SMTPサービスを有効にしてから、Webサービスを再起動します。
Title	ユーザーの役職。
Department	所属部門。
Phone	ユーザーの電話番号。
Notes	ユーザーに関するメモ。

ユーザーを作成するには

1. **[User Management] > [Users and User Lists]** をクリックします。
2. **[New User]** をクリックします。
3. ユーザーの詳細の値を入力します。
4. **[Save]** をクリックします。

管理対象ノードからユーザーをインポートするには

1. **[User Management] > [Users and User Lists]** をクリックします。
2. [**Import User**] をクリックします。
3. ノードリストで、ユーザーのインポート元になるノードを選択します。
4. [**Import Users**] ページで、矢印キーを使用して、選択したユーザーを [**Available Users**] リストから [**Selected Users**] リストに移動します。
5. [**Import**] をクリックします。選択したユーザーがArcMCにインポートされます。

ユーザーリストを作成するには

1. **[User Management] > [Users and User Lists]** をクリックします。
2. [**New User List**] をクリックします。
3. [**User List Name**] にユーザーリストの名前を入力します。
4. [**Selected Users**] カラムに、ユーザーリスト用に現在選択されているすべてのユーザーが表示されます。方向矢印を使用して、[**Available Users**] リストと [**Selected Users**] リストとの間でユーザーの追加または削除を行います。
5. [**Save**] をクリックします。

ユーザーまたはユーザーリストを編集するには

1. **[User Management] > [Users and User Lists]** をクリックします。
2. [**Users and User Lists**] ページで、編集するユーザーまたはユーザーグループの名前をクリックします。
3. 必要に応じてユーザーまたはユーザーリストを編集してから、[**Save**] をクリックします。ユーザーリストを新しい名前で保存するには [**Save As**] をクリックします。

ユーザーまたはユーザーリストを削除するには

ユーザーを削除する際には注意してください。ArcMCでユーザーを削除すると、関連付けの一部としてそのユーザーがプッシュされたすべてのノードから、そのユーザーが削除されます。

ユーザーを削除するには、そのユーザーが存在するすべてのノードがArcMCと通信できる状態である必要があります。

ユーザーリストを削除できるのは、ユーザーリストがどの関連付けにも含まれていない場合のみです。関連付けに含まれるユーザーリストを削除するには、最初にその関連付けを削除します。

1. **[User Management] > [Users and User Lists]** をクリックします。
2. [**Users and User Lists**] ページで、削除するユーザーまたはユーザーリストを選択します。

3. ツールバーの [**Delete**] をクリックします。
4. [**Yes**] をクリックして削除を確定します。

ユーザーをロールに割り当てる方法については、「ロール」(183ページ) を参照してください。

権限グループ

権限グループは、アクセス権限のセットです。アクセス権限は機能別に構成されているため、さまざまな機能やさまざまな製品アクセスをユーザーに割り当てることができます。

権限グループは、ロールの構成要素になります。権限グループ自体は、ユーザーに対してアクセスを許可するものではありません。権限グループはロールにバンドルすることができ、該当するロールがユーザーに割り当てられると、個々の権限グループで許可される権限がユーザーに付与されます。

ArcMCでは、権限グループの作成、管理対象ノードからのインポート、編集、および削除を行うことができます。

ArcMCでは、以下のタイプの権限グループを作成できます。

グループタイプ	アクセスが許可される機能
System Admin	システム管理とプラットフォーム設定
Logger Rights	Loggerの一般的な機能。Logger ReportsおよびLogger Searchの権限は含まれません。
Logger Reports	Loggerのレポート機能。
Logger Search	Loggerの検索機能。
Conapp Rights	コネクターアプライアンスの一般的な機能。
ArcMC Rights	ArcSight Management Centerの一般的な機能。 オプションの表示およびオプションの編集、保存、削除のArcMC権限は、管理の表示または管理の編集、保存、削除の権限を持つグループのみに許可できます。

さまざまな管理アクセスレベルを反映して、異なる複数の権限グループを作成できます。たとえば、リブートおよび更新の権限にアクセスできる権限グループと、グローバル設定にアクセスできる権限グループの、2つのシステム管理権限グループを作成することができます。ただし、ロールに割り当てることができるのは、グループタイプごとに1つの権限グループのみです。

権限グループを作成するには

1. **[User Management] > [Permission Groups]** を選択します。
2. [**Permission Groups**] ページで、[**New**] をクリックします。

3. [**Group Name**] に新しいグループの名前を入力します。
4. [**Group Type**] ドロップダウンリストからタイプを選択します。
5. [**Description**] に、権限グループの簡単な説明を入力します。
6. [**Rights**] リストで、権限グループで制御する権限を選択します (リスト内のすべての権限を選択するには、[**Select All**] をクリックします)。
7. [**Save**] をクリックします。

管理対象ノードから1つ以上の権限グループをインポートするには

1. **[User Management] > [Permission Groups]** を選択します。
2. [**Permission Groups**] ページで、[**Import**] をクリックします。
3. 管理対象ノードのリストから、グループのインポート元となるノードを選択し、[Next] をクリックします。
4. [**Available Permission Group(s)**] カラムには、管理対象ノードの利用可能な権限グループが表示されます。1つ以上のグループを選択し、[Add] ボタンを使用して、選択したグループを [**Selected Permission Group(s)**] カラムに移動します (ArcMC内にすでに存在する権限グループは無効と表示され、選択することはできません)。
5. [**Import**] をクリックします。グループがArcMCにインポートされます。

権限グループを編集するには

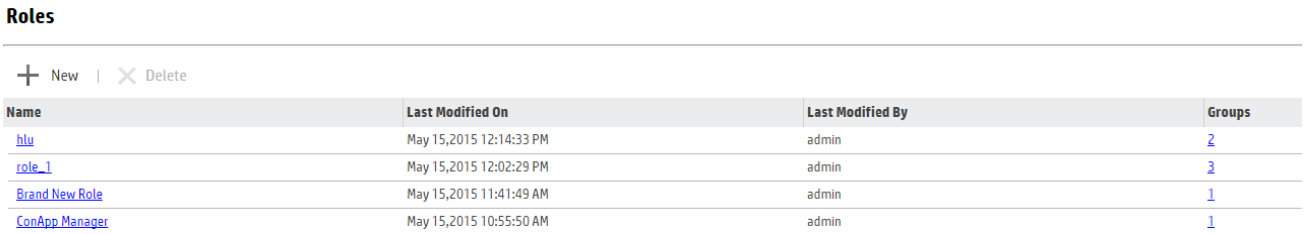
1. **[User Management] > [Permission Groups]** を選択します。
2. グループのリストから、編集するグループの名前をクリックします。
3. 必要に応じて値を入力するか、権限を選択します。
4. [**Save**] をクリックします (グループを新しい名前で保存するには **[Save As]** をクリックします)。

権限グループを削除するには

削除できるのは、どのロールにも割り当てられておらず、どのフィルター設定にも含まれていない権限グループのみです。
ロールに含まれている権限グループを削除するには、最初にそのロールを削除します。
フィルター設定に含まれている権限グループを削除するには、そのフィルター設定から権限グループを削除します。

1. **[User Management] > [Permission Groups]** を選択します。
2. グループのリストから、削除するグループを選択します。
3. [**Delete**] をクリックします。
4. [**Yes**] をクリックして削除を確定します。

ロール



ロールは、権限グループをまとめたものです。ロールを関連付けに割り当てることにより、ロールの構成要素の権限グループによって有効になるすべての権限を、関連付けのすべてのユーザーまたはユーザーリストに付与します。

ロールの作成および削除は、ArcMCで行うことができます。

ロールを作成するには

ロールを作成する前に、ロールに含める権限グループを作成します。

1. **[User Management] > [Roles]** を選択します。
2. **[New]** をクリックします。
3. **[Role Name]** にロールの名前を入力します。
4. **[Available Permission Group(s)]** カラムで、1つ以上の権限グループを選択します。**[Add]** ボタンを使用して、選択した権限グループを **[Available Groups]** カラムから **[Selected Permission Group(s)]** カラムに移動します。
5. **[Save]** をクリックします。

1つ以上のロールを削除するには

ロールを削除する前に、ロールが含まれている関連付けを編集し、各関連付けからロールを削除します。

1. **[User Management] > [Roles]** を選択します。
2. ロールのリストから、削除するロールを1つ以上選択します。
3. **[Delete]** をクリックします。
4. **[Yes]**をクリックして削除を確定します。

関連付けの割り当てについては、「関連付け」(185ページ) を参照してください。

ノードリスト

ノードリストは、一連の管理対象ノードに名前を付けたものです。ノードリストを使用すると、複数のノードをまとめて、それらのノードのユーザーを1つのグループとして管理できます。

特定の関連付けに含まれているノードリスト内のノードはすべて、その関連付けのプッシュをArcMCから受け取ります。

> 関連付けは、その関連付けに含まれるノード (またはノードリスト) に対してのみプッシュされます。関連付けを特定のノードに対してプッシュするには、直接またはノードリストの一部として、ノードをその関連付けに含める必要があります。

ノードリストは作成、編集、削除できます。

ノードリストを作成するには

1. **[User Management] > [Node Lists]** をクリックします。
2. **[New]** をクリックします。
3. [**Available Nodes**] カラムで、リストに含める複数のノードまたはノードリストを選択します。[**Add**] ボタンを使用して、選択内容を [**Selected Nodes**] カラムに移動します。
4. **[Save]** をクリックします。

ノードリストを編集するには

1. **[User Management] > [Node Lists]** をクリックします。
2. 編集するノードリストを選択します。
3. 必要に応じてノードリストを編集します。
4. **[Save]** をクリックします。ノードリストを新しい名前で保存するには **[Save As]** をクリックします。

1つ以上のノードリストを削除するには

> ノードリストを削除できるのは、ノードリストがどの関連付けにも割り当てられていない場合のみです。関連付けに含まれているノードリストを削除するには、最初に関連付けからノードリストを削除するか、関連付けを削除します。

1. **[User Management] > [Node Lists]** をクリックします。
2. ノードリストのリストから、削除するノードリストを1つ以上選択します。
3. **[Delete]** をクリックします。
4. **[Yes]** をクリックして削除を確定します。

関連付け

関連付けは、ユーザー (またはユーザーリスト) のグループに、任意の数の重複のないロールと、任意の数のノード (またはノードリスト) をバンドルしたものです。関連付けはArcMCで管理し、管理対象ノードのユーザーに対して権限を付与する場合に、それらのノードに対してプッシュします。

関連付けの作成、関連付けに含まれるノードへの関連付けのプッシュ、および関連付けの削除を行うことができます。

関連付けを作成するには

関連付けを作成する前に、関連付けに含めるすべてのユーザー (またはユーザーリスト)、ノードリスト、およびロールを作成します。

1. **[User Management] > [Associations]** をクリックします。
2. [**New**] をクリックします。
3. [**Association Name**] に、新しい関連付けの名前を入力します。
4. [**Available Users and User Lists**] カラムで、追加する複数のユーザーまたはユーザーリストを選択します。[**Add**] ボタンを使用して、選択内容を [**Selected Users and User Lists**] カラムに移動します。
5. [**Next**] をクリックします。
6. [**Assign Roles**] ページの [**Available Roles**] カラムで、追加するロールを1つ以上選択します。[**Add**] ボタンを使用して、選択内容を [**Selected Roles**] カラムに移動します。
7. 1つの関連付けに含まれるロールは、製品タイプに関して重複しないようにする必要があります。
8. [**Next**] をクリックします。
9. [**Available Nodes and Node Lists**] カラムで、追加する複数のノードまたはノードリストを選択します。[**Add**] ボタンを使用して、選択内容を [**Selected Nodes and Node Lists**] カラムに移動します。
10. [**Check Conflicts**] をクリックします。関連付け内で割り当てられている権限が、同じ権限グループタイプが割り当てられている他の関連付けと競合している場合、競合が返されます。たとえば、既存の関連付けによって読み取り/書き込みアクセスがユーザーAに対して割り当てられていて、新しく作成された関連付けによって読み取り専用権限がユーザーAに割り当てられた場合、競合が返されます。

- 関連付けに競合が見つかった場合は、関連付けを編集して競合を修正します。
- 競合が見つからなかった場合は、[**Yes**] をクリックして、新しい関連付けを関連付けに含まれるすべてのノードに対してプッシュします。

関連付けに含まれるノードに対して関連付けをプッシュするには

1. **[User Management] > [Associations]** をクリックします。
2. プッシュする関連付けの名前をクリックします。
3. [**Push**] をクリックします。関連付けに含まれるノードに対して関連付けがプッシュされます。

関連付けは、それに含まれるノード (またはノードリスト) に対してのみプッシュされます。関連付けを特定のノードに対してプッシュするには、直接またはノードリストを介して、ノードをその関連付けに含める必要があります。

関連付けを編集するには

1. **[User Management] > [Associations]** をクリックします。
2. 編集する関連付けの名前をクリックします。
3. 関連付けの構成要素を必要に応じて編集します。
4. [**Save**] をクリックします。

1つ以上の関連付けを削除するには

1. **[User Management] > [Associations]** を選択します。
2. 関連付けのリストから、削除する関連付けを1つ以上選択します。
3. [**Delete**] をクリックします。
4. [**Yes**] をクリックして削除を確定します。

コンプライアンスレポート

コンプライアンスレポートでは、管理元のArcMC上のユーザーと (該当ノードを含む関連付けがプッシュされた) 管理対象ノード上の同一ユーザーとの準拠ステータスを検証して表示します。準拠ステータスには、権限、名前、およびその他のユーザーデータが含まれます。

コンプライアンスレポートを実行するには

1. **[User Management] > [Compliance Report]** をクリックします。レポートに準拠状況が表示されます。

[**User Info in Managing ArcMC**] カラムには、ノードにプッシュされた関連付けに含まれる、管理元の各ArcMCにリストされているユーザー (またはユーザーグループ) が表示されます。

- 矢印をクリックしてカラムを展開すると、各ユーザーまたはユーザーグループの権限グループが詳しく表示されます。
- ユーザー名またはユーザーグループ名をクリックすると、各ユーザーまたはユーザーグループに割り当てられている権限グループが表示されます。
- User N/Aは、ユーザーが管理対象ノード上に存在しているが、管理元のArcMCに存在していないことを示します。
- Permission Group N/Aは、ユーザーまたはユーザーグループが管理対象ノード上で、プッシュ先に割り当てられていない権限を持っていることを示します。
- ノードにプッシュされた関連付けに含まれていないユーザーは、表示されません。

[**User Info on Managed Node**] カラムには、比較対象の管理対象ノード上にリストされているユーザー、ユーザーグループ、または権限グループが表示されます。

[**Compliance**] カラムには、管理元のArcMC上のユーザーに対する管理対象ノード上のユーザーの準拠状況が示されます。ステータスがCompliantになっている場合は、すべてのユーザー値が一致しています。Non-Compliantの場合は、1つ以上の値が一致していないか欠落しています。

準拠ステータスをクリックすると、各ユーザー値の詳細が表示されます。

Matches	管理対象ノード上の値が管理元のArcMC上の値と一致していることを示します。
Does Not Match	管理対象ノードと管理元のArcMCの値に不一致があることを示します。
Missing Value(s)	1つまたは複数の値が欠落していて、比較できない状態です。

カラムヘッダーを使用すると、表の結果をソートできます。

コンプライアンスレポートをPDFファイルにエクスポートするには、[**Export to PDF**] をクリックします。

第8章: ダッシュボード

ここでは、以下の内容について説明します。

概要

ArcSight Management Centerを使用すると、すべての管理対象ノードのヘルスステータスを監視できます。また、要件に応じて重要な問題に関する警告やアラートを設定することもできます。

注: 製品を監視するには、監視する製品をArcSight Management Centerにノードとして追加する必要があります。ノードの管理の詳細については、「ノードの管理」(42ページ)を参照してください。

監視は **[Dashboard] > [Monitoring Summary]** ページに表示されます。ArcSight Management Centerでは、すべての管理対象ノードが自動的に監視されます。

また、管理対象ノードのステータスに関する通知 (電子メール、SNMP、および監査の転送) を設定することもできます。

ArcSight Management Centerダッシュボード

ArcSight Management Centerの監視では、**[Dashboard] > [Monitoring Summary]** ページに、すべての管理対象ノード (ソフトウェアおよびハードウェア) の現在のヘルスステータスが表示されます。

- ソフトウェアノード (ソフトウェアコネクターアプライアンスなど) の監視対象メトリックには、CPU使用量、イベントフロー、およびディスク使用量などのソフトウェアパラメーターが含まれます。
- ハードウェアアプライアンス (Loggerアプライアンスなど) の監視対象メトリックには、ソフトウェア関連の属性とハードウェア関連の属性 (残りディスク容量やハードウェアステータスなど) の両方が含まれます。

監視サマリー

監視サマリーには、管理対象製品のヘルスやステータスに関する監視情報を表示するさまざまなパネルが存在します。

監視サマリーを表示するには、**[Dashboard] > [Monitoring Summary]** をクリックします。

ノードの合計数

[Total Number of Nodes] パネルの各タイルには、ADP環境内の指定されたタイプの管理対象ノードの数が表示されます。これらのタイプは、次のように定義されます。

タイル	カウント
Devices	イベントを転送しているデバイスの数。
ArcMC/CHA	管理対象のArcMCおよびコネクターホスティングアプライアンス (ハードウェアおよびソフトウェアの両方) が含まれます。
Connectors	管理対象コネクター数。
Logger	管理対象Logger数 (ハードウェアおよびソフトウェア)。
Nodes	管理対象Event Broker上のノード数。(Event Brokerをアップグレードした場合、Event Brokerの新しい証明書をArcMCにインポートするまでは、監視サマリーに正しいEvent Broker情報が反映されません。詳細は、「ホストの証明書のダウンロードとインポート」(72ページ)を参照してください。)

特定のノードタイプの詳細を参照するには、そのノードタイプに対応するタイルをクリックします。たとえば、すべてのコネクターの詳細を表示するには、**[Connectors]** をクリックします。

デバイス製品別のデバイス数

[Devices by Device Product] ディスプレイには、ネットワーク内で使用されている各種デバイスタイプの色分けされたサンバーストグラフが表示されます。テーブルには、デバイス製品別のアクティブなデバイスとアクティブでないデバイスの合計数が表示されます。

サンバーストの内側のリングには、合計デバイス数が表示されます。

サンバーストの外側のリングには、製品タイプの合計数が表示されます。

> 分かりやすくするため、製品タイプの数が1000を超える場合、外側のリングは表示されません。

特定のデバイスタイプの詳細を表示するには、グラフの対応するタイルをクリックするか、テーブルの該当エントリをクリックします。詳細ビューには、以下の設定項目があります。

- **Device Product Time-out Interval:** この期間中にデバイスが更新を受信しない場合、非アクティブのフラグが付けられ、赤く表示されます。
- **Device Age-out Interval:** このインターバルの後に、デバイスの製品タイプのすべてのデバイスが非アクティブである場合、この製品タイプと関連するすべてのデバイスがトポロジビューとサマリービューから削除されます。
- **Disable Device Tracking:** 選択されている場合、[Device Product Time-Out Interval] の期間を経過した後に、その製品タイプでのデバイス追跡が停止し、その製品タイプに関連するデバイスに非アクティブのフラグが付けられます。

これらの設定項目を変更するには、必要に応じて編集を行った後に、[**Save**] をクリックします。

ライセンス使用状況グラフ

ArcMCがライセンスサーバーとして有効になっている場合、毎日の使用状況を示す棒グラフに、全体でのADPライセンス使用量が日単位で表示されます。毎日のライセンス使用状況は、以下に基づいて、管理対象のADPコネクター (バージョン7.3.0以降) と管理対象のADP Loggerから算出されます。

- ADPコネクターをArcMCで管理している場合、ArcMCは、ADPの毎日のライセンス使用状況の計算に、ADP以外または管理対象以外のすべてのソースデバイスからのイベント取り込みを含めます。ソースが管理対象のADPコンポーネントでもある場合、このソースから管理対象のADPコネクターへのイベントフローは追跡されません。
- ADP LoggerをArcMCで管理している場合、ArcMCは、ADPの毎日のライセンス使用状況の計算に、ADP以外または管理対象以外のすべてのソースデバイスからのイベント取り込みを含めます。ソースが管理対象のADPコンポーネントでもある場合、このソースから管理対象のADP Loggerへのイベントフローは追跡されません。

ArcMCは、各ADPコネクターおよび各ADP Loggerから、日次の取り込み情報を毎日収集します。取り込み収集の時刻 (デフォルトでArcMCローカル時刻の毎日1:00:00) にArcMCに対して到達不可である場合、ADPコネクターおよびLoggerは、取り込みの累計を提供します。このシナリオは、次の場合に発生する可能性があります。

- ADPコネクターまたはLoggerがダウンした場合。
- ADPコネクターまたはLoggerのサーバー証明書が変更された場合。
- ADPコネクターまたはLoggerがArcMCによって管理されなかった場合。

毎日のADP取り込み収集は、ライセンスサーバーのArcMCおよびライセンスサーバーによって管理されるArcMCにのみ適用されます。

個別のADP Loggerの取り込みレポートには、[00:00:00 – 23:59:59] GMTの時間枠中の前日の取り込みが含まれます。一方、ADPライセンス使用状況の計算の場合は、[01:00:00 – 24:59:59] (ArcMCローカル時刻) の時間枠中の前回のADP Loggerの取り込みが収集されます。これは、個別のLogger取り込み追跡に使用される時間枠と、ADP取り込み計算

に使用される時間枠が異なるためです。このように、これらのレポートでは異なる数値をレポートしているため、2つのレポートを比較することはお勧めしません。

ドリルダウン

問題のあるノードの詳細を表示して、問題点を修復するためのアクションを実行できます。

問題のあるノードの詳細を表示するには、上側のテーブルでノードを選択します。下側のテーブルに、そのノードに関連する問題が表示されます。問題ごとに、次の識別情報が表示されます。

- **Metric Type:** 問題に関連するメトリック。
- **Metric Name:** メトリックの名前。
- **First Occurrence:** 問題が最初に発生したローカル時刻。
- **Last Occurrence:** 問題が最後に発生したローカル時刻。
- **Severity:** 問題の緊急度。
- **Description:** 問題の概略説明。

問題の詳細を緊急度別に表示するには

1. メニューバーで、**[Dashboard] > [Monitoring Summary]** をクリックします。
2. 監視対象の製品タイプに対応するリングメーターで、表示する緊急度に対応した部分をクリックします(たとえば、現在警告ステータスになっているすべてのノードを表示するには、リングの警告 (黄色) の部分をクリックします)。対応する [**Severity Issue Summary**] が表示されます。
3. [**Severity Issue Summary**] ページで:

   上側のテーブルには、以下の識別情報と共に問題のあるすべてのノードのリストが表示されます。

   - **Name:** ノード名。
   - **Path:** ノードへのパス。
   - **Type:** ノードのタイプ。
   - **Lead/Breach:** このノードでレポートされた最も緊急度の高い問題の簡単なサマリー。ノードでは、これより緊急度の低い問題も発生している可能性があります。
   - 履歴やステータスなど、問題のあるノードのヘルスの詳細を表示するには、[**Details**] をクリックします。データテーブルに、選択したノードのパラメーターが表示されます。

データチャート

各データチャートには、時間の経過に伴うパラメーターの値が表示されます。ドロップダウンリストを使用し、過去4時間、前日、または先週から表示間隔を変更します。データチャートには、[Valid Values for Metric Types] テーブルに表示されるメトリックを任意に含めることができます。

チャートで対応する線の表示を切り替えるには、データの凡例をクリックします。線の数が多い場合は、一部の線を非表示にするとチャートが見やすくなる場合があります。

過去30日間のADPライセンス使用状況

ADPライセンスでは、指定された数の管理対象製品および指定された量の管理対象トラフィックを使用する権利が付与されます。[**ADP Licensed Usage for the Last 30 Days**] パネルには、前月のADPデータ使用状況が表示されます。

グラフには、ADP環境内のすべてのトラフィックが表示されます。デフォルトの色は緑で、データ使用状況がライセンスの制限範囲内であることを示します。

- 黄色は、データ使用状況がライセンスされたトラフィック制限に近づいた期間を示します。
- 赤は、データ使用状況がライセンスされたトラフィック制限を超えた期間を示します。

[**Active Loggers**] は、データがライセンス監視レポートに関与しているADP Loggerの数を示します。詳細情報が必要な場合は、ライセンスレポートをPDF形式にエクスポートできます。これには、過去365日間のデータが含まれます。

ADPライセンス使用状況の表示を有効にするには

1. ArcMCをADPライセンスサーバーとして有効にします。ArcMCのツールバーで、[**ADP License Server**] をクリックしてから、[**Yes**] をクリックします。
2. [**License and Upgrade**] ページで、有効な容量のライセンスをArcMCにアップロードします。

ライセンスレポートをPDF形式でエクスポートするには

1. [**Export License Report**] をクリックします。
2. PDFファイルがローカルシステムにダウンロードされます。

監視ルール

監視ルールは、管理対象の製品タイプごとに監視警告を生成する場合に定義します。ArcMCには、すぐに使用できる数多くのプリセット監視ルールが含まれています。これらのルールは、そのまま使用することも、独自の用途に合わせてカスタマイズすることもできます。さらに、独自のカスタム監視ルールを作成することもできます。

監視ルールは、論理、パフォーマンス、ヘルス、またはその他の一連の条件で構成されています。ルール内のすべての条件を合わせて評価することで、ルールの全体として効果が特定され、これに基づいてArcMCからアラートが生成されます。

たとえば、ルールを用いて、特定のタイプのデバイス(条件#2)に到達する1秒あたりの入力イベントの数 (条件#1)をチェックするとします。この数が指定されたレベル(条件#4)を超えた(条件#3)場合、警告 (アラート)が返されます。

アラートは電子メールまたはSNMPで配信するか、監査ログに記録することができます。

> 電子メール通知が設定されている場合は、監視ルールが定義されていなくても、管理対象ノードがダウンまたは到達不能になったときに、これを示す自動電子メールアラートが送信されます。電子メールアラートは、ダウンしたノードや到達不能なノードが復旧または到達可能になったときにも送信されます。

ルールの管理と作成の詳細については、「ルールの管理」(194ページ)を参照してください。

プリセットルール

ArcSight Management Centerには、監視に役立つプリセットルールが含まれています。これらのプリセットルールは、そのまま使用することも、独自の用途に合わせてカスタマイズすることもできます。ユーザー独自のカスタムルールを作成することもできます。

デフォルトで、ArcMCのプリセットルールは無効になっています。プリセットルールを適用してアラートをトリガーするには、プリセットルールを有効にする必要があります。

> 以前のバージョンのArcMCを使用し、既存のルールをすでにお持ちのお客様は、ArcMCに含まれるプリセットルールがお持ちの既存のルールに追加されます。

プリセットルールを確認するには

1. **[Dashboard] > [Rules]** をクリックします。監視ルールのサマリーが表示されます。
2. ルールの設定を詳しく表示するには、**[Name]** カラムで、ルール名をクリックします。
3. 無効なプリセットルールを有効にするには、**[Status]** で **[Enable]** を選択してから、**[Save]** をクリックします。

ルールの管理

カスタムルールを作成するには

1. **[Dashboard] > [Rules]** をクリックします。
2. ツールバーの [**New**] をクリックします。
3. ルールのパラメーターの値を選択します。
4. [**Save**] をクリックします。

既存のルールを編集するには

1. **[Dashboard] > [Rules]** をクリックします。
2. [**Monitoring Rules**] で、編集するルールを選択します。
3. [**Name**] カラムで、ルール名をクリックします。
4. 必要に応じて、ルールのパラメーターの値を選択し直します。
5. [**Save**] をクリックします。あるいは、[**Save As**] をクリックし、編集したルールを別の名前で保存します。

ルールを有効 (または無効) にするには

1. **[Dashboard] > [Rules]** をクリックします。
2. 管理パネルの [**Monitoring Rules**] で、有効または無効にするルールを選択します。
3. [**Name**] カラムで、ルール名をクリックします。
4. [**Status**] で、ステータスを [**Enable**] (または [**Disable**]) に切り替えます。
5. [**Save**] をクリックします。

ルールを削除するには

1. **[Dashboard] > [Rules]** をクリックします。
2. [**Monitoring Rules**] で、削除するルールを選択します。
3. [**Delete**] をクリックします。
4. [**OK**] をクリックして削除を確定します。

すべてのルールをテキストファイルにエクスポートするには

1. **[Dashboard] > [Rules]** をクリックします。
2. ツールバーの [**Export**] をクリックします。ルールは、`monitor_breach_rules.properties`.という名前のローカルのテキストファイルにエクスポートされ、ローカル環境にダウンロードされます。

監視ルールのパラメーター

監視ルールは、ルールのパラメーターを使って定義します。次の表は、監視ルールのパラメーターとそれぞれの有効な値について説明したものです。

監視ルールのパラメーター

パラメーター	説明
Name	ルールの名前。(最大文字数は50文字)
Metric Type	測定される判定基準。メトリックタイプの有効な値については、下記の表「**メトリックタイプの有効な値**」を参照してください。各メトリックタイプには値タイプがあり、割り当て可能な値の種類が制限されます。
Product Type(s)	ルールが適用される管理対象の1つまたは複数の製品タイプ。これらはメトリックタイプに基づいて自動的に選択されます。 たとえば、ハードウェアのみに適用されるメトリックタイプ (Voltageなど) を選択した場合は、ハードウェアフォームファクターの製品のみを選択できます。 また、該当する場合は、ルールが適用されるタイプを選択解除することもできます。
Specific Node Selector	[**View/Choose**] をクリックし、ルールの適用対象となる1つ以上のノードを選択します。何も選択しなかった場合は、選択した製品タイプのすべてのノードにルールが適用されます。
Severity	違反の緊急度。有効な値は、Healthy、Warning、Critical、Fatalです。これらの各値のしきい値は、管理者が定義します。
Aggregation	メトリックタイプのデータポイントに適用される集計機能。有効な値は次のとおりです。 • ANY: 任意の値 • AVG: 平均値 (数値のみ) • MIN: 最小値 (数値のみ) • MAX: 最大値 (数値のみ)
Measurement	2つの判定基準の比較。有効な値は次のとおりです。 • GREATER: 一方のフィールドがもう一方のフィールドより大きい • LESS: 一方のフィールドがもう一方のフィールドより小さい • EQUAL: 一方のフィールドともう一方のフィールドが等しい • NOT_EQUAL: 2つのフィールドが等しくない

監視ルールのパラメーター (続き)

パラメーター	説明
Value	比較用のしきい値。有効な値はメトリックタイプによって異なります。 • Percentage: 1～100の数値 (%記号なし)。 • Numeric: 数値文字列。 • Boolean: true/false (大文字/小文字を区別しない) • Literal Status: アプライアンスコンポーネントのステータスで、次の値のいずれか: Ok、Degraded、Rebuilding、Failed、Unavailable
Notify Me	ルールに関するアラートの1つまたは複数の通知メカニズム (電子メール、SNMP、または監査の転送) を選択します。
Status	[**Enabled**] の場合、ルールが適用され、[**Notify Me**] での指定に従ってアラートが生成されます(ArcMCのプリセットルールは、デフォルトで無効になっています)。
Time Range	評価間隔 (時間および分単位)。時間および分の合計が、168時間 (7日) を超えることはできません。
Description	ルールの概略説明。(最大文字数は300文字)

注: 複合ルール (AND/OR) はサポートされていません。

メトリックタイプの有効な値

値	説明	値タイプ
コネクターアプライアンスまたはLoggerの場合のみ		
CPU Usage	CPU使用率 (%)。	Percentage
JVM Memory	Java仮想マシンのメモリ。	Numeric
Disk Read	ディスクの読み取り回数。	Numeric
Disk Write	ディスクへの書き込み回数。	Numeric
Network Received	受信したネットワークトラフィック (MB/秒)。	Numeric
Network Sent	送信したネットワークトラフィック (MB/秒)。	Numeric
All EPS In	1秒あたりの総イベント数 (受信)。	Numeric
All EPS Out	1秒あたりの総イベント数 (送信)。	Numeric
コネクターの場合のみ		
EPS In	1秒あたりのイベント数 (EPS) (受信)。	Numeric
EPS Out	1秒あたりのイベント数 (EPS) (送信)。	Numeric

メトリックタイプの有効な値 (続き)

値	説明	値タイプ
Events Processed	処理されたイベント数。	Numeric
Events Processed (SLC)	処理されたイベント数 (前回チェック以降)。	Numeric
Events Per Second	1秒あたりのイベント数。	Numeric
FIPS Enabled	1= FIPS有効、0=FIPS無効。	Boolean
Command Responses Processed	処理されたコマンド応答数。	Numeric
Queue Drop Count	キュードロップ数。	Numeric
Queue Rate (SLC)	キューレート (前回チェック以降)。	Numeric
Active Thread Count	アクティブスレッド数。	Numeric
ハードウェアフォームファクター製品の場合のみ		
Fan	ハードウェアのファンのステータス。	Literal Status
Disk Space	ハードウェアのディスク領域のステータス。	Literal Status
Voltage	ハードウェアの電圧のステータス。	Literal Status
Current	ハードウェアの電流のステータス。	Literal Status
Temperature	ハードウェアの温度のステータス。	Literal Status
Power Supply	ハードウェアの電源のステータス。	Literal Status
RAID Controller	RAIDコントローラーのステータス。	Literal Status
RAID Battery	RAIDバッテリのステータス。	Literal Status
Hard Drive	ハードドライブのステータス。	Literal Status
Loggerの場合のみ		
Storage Group Usage	現在のストレージグループ使用量 (バイト数)。	Numeric
Storage Group Capacity	現在のストレージグループ容量 (バイト数)。	Numeric

メトリックタイプの有効な値 (続き)

値	説明	値タイプ
Event Brokerの場合のみ		
Event Broker All Bytes In	Event Brokerクラスターで受信されたすべてのバイト数。	Numeric
Event Broker All Bytes Out	Event Brokerクラスターで送信されたすべてのバイト数。各トピックの複製により、送信バイト数が常に受信バイト数を上回ります。	Numeric
Event Broker Disk Usage	Event Brokerの個別ノードのディスク使用量。	Numeric
Event Broker Memory Usage	Event Brokerの個々のノードのメモリ使用量。	Numeric
Event Broker SP EPS	Event Brokerのストリームプロセッサーで受信された1秒あたりのイベント数。	Numeric
Event Broker Error	エラーを生成したEvent Brokerのストリームプロセッサーで受信された処理待ち中の1秒あたりのイベント数。	Numeric
Event Broker Lag	Event Brokerのストリームプロセッサーによる受信待ち中の1秒あたりのイベント数。	Numeric
Event Broker CPU Usage	Event Brokerの個々のノードのCPU使用量。	Numeric
Event Broker EPS In	Event Brokerクラスターで受信された1秒あたりのイベント数。	Numeric

ルールの検証

構文的に正しいルールであっても、返されるアラートが明確で意味があるものになるとは限りません。たとえば、CPU使用率が101%未満の場合にアラートをトリガーする構文的に正しいルールを作成したとしても、このルールでは有用なアラートは得られません (常にアラートが生成されるためです)。

ルールの検証を行い、問題の適切な検出に役立つように、ルールから意味のある値が返されるようにする必要があります。

注: カスタムポーリング間隔: ArcSight Management Centerでは、各種ArcSight製品のメトリックデータのアーカイブタイプに関連付けられた3種類のポーリング間隔 (4時間、1日、1週) が使用されます。これらの間隔は必要に応じて適切に調整できます。

これらの間隔の調整は、変更の影響を十分に理解した上で行うことを強くお勧めします。

ポーリング間隔は、テキストエディターを使用して、logger.propertiesファイルで指定できます。

- 4時間のデータ(最小許容間隔1分):
  `monitoring.data.poll.4hour.cron=10 0/3 * * * ?`
  このプロパティは、3分間隔でのポーリングを示します。
- 1日のデータ(最小許容間隔5分):
  `monitoring.data.poll.1day.cron=15 0/10 * * * ?`
  このプロパティは、10分間隔でのポーリングを示します。
- 1週のデータ(最小許容間隔1時間):
  `monitoring.data.poll.1week.cron=20 2 * * * ?`
  このプロパティは、2時間間隔でのポーリングを示します。

ファイルを編集して保存した後、変更内容を有効にするには、サーバーを再起動する必要があります。

カスタムルールの例

ここでは、カスタム監視ルールの例を示します。

例1: Warning違反

この例では、以下のWarning条件を指定します。

「過去30分間に任意のArcMCの平均CPU使用率が70%を上回った場合に、Warning違反を生成します。」

Name: ArcMC Warning

Metric Type: CPU Usage

Product Type: ArcMCs

Severity: Warning

Aggregation: AVG

Measurement: GREATER

Value: 70

Timespan: 30分

例2: Critical違反

例2では、以下のCritical条件を指定します。

「過去1時間に任意のLoggerアプライアンスで電源が故障した場合に、Critical違反を生成します。」

Name: Logger Warning

Metric Type: Power Supply

Product Type: Logger

Severity: Critical

Aggregation: ANY

Measurement: EQUAL

Value: Failed

Timespan: 60分

電子メール通知の設定

電子メール通知では、監視対象ノードがダウンまたは通信できなくなっていることを受信者に通知します。

注: 電子メールアラートには、ソフトウェアコネクターに関する問題は含まれません。ただし、コンテナーは電子メールアラートの対象になる場合があります。

電子メール通知を設定する前に、**[System Admin] > [System] > [SMTP]** でお使いのSMTPの設定に合わせた値が指定されていることを確認します。SMTP設定の詳細については、「SMTP」(234ページ) を参照してください。

設定後、アラートをトリガーする通知ルールごとに電子メール通知を設定する必要があります。

電子メール通知を設定するには

1. テキストエディターで、.../userdata/arcmc/logger.propertiesファイルを開きます。(ファイルが存在しない場合は、テキストエディターでファイルを作成します。ファイルを作成する際には、root以外のユーザーを所有者にする必要があります。)
2. monitoring.notification.emailsという名前の新しいプロパティを用いて行を新規に追加し、通知の送付先のすべての管理者のメールアドレスのカンマ区切りのリストと同じ値を追加します。たとえば、次の値の場合は、address1@example.comとaddress2@example.comに電子メールアラートが送信されます。

```
monitoring.notification.emails=address1@example.com,
address2@example.com
```

3. 変更したlogger.propertiesファイルを保存します。
4. ArcMC Webプロセスを再起動します。
5. ルールエディターで、電子メールアラートをトリガーする通知ルールを開き、[**Notify Me**] で [Email] を選択します。

電子メール通知の例

ここでは、受信者に送信する電子メールの例を示します。

<URI>は問題のあるノードのURIです。

ノードNは問題のあるノードのホスト名です。

この情報は、ノード管理の [**Hosts**] タブに表示されています。

Subject: <電子メールのタイトル>
次のノードがダウンしているか、ArcSight Management Centerから到達不能になっています。

//デフォルト/<URI>/<ノード1>

//デフォルト/<URI>/<ノード2>

SNMP通知の設定

SNMP通知では、監視対象ノードがダウンまたは通信できなくなっていることに関するSNMPトラップを送信します。

ArcMCアプライアンスでSNMP通知を設定するには

1. **[Administration] > [System Admin] > [System] > [SNMP]** で、SNMPを有効にします。次に、お使いのSNMP環境に合わせて、ポート、SNMPバージョン、およびその他の必要な設定の値を入力します。
2. ルールエディターで、SNMPアラートをトリガーする通知ルールを開き、[**Notify Me**] で [SNMP] を選択します。SNMPアラートをトリガーする各ルールについて、この操作を繰り返します。

ソフトウェアArcMCでのSNMPの有効化

ソフトウェアArcMCには、SNMP設定用のUIコントロールがありません。この場合は、次の手順を実行して、ソフトウェアArcMCのSNMP通知と監視を設定します。

ソフトウェアホストでSNMP通知を有効化するには

1. システムに次のRPMパッケージがインストールされていることを確認します: net-snmp、net-snmp-utils、net-snmp-libs、lm_sensors-libs

2. 次のコマンドで、SNMPサービスを有効にします: chkconfig snmpd on

3. 次のコマンドで、SNMPサービスを開始します: service snmpd start

4. テキストエディターで、次のパラメーターを使用して、/opt/arcsight/userdata/platform/snmp.propertiesファイルを作成します。カッコ<>内の項目は、お使いの環境に合わせた値に置き換えます。

```
snmp.enabled=true

snmp.version=V3

snmp.port=161

snmp.v3.authprotocol=SHA

snmp.v3.authpassphrase=<パスワード>

snmp.v3.privacyprotocol=AES128

snmp.v3.privacypassphrase=<パスワード>

snmp.user=<SNMPユーザー名>

snmp.community=public

snmp.system.location=<SNMPロケーション>

snmp.system.name=ArcMC Node 247

snmp.system.contact=<サポートのメールアドレス>

snmp.trap.enabled=true

snmp.trap.version=V3

snmp.trap.port=162

snmp.trap.nms=<NNMIのIPアドレス>

snmp.trap.user=<SNMPトラップのユーザー名>

snmp.trap.community=public

snmp.trap.v3.authprotocol=SHA

snmp.trap.v3.authpassphrase=<パスワード>

snmp.trap.v3.privacyprotocol=AES128

snmp.trap.v3.privacypassphrase=<パスワード>
```

---

5. 次のように、rootユーザーとしてスクリプトarcsight_snmpconfを実行します。

```
<ArcSight_Home>/current/arcsight/aps/bin/arcsight_snmpconf <ArcSight_
Home> /userdata/platform/snmp.properties trap
```

6. 次のように、もう一度スクリプトを実行します。

```
<ArcSight_Home>/current/arcsight/aps/bin/arcsight_snmpconf <ArcSight_
Home> /userdata/platform/snmp.properties poll
```

このスクリプトでは、/etc/snmp/snmpd.confファイルがセットアップされ、SNMPサービスが再起動されます。

7. 次のコマンドで、SNMPサービスを再起動します: `service snmpd restart`

8. ルールエディターで、SNMPアラートをトリガーする通知ルールを開き、[**Notify Me**] で [SNMP] を選択します。SNMPアラートをトリガーする各ルールについて、この操作を繰り返します。

トポロジビュー

トポロジビューには、ネットワークコンポーネントとコンポーネント間の関係がグラフィック形式で表示されます。このビューには、ArcMCのロケーションごとの、ネットワークデバイス (イベントプロデューサー)、コネクター、および通知先の間の関係が表示されます。

トポロジビューを表示するには、[Dashboard] > [Topology View] をクリックします。

左側のカラムでは、現在のトポロジビューが強調表示されます。利用可能なビューは、ArcMCで定義されたロケーションに基づいています。

トポロジビュー内の各項目のヘルスステータスは、色で示されます。項目のステータスには、Healthy (緑)、Fatal (赤)、Critical (アンバー)、Warning (黄)、またはUnknown (グレー) があります。

モニターアイコンはそれぞれが1つのデバイス製品タイプを表します。各モニターアイコンの左側のバブルは、デバイス製品タイプごとのデバイス数を示します。

緑のバブルは、アクティブなデバイス (イベントを受信しているデバイス) を示します。赤いバブルが存在する場合、これは非アクティブなイベントの数を示します。

緑のバブルまたは赤いバブルをクリックすると、その製品タイプのアクティブなホストまたは非アクティブなホストを示す詳細ページが表示されます。

[**Devices**] 領域には、ネットワーク内でイベントを転送しているデバイスが表示されます。

- 特定のデバイスとの間のEPS (1秒あたりのイベント数) トラフィックを表示するには、デバイス上にマウスカーソルを重ねます。

[**Connectors**] 領域には、現在のトポロジビュー内のコネクターが表示されます。

- 特定のコネクターとの間のEPS (1秒あたりのイベント数) トラフィックを表示し、コネクターステータスの概要を把握するには、コネクター上にマウスカーソルを重ねます。また、名前、デバイスタイプ、ステータス、パス、ルール違反 (存在する場合)、およびArcMC管理対象も表示されます。
- ドリルダウンして、ヘルス履歴を含めたコネクターのヘルスを詳しく表示するには、コネクターをクリックします。
- コネクターノードを追加した直後など、場合によっては、管理対象でないコネクターが表示されることがあります。これは、数回の収集サイクルの間に、新しいコネクターからデータが収集されて、該当するコネクターデータに置き換えられます。
- 記号  付きで表示されるコネクターは、表示用に現在選択しているのとは別のロケーションに含まれています。

[**Destinations**] 領域には、コネクター通知先が表示されます。

- ドリルダウンして、ArcMC管理対象の通知先のヘルスを詳しく表示するには、通知先をクリックします。

トポロジビューは、1分おきに自動更新されます(自動データ更新のオンとオフは、[**Auto Refresh**] コントロールで切り替えることができます)。ビューを手動で更新するには、ツールバーの [**Refresh**] をクリックします。

また、[**Legends**] コントロールを使って、グラフィックの凡例の表示を切り替えることもできます。

ネットワーク内に管理対象でないコネクター (またはその他のノード) が存在する場合は、トポロジビューでそのように表示されます。ArcMCでは、管理対象でないコネクターや、管理対象でないコネクターからのトラフィックを表示できません。このようなビューに関するさまざまなシナリオ、および各シナリオの結果については、こちらで詳しく説明しています。お使いのネットワークを詳細かつ正確に把握するには、ArcMCを使用して論理トポロジに含まれるすべてのコネクターを管理することを強く推奨します。

第9章: バックアップと復元の管理

ここでは、以下の内容について説明します。

概要

[**Backup**] および [**Restore**] メニュー項目では、ArcSight Management Centerの設定のバックアップと復元を行うことができます。完全なバックアップには、管理対象ノード、設定、システム管理、コネクターデータ (agentdataフォルダー)、およびすべてのリポジトリファイルのすべてのデータが含まれます。また、このデータの中から選別した内容をバックアップファイルに含めることで、バックアップファイルを小さくて管理しやすいものにすることもできます。

バックアップ

現在のArcSight Management Centerの設定を、ネットワーク上のリモートシステムまたはローカルシステムに、必要な頻度でバックアップすることができます。

ArcSight Management Center 構成をバックアップするには

1. **[Administration] > [Application] > [Backup]** をクリックします。
2. [**Enter Backup Parameters**] で、次の表に示すパラメーターの値を入力します。

パラメーター	説明
Protocol	セキュアコピーを使用するには、**SCP**を選択して、ネットワーク上のリモートシステムにバックアップファイルを保存します。適切なフィールドに、IPアドレスまたはホスト名、ユーザー名とパスワード、および宛先ディレクトリを指定する必要があります。 バックアップファイルをローカルシステムに保存するには、[**Save to Local**] を選択します。このオプションを選択すると、[**Port**]、[**IP/Host**]、[**User**]、[**Password**]、および [**Remote Directory**] の各フィールドは不要になるため、無効 (グレー表示) になります。
Port	SCPのみ。デフォルトのポートは22です。
Backup Server IP Address	SCPのみ。バックアップファイルを受け取る宛先のIPアドレス。

パラメーター	説明
User	SCPのみ。宛先のユーザー名。
Password	SCPのみ。指定したユーザー名のパスワード。
Remote Directory	SCPのみ。設定バックアップファイルを受け取る指定した宛先のサブディレクトリ。
Schedule/ One time only	**One Time Only** SCPのみ。「一度だけ」のバックアップを行うことができます。 **Schedule** 日数、時間、または分数単位でバックアップ時間を指定するオプションが利用できます。 このオプションでは、次のルールに注意してください。 • 使用できる曜日は、**M、Tu、W、Th、Fr、Sa、Su**です。 • 英字は大文字/小文字を区別しません。 • 分数は15分間隔より大きくなければなりません。 • **分数**の間隔は、要求が行われた時刻ではなく、**毎時00分**から始まります。 • **時間**の間隔は、要求が行われた時刻ではなく、**午前0時**から始まります。
Backup	• 管理対象ノード、設定、システム管理、コネクター、およびリポジトリのすべてのデータを含むバックアップファイルを作成するには、[**All**] を選択します。 **ヒント**: [**All**] を選択すると、作成される.tar.gzファイルが非常に大きくなり、データの復元に失敗する可能性があります。これを防ぐため、バックアップファイルから**コネクターデータ**と**リポジトリデータ**を除外することができます。 • リポジトリ内のファイルを含まないバックアップファイルを作成するには、[**Exclude Repository Data**] を選択します。 • コネクターデータを含まないバックアップファイルを作成するには、[**Exclude Connector Data**] を選択します(ArcMCアプライアンスのみ)。 • リポジトリファイルとコネクターデータを含まないバックアップファイルを作成するには、[**Exclude Connector and Repository Data**] を選択します(ArcMCアプライアンスのみ)。

3. 設定をバックアップするには、[**Save**] をクリックしてから、ファイルを保存する場所を選択します。

復元

以前のバックアップからArcSight Management Centerの設定を復元することができます。復元には次の条件が適用されます。

- バックアップを復元するのに使用するArcSight Management Centerのバージョンは、バックアップを作成するのに使用したのと同じバージョンである必要があります。

- rootインストールで実行されたバックアップを使用して、root以外のインストールを復元することはできません。
- ソフトウェアArcSight Management Centerでは、復元されたソフトウェアArcMCのインストールパスがバックアップのパスと同じである必要があり、バックアップを行ったのと同じrootまたはroot以外のユーザーがインストールを行う必要があります。

設定を復元するには

1. **[Administration] > [Application] > [Restore]** をクリックします。
2. [**Upload Backup for Restore**] で、[**Choose File**] をクリックします。
3. バックアップファイルを選択します。
4. [**Upload**] をクリックして、指定したバックアップファイルから設定を復元します。

   注意: バックアップを復元するのに使用するArcSight Management Centerのバージョンは、バックアップを作成するのに使用したのと同じバージョンである必要があります。

5. ソフトウェアArcMCの場合は、ArcSight Management Center Webプロセスを再起動します。ArcMCアプライアンスの場合は、アプライアンスをリブートします。
6. オプションで、各コンテナーのSSL証明書を再度インポートします。 アイコンをクリックして、**Certificate Download**ウィザードを実行し、有効な証明書をインポートします。また、いずれかのリモートノードで証明書の不一致が示された場合は、そのノードのサーバー証明書を再度インポートします。

設定の復元後の注意点:

- 復元後のキャッシュサイズが、バックアップファイル内のキャッシュサイズと異なっていても構いません。たとえば、設定の復元後に、コネクターで受信するイベント数を増やことや、使用するキャッシュを増やすことが可能です。
- 復元後のコンテナーのバージョン (存在する場合) が、バックアップファイル内のものと異なっていても構いません。
- [**Connectors**] タブの [**Cache**] カラムで、コネクターの最新のキャッシュサイズが反映されるのに数分かかる場合があります。

注: システムの復元: アプライアンスの工場出荷時設定への復元については、「工場出荷時設定の復元」(318ページ) を参照してください。

第 10章： スナップショット

ここでは、以 下 の内 容 について説 明します。

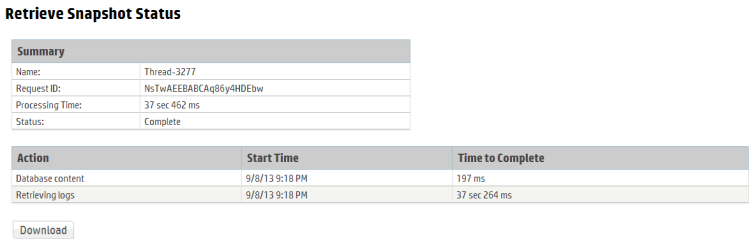
概 要

ArcSight Management Centerでは、通 常 動 作 中 に発 生 する問 題 の詳 細などの、監 査 およびデバッグ情 報 を記 録します。これらのシステムログから、ArcSight Management Centerのアクティビティのスナップショット が作 成 されます。システムログは、問 題 のトラブルシューティングに役 立 ちます。

HPE ArcSightカスタマーサポート から、インシデント 調 査 の一 環 として、システムログの取 得 および送 信 を求 められる場 合 があります。

スナップショット の作 成

ArcSight Management Centerのスナップショット を作 成 すると、zip圧 縮 された一 連 のログファイルが作 成 されます。これらのファイルは、ローカルにダウンロード できます。



スナップショット を作 成 するには

1. **[Administration] > [Application] > [Snapshot]** をクリックします。
2. [**Retrieve Snapshot Status**] ページが表 示 されます。スナップショット の生 成 に要 する時 間 は、ログファイルのサイズによって異 なります。
3. 準 備 ができたら、[**Download**] をクリックしてZIPファイルをローカルにダウンロードします。

HPE ArcSightカスタマーサポート の指 示 に従 って、スナップショット ファイルを送 信 します。

注: ArcSight Management Centerのスナップショットには、リモートから管理されるホスト上のArcSight Management Centerエージェントのアクティビティに関する情報は含まれません。

管理対象ホスト上のArcSight Management Centerエージェントのアクティビティに関するログを取得するには、リモートホストにアクセスします。**[Setup] > [Appliance Snapshot]** で、[**Download**] ボタンをクリックします。

第11章: Logger Consumptionレポート

Logger Consumptionレポートには、Loggerのデータ消費量に関する情報が記載されます。レポートに含める管理対象のLogger (バージョン6.1以降) ノードを選択することができます。

Logger Consumptionレポートを生成するには

1. **[Administration] > [Application] > [Consumption Report]** をクリックします。
2. **追加**および**削除**の矢印を使用し、[**Available Nodes**] カラムから [**Selected Nodes**] カラムへのノードの追加または削除を行います。
3. [**Run Report**] をクリックします。レポートが選択したノードに対して生成されます。
4. [**+**] をクリックしてノードのデータを展開し、ライセンスの詳細を表示します。
5. ライセンスレポートをPDFファイルにエクスポートする場合は、[**Export to PDF**] をクリックします。
6. レポートの時間範囲を指定します。
7. [**OK**] をクリックして、レポートを終了します。

レポートデータ

レポートには、管理対象のLoggerによるデータ消費量のライセンスの値と実際の値が表示されます。

値	説明
Licensed Consumption	ライセンスで許可されたデータ消費量が表示されます。個々のADP Loggerのライセンス制限は「Not Applicable」と表示されます。これは、ArcMCが個々のLoggerのデータ制限ではなく、ADP全体のデータ制限を追跡しているためです。 **注:** ADP Loggerをバージョン2.5より前のArcMCで管理している場合、レポートのライセンス制限が「Unlimited」と誤って表示されます。
Actual Consumption	データ消費量の現在値が表示されます。値をクリックすると、データ消費量の詳細を示す消費量チャートが表示されます。
Status	ステータスのハイパーリンクをクリックすると、過去30日間の個々のLoggerのデータが表示されます。ステータスの値は、次のように表示されます。 OK: 実際の値がライセンスの値以下である場合。 In Violation: 実際の値がライセンスの値を超えていて、ライセンス条件に違反した状態になっている場合。ライセンスでは30日間ごとに一定数の違反が許容されています。これは、Violations Last 30 Daysの行に表示されます。 ハイパーリンクをクリックすると、過去30日間の個々のLoggerのデータが表示されます。

第12章: リポジトリの管理

ここでは、以下の内容について説明します。

概要

一部の管理操作には、特定のアップグレードまたはコンテンツ更新 (.enc) ファイルか、証明書が必要です。ログの表示など、その他の操作には、ログをログリポジトリにロードする必要があります。また、ArcSight Management Centerでは、ホスト設定および管理用のファイルの一元的なリポジトリを維持管理することができます。

デフォルトでは、いくつかのリポジトリがあらかじめ定義されています。しかし、要件に合わせて追加でリポジトリを作成できます。ユーザーが作成したリポジトリは、ユーザー定義リポジトリと呼びます。

リポジトリ機能では、以下のコントロールを使用します。

- **Retrieve Container Files**: 1つ以上の管理対象ホストから、ファイルをリポジトリにコピーします。
- **Upload to Reposity**: ローカルコンピューター (ブラウザーが動作しているコンピューター)、またはローカルコンピューターからアクセス可能なネットワークホストからリポジトリにファイルを送信します。
- **Retrieve**: リポジトリからファイルをダウンロードします。
- **Upload**: リポジトリから1つ以上の管理対象ノードにファイルをコピーします。

リポジトリを使用して、以下の操作を実行できます。

- Logsリポジトリ内のログの管理
- CA Certsリポジトリ内のCA証明書の管理
- Upgradeリポジトリ内で使用できるアップグレードファイルを使用したコネクターのアップグレード

- 1つ以上のコネクターでのコンテンツAUP (ArcSight Update Pack) の適用
- コネクター設定および管理用のファイルの一元的なリポジトリの維持管理

Logsリポジトリ

ログを表示する場合、まずコネクターが含まれているコンテナーのログをLogsリポジトリに**ロード**し、次にログを**取得**して表示する必要があります。

注: コンテナーに複数のコネクターが含まれている場合、すべてのコネクターのログが取得されます。

コンテナーログのロード、取得、削除については、「コンテナーログの表示」(90ページ) を参照してください。

Logsリポジトリへのファイルのロード

ファイルをLogsリポジトリにアップロードすることは、注釈付きのログやその他のファイルを他のユーザーと共有するのに便利です。アップロードファイルは.zip形式になっている必要があります。

ZIPファイルをアップロードするには

1. **[Administration] > [Repositories]** をクリックします。
2. 左パネルで**[Logs]**をクリックします。
3. 管理パネルで **[Upload]** をクリックします。
4. ローカルファイルパスを入力するか、**[Browse]** をクリックしてZIPファイルを選択します。
5. **[Submit]** をクリックして指定したファイルをリポジトリに追加するか、**[Cancel]** をクリックして終了します。

Internet Explorer 11では、ブラウザーの制限により、ファイルアップロードの進行状況は表示されません。

CA Certsリポジトリ

コネクターには、通知先と安全に通信するために、CA (認証局) から発行されるか自己署名されたSSL証明書が必要です。(以下に説明するように) CA Certsリポジトリを使用すると、CA証明書ファイル (1つ以上の証明書を含む) と単一のCA証明書を格納できます。CA Certsリポジトリに証明書が格納されている場合、コンテナー内のコネクターが設定された通知先を検証できるように、コンテナーに証明書を追加することができます。

単一の証明書は、FIPSモードまたは非FIPSモードのコンテナーに追加できます。CA証明書ファイルは、非FIPSモードのコンテナーのみに追加できます。

CA証明書をコネクターに関連付けるには、以下のことが必要です。

- CA証明書またはCA証明書ファイルをCA Certsリポジトリにアップロードします (後述)。
- CA証明書をCA Certsリポジトリからコネクターが含まれるコンテナーに追加します (「コンテナー上の証明書の管理」(94ページ) を参照)。

CA証明書のリポジトリへのアップロード

CA証明書ファイルまたは単一の証明書をCA Certsリポジトリにアップロードできます。

ヒント: 単一のCA証明書をアップロードする前に、ローカルコンピューター上の証明書の名前を、容易に認識できる名前に変更します。これにより、Certificate Management ウィザードに表示されるときに証明書が区別しやすくなります。

証明書をリポジトリにアップロードするには

1. **[Administration] > [Repositories]** をクリックします。
2. 左パネルで**[CA Certs]**をクリックします。
3. 管理パネルで **[Upload]** をクリックします。
4. CA証明書ファイルまたは証明書のローカルパスを入力するか、**[Browse]**をクリックしてファイルを選択します。
5. **[Submit]**をクリックして指定したCA証明書ファイルまたは証明書をリポジトリに追加するか、**[Cancel]**をクリックして終了します。

[CA Certs Repositories] タブには、アップロードされたすべてのCA証明書ファイルと単一の証明書が表示されます。[Type] 列には、単一の証明書の場合は「CERTIFICATE」が、CA証明書ファイルの場合は「CACERT」が表示されます。

CA証明書のリポジトリからの削除

リポジトリから削除したCA証明書ファイルまたは単一の証明書は、ArcSight Management Centerから削除されます。

注: CA証明書ファイルまたは単一の証明書をCA Certsリポジトリから削除しても、コンテナーは影響を受けません。コネクターは、コンテナーに追加された後にトラストストアにある証明書を使用し続けます。CA証明書のコンテナーへの追加については、「コンテナー上の証明書の管理」(94ページ) を参照してください。

証明書をリポジトリから削除するには

1. **[Administration] > [Repositories]** をクリックします。
2. 左パネルで **[CA Certs]** をクリックします。
3. 削除する証明書またはCA証明書ファイルを特定して、それに関連付けられている **[Remove]** ボタン ( ) をクリックします。

Upgrade Filesリポジトリ

Upgrade Filesリポジトリを使用すると、いくつかのコネクターアップグレードファイルを保持できます。これらのアップグレードファイルは、特定のバージョンをアップグレードする必要があるときに適用できます。その結果、コンテナー内のすべてのコネクターが、コンテナーに適用したバージョンにアップグレードされます。

注： LoggerアプライアンスのリモートアップグレードにはLoggerのENCファイルが必要です。詳細については、「Loggerのアップグレード」(82ページ) を参照してください。

AUPアップグレード処理について

注： ここで説明する処理は、コネクターのアップグレードと、リモートで管理されるコネクターアプライアンスのアップグレードにのみ適用されます。ローカルのArcSight Management Center (ローカルホスト) をアップグレードする場合は、代わりにENCファイルを使用します。

コネクターまたはリモートで管理されるコネクターアプライアンスをアップグレードするには、以下のことを行う必要があります。

- 適切な.aupアップグレードファイルをUpgrade Filesリポジトリにアップロードします (後述)。
- .aupアップグレードファイルをUpgrade Filesリポジトリからコンテナーに適用します (「コンテナー内のすべてのコネクターのアップグレード」(88ページ) を参照)。

AUPアップグレードファイルのリポジトリへのアップロード

AUPアップグレードファイルをリポジトリにアップロードするには

1. コネクターまたはリモートコネクターアプライアンス用のアップグレードファイルを、ArcSightカスタマーサポートサイト (http://softwaresupport.hpe.com/) から、ブラウザーベースのインターフェイスに接続するために使用するコンピューターにダウンロードします。
2. アップグレードファイルをダウンロードしたコンピューターから、ブラウザーベースのインターフェ

イスにログインします。

3. **[SetupConfiguration]** > **[Administration]** > **[Repositries]** をクリックします。
4. 左パネルで **[Upgrade AUP]**をクリックします。
5. 管理パネルで **[Upload]** をクリックします。
6. **[Browse]**をクリックし、ダウンロードしたファイルを選択します。
7. **[Submit]**をクリックして指定したファイルをリポジトリに追加するか、**[Cancel]**をクリックして終了します。
8. 続いて、AUPアップグレードファイルを使用して、コンテナーを特定のバージョンにアップグレードできます。「コンテナー内のすべてのコネクターのアップグレード」(88ページ) の説明を参照してください。

コネクターアップグレードのリポジトリからの削除

不要になったコネクターアップグレードファイルはリポジトリから削除できます。リポジトリから削除したコネクターアップグレードファイルは、ArcSight Management Centerから削除されます。

コネクターアップグレードをリポジトリから削除するには

1. **[SetupConfiguration]** > **[Administration]** > **[Repositries]** をクリックします。
2. 左パネルで**[Upgrade AUP]**をクリックします。
3. 削除するアップグレードファイルを探し、対応する✕アイコンをクリックします。

Content AUPリポジトリ

ArcSightは、新しいコネクターイベント分類マッピングを継続的に作成します。これをコンテンツと呼ぶことがあります。このコンテンツは、ArcSight Update Packs (AUP) ファイルにパッケージ化されます。既存のすべてのコンテンツがメジャー製品リリースに含まれていますが、最新の定期的なコンテンツ更新を、ArcSightのアナウンスとそのカスタマーサポートサイトを通じて受信することで、完全に最新の状態に保つことができます。AUPファイルは、[Content Subscription Downloads] の下にあります。

ArcSightArcSightコンテンツAUP機能を使用すると、AUPファイルを、管理している該当のコネクター通知先に適用できます。この機能を使用してコネクターに適用できるのは、イベント分類情報のみです。

Content AUPリポジトリには、複数のコンテンツAUPファイルを保持できます。すでにリポジトリに格納されているものよりもバージョン番号が大きなAUPファイルがロードされると、管理対象のコネクター通知先に自動的にプッシュされます。ただし、以下のコネクターまたはコネクター通知先はスキップされます。

- AUPファイルのプッシュ時点で使用不能なコネクター
- 現在のバージョンが、コンテンツAUPがサポートしているバージョンの範囲内にないコネクター
- コネクター上のESM通知先
- AUP Masterフラグが Yesに設定されたESM通知先を持つコネクターのすべての通知先

また、新しいコネクターが追加された場合、最も大きな番号のコンテンツAUPがその通知先に自動的にプッシュされます。

新しいコンテンツAUPの適用

新しいコンテンツAUPファイルをリポジトリに追加し、該当するすべての管理対象ノードに自動的にプッシュできます。

新しいコンテンツAUPを適用するには

1. 新しいコンテンツAUPバージョンを、サポートサイト (http://softwaresupport.hpe.com/) から、ブラウザーベースのインターフェイスに接続するために使用するコンピューターにダウンロードします。
2. AUPファイルをダウンロードしたコンピューターから、ブラウザーベースのインターフェイスにログインします。
3. **[Administration] > [Repositories]** をクリックします。
4. 左パネルで **[Content AUP]** をクリックします。
5. 管理パネルで **[Upload]** をクリックします。
6. **[Browse]** をクリックし、ダウンロードしたファイルを選択します。
7. **[Submit]**をクリックして指定したファイルをリポジトリに追加し、該当するすべてのコネクターに自動的にプッシュするか、**[Cancel]** をクリックして終了します。

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

- ノード通知先で`GetStatus`コマンドを実行し、`aup[acp].version`の値が適用したAUPバージョンと同じであることを確認します。コネクター通知先でのコマンドの実行については、「コネクターへのコマンドの送信」(112ページ) を参照してください。
- マウスカーソルをコネクター名に合わせて、そのコネクターのすべての通知先に適用されているAUPバージョンを表示します。

古いコンテンツAUPの適用

古いコンテンツAUPをContent AUPリポジトリから適用する必要がある場合は、リポジトリ内の、適用するバージョンよりも新しいすべてのバージョンを削除します。残っているAUPファイルの最新版が、該当するすべてのコネクターに自動的にプッシュされます。

コンテンツAUPをContent AUPリポジトリから削除するには

1. **[Administration] > [Repositories]** をクリックします。
2. 左パネルで**[Content AUP]**をクリックします。
3. 削除するAUPファイルを探し、対応する✕アイコンをクリックします。複数のファイルに対して繰り返します。

緊急復元

緊急復元を使用すると、アプライアンス上の大きく損傷したローカルコンテナーを復元できます。この機能は、ArcSight Management Centerのハードウェアアプライアンスバージョンの、ローカルホスト上のコンテナーでのみサポートされます。

ArcSightでは、コンテナーが大幅に損傷し、使用できなくなった場合のみこの処理を使用することをお勧めします。緊急復元処理では、そのコンテナーに関するすべての情報が削除され、コンテナーが空になります。コネクターは、選択したAUPバージョンに復元されます。

緊急復元を実行するには

1. **[System Admin] > [Repositories]** をクリックします。
2. ナビゲーションパネルで **[Emergency Restore]** をクリックします。
3. ウィザードの指示に従います。
4. コンテナーのSSL証明書を再度インポートします。

ユーザー定義リポジトリ

ユーザー定義リポジトリは、ユーザーが名前を付けた設定の集合であり、コネクターからリポジトリへの特定のファイルのアップロードとダウンロードを制御します。各リポジトリは、指定された`$ARCSIGHT_HOME/user/agent`からの相対的なパスを、アップロードまたはダウンロードされるファイルとして使用します。ArcSightコネクターは、標準的なディレクトリ構造を使用するため、たとえばマップファイルは必ず`$ARCSIGHT_HOME/user/agent` (つまり、インストールパスのルートディレクトリ`$ARCSIGHT_HOME`) の`map/`というフォルダーにあります。

作成されたユーザー定義リポジトリは、左側のメニューの**[New Repository]**という見出しの下に、ユーザー指定の表示名で表示されます。

ユーザー定義リポジトリは、ログファイル、証明書ファイル、マップファイルなど、ファイルの種類と目的でグループ化する必要があります。各ユーザー定義リポジトリには、名前、表示名、項目表示名があます。これらは、リポジトリの [**Settings**] タブの下に記載されます。

ユーザー定義リポジトリ内で参照されるファイルは、指定したホストで一括処理でき、ユーザーのブラウザーホストと交換できます。

ユーザー定義リポジトリの作成

新しいリポジトリはいつでも作成できます。

リポジトリには正しいディレクトリパスが必要です。入力されたパスに、余分なスペースやスペルミスなどの誤りが含まれていると、ファイルは誤ったディレクトリに適用されます。ディレクトリパスを確認するには、Directory.txtファイルにアクセスします。このファイルには、入力したすべてのパスのディレクトリ構造が格納されています。Directory.txtファイルを表示するには、コンテナーログにアクセスして、Directory.txtファイルを探します。

新しいユーザー定義リポジトリを作成するには

1. **[Administration] > [Repositories]** をクリックします。
2. 左パネルの **[Repositories]** セクションにある **[New Repository]** をクリックします。
3. 新しいリポジトリについて、以下の表に示すパラメーターを入力します。

パラメーター	説明
Name	リポジトリの一意の名前。一般に、格納するファイルの種類に基づいて名前を付けます。
Display Name	左側のメニューとタブに表示される名前。[Process 名前]、[View 名前]、[Settings for 名前] のようになります。一般には複数形になります。
Item Display Name	単一の項目を表すために使用される名前。
Recursive	サブフォルダーを含めるにはオンにします。
Sort Priority	デフォルトでは-1。
Restart Connector Process	ファイル操作後にコネクタープロセスを再起動するにはオンにします。
Filename Prefix	取得したファイルの名前に含まれる、識別用の単語。たとえば、マップファイルは次のようにファイル名中の「Map」で識別されます。`localhost_Container_-1.Map-2009-04-06_12-22-25-607.zip`
Relative path (Download)	`$ARCSIGHT_HOME`からの相対的なダウンロード用のパス。たとえば、`user/agent/map`または`user/agent/flexagent`のようになります。`$ARCSIGHT_HOME`中のファイルを指定するには、このフィールドを空白のままにします。 **注**: 相対パスはダウンロードのみで使用されます。

パラメーター	説明
Include Regular Expression	含めるファイル名の記述。すべてのファイルを指定するには「.*」を使用します。次の例では、「map.」、1個以上の数字、「.properties」からなるプロパティファイルを選択します。 map\.[0-9]+\.properties$
Exclude Regular Expression	除外するファイル名の記述。次の例では、特定のプレフィックスを持つファイル、またはagentdataフォルダーに格納されているファイルをすべて除外します。 (agentdata/|cwsapi_fileset_).*$
Delete Before Upload	アップロード前に以前のコピーを削除するにはオンにします。 **注意**: **[Delete Before Upload]**をオンにし、[Relative path (Upload)] を指定しなかった場合、current/user/agent内のすべてのファイルとフォルダーが削除されます。
Delete Groups	$ARCSIGHT_HOME/user/agent/mapディレクトリ内のフォルダーを再帰的に削除するかどうか。
Relative path (Upload)	$ARCSIGHT_HOME/current/user/agent/flexagent/ <コネクター名>からの相対的なアップロード用パス。
Delete Relative Path	リポジトリからファイルをアップロードするときに、**[Relative Path (Upload)]**で指定されたディレクトリとその内容を削除するかどうか。
Delete Include Regular Expression	通常は [Include Regular Expression] と同じ。
Delete Exclude Regular Expression	通常は [Exclude Regular Expression] と同じ。

4. ページの下部にある **[Save]** をクリックします。

   新しいリポジトリが、左側のウィンドウパネルの見出し **[New Repository]** の下に表示されます。

コンテナーファイルの取得

[Retrieve Container Files] ボタンは、1つ以上のコンテナーからファイルをリポジトリにコピーします。取得される具体的なファイルは、リポジトリの設定によって変わります。

コンテナーファイルを取得するには

1. **[Administration] > [Repositories]** をクリックします。
2. 左パネルの **[Repositories]** の下で、コネクターファイルのコピー先のリポジトリの名前をクリックします。
3. 管理パネルで **[Retrieve Container Files]** をクリックします。
4. Retrieve Container Filesウィザードの指示に従います。

リポジトリへのファイルのアップロード

ファイルをリポジトリにアップロードするには

1. **[Administration] > [Repositories]** をクリックします。
2. 左下のパネル (**[Repositories]**の下) で、ファイルのアップロード先のリポジトリの名前をクリックします。
3. 管理パネルで **[Upload To Repository]** をクリックします。
4. Repository File Creationウィザードの指示に従います。[**Individual files**] を選択し、適切なパス情報を使用してZIPファイルを作成します。

   注意: Repository File Creationウィザードの **[Enter the sub folder where the files will be uploaded]** ページで、デフォルトのサブフォルダー名 `lib`を変更**しない**でください。

ユーザー定義リポジトリの削除

ユーザー定義リポジトリを削除するには

1. **[Administration] > [Repositories]** をクリックします。
2. 左パネルで、削除するリポジトリの名前をクリックします。
3. 管理パネルで **[Remove Repository]** をクリックします。

リポジトリ設定の更新

ユーザー定義リポジトリの設定を更新するには

1. **[Administration] > [Repositories]** をクリックします。
2. 左パネルで、設定を更新するリポジトリの名前をクリックします。
3. 管理パネルで **[Settings for <リポジトリ名>]** タブをクリックします。
4. 設定を更新します。
5. ページの下部にある **[Save]** をクリックします。

リポジトリ内のファイルの管理

リポジトリからのファイルの取得

リポジトリからファイルを取得するには

1. **[Administration] > [Repositories]** をクリックします。
2. 左パネルで、ファイルが存在するリポジトリの名前をクリックします。
3. 管理パネルで、取得するファイルに対する  をクリックします。
4. ファイルダウンロード指示に従ってファイルをローカルコンピューターにコピーします。

リポジトリからのファイルのアップロード

リポジトリからファイルをアップロードするには

1. **[Administration] > [Repositories]** をクリックします。
2. 左パネルで、ファイルが存在するリポジトリの名前をクリックします。
3. 管理パネルで、アップロードするファイルの **[Upload to Repository]** をクリックします。
4. Upload Container Filesウィザードの指示に従って、選択したコンテナーにファイルをアップロードします。
5. ファイルが正しくアップロードされていることを以下のようにして確認します。
   - コネクターにSSHアクセスが可能な場合は、コネクターに接続してファイル構造を確認します。
   - コネクターのログを取得して、各コネクターの`Directory.txt`ファイルの内容を確認します。

リポジトリからのファイルの削除

リポジトリからファイルを削除するには

1. **[Administration] > [Repositories]** をクリックします。
2. 左パネルで、ファイルが存在するリポジトリの名前をクリックします。
3. 管理パネルで、削除するファイルの✕をクリックします。

定義済みリポジトリ

コネクター関連の任意のファイルに対してリポジトリを定義できます。以下のリポジトリがあらかじめ定義されています。

- **Backup Files**: コネクターのクローニング (「Backup Files」(226ページ) を参照)
- **Map Files**: イベントデータの強化
- **Parser Overrides**: パーサーのカスタマイズ (「パーサーオーバーライドの追加」(227ページ) を参照)
- **Flex Connector Files**: ユーザー設計コネクターの展開
- **Connector Properties**: `agent.properties`: クローニングのサブセット
- **JDBC Drivers**: データベースコネクター

定義済みリポジトリの設定を表示するには、リポジトリ名をクリックし、管理パネルの **[Settings]** タブをクリックします。定義済みリポジトリの設定は読み取り専用です。

Backup Filesの設定

バックアップファイルのデフォルト設定

名前	デフォルト設定
Name	backup
Display Name	Backup Files
Item Display Name	Backup File
Recursive	オン (はい)
Sort Priority	0
Restart Connector Process	オン (はい)
Filename Prefix	ConnectorBackup
Download Relative Path	
Download Include regular expression	
Download Exclude regular expression	(agentdata/|cwsapi_fileset_).*$
Delete before upload	オン (はい)
Delete groups	オン (はい)
Upload Relative Path	

バックアップファイルのデフォルト設定 (続き)

名前	デフォルト設定
Delete Relative Path	
Delete Include regular expression	
Delete Exclude regular expression	(agentdata/|cwsapi_fileset_).*$

Map Filesの設定

次の表は、マップファイルのデフォルト設定を示しています。

マップファイルの設定

名前	デフォルト設定
Name	map
Display Name	Map Files
Item Display Name	Map File
Recursive	オフ (いいえ)
Sort Priority	5
Restart Connector Process	オフ (いいえ)
Filename Prefix	Map
Download Relative Path	map
Download Include regular expression	map\.[0-9]+\.properties$
Download Exclude regular expression	
Delete before upload	オン (はい)
Delete groups	オフ (いいえ)
Upload Relative Path	
Delete Relative Path	map
Delete Include regular expression	map\.[0-9]+\.properties$
Delete Exclude regular expression	

Parser Overridesの設定

次の表は、パーサーオーバーライドのデフォルト設定を示しています。

パーサーオーバーライドの設定

名前	デフォルト設定
Name	parseroverrides
Display Name	Parser Overrides
Item Display Name	Parser Override
Recursive	オン (はい)
Sort Priority	10
Restart Connector Process	オン (はい)
Filename Prefix	Parsers
Download Relative Path	fcp
Download Include regular expression	.*
Download Exclude regular expression	
Delete before upload	オン (はい)
Delete groups	オン (はい)
Upload Relative Path	
Delete Relative Path	fcp
Delete Include regular expression	.*
Delete Exclude regular expression	

FlexConnector Filesの設定

次の表は、FlexConnectorファイルのデフォルト設定を示しています。

FlexConnectorの設定

名前	デフォルト設定
Name	flexconnectors
Display Name	FlexConnector Files
Item Display Name	FlexConnector File
Recursive	オン (はい)
Sort Priority	15
Restart Connector Process	オン (はい)
Filename Prefix	FlexConnector
Download Relative Path	flexagent

FlexConnectorの設定 (続き)

名前	デフォルト設定
Download Include regular expression	.*
Download Exclude regular expression	
Delete before upload	オン (はい)
Delete groups	オン (はい)
Upload Relative Path	
Delete Relative Path	flexagent
Delete Include regular expression	.*
Delete Exclude regular expression	

Connector Propertiesの設定

コネクタープロパティのデフォルト設定

名前	デフォルト設定
Name	connectorproperties
Display Name	Connector Properties
Item Display Name	Connector Property File
Recursive	オフ (いいえ)
Sort Priority	20
Restart Connector Process	オン (はい)
Filename Prefix	ConnectorProperties
Download Relative Path	
Download Include regular expression	agent\.*
Download Exclude regular expression	
Delete before upload	オフ (いいえ)
Delete groups	オフ (いいえ)
Upload Relative Path	
Delete Relative Path	
Delete Include regular expression	agent\.*
Delete Exclude regular expression	

JDBCドライバーの設定

次の表は、JDBCドライバーのデフォルト設定を示しています。

JDBCドライバーの設定

名前	デフォルト設定
Name	jdbcdrivers
Display Name	JDBC Drivers
Item Display Name	Connector JDBC Driver File
Recursive	オフ (いいえ)
Sort Priority	25
Restart Connector Process	オン (はい)
Filename Prefix	
Download Relative Path	lib
Download Include regular expression	
Download Exclude regular expression	
Delete before upload	オフ (いいえ)
Delete groups	オフ (いいえ)
Upload Relative Path	
Delete Relative Path	lib
Delete Include regular expression	
Delete Exclude regular expression	

Backup Files

Backup Filesリポジトリを使用して、コンテナーを他のコンテナーに素早くコピーできます。その結果、コピー元コンテナー内のすべてのコネクターが、コピー先コンテナーにコピーされます。この処理は、コンテナー設定のクローニングと呼ばれます。コンテナーは、一度に複数のコンテナーにクローニングできます。コピー元コンテナーの内容で、コピー先コンテナーの現在の内容が置き換えられます。

注意: ArcSight Management Center上のコンテナーは、最新のコネクターリリースとともにプリインストールされます。古いソフトウェアベースのコネクター (ビルド4.0.8.4964など) を、新しいコネクタービルド (4.0.8.4976以降など) のコンテナーにクローニングしないでください。

Backupリポジトリを使用したコネクターのクローニングは、コネクターのバージョン番号が同じ場合のみ機能します。

Backup Filesリポジトリを使用してコンテナーをクローニングするには

1. **[Node Management] > [View All Nodes]** をクリックします。
2. **[Containers]** タブをクリックして、コンテナーの一覧を表示し、クローニングのコピー元とコピー先を決定します。
3. **[Administration] > [Repositories]** をクリックします。
4. 管理パネルの **[Repositories]** セクションにある **[Backup Files]** をクリックします。
5. クローニングで使用する必要があるバックアップファイルがリポジトリに存在する場合は、次のステップに進みます。そうでない場合は、「リポジトリからのファイルの取得」(221ページ)の手順に従って、コンテナーのバックアップファイルをBackupリポジトリに取得します。

   取得したファイルの名前の形式は、<コネクター名> ConnectorBackup <日付>となります。
6. 「リポジトリからのファイルのアップロード」(221ページ) の手順に従って、バックアップファイルを1つ以上のコンテナーにアップロードします。

   コピー先コンテナーは、バックアップファイルが適用されコネクターが再起動されている間は使用できません。

   注： バックアップファイルには、コンテナーの証明書が含まれていません。バックアップファイルをアップロードした後で、証明書をコンテナーに適用し直す必要があります。

   証明書を適用した後、コピー先コンテナーのステータスでコンテナーが使用可能になっていることを確認してください。

パーサーオーバーライドの追加

パーサーオーバーライドは、ArcSightによって提供されるファイルであり、特定のコネクターでのパーサーの問題を解決したり、ログファイルの形式がわずかに変更されるか、新たなイベントタイプが追加された、サポートされているデバイスの新バージョンをサポートするために使用されます。

パーサーオーバーライドを使用するには、以下の手順を実行する必要があります。

- パーサーオーバーライドファイルを、**Parser Overrides**リポジトリにアップロードします。
- パーサーオーバーライドファイルを、パーサーオーバーライドを使用するコネクターが格納されているコンテナーにダウンロードします。

以下の手順に従ってください。

パーサーオーバーライドファイルをアップロードするには

1. **[Administration] > [Repositories]** をクリックします。
2. 管理パネルの **[Repositories]** セクションにある **[Parser Overrides]** をクリックします。
3. **[Parser Overrides]** タブで、**[Upload To Repository]** ボタンをクリックします。
4. ウィザードに従ってファイルをアップロードします。ウィザードから入力を求められた場合は、以下のようにします。
   - **[Select the type of file that you want to upload]** フィールドから **[Individual Files]** オプションを選択します。
   - フォルダー名を **[Enter the sub folder where the files will be uploaded]** フィールドに追加する前に、fcpの後にスラッシュ (/) を追加します。たとえば、`fcp/multisqlserver_audit_db`と指定します。

     アップロードが完了すると、パーサーオーバーライドファイルが [Parser Overrides] タブの表に表示されます。

パーサーオーバーライドファイルをコンテナーにダウンロードするには

1. **[Administration] > [Repositories]** をクリックします。
2. 管理パネルの **[Repositories]** セクションにある **[Parser Overrides]** をクリックします。
3. **[Parser Overrides]**タブの表で、ダウンロードするパーサーオーバーライドファイルを探し、ファイルの横の上矢印をクリックします。
4. ウィザードに従って、パーサーオーバーライドの追加先となるコンテナーを選択します。

   ウィザードが完了すると、パーサーオーバーライドが選択したコンテナーに展開されます。

> **注：** パーサーオーバーライドファイルはArcExchangeからダウンロードできます。詳細については、「ArcExchangeでのコネクターの共有」(119ページ) を参照してください。

パーサーオーバーライドが正常に適用されていることを確認するには、コネクターに対してGet Statusコマンドを実行します。「コネクターへのコマンドの送信」(112ページ) を参照してください。表示されるレポートで、`ContentInputStreamOverrides`というテキストで始まる行を確認してください。

第13章: システム管理

この章では、ユーザーとユーザーグループの作成および管理、SMTPなどのシステム設定システムのネットワーク、ストレージ、セキュリティ設定を行うためのシステム管理ツールについて説明します。

この章には、次の領域のシステム管理に関する情報が含まれています。

システム

[System] タブでは、ネットワーク設定 (該当する場合) やSMTPなどのシステム固有の設定項目を設定できます。

システムの再起動

システムを再起動またはシャットダウンするには

1. 上部のメニューバーから **[Administration] > [Setup] > [System Admin]** をクリックします。
2. **[System]**セクションの**[System Reboot]**をクリックします。
3. 以下のオプションから選択します。

ボタン	説明
Reboot	システムは約60秒後に再起動します。 再起動処理には、一般に5〜10分かかり、その間はシステムを使用できなくなります。
Reboot in 5 Minutes	システムは5分間の遅延後に再起動します。 再起動処理には、一般に5〜10分かかり、その間はシステムを使用できなくなります。
Shutdown	システムを自動的にシャットダウン (電源オフ) します。

注: 上記の各アクションはキャンセルできます。[Reboot] と [Shutdown] では、**60秒** 以内であればキャンセルできます。[Reboot in 5 Minutes] は、**300秒** 以内であればキャンセルできます。

4. **[Reboot]**、**[Reboot in 5 Minutes]**、または**[Shutdown]**をクリックして選択したアクションを実行します。

ネットワーク

System DNS

[**System DNS**] タブでは、DNS設定の編集や、DNS検索ドメインの追加を行うことができます。

DNS設定を変更するには

1. 上部のメニューバーから **[Administration] > [Setup] > [System Admin]** をクリックします。
2. **[System]**セクションの**[Network]**をクリックします。
3. **[System DNS]**タブで、プライマリおよびセカンダリDNSサーバーのIPアドレスの新しい値を入力するか、検索ドメインのリストを編集します。

   新しいドメインを追加するには、⊞アイコンをクリックします。ドメインを削除するには、⊟アイコンをクリックします。ドメインの検索順序を変更するには、ドメイン名を選択し、上下の矢印をクリックして、ドメインを目的の位置に移動します。
4. **[Save]** をクリックします。
5. **[Restart Network Service]** をクリックして、変更内容を有効にします。

Hosts

[Hosts] タブでは、システムの`/etc/hosts`ファイルを直接編集できます。[System Hosts] テキストボックスにデータを入力するか、ローカルファイルからデータをインポートします。

ホスト情報を変更するには

1. 上部のメニューバーから **[Setup] > [System Admin]** をクリックします。
2. **[System]**セクションの**[Network]**をクリックし、**[Hosts]**タブをクリックします。
3. **[System Hosts]**テキストボックスに、次の形式でホスト情報を入力します (1行に1ホスト)。

   ```
   <IP Address> <hostname1> <hostname2> <hostname3>
   ```

ファイルから情報をインポートするには、**[Import from Local File]** をクリックし、システムへのアクセスに使用しているコンピューター上のテキストファイルを参照します。

4. [**Save**] をクリックします。

NICs

[NICs]タブでは、システム上のNIC (ネットワークインターフェイスカード) のIPアドレスを設定できます。また、システムのホスト名とデフォルトゲートウェイを設定することもできます。

NICを設定または設定変更するには

1. 上部のメニューバーから **[Setup] > [System Admin]** をクリックします。
2. **[System]**セクションの**[Network]** をクリックします。
3. **[NICs]** タブで、以下の設定を入力します。NICのIPアドレス、サブネットマスク、または速度/二重モードを編集するには、NICを選択し、[NIC Name] リストの上にある **[Edit]** をクリックします。

設定	説明
Default Gateway	デフォルトゲートウェイのIPアドレス。
Hostname	このシステムのネットワークホスト名。DNSが、指定したホスト名をシステムのIPアドレスに解決できることを確認してください。DNSがホスト名を解決できない場合、パフォーマンスに大きな影響があります。 この名前は、「CSR (証明書署名リクエスト) の生成」(259ページ) で説明する証明書署名リクエストで指定したドメインと同じであることが必要です。 **注:** 以前自己署名証明書またはCA署名証明書をこのシステムで使用しており、ここでそのホスト名を変更しようとしている場合、新しい自己署名証明書またはCSRを生成し直す必要があります。取得した新しい証明書をアップロードして、システムと通信するコネクターがホスト名を検証できるようにする必要があります。CSRの生成の詳細については、「CSR (証明書署名リクエスト) の生成」(259ページ) を参照してください。
Automatically route outbound packets (interface homing)	このオプションを有効 (チェックボックスをオン) にすると、要求パケットが到着したのと同じシステムインターフェイス上で応答パケットが返送されます。このオプションを有効にすると、パフォーマンスが向上する可能性があります。システムからパケットを送出するために、デフォルトゲートウェイの情報と静的経路を使用したルーティングの判断を行う必要がなくなるためです。静的経路を設定している場合、この機能を有効にすると、設定済みの静的経路は無視されます。 この機能を無効 (チェックボックスをオフ) にすると、静的経路 (設定している場合) を使用して応答パケットをシステムから送出するインターフェイスが決定されます。 ネットワークインターフェイスを1つしか設定しない場合、この設定項目による利点はありません。

設定	説明
IP Address	システム内の各NIC (ネットワークインターフェイスカード) のIPアドレス。 **NICエイリアスの追加** 表示されているどのNICにもエイリアスを作成できます。そのためには、以下の手順を実行します。 a. エイリアスを作成するNICを強調表示します。 b. **[Add]** をクリックします。 c. エイリアス用に別のIPアドレスを作成します。 d. **[Save]** をクリックします。 オリジナルには、コロンと、特定のNICに対して作成したエイリアスの数を示す数字が追加されるので、エイリアスと区別できます。 **注:** • IPエイリアスの速度を変更することはできません。 • エイリアスは何個でも作成できます。
Subnet Mask	NICに入力したIPアドレスに対応するサブネットマスク。
Speed/Duplex	速度と二重モードを選択するか、ネットワーク速度をシステムに自動判定させます。 Auto (推奨) 10 Mbps - Half Duplex 10 Mbps - Full Duplex 100 Mbps - Half Duplex 100 Mbps - Full Duplex 1 Gbps - Full Duplex

4. **[Save]** をクリックします。
5. **[Restart Network Service]** をクリックして、変更内容を有効にします。

Static Routes

システム上のNICに静的経路を指定できます。

静的経路を追加、編集、削除するには

1. 上部のメニューバーから **[Setup] > [System Admin]** をクリックします。
2. **[System]** セクションの **[Network]** をクリックします。
3. **[Static Routes]** タブで、以下の手順を実行します。
   - 新しい静的経路を追加するには、**[Add]** をクリックします。
   - 既存の経路を編集または削除するには、まず経路を選択し、**[Edit]** または **[Delete]** をクリックします。

静的経路を追加または編集する場合は、次の設定項目を設定する必要があります。

設定	説明
Type	静的経路がネットワーク宛かホスト宛か
Destination	静的経路の宛先のIPアドレス
Subnet Mask	宛先としてネットワークを指定した場合はサブネットマスク
Gateway	経路のゲートウェイのIPアドレス

4. **[Save]** をクリックします。

Time/NTP

[**Time/NTP**] タブでは、システム時刻、日付、ローカルタイムゾーン、およびNTPサーバーを設定できます。HPE Securityでは、システムの時刻と日付を手動で設定する代わりに、NTPサーバーを使用することを強く推奨しています。

システム時刻、日付、タイムゾーンを手動で設定または変更するには

注意: 日付と時刻を手動で設定し、NTPサービスも使用している場合、手動で入力する日付と時刻は、NTPサーバーから渡される日付と時刻よりも16分以上進んでいたり遅れていたりしてはなりません。手動で入力した時刻がNTPサーバーの時刻と16分以上違う場合、NTPサービスが起動に失敗します。

1. 上部のメニューバーから **[Setup] > [System Admin]** をクリックします。
2. **[System]** セクションの **[Network]** をクリックします。
3. [**Time/NTP**] タブで、次の設定項目を設定します。

設定	説明
Current Time Zone	システムの場所に該当するタイムゾーン。この設定を変更するには、**[Change Time Zone]** をクリックします。 ローカルタイムゾーンは、その地域のDST (サマータイム) 規則に従います。GMT (グリニッジ標準時刻) +および-タイムゾーンは、DSTに関知しません。 たとえば、米国/ロサンゼルスのタイムゾーンは、DSTが開始および終了する際に、GMTと比べて1時間違います。 • 太平洋標準時 (PST) = GMT-8 • 太平洋夏時間 (PDT) = GMT-7
Current Time	システムがある場所の現在の日付と時刻。この設定を変更するには、[**Change Date/Time...**] をクリックして、現在の日付と時刻を入力します。

4. タイムゾーンを変更すると、アプライアンスの再起動が必要になります。ただし、現在時刻の変更はすぐに有効になります。

NTPサーバーとしてシステムを設定、またはシステムに対するNTPサーバーを使用するようにシステムを設定するには

1. 上部のメニューバーから **[Setup] > [System Admin]** をクリックします。
2. **[System]** セクションの **[Network]** をクリックします。
3. **[Time/NTP]** タブをクリックします。
4. **[NTP Servers]** で以下の設定を行います。

   新しいNTPサーバーを追加するには、⊞アイコンをクリックします。サーバーを削除するには、⊟アイコンをクリックします。NTPサーバーを使用する順序を変更するには、サーバーを選択し、NTPサーバーを目的の位置になるまで上下矢印をクリックします。

設定	説明
Enable as an NTP server	このシステムをNTPサーバーとして使用する場合はこの設定をオンにします。
NTP Servers	NTPサーバーのホスト名を入力します。たとえば、time.nist.govと入力します。 HPE Securityでは、システムの時刻が正確になるように、2台以上のNTPサーバーを使用することをお勧めします。複数のNTPサーバーを入力するには、1行に1つのサーバー名を入力します。 注: • ArcSightシステムは、他のArcSightシステムに対するNTPサーバーとしての役割を果たすことができます。 • システムAがシステムBに対するNTPサーバーとして機能する場合、システムBでは、システムAが **[NTP Servers]** リストに表示されている必要があります。 • **[Test Servers]** ボタンを使用すると、**[NTP Servers]** ボックスに入力したサーバーのステータスを確認できます。

5. **[Save]** をクリックします。

   ヒント: [Save] ボタンと **[Restart NTP Service]** ボタンを表示するには、下にスクロールすることが必要な場合があります。

6. **[Restart NTP Service]** をクリックして、変更内容を有効にします。

SMTP

システムは、SMTP (Simple Mail Transfer Protocol) 設定を使用して、アラートやパスワードリセットのメールなど、メール通知を送信します。

SMTPの設定を追加または変更するには

1. **[Administration] > [Setup] > [System Admin]** をクリックします。
2. **[System]** セクションの **[SMTP]** をクリックし、以下の設定の値を入力します。

設定	説明
Primary SMTP Server	送信メールを処理するSMTPサーバーのIPアドレスまたはホスト名。
Backup SMTP Server	プライマリSMTPサーバーが使用不能な場合に送信メールを処理するSMTPサーバーのIPアドレスまたはホスト名。
Outgoing Email Address	送信メールの「From:」フィールドに表示されるメールアドレス。

3. **[Save]** をクリックします。

ライセンスと更新

このページには、ライセンス情報、コンポーネントのバージョン、最後にArcSight Management Centerを再起動再起動してからの経過時間が表示されます。ここから、ArcSight Management Centerの更新やライセンスの適用を行うことができます。

アプライアンスの更新

ArcSight Management Centerを更新するには

1. HPEサポートサイト (http://softwaresupport.hpe.com) から、ArcSight Management Centerに接続できるコンピューターに更新ファイルをダウンロードします。
2. 上部のメニューバーから **[Administration] > [Setup] > [System Admin]** をクリックします。
3. **[System]**セクションの**[License & Update]**をクリックします。
4. **[Browse]**をクリックしてファイルを探します。
5. **[Upload Update]**をクリックします。

   [Update in Progress] ページに更新の進行状況が表示されます。
6. 更新が完了すると、[Update Results] ページに更新結果 (成功/失敗) と、再起動が必要かどうかが表示されます。再起動が必要な場合、ArcSight Management Centerは自動的に再起動します。

ライセンスファイルの更新

ライセンスファイルを更新するには

1. HPEサポートサイト (http://softwaresupport.hpe.com) から、ArcSight Management Centerにブラウザーで接続できるコンピューターにライセンス更新ファイルをダウンロードします。
2. ライセンス更新ファイルをダウンロードしたコンピューターから、管理者 (アップグレード) 権限を持っているアカウントを使用して、ArcSight Management Centerユーザーインターフェイスにログインします。
3. **[Administration] > [System Admin]** をクリックします。
4. **[System]** セクションの **[License & Update]** をクリックします。
5. ダウンロードしたライセンスファイルを参照し、**[Upload Update]** をクリックします。
   [Update in Progress] ページに更新の進行状況が表示されます。

更新が完了すると、[Update Results] ページに更新結果 (成功/失敗) が表示されます。ライセンスのインストールまたは更新だけを行う場合、リブート再起動は不要です。

注: ライセンスファイルの更新が済んだら、ブラウザーを更新して、有効になっている機能の最新リストを確認してください。

Process Status

[Process Status]ページには、システムに関連するすべてのプロセスの一覧が表示され、それらのプロセスの詳細を表示したり、プロセスを開始、停止、再起動できます。

[Process Status] ページを表示するには

1. **[Administration] > [Setup] > [System Admin]** をクリックします。
2. **[System]** セクションで **[Process Status]** をクリックします。
3. プロセスの詳細を表示するには、プロセス名の左側にある⊞アイコンをクリックします。
4. プロセスを開始、停止、再起動するには、プロセスを選択して、**[Processes]** リストの上部にある **[Start]**、**[Stop]**、または**[Restart]**をクリックします。

System Settings

インストール手順の中で、ArcSight Management Centerをサービスとして起動することを選択しなかった場合は、**[System Settings]**ページを使用してこの設定を行うことができます。

サービスとして起動するようにArcSight Management Centerを設定するには

1. **[Administration] > [Setup] > [System Admin]** をクリックします。
2. 左パネルで **[System Settings]** をクリックします。
3. **[Service Settings]** の下で、以下の適切なオプションを選択します。
   - Start as a Service
   - Do not start as a Service
4. **[Save]** をクリックします。

SNMP

SNMP (Simple Network Management Protocol) を使用すると、アプライアンスのヘルスを監視できます。ArcMCは、SNMPのバージョン2cおよび3をサポートしています。

SNMP設定

SNMPのポーリングと通知を設定できます。SNMPポーリングが設定されている場合、管理ステーションからArcMC上にあるSNMPエージェントにクエリを実行できます。取得した情報から、ハードウェアレベルおよびOSレベルの詳細を把握できます。

SNMPポーリングを設定するには

1. メインのメニューバーで、**[Adminstration] > [Setup] > [System Admin]** をクリックします。
2. ナビゲーションツリーの [**System**] の下で、[**SNMP**] をクリックします。
3. [**SNMP Poll Configuration**] タブで、[**Enabled**] が選択されていることを確認します。
   - [**Port**] は、デフォルトは161ですが、利用可能な任意のポートを指定できます。指定したポートはファイアウォール上で開いておく必要があります。
   - [**SNMP version**] では、V2cまたはV3を選択します。
     - V2cを選択した場合は、英数字、アンダースコア、およびダッシュから成る6～128文字のコミュニティ文字列を指定します。
     - V3を選択した場合は、ユーザー名 (4～16文字の英数字の小文字の文字列で、必ず英字から始まり、アンダースコアを含めることができます)、認証プロトコル、認証パスフレーズ (4～256文字)、プライバシープロトコル、およびプライバシーパスフレーズ (4～256文字) を指定します。
4. **[Save]** をクリックします。

SNMP通知先が設定されている場合、ArcMCは一部のイベントに関する通知を送信できます (「SNMPシステム情報の表示」(238ページ) を参照)。

SNMP通知は、コネクターによって送信される、一般的なArcSightイベントに関する通知とは異なります。ここに示す通知は単一のイベントに対応したもので、HPE NMMiなどのネットワーク管理システムを使用することで容易に把握できます。

SNMP通知の通知先を設定するには

1. メインのメニューバーで、**[Adminstration] > [System Admin]** をクリックします。
2. ナビゲーションツリーの **[System]** の下で、**[SNMP]** をクリックします。
3. [**SNMP Destination**] タブで、[**Enabled**] が選択されていることを確認します。続いて、既存のNMSのSNMP設定に合わせて、その他のパラメーターの値を入力します。
   - [Port] には、162を入力します。(注: デフォルト以外のポートを指定すると、短時間の遅延が発生することがあります。処理が完了するのを待ちます。)
   - [SNMP version] では、V2cまたはV3を選択し、要求された設定項目の値を入力します。
4. **[Save]** をクリックします。

SNMPシステム情報の表示

SNMP通知は、任意のMIBブラウザーで表示できます。次のSNMP通知がサポートされています。

- **Application**
  - Login attempt failed
  - Password change attempt failed
  - User account locked
  - Reboot command launched
  - Manual backup failed
  - Enable FIPS mode successful
  - Disable FIPS mode successful
  - Enable FIPS mode failed
  - Disable FIPS mode failed
- **Platform**
  - CPU Usage
  - Memory Usage
  - Disk Almost Full
  - Fan Failure
  - Power Supply Failure
  - Temperature Out of Range
  - Ethernet Link Down

MIBブラウザーでシステム通知を表示するには

アプライアンス上で次の操作を実行します。

以下のURLを使用して、ArcSight MIBファイルおよび他の標準のNet-SNMP MIBファイルをダウンロードできます。

- https://<system_name_or_ip>/platform-service/ARCSIGHT-EVENT-MIB.txt
- https://<system_name_or_ip>/platform-service/DISMAN-EVENT-MIB.txt
- https://<system_name_or_ip>/platform-service/HOST-RESOURCES-MIB.txt
- https://<system_name_or_ip>/platform-service/IF-MIB.txt
- https://<system_name_or_ip>/platform-service/UCD-SNMP-MIB.txt

標準MIBブラウザーで次の操作を実行します。

1. MIBをロードします。
2. SNMPエージェント (ここではアプライアンス) のアドレスとポート番号を指定します。
3. アプライアンス上で設定されているコミュニティ文字列を設定します。
4. ブラウザーからOIDのsnmp WALK操作を開始します。
5. SNMPデータが返されたら、このセクションで説明した情報に基づいて解釈します。

MIBコンテンツ

通知はMIBファイルの以下のモジュールに書き込まれます。

モジュール	通知タイプ
HOST-RESOURCES-MIB	標準的なハードウェアパラメーター。
IF-MIB	ネットワークインターフェイスのオブジェクト。
IP-MIB	IPおよびICMPのインプリメンテーション。
DISMAN-EVENT-MIB	標準的なネットワーク管理用のイベントトリガーおよびアクション。

アプライアンスへのSSHアクセス

アプライアンスへのSSHアクセスを有効にすることができます。デフォルトでは、アプライアンスへのSSHアクセスは無効になっています。セキュリティを適切に確保するため、トラブルシューティング時など、必要な場合にのみSSHアクセスを有効にすることを強く推奨します。

注意: デフォルトでは、SSHを使用してログインする際に、チャレンジ/レスポンスの入力は求められません (これは、コネクターアプライアンスの設定からの変更点です)。

このため、ArcSight Management Centerアプライアンスの “root” アカウントのデフォルトパスワードは、できるだけ早く新しい強力なパスワードに変更する必要があります。デフォルトのrootパスワードを入手する必要がある場合は、HPE ArcSightカスタマーサポートまでご連絡ください。

有効化に関するオプションは、次のとおりです。

- Disabled: SSHアクセスは有効ではありません。これがデフォルト値です。
- Enabled: SSHアクセスは常に有効です。
- Enabled, only for 8 hours: SSHアクセスは、有効にしてから8時間後に自動的に無効になります。
- Enabled, only during startup/reboot: SSHアクセスは、アプライアンスが再起動している間だけ有効になります。アプライアンス上のすべてのプロセスが起動されると無効になります。このオプションは、アプライアンスが再起動後に正常に起動しないといった状況で、最低限の期間のSSHアクセスを可能にします。

  注: アプライアンスでSSHが無効になっている場合でも、HPE Security ProLiant Integrated Lights-Out (iLO) Advancedリモート管理カードを使用して、リモートアクセス用にコンソールが設定されていれば、コンソールにアクセスできます。

SSHアクセスの有効化と無効化

アプライアンスへのSSHアクセスを有効または無効にするには

1. 上部のメニューバーから **[Administration] > [Setup] > [System Admin]** をクリックします。
2. **[System]** セクションの **[SSH]** をクリックします。
3. SSHの有効化に関するオプションを選択します。
4. 選択したオプションを確認します。変更内容はただちに反映されます。

SSHを使用したアプライアンスへの接続

SSHアクセスを有効にした後、SSHを使用してアプライアンスに接続するには、以下の手順に従います。

1. SSHクライアントを使用し、「root」としてアプライアンスに接続します。
2. パスワードの入力を求めるプロンプトが表示されたら、パスワードを入力し、**Enter**を押します。

診断ツール

ArcSight Management Centerでは、アプライアンスのセットアップ、管理、およびトラブルシューティングに役立つ複数の診断ツールが利用できます。これらの診断ツールは、ローカルのアプライアンスに対してのみ実行できます。リモートコンテナーに対して診断ツールを実行する場合は、「コンテナーに対する診断の実行」(98ページ)を参照してください。

診断ツールにアクセスするには

1. 上部のメニューバーから **[Administration] > [Setup] > [System Admin]** をクリックします。
2. 左パネルの [**System**] セクションにある [**Diagnostic Tools**] をクリックして、[Diagnostic Tools] ページを開きます。
3. [**Tools**] ドロップダウンメニューから、使用するツールを選択します。
4. 選択したツールに必要なパラメーターを入力し、[**Run**] をクリックします (Edit text fileツールの場合は、[**Edit**] をクリックします)。

各ツールおよび使用可能なパラメーターとボタンについての説明を以下に示します。

Display I/O Statistics

Display I/O Statisticsツールは、アプライアンス上のデバイス、パーティション、およびネットワークファイルシステムのI/O統計情報を監視するのに使用します。このツールは、Linuxコマンド `iostat`と同等です。

このツールでは、以下に示すパラメーターを使用します。

パラメーター	説明
Match Expression	式を入力すると、その式と一致するファイル内の行のみが表示されます。Linuxの正規表現がサポートされています。 **注:** 正規表現では、大文字と小文字を区別します。
Exclude Expression	式を入力すると、その式と一致する行が表示から除外されます。Linuxの正規表現がサポートされています。 **注:** 正規表現では、大文字と小文字を区別します。

Display file

Display fileツールは、ファイルの内容を表示するのに使用します。このツールは、Linuxコマンド `cat`と同等です。

このツールでは、以下に示すパラメーターを使用します。

パラメーター/ボタン	説明
Category	表示するファイルのタイプを選択します。
File	[**Category**] フィールド (上記) で選択したタイプのファイルのリストが表示されます。リストから表示するファイルを選択します。 **注:** アプライアンスモデルCx400には、ブートログファイルが存在しません。[**File**] のリストから [**Boot Log**] を選択すると、空のポップアップウィンドウが表示されます。
Match Expression	式を入力すると、その式と一致するファイル内の行のみが表示されます。Linuxの正規表現がサポートされています。 **注:** 正規表現では、大文字と小文字を区別します。
Exclude Expression	式を入力すると、その式と一致する行が表示から除外されます。Linuxの正規表現がサポートされています。 **注:** 正規表現では、大文字と小文字を区別します。
Display	表示する行数を制限できます。 • ファイルの先頭から数えて、[**Number of Lines**] フィールド (下記) で指定した行数のみを表示する場合は、[**Beginning of file**] を選択します。 • ファイルの末尾から数えて、[**Number of Lines**] フィールド (下記) で指定した行数のみを表示する場合は、[**End of file**] を選択します。 **注:** [**Beginning of file**] または [**End of file**] を選択した場合は、下記の [**Number of Lines**] フィールドの値も指定する必要があります。 ファイル内のすべての行を表示する場合は、[**Display**] と [**Number of Lines**] フィールドを両方とも空白のままにしておきます。
Number of Lines	ファイルの先頭または末尾から表示する行数を指定します。 一致式を入力した場合は、その式のファイルの先頭 ([Beginning of file] を選択した場合) または末尾 ([End of file] を選択した場合) から数えた件数の表示が表示に含まれ、除外式を入力した場合は、表示から除外されます。たとえば、[**Exclude Expression**] フィールドにTCPと入力し、[**Display**] ドロップダウンから [**Beginning of file**] を選択して、[**Number of Lines**] フィールドに10と入力した場合、式TCPに一致する箇所のうち、ファイルの先頭から数えて最初の10個が表示に含まれます。 **注:** ファイル内のすべての行を表示する場合は、このフィールドと [**Display**] フィールド (上記) を空白のままにしておきます。
Run	このボタンをクリックすると、選択したファイルの内容が表示されます。ファイルの内容はポップアップウィンドウに表示されます。

Display network connections

Display network connectionsツールは、ネットワーク接続とトランスポートプロトコルの統計情報を確認するのに使用します。ステータス情報から、プロトコルで問題の起きている領域を把握できます。

このツールは、Linuxコマンド `netstat -pn [-t] [-u] [-w] [a] [-l] [-c]` と同等です。

このツールでは、以下に示すパラメーターを使用します。

パラメーター/ボタン	説明
Protocol	このフィールドを空白のままにして、すべてのトランスポートプロトコルの統計情報を表示するか、次のオプションの中から選択します。 • **RAW only**: Raw IPプロトコルの統計情報が表示されます。このオプションは、`netstat` Linuxコマンドの`-w`オプションと同等です。 • **TCP only**: TCPプロトコルの統計情報が表示されます。このオプションは、`netstat` Linuxコマンドの`-t`オプションと同等です。 • **UDP only**: UDPプロトコルの統計情報が表示されます。このオプションは、`netstat` Linuxコマンドの`-u`オプションと同等です。
Connection	このフィールドを空白のままにして、すべての非リッスン接続の統計情報を表示するか、次のオプションの中から選択します。 • **All connections**: 現在のすべての接続の情報が表示されます。このオプションは、`netstat` Linuxコマンドの`-a`オプションと同等です。 • **Listening connections**: リッスンしている接続のみの情報が表示されます。このオプションは、`netstat` Linuxコマンドの`-l`オプションと同等です。
Mode	[**Run Continuously**] を選択すると、ネットワークステータスが5分おきに継続的にポーリングされます。このオプションは、`netstat` Linuxコマンドの`-c`オプションと同等です。 [**Run Continuously**] を選択しない場合は、ネットワークステータスが1回だけポーリングされます。
Match Expression	式を入力すると、その式と一致する行のみが出力に表示されます。Linuxの正規表現がサポートされています。
Exclude Expression	式を入力すると、その式と一致する行が出力から除外されます。Linuxの正規表現がサポートされています。
Run	このボタンをクリックすると、ネットワーク接続情報が表示されます。この情報はポップアップウィンドウに表示されます。

Display network interface details

Display network interface detailsツールは、アプライアンス上の現在アクティブなインターフェイスのステータスを表示するのに使用します。このツールは、Linuxコマンド`ifconfig`と同等です。

このツールでは、以下に示すパラメーターを使用します。

パラメーター/ボタン	説明
Interface	ステータスを表示するアプライアンス上のネットワークインターフェイスを選択します。 **注:** このフィールドを空白のままにすると、アクティブなすべてのネットワークインターフェイスのステータスが表示されます。
Run	このボタンをクリックすると、選択したネットワークインターフェイスのステータスが表示されます。ステータスはポップアップウィンドウに表示されます。

Display network traffic

Display network trafficツールは、ネットワークで送受信されるパケットを監視するのに使用します。このツールは、Linuxコマンド`tcpdump`と同等です。

このツールでは、以下に示すパラメーターを使用します。

パラメーター/ボタン	説明
Host	監視するホストのIPアドレスまたはホスト名を指定します。
Match Expression	式を入力すると、その式と一致するネットワークトラフィックのみが表示されます。たとえば、式`echo`を指定すると、式`echo`を含む指定されたホストからのネットワークトラフィックのみが表示されます。 Linuxの正規表現がサポートされています。
Exclude Expression	式を入力すると、その式と一致するネットワークトラフィックが表示から除外されます。たとえば、式`echo`を指定すると、`echo`を含むトラフィックを除くすべてのトラフィックが表示されます。 Linuxの正規表現がサポートされています。
Run	このボタンをクリックすると、アプライアンスと指定されたホストとの間のネットワークトラフィックが表示されます。この情報はポップアップウィンドウに表示されます。

Display process summary

Display process summaryツールは、現在実行中のプロセスのリストを表示し、実行されている時間を確認するのに使用します。このツールは、次のLinuxコマンドと同等です。

```
top -b -n 1
```

このツールでは、以下に示すパラメーターを使用します。

パラメーター/ボタン	説明
Match Expression	式を入力すると、その式と一致するプロセスのみが表示されます。Linuxの正規表現がサポートされています。
Exclude Expression	式を入力すると、その式と一致するプロセスが出力から除外されます。Linuxの正規表現がサポートされています。
Run	このボタンをクリックすると、現在実行中のプロセスのリストが表示されます。リストはポップアップウィンドウに表示されます。

Display routing table

Display routing tableツールは、アプライアンスからのトラフィックが経由しているルートを参照するのに使用します。このツールは、Linuxコマンド`ip route`と同等です。

このツールでは、以下に示すパラメーターを使用します。

パラメーター/ボタン	説明
Destination Host	• IPルーティングテーブル全体を参照するには、このフィールドを空白のままにします。 • アプライアンスからホストへのIPルーティング情報を参照するには、そのホストのIPアドレスまたはホスト名を指定します。
Run	このボタンをクリックすると、ルーティングテーブルが取得されます。ルーティングテーブルは、ポップアップウィンドウに表示されます。

Edit text file

Edit text fileツールは、アプライアンス上のファイルを編集するのに使用します。このツールでは、以下に示すパラメーターを使用します。

パラメーター/ボタン	説明
Category	編集するファイルのタイプを選択します。
File	[**Category**] フィールド (上記) で選択したタイプのファイルのリストが表示されます。編集するファイルを選択します。
Edit	このボタンをクリックすると、編集用にファイルが表示されます。ファイルの編集が済んだら、[**Save**] または [**Revert**] をクリックします。
Save	このボタンをクリックすると、ファイルの編集内容が保存されます。
Revert	このボタンをクリックすると、ファイルの編集内容がキャンセルされます。[**Revert**] をクリックした後に [**Save**] をクリックすると、元に戻したテキストが保存されます。

List directory

List directoryツールは、アプライアンス上のディレクトリの内容を表示するのに使用します。このツールは、Linuxコマンド`ls -alh`と同等です。

このツールでは、以下に示すパラメーターを使用します。

パラメーター/ボタン	説明
Directory	内容を表示するディレクトリを指定します。例: `/opt/arcsight/appliance`
Run	このボタンをクリックすると、ディレクトリのリストが表示されます。リストはポップアップウィンドウに表示されます。

List open files

List open filesツールは、使用中のファイルのリストを表示するのに使用します。このツールでは、以下に示すパラメーターを使用します。

パラメーター/ボタン	説明
Match Expression	式を入力すると、その式と一致する上位プロセスのみが表示されます。Linuxの正規表現がサポートされています。
Exclude Expression	式を入力すると、その式と一致するプロセスが出力から除外されます。Linuxの正規表現がサポートされています。
Run	このボタンをクリックすると、上位プロセスのリストが表示されます。リストはポップアップウィンドウに表示されます。

List processes

List processesツールは、メモリおよびリソース情報と共に、現在実行中の上位CPUプロセスを表示するのに使用します。このツールは、次のLinuxコマンドと同等です。
`ps -ef`

このツールでは、以下に示すパラメーターを使用します。

パラメーター/ボタン	説明
Match Expression	式を入力すると、その式と一致する上位プロセスのみが表示されます。Linuxの正規表現がサポートされています。
Exclude Expression	式を入力すると、その式と一致するプロセスが出力から除外されます。Linuxの正規表現がサポートされています。
Run	このボタンをクリックすると、上位プロセスのリストが表示されます。リストはポップアップウィンドウに表示されます。

Ping host

Ping hostツールは、IPネットワークで特定のホストに到達可能かどうかをテストし、アプライアンスからホストへ送信されたパケットのラウンドトリップ時間を測定するのに使用します。このツールは、Linuxコマンド`ping`と同等です。

このツールでは、以下に示すパラメーターを使用します。

パラメーター/ボタン	説明
Host	pingするホストのIPアドレスまたはホスト名を指定します。
Run	このボタンをクリックすると、指定されたホストに対してpingが実行されます。pingの結果は、ポップアップウィンドウに表示されます。

Resolve hostname or IP Address

Resolve hostnameツールは、ドメインネームサーバーでホスト名を検索し、ホスト名をIPアドレスに変換するのに使用します。このツールは、Linuxコマンド`host`と同等です。

このツールでは、以下に示すパラメーターを使用します。

パラメーター/ボタン	説明
Hostname	IPアドレスに解決するホスト名を指定します。
Run	このボタンをクリックすると、ドメインネームサーバーでホスト名が検索されます。結果はポップアップウィンドウに表示されます。

Scan network ports

Scan network portsツールは、ネットワーク上の特定のホストでオープンポートをスキャンするのに使用します。このツールは、Linuxコマンド`nmap [-p]`と同等です。

このツールでは、以下に示すパラメーターを使用します。

パラメーター/ボタン	説明
Host	ポートをスキャンするホストのIPアドレスまたはホスト名を指定します。
Port Range	オプション。スキャンするポートの範囲を指定します。一定範囲のポート番号はダッシュ(-)で区切り、個々のポート番号はカンマで区切ります。たとえば、「80-90, 8080」のようになります。 ポート範囲を指定しない場合は、指定されたホスト上のすべてのポートがスキャンされます。 このオプションは、`netstat` Linuxコマンドの`-p`オプションと同等です。

パラメーター/ボタン	説明
Run	このボタンをクリックすると、指定されたホスト上でポートのスキャンが開始されます。結果はポップアップウィンドウに表示されます。

Send signal to container

Send signal to containerツールは、終了コマンドをコンテナーに送信するのに使用します。このツールは、Linuxコマンド`kill -severity` (ここで、`severity`は`-15`または`-9`) と同等です。

このツールでは、以下に示すパラメーターを使用します。

パラメーター/ボタン	説明
Severity	コンテナーに送信する終了コマンドのシグナルを選択します。KILL (Linux `kill`コマンドオプション`-9`) またはTERM (Linux `kill`コマンドオプション`-15`) を選択できます。
Container	シグナルの送信先となるコンテナーを選択します。
Run	このボタンをクリックすると、シグナルが送信されます。結果はポップアップウィンドウに表示されます。

Tail file

Tail fileツールは、システム、アプリケーション、またはログファイルの最後の10行を表示するのに使用します。このツールは、Linuxコマンド`tail -f`と同等です。

このツールでは、以下に示すパラメーターを使用します。

パラメーター/ボタン	説明
Category	編集するファイルのタイプを選択します。
File	[**Category**] フィールド (上記) で選択したカテゴリのファイルのリストが表示されます。最後の10行を表示するファイルを選択します。
Match Expression	式を入力すると、その式と一致する行のみが表示されます。Linuxの正規表現がサポートされています。
Exclude Expression	式を入力すると、その式と一致する行が表示から除外されます。Linuxの正規表現がサポートされています。
Run	このボタンをクリックすると、選択したファイルの最後の10行が表示されます。これらはポップアップウィンドウに表示されます。

Trace network route

Trace network routeツールは、アプライアンスと指定されたホストとの間のネットワークルートを表示するのに使用します。このツールは、Linuxコマンド`traceroute`と同等です。

このツールでは、以下に示すパラメーターを使用します。

パラメーター/ボタン	説明
Host	ルートをトレースするホストのIPアドレスまたはホスト名を指定します。
Run	このボタンをクリックすると、ネットワークルートが表示されます。この情報はポップアップウィンドウに表示されます。

ログ

システムは、アプリケーションレベルとプラットフォームレベルで監査ログを生成できます。[Logs]サブメニューは、監査ログを検索する場合や、監査の転送を設定して、システムがESMなどの通知先に監査イベントを送信できるようにする場合に使用します。

監査ログ

システムの監査ログを表示できます。監査ログは、CEF (共通イベントフォーマット) の監査イベントとしてArcSight ESMに直接送信し、分析と関連付けを行うことができます。監査イベントの転送については、「特定の通知先に対する監査の転送の設定」(250ページ)を参照してください。

監査ログは、ArcMCによって恒久的に保持されます。

監査ログを表示するには

1. **[Administration] > [System Admin]** をクリックします。
2. **[Logs]** セクションの **[Audit Logs]** をクリックします。
3. ログを取得する日付と時刻の範囲を選択します。
4. (オプション) 監査ログの検索を絞り込むには、**[Description]** フィールドに文字列を指定し、**[User]** フィールドにユーザー名を指定します。文字列を指定した場合、**[Description]** フィールドにその文字列が含まれるログのみが表示されます。同様に、ユーザーを指定した場合、**[User]** フィールドにそのユーザー名が含まれるログのみが表示されます。
5. **[Search]**をクリックします。

監査の転送の設定

監査の転送を設定するには、ArcSight Management Centerのコンテナーにsyslogコネクターを1つインストールする必要があります(このコネクターは、そのコンテナー内の唯一のコネクターになる可能性があります)。

ソフトウェアArcSight Management CenterとArcSight Management Centerアプライアンスでは、監査の転送を設定する手順が異なります。

注: rootユーザーでArcSight Management Centerをインストールした場合は、Syslogコネクターもrootユーザーで設定する必要があります。

root以外のユーザーでインストールした場合は、Syslogコネクターを同じroot以外のユーザーで設定する必要があります。

ソフトウェアArcSight Management Centerの場合

ソフトウェアArcSight Management Centerで監査の転送を設定するには

1. ローカルSyslog Daemonコネクターを`/opt/arcsight/connector`にインストールします。
2. Syslog Daemonコネクターが存在するコンテナーで、監査の転送を設定します。「特定の通知先に対する監査の転送の設定」(250ページ) を参照してください。
3. メニューバーから **[System Admin]** をクリックします。ナビゲーションツリーで、新しくインストールしたSyslogコネクターを選択し、監査の転送を有効にします。

ArcSight Management Centerアプライアンスの場合

ArcSight Management Centerアプライアンスで監査の転送を設定するには

1. メニューバーで、**[Node Management]** をクリックします。
2. ナビゲーションツリーで、デフォルトのロケーションを選択します。次に、管理パネルで、ローカルのホストを選択します。
3. Syslogコネクターをインストールするコンテナーを選択します。
4. **[Add Connector]** をクリックし、インストールするコネクターとしてsyslogを選択します。
5. Syslog Daemonコネクターが存在するコンテナーで、監査の転送を設定します。「特定の通知先に対する監査の転送の設定」(250ページ) を参照してください。
6. メニューバーから **[System Admin]** をクリックします。ナビゲーションツリーで、新しくインストールしたSyslogコネクターを選択し、監査の転送を有効にします。

特定の通知先に対する監査の転送の設定

監査イベントとシステムヘルスイベントを、ArcSightのESM通知先に転送して関連付けと分析を行い、Loggerに転送してイベント収集を行うことができます。

監査イベントを特定の通知先に転送するには

1. 上部のメニューバーから **[Setup] > [System Admin]** をクリックします。
2. **[Logs]**セクションの**[Audit Forwarding]**をクリックします。
3. **[Available Destinations]**リストから通知先を選択し、右矢印アイコン () をクリックして、選択した通知先を**[Selected Destinations]**リストに移動します。

   一度に複数の通知先を選択して移動したり、  アイコンをクリックして使用可能なすべての通知先を移動できます。
4. **[Save Settings]**をクリックします。

注: 通知先は、ソフトウェアArcSight Management Centerには表示されません。

ストレージ

[Storage] サブメニューは、NFSマウントやCIFSマウント、またはSAN (該当する場合) を追加、およびハードディスクアレイ (RAID) コントローラーと特定のシステムプロセスのステータスを表示するために使用します。

RAID Controller/Hard Disk SMART Data

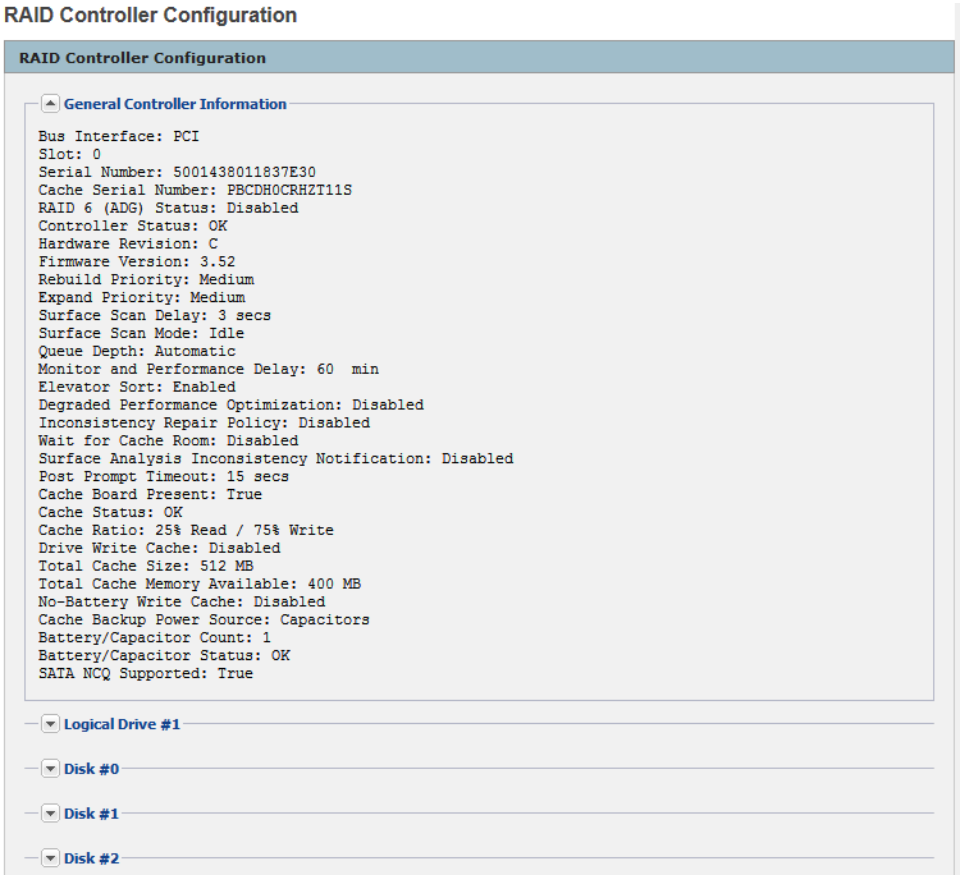
RAIDコントローラーに関する情報またはハードディスクのSMARTデータを、[General Controller Information] 画面で確認できます。この情報は、通常のシステム運用では不要ですが、特定のハードウェアの問題を診断する際に役立つ可能性があります。RAIDストレージは、その性質上冗長であるため、単一のドライブ障害が起きてもシステムが使用不能になりません。代わりにパフォーマンスが低下します。このレポートを使用して、パフォーマンスの問題がディスク障害によって引き起こされているかどうかを判断してください。カスタマーサポートも問題を診断するためにこの情報を使用することがあります。

[General Controller Information] 画面を表示するには

1. 上部のメニューバーから **[Administration] > [Setup] > [System Admin]** をクリックします。
2. 左パネルの **[Storage]** セクションにある **[RAID Controller]** をクリックします。

   注: 一部の旧式のモデルでは、[RAID Controller] メニュー項目の代わりに、[Hard Disk SMART Data] メニュー項目が左パネルに表示されます。左パネルの [**Storage**] セクションにある [**Hard Disk SMART Data**] をクリックし、ハードドライブからの診断情報を表示します。
3. 表示される情報は、システムのハードウェアモデルによって変わります。矢印をクリックする

と、セクションを開いたり閉じたりできます。



FTP

ArcSight Management Centerでは、FTPまたはFTPS (FTP over SSL) を使用して、アプライアンスにログファイルを配布できます。FTPおよびFTPSは、デフォルトで**無効**になっています。

Blue Coat ProxySGアプライアンスでは、特に、ファイルをArcSight Management Centerに転送する手段としてFTPおよびFTPSをサポートしています (この方法およびその他の方法の詳細については、『SmartConnector Configuration Guide for Blue Coat ProxySG』を参照してください)。

FTPS

FTPはセキュアチャネル (SSL) 上でも使用できます。**FTPS**を使用するには、ArcSight Management Centerで証明書を生成する必要があります。この証明書は、自己署名証明書またはCA (認証局) によって署名された証明書のどちらでも構いません。このオプションの詳細については、「FTPS (FTP over SSL) の使用」(255ページ) を参照してください。

FTPをサポートしているモデル

次の表に、FTPの使用をサポートしているArcSight Management Centerのモデルを示します。これは、これらのプロトコルを使用して受信したファイルを保管するのに使用できる最大ディレクトリサイズを判断するのにも役立ちます。

注: 最大ディレクトリサイズを超えると、FTPは無効になり、監査イベント`platform:453, FTP service stopped`が送信されます。ディレクトリサイズが小さくなるまで、FTP接続はすべて拒否されます。

モデル名	最大ディレクトリサイズ (GB)
C1400	275
C3400	275
C3500	475
C5400	235
C5500	475
C6500	500
C6600	500

FTPの有効化

FTPプロトコルを使用するには、アプライアンス上でFTPを有効にし、蓄積されるファイル用の最大ディレクトリサイズを設定する必要があります。

1. 上部のメニューバーから **[Administration] > [Setup] > [System Admin]** をクリックします。
2. [**Storage**] セクションにある [**FTP**] をクリックします。
3. [**FTP Settings**] 内で、[**Enable FTP**] チェックボックスをオンにします。
4. FTPクライアントがファイアウォール環境内に存在し、パッシブモードのデータ転送に使用するポートを制限する必要がある場合は、[**Restrict port range...**] チェックボックスをオンにします。
   - [**Port Range**] では、個別ポート (例: `12345`) または1つのポート範囲 (例: `20001-20010`) を設定できます。指定したポートはすべてファイアウォール上で開いておく必要があります。

     注: ポートまたはポート範囲を指定する際には、未使用であると考えられるポートを使用してください。選択したポートがすでに使用中の場合、FTPデータ転送は失

敗します。このため、HPE Securityでは、10000以上の範囲のポートを使用することを推奨しています。

- パッシブモードの同時FTPクライアント数は、指定したポート数までに制限されます。たとえば、指定範囲のポート数が10である場合、一度に転送を行える同時パッシブFTPクライアントは10個のみです。

ヒント: [**Is FTP Running?**] (**Yes**または**No**) では、FTPサーバーが正常に実行されているかどうかの確認が行われます。

5. 最大ディレクトリサイズを入力します。
   - 最大ディレクトリサイズを、お使いのアプライアンスモデルで許容されている値よりも大きくすることはできません (「FTPをサポートしているモデル」(253ページ) を参照)。
   - 最大サイズを変更する場合は、[**Current Size**] フィールドの値よりも大きくする必要があります。
   - [**Current Size**] には、`/opt/arcsight/incoming`とその下のすべてのサブディレクトリが含まれます。
   - 設定した最大サイズを超えると、FTPは自動的に停止します。
   - ファイル制限が範囲内に戻ると、FTPは自動的に再開されます。
6. パスワードを入力します。

注意: 匿名FTPはサポートされていません。

7. **[Save]** をクリックします。
   - FTPサーバーでは、ファイルのput操作のみがサポートされます。アプライアンスからデータを取得する機能はありません。
   - 少数の大きなファイルではなく、多数の小さなファイルで転送した場合の方が、データ処理が高速かつ効率的に行われます。

サブディレクトリの追加

命名規則に基づいているため、さまざまなデバイスから受信したログファイルが同じディレクトリ内で競合する可能性があります。これを防ぐには、サブディレクトリを作成してファイルを分けます。このウィンドウには、サブディレクトリの現在のサイズも表示されます。

ヒント: 使用中の容量を確認し、ファイルデータの一部を容易に削除することが可能になるため、サブディレクトリを作成することをお勧めします。

ファイルをサブディレクトリに追加するには

1. アプライアンス内で、**[Setup] > [System Admin] > [FTP]** に移動します。
2. [**Subdirectory**] ウィンドウで、[**Add**] をクリックしてサブディレクトリの名前を指定します。
   サブディレクトリ名がウィンドウに表示され、そのサブディレクトリの現在のサイズが表示されます。ディレクトリ名がFTPサーバーで設定した名前と一致していることを確認します。

   注: サブディレクトリの命名時には、標準的なLinuxのディレクトリ命名規則が適用されます。

FTP経由で受信したログデータの処理

FTP経由でコネクターから入力を受信するには、アプライアンス外でいくつかの手順を実行する必要があります。以下の手順を実行することで、ログデータを正常に転送できるようになります。

1. アプライアンスでFTPを有効にします。詳しい手順については、「FTPの有効化」(253ページ) を参照してください。
2. SmartConnectorを設定します。設定方法については、『SmartConnector Configuration Guide for Blue Coat ProxySG』を参照してください。

   ヒント: Blue Coat SmartConnectorをFTPで使用するように設定する場合は、処理後にファイルを削除するようにSmartConnectorをセットアップします。これにより、FTPサーバーにファイルが過剰に蓄積されるのを防ぐことができます。

   これを行うには、`agent.properties`で、`agents[0].foldertable [0].mode=RenameInSameDirectory`を`agents[0].foldertable [0].mode=`**DeleteFile**に変更します。

   ヒント: Blue Coat SmartConnectorをFTPで使用するように設定する場合は、コネクターを`/opt/arcsight/incoming/<必要に応じてサブディレクトリ>`にポイントします。

3. デバイスを設定します。設定方法については、デバイスのドキュメントを参照してください。

FTPS (FTP over SSL) の使用

FTPSは、セキュアなSSLチャネル上で使用します。**FTPS**を使用するには、ArcSight Management Centerで証明書を生成する必要があります。

Blue Coat ProxySGでのFTPSの使用

FTPSを使用するには、ArcSight Management CenterとBlue Coat ProxySGアプライアンスの両方で、複数のステップを実行する必要があります。最初のステップでは、**自己署名証明書**または**CSR**をArcSight Management Centerで生成します。証明書を自己署名する場合は、自己署名証明書をBlue Coat ProxySGアプライアンスにインポートする必要があります。CAで署名する場合は、CAの証明書をBlue Coat ProxySGアプライアンスにインポートする必要があります。

ArcSight Management Centerで次の手順を実行します。

1. ArcSight Management Centerで**証明書を生成**します(自己署名証明書またはCSR)。
   - 自己署名証明書については、「自己署名証明書の生成」(257ページ)を参照してください。
   - CA署名証明書については、「CSR(証明書署名リクエスト)の生成」(259ページ)および「証明書のインポート」(260ページ)を参照してください。
2. コネクターアプライアンスで**FTPを有効化**します。詳しい手順については、「FTPの有効化」(253ページ)を参照してください。

Blue Coat ProxySGアプライアンスで次の手順を実行します。

以下の手順の詳細については、Blue Coat ProxySGの最新のドキュメントを参照してください。

1. Blue Coat ProxySGアプライアンスに、**自己署名証明書またはCAの証明書をインポート**します。自己署名証明書をBlue Coat ProxySGアプライアンスにインポートする場合は、[**Generate Certificate**] ページで [**View Certificate**] ボタンをクリックして、FTPSで使用する証明書を表示します。証明書の内容全体をコピーして、BlueCoat ProxySGアプライアンスの [Import CA Certificate] ウィンドウに貼り付けます。
2. Blue Coat ProxySGで、**インポートした証明書をブラウザーの信頼済みCA証明書リストに追加**します。
3. Blue Coat ProxySGアプライアンスで、**FTPアップロードクライアントの設定**を行い、**セキュア接続を使用するオプションを選択**していることを確認します。
4. Blue Coat ProxySGアプライアンスで、**アップロードテストを実行**し、FTPSを介してコネクターアプライアンスにログファイルを正常にアップロードできることを確認します。

セキュリティ

セキュリティ設定では、SSLサーバー証明書の設定、システムでのFIPS (Federal Information Processing Standard) モードの有効化と無効化、クライアント証明書およびCAC (Common Access Card) に対応したSSLクライアント認証の設定を行うことができます。

ヒント: ユーザーDNを作成するための手順については、「ユーザー」(274ページ)と、パラメーターの表の「Use Client DN」を参照してください。

SSLサーバー証明書

SmartMessagingテクノロジーや他のArcSightシステムを使用する際、SmartConnectorなどのクライアントと暗号化されたチャネル上で安全に通信するために、SSL (Secure Sockets Layer) テクノロジーが使用されます。システムには自己署名証明書が付属しており、アプライアンスを初めて使用するときにSSLセッションを確立できるようになっています。このオプションの詳細については、「自己署名証明書の生成」(257ページ)を参照してください。

自己署名証明書が付属してはいますが、CA (認証局) が署名した証明書を使用する必要があります。CAが署名した証明書の入手を容易にするため、システムで証明書署名リクエストを生成できます。署名済みの証明書ファイルをCAから入手したら、システムにアップロードして以降の認証で使用できます。詳しい手順については、「CSR (証明書署名リクエスト) の生成」(259ページ)を参照してください。

インストールされているSSL証明書が30日未満で失効する場合や、すでに失効している場合、監査イベントが生成されます。30日以内に失効しない証明書で証明書を置き換えるまで、デバイスイベントクラスIDが「`platform:407`」のイベントが定期的に生成されます。

自己署名証明書の生成

システムには自己署名証明書が付属しており、初めて接続するときにSSLセッションを確立できるようになっています。この種の証明書には、別の団体からの署名が不要で、すぐに使用できます。

自己署名証明書を生成するには

1. **[Administration] > [Setup] > [System Admin]** をクリックします。
2. 左パネルの **[Security]** セクションにある **[SSL Server Certificate]** をクリックし、**[Generate Certificate/Certificate Signing Request]** ページを表示します。
3. **[Generate Certificate]**タブをクリックします。
4. [**Generate Certificate For Protocol**] フィールドで、[**Network Protocol**] ドロップダウンメニューを使用して適切なプロトコルを選択します。

パラメーター	説明
HTTPS	このオプションは、HTTPSプロトコルで使用するCSRを生成する場合に選択します。これは最も一般的に使用されるオプションです。
FTPS	このオプションは、FTPSで使用するCSRを生成する場合にのみ選択します。

5. [**Enter Certificate Settings**] で、以下のフィールドに新しい値を入力します。

パラメーター	説明
Country	ISO 3166-1の2文字の国コード (たとえば米国の場合は「US」)。
State/Province	州または県名 (例:「California」)。
City/Locality	都市名 (例:「Sunnyvale」)。
Organization Name	会社名、政府機関などの大きな組織。
Organizational Unit	組織内の部門または部署。
Hostname	このシステムのホスト名またはIPアドレス。 ホスト名を指定する場合には、この名前がシステムのDNS (Domain Name Service) サーバーに登録されている名前に一致することを確認してください。また、この名前は、「NICs」(231ページ) で指定したホスト名と同じである必要があります。 **注:** このシステムのホスト名またはIPアドレスが将来変わった場合は、新しい自己署名証明書またはCSRを生成する必要があります。新しい証明書を入手したら、証明書をアップロードして、システムと通信するコネクターがホスト名を検証できるようにする必要があります。
Email Address	このCSRの管理者または窓口のメールアドレス。
Private Key Length	プライベートキーの長さは、2048ビットです。

CSRまたは自己署名証明書を生成するには、最初の2個のボタンを使用します。**[View Certificate]** ボタンは、生成された証明書を表示するためだけに使用します。

ボタン	説明
Generate CSR	クリックすると、CSR (証明書署名リクエスト) が生成されます。
Generate Certificate	クリックすると自己署名証明書が生成されます。
View Certificate	クリックすると、生成された証明書が表示されます。

6. **[Generate Certificate]** ボタンをクリックして自己署名証明書を生成します。
7. 確認メッセージが表示されたら、[**OK**] をクリックします。
8. **[View Certificate]** ボタンをクリックしてPEMエンコードされた自己署名証明書を生成します。

CSR (証明書署名リクエスト) の生成

CAが署名した証明書を入手するための最初のステップは、CSR (証明書署名リクエスト) を生成することです。CSRは、証明書を要求するシステム上で生成する必要があります。つまり、システムA用のCSRをシステムBで生成したり、サードパーティ製のユーティリティを使用して生成することはできません。

生成されたCSRをVeriSignなどのCAに送信し、署名済み証明書ファイルを返送してもらう必要があります。

証明書署名リクエストを生成するには

1. **[Administration] > [System Admin]** をクリックします。
2. 左パネルの **[Security]** セクションにある **[SSL Server Certificate]** をクリックし、**[Generate Certificate/Certificate Signing Request]** ページを表示します。
3. **[Generate Certificate]** タブをクリックします。
4. [**Generate Certificate For Protocol**] フィールドで、[**Network Protocol**] ドロップダウンメニューを使用して適切なプロトコルを選択します。[**Generate Certificate For Protocol**] フィールドで、[**Network Protocol**] ドロップダウンメニューを使用して適切なプロトコルを選択します。

パラメーター	説明
HTTPS	このオプションは、HTTPSプロトコルで使用するCSRを生成する場合に選択します。これは最も一般的に使用されるオプションです。
FTPS	このオプションは、FTPSで使用するCSRを生成する場合にのみ選択します。

5. [**Enter Certificate Settings**] で、以下のフィールドに新しい値を入力します。

パラメーター	説明
Country	2文字の国コード (たとえば米国の場合は「US」)。
State / Province	州または県名 (例:「California」)。
City / Locality	都市名 (例:「Sunnyvale」)。
Organization Name	会社名、政府機関などの大きな組織。
Organizational Unit	組織内の部門または部署。

パラメーター	説明
Hostname	このシステムのホスト名またはIPアドレス。 ホスト名を指定する場合には、この名前がシステムのDNS (Domain Name Service) サーバーに登録されている名前に一致することを確認してください。また、この名前は、「NICs」(231ページ) で指定したホスト名と同じである必要があります。 **注:** このシステムのホスト名またはIPアドレスが将来変わった場合は、新しい自己署名証明書またはCSRを生成する必要があります。新しい証明書を入手したら、証明書をアップロードして、システムと通信するコネクターがホスト名を検証できるようにする必要があります。
Email Address	このCSRの管理者または窓口のメールアドレス。
Private Key Length	プライベートキーの長さ (ビット単位)。**1024**、**2048**、**4096**、**8192**のいずれかを選択します。

6. CSRまたは自己署名証明書を生成するには、最初の2個のボタンを使用します。**[View Certificate]**ボタンは、生成された証明書を表示するためだけに使用します。

ボタン	説明
Generate CSR	クリックすると、CSR (証明書署名リクエスト) が生成されます。
Generate Certificate	クリックすると自己署名証明書が生成されます。
View Certificate	クリックすると、生成された証明書が表示されます。

7. **[Generate CSR]**を選択して、証明書署名リクエストを生成します。
8. CSRが正常に生成されると、ポップアップウィンドウが表示され、CSRファイルをダウンロードするか、その内容をカット & ペーストできるようになります。

   それを行うには、 `-----BEGIN CERTIFICATE REQUEST-----` から`-----END CERTIFICATE REQUEST-----`までのすべての行をコピーします。
9. CSRファイルを認証局に送付し、CA署名証明書を入手します。
10. CA署名証明書ファイルを入手したら、次の「証明書のインポート」(260ページ)に進みます。

証明書のインポート

CA (認証局) から証明書を入手したら、以下の手順に従ってシステムにインポートします。

1. **[Administration] > [System Admin]** をクリックします。
2. 左パネルの**[Security]**セクションにある**[SSL Server Certificate]**をクリックします。
3. **[Import Certificate]** タブを選択します。
4. **[Import Certificate For Protocol]** フィールドで、**[Network Protocol]** ドロップダウンメニューを使用して適切なプロトコルタイプを選択します。

パラメーター	説明
HTTPS	HTTPS証明書をインポートする場合に選択します (このオプションでは、再起動が必要になる場合があります)。
FTPS	FTPS証明書をインポートする場合に選択します。

5. **[Browse]** ボタンをクリックし、ローカルファイルシステム上の署名された証明書ファイルを探します。

   注: インポートする証明書は、**PEM (Privacy Enhanced Mail)**形式になっている必要があります。

6. **[Import and Install]** をクリックして指定した証明書をインポートします。
7. **HTTPS**を使用する場合、ブラウザーによっては、新しい証明書を有効にするために、ブラウザーを閉じてから再起動する必要があります。ブラウザーの要件が不明な場合は、ブラウザーを閉じてから再起動してください。

SSLクライアント認証

システムでは、SSL証明書を使用したクライアント認証がサポートされています。SSLクライアント認証はTwo-Factor認証の1つの形であり、ローカルパスワード認証の代替手段または追加手段として使用できます。

注: CACは、クライアント証明書認証の1つの形態です。クライアント証明書認証に関する情報は、CACに適用されます。

CACをサポートするようにArcMCを設定するには、信頼済みの証明書をアップロードし、クライアント証明書認証を有効にする必要があります。

信頼済みの証明書のアップロード

信頼済みの証明書は、システムにログインするユーザーを認証するために使用されます。信頼済みの証明書のアップロードは、LDAPS認証を使用する場合に必要です。信頼済みの証明書は、リモートLDAPSサーバーを認証するために使用されます。証明書は、PEM (Privacy Enhanced Mail) 形式になっている必要があります。

信頼済みの証明書をアップロードするには

1. **[Administration] > [Setup] > [System Admin]** をクリックします。
2. 左パネルの **[Security]** セクションにある **[SSL Client Authentication]** をクリックします。
3. **[Trusted Certificates]** タブで **[Browse]** をクリックし、ローカルファイルシステム上の信頼済みの証明書を参照します。
4. **[Upload]** をクリックします。

信頼済みの証明書がアップロードされ、アップロードを行った同じページの [Certificates in Repository] リストに表示されます。

信頼済みの証明書の詳細を表示するには、[Certificate Name] 欄に表示されるリンクをクリックします。

信頼済みの証明書を削除するには、証明書を選択して **[Delete]** をクリックします。

証明書取り消しリストのアップロード

CRL (証明書取り消しリスト) は、コンピューターによって生成された記録であり、有効期限の前に取り消されるか保留された証明書を識別します。CACをサポートするには、CRLファイルをArcSightシステムにアップロードする必要があります。CRLファイルはPEM形式になっている必要があります。

CRLファイルをアップロードするには

1. **[Administration] > [System Admin]** をクリックします。
2. 左パネルの **[Security]** セクションにある **[SSL Client Authentication]** をクリックします。
3. **[Certificate Revocation List]** タブで **[Browse]** をクリックし、ローカルファイルシステム上のCRLファイルを参照します。
4. **[Upload]** をクリックします。

   CRLがアップロードされ、[Certificate Revocation]リストに表示されます。

   CRLの詳細を表示するには、[Issuer Name] 欄に表示されるリンクをクリックします。

   CRLファイルを削除するには、ファイルを選択して**[Delete]**ボタンをクリックします。

クライアント証明書認証の有効化

クライアント証明書認証を有効にするには、「クライアント証明書認証」(268ページ) を参照してください。

FIPS 140-2

システムでは、FIPS 140-2 (Federal Information Processing Standard 140-2) がサポートされています。FIPS 140-2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。米国連邦政府は、SBU (取り扱い注意ではあるが機密扱いでない) 情報を扱うすべてのIT製品がこれらの規格に準拠していることを義務付けています。

システムをFIPS 140-2準拠にする必要がある場合は、FIPSを有効にできます。いったん有効にすると、NISTによりFIPS 140-2用に定義されている暗号化アルゴリズムが、内部コンポーネントと外部コンポーネントの間のすべての暗号化された通信に使用されます。

注: FIPSモードの変更処理が完了するまでは、アプライアンス上でFIPSに関連する操作を実行しないでください。

完全にFIPS 140-2準拠にするには、連携するすべてのコンポーネントをFIPSモードにする必要があります。たとえば、ArcSight Management CenterでFIPSを有効にした場合、アプライアンスがFIPS対応になり、NISTで定義された暗号化アルゴリズムに関する標準規格に準拠します。ただし、コンテナーでもFIPSが有効になっている必要があります。

注: ArcSight Management Centerで、FIPSモードを有効にすると、自己署名証明書を再生成できなくなります。

FIPSモードを有効または無効にするには

1. 上部のメニューバーから **[Administration] > [Setup] > [System Admin]** をクリックします。
2. 左パネルの [Security] セクションにある**[FIPS 140-2]** をクリックします。
3. [Select FIPS Mode] オプションで**[Enable]**または**[Disable]**をクリックします。
4. **[Save]**をクリックします。
5. **アプリケーションのリブート再起動が必要**であることを示すメッセージが表示されたら、システムを再起動します。[**System Reboot**] のリンクをクリックします。
6. 適切なCA証明書がトラストストアに格納されており、コネクターがそれぞれの通知先 (ArcSight ESMまたはArcSight Management Center) を正常に検証できるようになっていることを確認します。適切なCA証明書がトラストストアに存在しない場合は、CA証明書を追加する必要があります。証明書の表示および追加の詳細については、「コンテナーへのコマンドの送信」(87ページ)を参照してください。

ArcMCのユーザー/グループ

ArcMCでユーザーおよびユーザーグループを設定し、認証オプションを設定するには、**[Users/Groups]** サブメニューを使用します。

管理対象製品のユーザーの管理については、「管理対象製品でのユーザーの管理」(177ページ)を参照してください。

認証

[Authentication Settings] では、ユーザーログインセッションの設定とポリシー、パスワード規則とロックアウト、外部認証オプションを指定できます。

セッション

[Session] タブでは、単一のユーザーアカウントに対する最大同時セッション数と、ユーザーセッションが自動的にログアウトされるかユーザーアカウントが無効にされるまでの時間の長さを指定できます。デフォルトでは、1つのユーザーアカウントでアクティブなセッションを同時に15個まで使用でき、15分間操作しないとユーザーアカウントがログアウトされます。

セッションの設定を変更するには

1. **[Administration] > [Setup] > [System Admin]** をクリックします。
2. **[Users/Groups]** セクションの **[Authentication]** をクリックします。
3. **[Sessions]** タブで、次の表で説明するパラメーターを更新します。

パラメーター	説明
Max Simultaneous Logins/User	1つのユーザーアカウントに許可される最大同時セッション数。デフォルトは **15セッション**です。
Logout Inactive Session After	操作のないセッションを自動的に終了させるまでの時間 (分単位)。デフォルトは**15分**です。 この値は、**[Monitor]** メニューを通じてアクセスしたユーザーインターフェイスページには適用されません。ユーザーがいずれかの [Monitor] メニューページを表示している場合は、指定された時間 (分) にわたってセッションでの操作が行われなくても、ユーザーのセッションはアクティブなままになります。
Disable Inactive Account After	アクティブでないユーザーアカウントを無効にするまでの日数。デフォルト値は**0**で、アカウントは無効にならないことを意味します。

4. **[Save]**をクリックして変更するか、別のタブをクリックしてキャンセルします。

ローカルパスワード

[Local Password] タブを使用すると、最小および最大文字数や、その他のパスワード要件など、パスワードポリシーを設定できます。

パスワード設定を変更するには

1. **[Administration] > [System Admin]** をクリックします。
2. **[Users/Groups]** セクションの **[Authentication]** をクリックします。
3. **[Local Password]** タブを選択します。
   次の表で説明するパラメーターを使用して、パスワード設定をカスタマイズします。

[Authentication Settings] の [Local Password] タブ

パラメーター	説明
Lockout Account (policy)	
Enable Account Lockout	以降の設定の定義に従ってユーザーアカウントのロックアウトを有効にするには、チェックボックスをオンにします。デフォルトでは、ポリシーは**disabled**になっています。
Lockout Account After	ユーザーアカウントをロックアウトするまでのログイン失敗回数。デフォルト値は**3**です。
Remember Failed Attempts For	失敗したログイン試行を記憶する時間 (分)。デフォルト値は**1**です。
Lockout Account For	ロックアウトされたアカウントのロックを解除できない時間 (分)。デフォルト値は**15**です。
Password Expiration (policy)	
Enable Password Expiration	以降の設定の定義に従ってユーザーパスワードの期限を有効にするには、チェックボックスをオンにします。デフォルトでは、ポリシーは**disabled**になっています。
Password Expires in	パスワードが期限切れになるまでの日数。デフォルト値は**90**です。
Notify User	期限切れの何日前にユーザーに通知するか。ユーザーが期限切れの前にパスワードを更新できるようにするには、このオプションを選択します。デフォルト値は**5**です。
Users Exempted From Password Expiration Policy	パスワードを期限切れにしないユーザーの数を設定するには、リンクをクリックします。 この機能の使用方法については、「パスワードの期限切れから除外するユーザー」(266ページ)を参照してください。
Password Strength Rules (policy)	
Enforce Password Strength	以降の設定の定義に従ってパスワードポリシーを適用するには、チェックボックスをオンにします。デフォルトでは、ポリシーは**disabled**になっています。
Minimum Length	パスワードに含まれる必要がある最小文字数。デフォルト値は**10**です。
Maximum Length	パスワードに含めることができる最大文字数。デフォルト値は**20**です。
Password Character Rules	
パスワード文字規則は、パスワードの強度を確保するための追加の文字要件を定義します。	
Numeric	パスワード内の数字 (0～9) の最小文字数。デフォルト値は**2**です。
Uppercase	パスワード内の大文字 (A～Z) の最小文字数。デフォルト値は**0**です。
Special	パスワードに必要な英数字以外の文字の最小文字数。デフォルト値は**2**です。

[Authentication Settings] の [Local Password] タブ (続き)

パラメーター	説明
Lowercase	パスワード内の小文字 (a～z) の最小文字数。デフォルト値は**0**です。
Password Must be At Least N Characters Different From Old Password	新しいパスワードと以前のパスワードで違っている必要がある最小文字数。デフォルト値は**2**です。
Include “Forgot Password” link on Login Screen	ユーザーがログインページ上の「Forgot Password」リンクを使用してローカルパスワードをリセットできるようにするには、このチェックボックスをオンにします。デフォルトでは、オプションは**disabled**になっています。 この機能が正常に動作するには、システム上でSMTPサーバーが設定されていて、ユーザー名に正しいメールアドレスが設定されている必要があります。 SMTPサーバーが設定されていない場合は、一時的なパスワードを含むメールを送信できないため、パスワードをリセットできません。 ユーザー設定で、ユーザー名としてメールアドレスを指定する必要があります。一時的なパスワードがそのメールアドレスに送信されます。メールアドレスが指定されていないか、メールアドレスが正しくない場合は、ユーザーにメールが送信されません。 この機能の使用方法については、「Forgot Password」(267ページ) を参照してください。

4. **[Save]**をクリックして変更内容を保存するか、別のタブをクリックしてキャンセルします。

パスワードの期限切れから除外するユーザー

ほとんどのユーザーに対してパスワードの有効期限ポリシーを設定した場合でも、パスワード有効期限が自動的に切れないユーザーを指定したい場合があります。

ユーザーをパスワードの有効期限ポリシーから除外するには

1. **[Administration] > [System Admin]** をクリックします。
2. **[Users/Groups]** セクションの **[Authentication]** をクリックします。
3. **[Local Password]** タブを選択し、**[Exempted From Password Expiration Policy]** をクリックします。
4. **[Exempt Users From Password Expiration]** ページが表示されます。
5. **[Non-exempted Users]** リストからユーザーを選択し、右矢印アイコンをクリックして、選択したユーザーを **[Exempted Users]** リストに移動します。除外するユーザーのリストからユーザーを削除するには、逆の操作を行います。

   一度に複数のユーザーを選択して移動できます。また、アイコンをクリックすれば、すべてのユーザーを移動できます。
6. **[Save]** をクリックしてポリシーを保存するか、**[Cancel]** をクリックして終了します。

Forgot Password

この機能は、[Authentication Settings] ページで **[Include “Forgot Password” link on Login Screen]** 設定 (**[Setup] > [System Admin] > [Authentication] > [Local Password]**) が **[Yes]** に設定されている場合のみ使用できます。デフォルトで、この設定は **[No]** に設定されています。この機能を使用するには、SMTPサーバーを設定されている必要があります。この設定を有効にする方法の詳細については、「ローカルパスワード」(264ページ)を参照してください。

システムパスワードを忘れた場合は、この機能を使用して、一時的なパスワードが格納されたメールを受信します。

一時的なパスワードは、メールで指定された時刻まで有効です。指定した時刻までにログインしなかった場合、管理者のみがパスワードをリセットして別の一時的なパスワードを生成できます。

パスワードをリセットするには

1. Login画面で **[Forgot Password]** リンクをクリックします。
2. [Reset Password] ダイアログボックスでユーザー名を入力します。
3. **[Reset Password]**をクリックします。
   一時的なパスワードが記載された自動的なメールが、そのユーザーの指定されたメールアドレスに送信されます。

外部認証

システムでは、ローカルパスワード認証方式が提供されるのに加えて、クライアント証明書/CAC、LDAP、およびRADIUS 認証がサポートされています。すべての認証方式を同時に有効にすることはできません。

注: CACは、クライアント証明書認証の1つの形態です。クライアント証明書認証に関する情報は、CACに適用されます。

[External Authentication] タブのドロップダウンメニューを使用して、以下の認証方式のいずれかを選択します。

- 「ローカルパスワード」(268ページ)
- 「クライアント証明書認証」(268ページ)
- 「クライアント証明書とローカルパスワード認証」(268ページ)
- 「LDAP/ADおよびLDAPS認証」(269ページ)
- 「RADIUS認証」(271ページ)

ローカルパスワード

このオプションはデフォルトの方式であり、**[Local Password]**タブで設定されたローカルパスワードポリシーを実装します。このデフォルトをそのままにするか、別のオプションから変更する場合は**[Save]**をクリックします。

クライアント証明書認証

この認証方式では、クライアント証明書を使用してユーザーを認証する必要があります。クライアント証明書ごとに、クライアント証明書のDN (Distinguished Name) と一致するDNを持つユーザーアカウントがシステム上に存在する必要があります。

注意: 認証に使用するすべてのSSLクライアント証明書は、システムでFIPSが有効になっていない場合でも、FIPS互換である (FIPS互換のアルゴリズムでハッシュ作成されている) ことが必要です。

クライアント証明書認証を構成するには

1. **[Administration] > [System Admin]** をクリックします。
2. **[Users/Groups]** セクションの **[Authentication]** をクリックします。
3. **[External Authentication]** タブを選択します。
4. ドロップダウンメニューから **[Client Certificate]** を選択します。
5. **[Allow Local Password Fallback]** には以下の2つのオプションがあります。
   - **[Allow Local Password Fallback for Default Admin Only]**
     このオプションを選択すると、クライアント証明書が使用できないか無効な場合に、デフォルト管理者ユーザーは、ユーザー名とパスワードのみを使用してログインできるようになります。この権限は、デフォルト管理者ユーザーのみに制限されます。他のユーザーがシステムにアクセスするには、有効なクライアント証明書が必要です。このオプションは、デフォルトで有効になっています。
   - **[Allow Local Password Fallback for All Users]**
     このオプションを選択すると、クライアント証明書が無効か使用できない場合に、すべてのユーザーがローカルユーザー名とパスワードを使用してログインできるようになります。
     詳細については、「ローカルパスワードフォールバック」(272ページ) を参照してください。
6. **[Save]** をクリックします。

クライアント証明書とローカルパスワード認証

この認証方式では、SSLクライアント証明書と有効なローカルパスワードを使用してユーザーを認証する必要があります。ローカルパスワードとは、**[Users/Groups]** セクションの **[User**

Management] で作成したユーザー資格情報に関連付けられたパスワードを指します。詳細については、「User Management」(273ページ) を参照してください。

システム上のユーザーアカウントは、クライアント証明書のDN (Distinguished Name) と一致するDNを使用して定義されている必要があります。

ユーザーDNを作成するための手順については、「ユーザー」(274ページ) と、パラメーターの表の「Use Client DN」を参照してください。

注意: 認証に使用するすべてのSSLクライアント証明書は、システムでFIPSが有効になっていない場合でも、FIPS互換である (FIPS互換のアルゴリズムでハッシュ作成されている) ことが必要です。

クライアント証明書とローカルパスワード認証を構成するには

1. **[Administration] > [System Admin]** をクリックします。
2. **[Users/Groups]** セクションの **[Authentication]** をクリックします。
3. **[External Authentication]** タブを選択します。
4. ドロップダウンメニューから **[Client Certificate AND Local Password]** を選択します。
5. **[Allow Local Password Fallback]** には以下の2つのオプションがあります。
   - **[Allow Local Password Fallback for Default Admin Only]**
     このオプションは常に有効であり、デフォルト管理者ユーザーは、ユーザー名とパスワードのみを使用してログインできます。
   - **[Allow Local Password Fallback for All Users]**
     このオプションは常に無効になっています。認証方法として、**クライアント証明書とローカルパスワード**を使用している場合は、有効にできません。
     詳細については、「ローカルパスワードフォールバック」(272ページ) を参照してください。
6. **[Save]** をクリックします。

LDAP/ADおよびLDAPS認証

この認証方式は、LDAPサーバーでユーザーを認証します。LDAPが有効になっていても、各ユーザーアカウントはシステム上にローカルに存在している必要があります。ローカルに指定されたユーザー名は、LDAPサーバー上で指定されたユーザー名と違っていてもかまいませんが、各ユーザーアカウントに指定されたDN (Distinguished Name) は、LDAPサーバー上のものと一致している必要があります。

ヒント: ユーザーDNの作成手順については、「ユーザー」(274ページ) と、「Use Client DN」(275ページ) パラメーターを参照してください。

LDAP認証を設定するには

1. **[Administration] > [System Admin]** をクリックします。
2. **[Users/Groups]** セクションの **[Authentication]** をクリックします。
3. **[External Authentication]** タブを選択します。
4. ドロップダウンメニューから **[LDAP]** を選択します。
5. **[Allow Local Password Fallback]** には以下の2つのオプションがあります。
   - **[Allow Local Password Fallback for Default Admin Only]**
     このオプションを選択すると、LDAP認証に失敗する場合に、デフォルト管理者ユーザーがユーザー名とパスワードのみを使用してログインできるようになります。この権限は、デフォルト管理者ユーザーのみに制限されます。他のすべてのユーザーはLDAPで認証する必要があります。このオプションは、デフォルトで有効になっています。
   - **[Allow Local Password Fallback for All Users]**
     このオプションを選択すると、LDAP認証に失敗する場合に、すべてのユーザーがローカルユーザー名とパスワードを使用してログインできるようになります。
     詳細については、「ローカルパスワードフォールバック」(272ページ)を参照してください。

     LDAPサーバーには以下のパラメーターがあります。

パラメーター	説明

Server Hostname [:port] (optional)	(オプション) LDAPサーバーのホスト名またはIPアドレスとポートを次の形式で入力します。
	`ldap://<ホスト名またはIPアドレス>:<ポート>`
	`ldaps://<ホスト名またはIPアドレス>:<ポート>`
	LDAPSを使用するには追加の手順が必要です。以下の「LDAPS (LDAP over SSL) プロトコルの使用」(270ページ)を参照してください。

Backup Server Hostname[:Port] (optional)	(オプション) プライマリサーバーが応答しない場合に使用する、バックアップLDAPサーバーを入力します。サーバーが認証失敗 (不正なパスワード、不明なユーザー名など) を返した場合は、バックアップサーバーが試行されません。バックアップサーバーは、プライマリサーバーが通信障害になった場合にのみ試行されます。 プライマリサーバーと同じ形式を使用してホスト名とポートを指定します。
Request Timeout	LDAPサーバーからの応答を待つ時間 (秒)。デフォルト値は**10**です。

6. 完了したら **[Save]** をクリックします。

LDAPS (LDAP over SSL) プロトコルの使用

LDAPSプロトコルを使用してユーザーを認証することを選択する場合は、以下の条件が満たされていることを確認してください。

- LDAPSサーバー用のSSL証明書が、トラストストアにアップロードされていること。
- 外部認証方式が「`LDAP`」に設定されていること。
- LDAPSサーバーのURLが「`ldaps://`」で始まること。

SSL証明書をアップロードした後、**aps**プロセスを再起動します (**[Setup] > [System Admin] > [Process Status] > [aps] > [Restart]**)。

注意: apsプロセスを再起動しないと、LDAPSを使用した認証に失敗します。

RADIUS認証

この認証方式では、RADIUSサーバーでユーザーを認証できます。RADIUS認証が有効になっていても、各ユーザーアカウントはシステム上にローカルに存在している必要があります。ユーザー名はRADIUSサーバー上のユーザー名と一致している必要がありますが、パスワードは違っていてもかまいません。ユーザーが正常に認証されるには、有効なユーザー名と(RADIUS) パスワードを入力する必要があります。

RADIUS認証の設定を行うには

1. **[Administration] > [System Admin]** をクリックします。
2. **[Users/Groups]** セクションの **[Authentication]** をクリックします。
3. **[External Authentication]** タブを選択します。
4. ドロップダウンメニューから **[RADIUS]** を選択します。
5. **[Allow Local Password Fallback]** には以下の2つのオプションがあります。
   - **[Allow Local Password Fallback for Default Admin Only]**
     このオプションを選択すると、RADIUS認証に失敗する場合に、デフォルト管理者ユーザーがユーザー名とパスワードのみを使用してログインできるようになります。この権限は、管理者ユーザーのみに制限されます。他のすべてのユーザーはRADIUSで認証する必要があります。このオプションは、デフォルトで有効になっています。
   - **[Allow Local Password Fallback for All Users]**
     このオプションを選択すると、RADIUS認証に失敗する場合に、すべてのユーザーがローカルユーザー名とパスワードを使用してログインできるようになります。詳細については、「ローカルパスワードフォールバック」(272ページ) を参照してください。

6. 必要に応じて**RADIUSサーバー**のパラメーターを更新します。

パラメーター	説明
Server Hostname [:port]	RADIUSサーバーのホスト名とポートを入力します。
Backup Server hostname[:port] (optional)	**(オプション)** プライマリサーバーが応答しない場合に使用する、バックアップRADIUSサーバーを入力します。サーバーが認証失敗 (不正なパスワード、不明なユーザー名など) を返した場合は、バックアップサーバーが試行されません。バックアップサーバーは、プライマリサーバーが通信障害になった場合にのみ試行されます。 プライマリサーバーと同じ形式を使用してホスト名とポートを指定します。
Shared Authentication Secret	RADIUSパスフレーズを入力します。
NAS IP Address	NAS (Network Access Server) のIPアドレス。
Request Timeout	RADIUSサーバーからの応答を待つ時間 (秒)。デフォルト値は**10**です。
Retry Request	RADIUSリクエストを再試行する回数。デフォルト値は**1**です。
RADIUS Protocol:	ドロップダウンメニューを使用してプロトコルオプションを選択します。デフォルトは**None**です。

7. **[Save]**をクリックします。

ローカルパスワードフォールバック

この機能を使用すると、外部認証 (証明書、LDAP、RADIUS) が失敗した場合や、認証サーバーのパスワードを忘れた場合、認証サーバーが利用できない場合に、ローカルユーザー名とパスワードを使用してログインできます。

[Use Local Authentication] を使用すると、リモート認証サーバーが使用できない場合でも、**[Use Local Authentication]** チェックボックスをログイン画面に追加することで、デフォルト管理者がログインできるようになります。初期状態では、デフォルト管理者のみに対してこのオプションが有効になっています。しかし、すべてのユーザーに対してローカルパスワードフォールバックを有効にすることができます。たとえば、ユーザーが設定された外部のRADIUSサーバーに対する認証に失敗した場合に、RADIUSの代わりにローカル認証を使用してログインできるように、RADIUS認証方式を設定することができます。

すべてのユーザーに対してローカルパスワードフォールバックを許可する方法については、「クライアント証明書認証」(268ページ)、「LDAP/ADおよびLDAPS認証」(269ページ)、または「RADIUS認証」(271ページ)を参照してください。

認証失敗時にログインするには

1. [**Use Local Authentication**] チェックボックスをオンにします。

   注: このオプションは、他のユーザーに対して有効にしていない限り、デフォルト管理者のみに対して使用できます。

2. ログインとパスワードを入力し、**[Login]** をクリックします。

ログインバナー

ログイン画面のメッセージは、ニーズに合わせてカスタマイズできます。**[Content]** フィールドに入力したテキストは、ログイン画面の [Username] および [Password] フィールドの上に表示されます。また、**[Username]** および **[Password]** フィールドを有効にするためにユーザーがクリックする必要がある確認メッセージも入力できます。

ログインバナーを編集するには、ユーザーアカウントに対する「Configure Login Settings」許可が有効になっている必要があります。

ログインバナーをカスタマイズするには

1. **[Administration] > [Setup] > [System Admin]** をクリックします。
2. **[Users/Groups]** セクションの **[Login Banner]** をクリックします。
3. ログインバナーとして表示するテキストを、**[Content]** フィールドに入力します。

   このフィールドには、書式設定されていないテキストのみを入力できますが、標準のHTMLタグを適用して、書式設定されたテキストを表示できます。このフィールドに画像をロードすることはできません。
4. (オプション) **[Confirmation]** フィールドにテキストを入力します。入力したテキストは、チェックボックスとともにログインバナーに表示されます。[**Username**] および [**Password**] フィールドを有効にするには、このチェックボックスをクリックする必要があります。たとえば、「Are you sure?」と入力した場合、ユーザーはログインを確認するために、チェックボックスをクリックする必要があります。
5. [**Save**] をクリックします。

User Management

[Users] および **[Groups]** タブでは、システム上のユーザーとユーザーグループを管理できます。ユーザーグループは、システムのさまざまな部分に対するアクセス制御を適用するための手段です。

ユーザー

システムにログインできるユーザーを管理するには、**[Users]** タブを開きます。新しいユーザーの追加、ユーザー情報の編集、ユーザーの削除はいつでも行うことができます。これらの機能を実行するには、適切なSystem Adminグループ権限を持っている必要があります。

新しいユーザーを追加するには

1. **[Administration] > [Setup] > [System Admin]** をクリックします。
2. 左パネルの **[Users/Groups]** セクションにある **[User Management]** をクリックします。
3. **[Users]** タブで、ページの左上にある **[Add]** をクリックします。

4. 以下のパラメーターを入力します。

パラメーター	説明
資格情報	
Login	ユーザーのログイン名。
Password	ユーザーのパスワード。
Confirm Password	ユーザーのパスワードを再度入力します。
連絡先情報	

Use Client DN	SSLクライアント証明書またはLDAP認証を有効にした場合は、このリンクをクリックして、ユーザーのDN (Distinguished Name、証明書サブジェクト) 情報を入力します。DNは、次のような形式になっている必要があります。
	`CN=UserA,OU=Engg Team,O=ArcSight\, Inc.,L=Cupertino,C=US,ST=California`
	DNを判定するには、次のURLを使用して証明書を表示します。
	`https://<ホスト名またはIPアドレス>/platform-service/DisplayCertificate`
	または
	システムに接続するためにユーザーが開くブラウザーから、ユーザーのDN情報を入手します。たとえば、Mozilla Firefoxの場合は、**[ツール]** > **[オプション]** > **[詳細]** > **[証明書]** > **[証明書を表示]** > **[あなたの証明書]** > <証明書を選択> > **[表示]** の順にクリックします。

First Name	ユーザーの名。
Last Name	ユーザーの姓。
Email	ユーザーのメールアドレス。
Phone Number	(オプション) ユーザーの電話番号。
Title	(オプション) ユーザーの肩書き。
Department	(オプション) ユーザーの部署。
Fax	(オプション) ユーザーのFAX番号。
Alternate Number	(オプション) ユーザーの他の電話番号。
Assign to Groups	このユーザーが属するグループを選択します。この設定は、ユーザーがこのArcSight Management Centerに対して持つ権限を制御します。

パラメーター	説明
System Admin	ドロップダウンリストから権限のレベルを選択します。 • デフォルトのSystem Admin Group: [System Admin] メニューで設定を変更する権限をユーザーに付与します。このオプションを選択すると、すべてのタブとメニューが表示されます。 • Read Only System Admin Group: ユーザーに読み取り専用アクセスを許可します。 • Unassigned: ユーザーは [System Admin] メニューにアクセスできません。
ArcMC Rights	ドロップダウンリストから権限のレベルを選択します。 • Default ArcMC Rights Group: **[Dashboard]**、**[Node Management]**、および [**Configuration Management**] メニューと、[**Backup/Restore**] および [**Repositories**] メニューへの権限をユーザーに付与します。このオプションを選択すると、すべてのタブとメニューが表示されます。 • Read Only ArcMC Group: ユーザーに読み取り専用アクセスを許可します。 • Unassigned: ユーザーはすべてのArcMCコンポーネントにアクセスできません。
Notes	(オプション) ユーザーに関するその他の情報。

5. **[Save and Close]** をクリックします。

ユーザーを編集するには

1. **[Administration] > [System Admin]** をクリックします。
2. 左パネルの**[Users/Groups]**セクションにある**[User Management]**をクリックします。
3. **[Users]**タブで、編集するユーザーを選択します (複数可)。
4. ページの左上にある **[Edit]** をクリックします。
5. 必要に応じてユーザー情報を更新します。
6. **[Save User]** をクリックします。

ユーザーを削除するには

1. **[Administration] > [System Admin]** をクリックします。
2. 左パネルの**[Users/Groups]** セクションにある **[User Management]** をクリックします。
3. **[Users]** タブで、削除するユーザーを選択します (複数可)。
4. ページの左上にある **[Delete]** をクリックします。

Reset Password

Reset Password機能を使用すると、パスワードを知らなくてもユーザーのパスワードをリセットできます。SMTPが設定されたサーバーを使用しており、ユーザーを作成および更新できる許

可があれば、**[Reset Password]** ボタンをクリックしてユーザーのパスワードをリセットできます。新しいパスワード文字列を含む電子メールが、ユーザー宛に自動送信されます。

一時的なパスワードを含む電子メールを自動送信するには、SMTPサーバーが設定されている必要があります。SMTPサーバーが設定されていない場合は、電子メールを送信できないため、パスワードはリセットされません。

ユーザーのパスワードをリセットするには

1. **[Administration] > [System Admin]** をクリックします。
2. 左パネルの**[Users/Groups]** セクションにある **[User Management]** をクリックします。
3. **[Users]** タブで、パスワードをリセットするユーザーを選択します (複数可)。
4. ページの左上にある **[Reset Password]** をクリックします。

ユーザーは、メールで指定された期間内に、一時的な文字列を使用してログインする必要があります。ユーザーが指定の期間内にログインしなかった場合、アカウントが非アクティブ化されます。アカウントが非アクティブ化された場合、管理者は、再度アカウントをアクティブ化してからパスワードをリセットする必要があります。

ユーザーをアクティブ化するには

1. **[Administration] > [System Admin]** をクリックします。
2. 左パネルの**[Users/Groups]** セクションにある **[User Management]** をクリックします。
3. **[Users]**タブで、アクティブ化するユーザーを選択します (複数可)。
4. **[Edit]** を選択します。
5. **[Active]** チェックボックスをオンにします。
6. 変更内容を**保存**します。

グループ

ユーザーグループは、システム上の特定の機能に対する権限を定義し、これらの機能に対するアクセス制御を適用するための役割を果たします。たとえば、ユーザーAにコネクターアプライアンスの管理に限定されないシステム管理に関連する操作を実行させる場合は、このユーザーをSystem Adminグループに割り当てますが、コネクターアプライアンスグループには割り当てません。

ユーザーグループは、以下のタイプに分類されます。System Adminのグループとコネクターアプライアンス Rightsのグループです。それぞれのタイプには、定義済みのデフォルトユーザーグループがあり、そのタイプのすべての権限が有効になっています。特定のグループタイプの権限の一部を許可するには、新しいユーザーグループを作成し、そのグループに許可する権限のみを有効にします。その後、制限するユーザーを新たに作成したグループに割り当てます。

System Adminのグループ

System Admin Group

System Admin Groupは、システムに対するシステム管理オペレーションを制御します。これには、ネットワーク情報の設定、ストレージマウントの設定、SSL証明書のインストール、およびユーザー管理などがあります。

Read Only System Admin Group

すべての権限を有効にするデフォルトのSystem Admin Groupに加えて、システムではRead Only System Admin Groupを使用できます。このグループに割り当てられたユーザーは、システム管理設定を表示できますが、変更はできません。

ArcSight Management Center用のArcSight Management Center Rightsグループ

ArcSight Management Center Rights Group

コネクターアプライアンス Rights Groupは、システムに対するArcSight Management Centerアプリケーションの動作を制御します。これには、ArcSight Management Centerダッシュボードの表示とバックアップ処理などがあります。

Read Only ArcSight Management Center Group

すべての権限を有効にするデフォルトのコネクターアプライアンス Rights Groupに加えて、コネクターアプライアンスでより細かく制御された許可と「表示専用」のデフォルトオプションが利用できます。 読み取り専用ユーザーは、タブとタブに表示される操作を参照でき、更新、証明書リストの表示、Logfuなどの操作を実行できます。

このグループに許可される権限の完全なリストについては、システムのユーザーインターフェイスを参照してください。

> アクセスの問題が発生する可能性があるため、デフォルト管理者ユーザーの権限は一切変更しないことを強く推奨します。

ユーザーグループの管理

新しいユーザーグループを作成するには

1. **[Administration] > [System Admin]** をクリックします。
2. 左パネルの **[Users/Groups]** セクションにある **[User Management]** をクリックします。
3. **[Groups]** タブをクリックします。
4. ページの左上にある **[Add]** をクリックします。

5. 次のようにして新しいグループを定義します。
   a. **[Group Name]** フィールドにグループ名を入力します。
   b. **[Description]** フィールドにグループの説明を入力します。
   c. [Group Type] ドロップダウンボックスで、グループタイプを選択します。
   d. グループタイプ名の横の下矢印アイコン ( ) をクリックし、このグループのユーザーに割り当てる権限を表示および選択します。
6. **[Save and Close]** をクリックしてグループの設定を保存するか、**[Save and Edit Membership]** をクリックしてこのグループにユーザーを追加します。

ユーザーグループを編集するには

1. **[Administration] > [System Admin]** をクリックします。
2. 左パネルの **[Users/Groups]** セクションにある **[User Management]** をクリックします。
3. **[Groups]** タブをクリックします。
4. 編集するグループを選択し、ページの左上にある **[Edit]** をクリックします。
5. ユーザーグループ情報を更新します。

   グループのメンバーシップを編集する必要がある場合は、次のようにします。
   a. **[Save and Edit Membership]** をクリックして [Edit Group Membership] ページを表示します。
   b. [Edit Group Membership] ページの左上から **[Add]** をクリックします。
   c. 追加するユーザーを選択します。デフォルトでは、編集中のタイプの他のグループに属していないユーザーのみを追加できます。他のグループに属しているユーザーを追加するには、**[Show users that belong to other <group_type> groups]** をクリックします。

      更新中のものとグループタイプが同じ別のグループに属しているユーザーを追加すると、そのユーザーは前のグループから自動的に削除されます。
   d. **[OK]** をクリックします。
   e. **[Back to Group List]** をクリックします。
6. **[Save and Close]** をクリックします。

ユーザーグループを削除するには

1. **[Administration] > [System Admin]** をクリックします。
2. 左パネルの **[Users/Groups]** セクションにある **[User Management]** をクリックします。
3. **[Groups]** タブをクリックします。
4. 削除するグループを選択します (複数可)。
5. ページの左上にある **[Delete]** をクリックします。

パスワードの変更

パスワードを変更するには **[Change Password]** メニューを使用します。この機能は、システム管理者がパスワードを知らなくてもユーザーのパスワードをリセットできるようにするためのパスワードリセット機能と異なり、すべてのユーザーがパスワードを変更するために使用できます。パスワードには、管理者ユーザーによって指定されたパスワードポリシーが適用されます。

パスワードを変更するには

1. **[Administration] > [Setup] > [System Admin]** をクリックします。
2. 左パネルの **[Users/Groups]** セクションにある **[Change Password]** をクリックして、**[Change Password for <ユーザー名>]** ページを表示します。
3. 以前のパスワード、新しいパスワードを入力し、確認用に新しいパスワードを再度入力します。

付録A: 監査ログ

ここでは、以下の内容について説明します。

監査イベントのタイプ

共通イベントフォーマット (CEF) のArcSight Management Centerアプリケーション監査イベントを、選択した通知先に転送することができます。

ArcSight Management Centerでは、次の複数のタイプの監査イベントが生成されます。

- **アプリケーションイベント:** ArcSight Management Centerの機能と設定変更に関連します。
- **プラットフォームイベント:** ArcSight Management Centerのシステムに関連します。
- **システムヘルスイベント:** ArcSight Management Centerのヘルスに関連します。

監査イベントの情報

ArcSight Management Centerの監査イベントには、次のプレフィックスフィールドに関する情報が含まれます。

- Device Event Class ID
- Device Severity
- Name
- Device Event Category (`cat`)

監査ログの生成方法の詳細については、「監査ログ」(249ページ) を参照してください。

注: Syslog Daemonコネクターがローカルマシンにインストールまたは設定されていない場合、監査イベントは表示されません。

アプリケーションイベント

アプリケーションイベント

シグネチャ	緊急度	説明	deviceEventCategory
コネクター			
connector:101	1	コネクターの登録に成功しました	/Connector/Add/Success
connector:102	1	コネクターが正常に削除されました	/Connector/Delete
connector:103	1	コネクターパラメーターの更新に成功しました	/Connector/Parameter/Update/Success
connector:104	1	AUPパッケージの作成に成功しました	/Connector/AUP Package/Create/Success
connector:105	1	AUPパッケージの展開に成功しました	/Connector/AUP Package/Deploy/Success
connector:201	1	コネクターの追加に失敗しました	/Connector/Add/Fail
connector:202	1	コネクターの削除に失敗しました	/Connector/Delete/Fail
connector:203	1	コネクターパラメーターの更新に失敗しました	/Connector/Parameter/Update/Fail
ArcSight Management Center			
arcmc:101	1	設定バックアップスケジューラーの追加に成功しました	/BackupScheduler/Add/Success
arcmc:102	1	設定バックアップスケジューラーの更新に成功しました	/BackupScheduler/Update/Success
arcmc:103	1	設定バックアップスケジューラーの削除に成功しました	/BackupScheduler/Delete/Success
arcmc:104	1	スケジュールされたバックアップがトリガーされました	/Backup/Scheduled/Trigger

アプリケーションイベント (続き)

シグネチャ	緊急度	説明	deviceEventCategory
arcmc:105	1	スケジュールされたバックアップが完了しました	/Backup/Scheduled/Complete/Success
arcmc:106	1	手動バックアップが完了しました	/Backup/Manual/Complete/Success
arcmc:107	1	ローカルバックアップが完了しました	/Backup/Local/Complete/Success
arcmc:108	1	ライセンスで許可されている管理対象コネクターの最大数を超えました	/RemotelyManagedConnectors/Exceeded
arcmc:110	1	ライセンスで許可されている管理対象製品の最大数を超えようとしています	/managedproducts/exceeded
arcmc:111	1	リブートコマンドが正常に実行されました	Node/reboot/launched/Success
arcmc:112	1	新規設定が正常に作成されました	/Configuration/Add/Success
arcmc:113	1	設定の編集に成功しました	/Configuration/Edit/Success
arcmc:114	1	設定の削除に成功しました	/Configuration/Delete/Success
arcmc:115	1	設定のプッシュに成功しました	/Configuration/Push/Success
arcmc:116	1	設定のインポートに成功しました	/Configuration/Import/Success
arcmc:117	1	設定に対するサブスクライバーの追加に成功しました	/Configuration/Subscribe/Success
arcmc:118	1	設定に対するノードのサブスクライブ解除に成功しました	/Configuration/Unsubscribe/Success
arcmc:119	1	設定の準拠状況のチェックに成功しました	/Configuration/Check Compliance/Success
arcmc:120	1	設定が正常に実行されました	/Node/Set/Configuration/Success
arcmc:121	1	設定が正常に追加されました	/Node/Append/Configuration/Success

アプリケーションイベント (続き)

シグネチャ	緊急度	説明	deviceEventCategory
arcmc:122	1	エージェントのインストールに成功しました	/ArcMCAgent/Install/Success
arcmc:123	1	エージェントのアップグレードに成功しました	/ArcMCAgent/Upgrade/Success
arcmc:124	1	Loggerピアの追加/プッシュに成功しました	/Logger/AddPeers/Success
arcmc:125	1	Loggerピアの削除に成功しました	/Logger/RemovePeers/Success
arcmc:127	1	Loggerピアグループの作成/インポートに成功しました	/Logger/AddPeerGrp/Success
arcmc:128	1	Loggerピアグループの削除に成功しました	/Logger/DeletePeerGrp/Success
arcmc:129	1	Loggerピアグループの編集に成功しました	/Logger/EditPeerGrp/Success
arcmc:130	1	初期設定のインポートに成功しました	/Logger/ImportInitConfig/Success
arcmc:131	1	初期設定をプッシュしました	/Logger/PushInitConfig/Success
arcmc:132	1	初期設定を削除しました	/Logger/DelInitConfig/Success
arcmc:133	1	ホストのアップグレードが開始されました。	/Node/Upgrade/Start
arcmc:134	1	ホストのアップグレードが成功しました。	/Node/Upgrade/Success
arcmc:138	1	ルールの更新	/ArcMC/UpdateRules/Success
arcmc:201	1	設定バックアップスケジューラーの追加に失敗しました	/BackupScheduler/Add/Fail
arcmc:202	1	設定バックアップスケジューラーの更新に失敗しました	/BackupScheduler/Update/Fail
arcmc:203	1	設定バックアップスケジューラーの削除に失敗しました	/BackupScheduler/Delete/Fail
arcmc:205	1	スケジュールされたバックアップに失敗しました	/Backup/Scheduled/Complete/Fail

アプリケーションイベント (続き)

シグネチャ	緊急度	説明	deviceEventCategory
arcmc:206	1	手動バックアップに失敗しました	/Backup/Manual/Complete/Fail
arcmc:212	1	新規設定の作成に失敗しました	/Configuration/Add/Fail
arcmc:213	1	設定の編集に失敗しました	/Configuration/Update/Fail
arcmc:214	1	設定の削除に失敗しました	/Configuration/Delete/Fail
arcmc:215	1	設定のプッシュに失敗しました	/Configuration/Import/Fail
arcmc:216	1	設定のインポートに失敗しました	/Backup/Local/Push/Fail
arcmc:217	1	設定に対するサブスクライバーの追加に失敗しました	/Configuration/Subscribe/Fail
arcmc:218	1	設定に対するノードのサブスクライブ解除に失敗しました	/Configuration/Unsubscribe/Fail
arcmc:219	1	設定の準拠状況のチェックに失敗しました	/Configuration/Check Compliance/Success
arcmc:220	1	設定の実行に失敗しました	/Node/Set/Configuration/ Fail
arcmc:221	1	設定の追加に失敗しました	/Node/Append/Configuration/ Fail
arcmc:222	1	エージェントのインストールに失敗しました	/ArcMCAgent/Install/Failure
arcmc:223	1	エージェントのアップグレードに失敗しました	/ArcMCAgent/Upgrade/Fail
arcmc:224	1	Loggerピアの追加/プッシュに失敗しました	/Logger/AddPeers/Fail
arcmc:225	1	Loggerピアの削除に失敗しました	/Logger/RemovePeers/Fail
arc mc:226	1	アラートメッセージのペイロード	/ArcMCMonitor/Breach
arcmc:230	1	初期設定のインポートに失敗しました	/Logger/ImportInitConfig/Fail

アプリケーションイベント (続き)

シグネチャ	緊急度	説明	deviceEventCategory
arcmc:234	1	ホストのアップグレードに失敗しました。	/Node/Upgrade/Fail
arcmc:250	1	ユーザー割り当て<割り当て名>のプッシュ	/ArcMCUM/Push
arcmc:251	1	ユーザー<ユーザー名>の廃止	/ArcMCUM/DeleteUser
arcmc:252	1	ユーザー<ユーザー名>の追加	/ArcMCUM/AddUser
通知先			
destination:102	1	通知先の更新に成功しました	/Connector/Destination/Update/Success
destination:103	1	通知先の削除に成功しました	/Connector/Destination/Delete/Success
destination:104	1	通知先設定の更新に成功しました	/Connector/Destination/Configuration/Update/Success
destination:105	1	通知先の登録に成功しました	/Connector/Destination/Registration/Success
destination:106	1	通知先設定の作成に成功しました	/Connector/Destination/Configuration/Add/Success
destination:107	1	通知先設定の削除に成功しました	/Connector/Destination/Configuration/Delete/Success
destination:202	1	コネクターの通知先の更新に失敗しました	/Connector/Destination/Update/Fail
destination:203	1	コネクターからの通知先の削除に失敗しました	/Connector/Destination/Delete/Fail
destination:204	1	通知先設定の更新に失敗しました	/Connector/Destination/Configuration/Update/Fail
destination:205	1	通知先の登録に失敗しました	/Connector/Destination/Registration/Fail
destination:206	1	通知先設定の追加に失敗しました	/Connector/Destination/Configuration/Add/Fail
destination:207	1	通知先設定の削除に失敗しました	/Connector/Destination/Configuration/Delete/Fail
コンテナー			

アプリケーションイベント (続き)

シグネチャ	緊急度	説明	deviceEventCategory
container:101	1	コンテナーのアップグレードに成功しました	/Container/Upgrade/Success
container:102	1	ユーザーファイルのプッシュに成功しました	/Container/UserFiles/Push/Success
container:103	1	コンテナーからのユーザーファイルの削除	/Container/UserFiles/Delete
container:104	1	コンテナーへのCA証明書のプッシュに成功しました	/Container/CACert/Push/Success
container:105	1	コンテナーのデモCAの有効化に成功しました	/Container/DemoCA/Enable/Success
container:106	1	コンテナーのデモCAの無効化に成功しました	/Container/DemoCA/Disable/Success
container:109	1	コンテナーからのプロパティの削除に成功しました	/Container/Property/Delete/Success
container:110	1	プロパティの変更に成功しました	/Container/Property/Update/Success
container:111	1	コンテナーパスワードの更新に成功しました	/Container/Password/Update/Success
container:112	1	コンテナーの追加に成功しました	/Container/Add/Success
container:113	1	コンテナーの編集	/Container/Update
container:114	1	コンテナーの削除	/Container/Delete
container:115	1	コンテナーの証明書の追加に成功しました	/Container/Certificate/Add/Success
container:116	1	証明書の削除に成功しました [addtrust class 1ca]	/Container/Certificate/Delete/Success
container:117	1	FIPSモードの有効化に成功しました	/Container/FIPS/Enable/Success
container:118	1	FIPSモードの無効化に成功しました	/Container/FIPS/Disable/Success

アプリケーションイベント (続き)

シグネチャ	緊急度	説明	deviceEventCategory
container:119	1	サポートの終了したアプライアンスモデル上に存在するコンテナーに対してアップグレードがトリガーされました	Container/FromEndOfLifeModel/Upgrade/Triggered
container:201	1	コンテナーのアップグレードに失敗しました	/Container/Upgrade/Fail
container:202	1	コンテナーへのユーザーファイルのプッシュに失敗しました	/Container/UserFiles/Push/Fail
container:204	1	コンテナーへのCA証明書のプッシュに失敗しました	/Container/CACert/Push/Fail
container:205	1	コンテナーのデモCAの有効化に失敗しました	/Container/DemoCA/Enable/Fail
container:206	1	コンテナーのデモCAの無効化に失敗しました	/Container/DemoCA/Disable/Fail
container:209	1	コンテナーからのプロパティの削除に失敗しました	/Container/Property/Delete/Fail
container:210	1	コンテナーのプロパティの更新に失敗しました	/Container/Property/Update/Fail
container:211	1	コンテナーパスワードの更新に失敗しました	/Container/Password/Update/Fail
container:212	1	コンテナーの追加に失敗しました	/Container/Add/Fail
container:215	1	コンテナーの証明書の追加に失敗しました	/Container/Certificate/Add/Fail
container:216	1	コンテナーの証明書の削除に失敗しました	/Container/Certificate/Delete/Fail
container:217	1	コンテナーでのFIPSの有効化に失敗しました	/Container/FIPS/Enable/Fail
container:218	1	コンテナーでのFIPSの無効化に失敗しました	/Container/FIPS/Disable/Fail

アプリケーションイベント (続き)

シグネチャ	緊急度	説明	deviceEventCategory
container:219	1	SSL証明書のダウンロードに成功しました	/Container/Certificate/Download/Success
container:220	1	SSL証明書のダウンロードに失敗しました	/Container/Certificate/Download/Fail
container:221	1	SSL証明書のインポートに成功しました	/Container/Certificate/Import/Success
container:222	1	SSL証明書のインポートに失敗しました	/Container/Certificate/Import/Fail
container:301	1	コンテナーのアップグレードが開始されました	/Container/Upgrade/Start
Event Broker			
eventbroker:146	1	Event Brokerのトピックの追加に成功しました	/EventBroker/Topic/Add/Success
eventbroker:147	1	Event Brokerのルートの削除に成功しました	/EventBroker/Route/Add/Success
eventbroker:148	1	Event Brokerのルートの追加に成功しました	/EventBroker/Route/Add/Success
eventbroker:149	1	Event Brokerのルートの更新に成功しました	/EventBroker/Route/Update/Success
eventbroker:241	1	Event Brokerのトピックの追加に失敗しました	/EventBroker/Topic/Add/Fail
eventbroker:242	1	Event Brokerのルートの削除に失敗しました	/EventBroker/Route/Add/Fail
eventbroker:243	1	Event Brokerのルートの追加に失敗しました	/EventBroker/Route/Add/Fail
eventbroker:244	1	Event Brokerのルートの更新に失敗しました	/EventBroker/Route/Update/Fail
ロケーション			
location:101	1	ロケーションの追加に成功しました	/Location/Add/Success
location:102	1	ロケーションの編集	/Location/Update
location:103	1	ロケーションの削除	/Location/Delete
location:201	1	ロケーションの追加に失敗しました	/Location/Add/Fail

アプリケーションイベント (続き)

シグネチャ	緊急度	説明	deviceEventCategory
ホスト			
host:101	1	ホストの追加に成功しました	/Host/Add/Success
host:103	1	ホストの削除	/Host/Delete
host:105	1	ホストの証明書のダウンロードおよびインポートに成功しました	/Host/Certificate/Download /Import/Success
host:201	1	ホストの追加に失敗しました	/Host/Add/Fail
host:205	1	ホストの証明書のダウンロードおよびインポートに失敗しました	/Host/Certificate/Download Import/Fail

プラットフォームイベント

プラットフォームイベント

シグネチャ	緊急度	定義	カテゴリ
platform:200	7	パスワードの変更に失敗しました	/Platform/Authentication/ PasswordChange/Failure
platform:201	7	ログインに失敗しました	/Platform/Authentication/Failure/ Login
platform:202	5	パスワードが変更されました	/Platform/Authentication/ Password
platform:203	7	アクティブでないユーザーによるログイン試行	/Platform/Authentication/ InactiveUser/Failure
platform:213	7	監査の転送が変更されました	/Platform/Configuration/Global/ AuditEvents
platform:220	5	証明書をインストールしました	/Platform/Certificate/Install
platform:221	7	証明書の不一致エラー	/Platform/Certificate/Mismatch
platform:222	1	証明書署名リクエストを作成しました	/Platform/Certificate/Request
platform:224	5	自己署名証明書の再生成	/Platform/Certificate/Regenerate

プラットフォームイベント (続き)

シグネチャ	緊急度	定義	カテゴリ
platform:226	7	アップロードした更新ファイルが損傷または破損しています	/Platform/Update/Failure/CorruptPackage
platform:227	5	更新のインストール成功	/Platform/Update/Applied
platform:228	7	更新のインストール失敗	/Platform/Update/Failure/Installation
platform:230	3	ログインに成功しました	/Platform/Authentication/Login
platform:234	7	ログインに失敗しました (ロック済み)	/Platform/Authentication/Failure/LOCKED
platform:239	1	ユーザーログアウト	/Platform/Authentication/Logout
platform:240	3	ユーザーグループを追加しました	/Platform/Groups/Add
platform:241	3	ユーザーグループを更新しました	/Platform/Groups/Update
platform:242	5	グループからすべてのメンバーを削除しました	/Platform/Authorization/Groups/Membership/Update/Clear
platform:244	3	ユーザーグループを削除しました	/Platform/Groups/Remove
platform:245	3	ユーザーを追加しました	/Platform/Users/Add
platform:246	3	ユーザーを更新しました	/Platform/Users/Update
platform:247	3	ユーザーを削除しました	/Platform/Users/Delete
platform:248	3	セッションが期限切れになりました	/Platform/Authentication/Logout/SessionExpiration
platform:249	7	アカウントがロックされました	/Platform/Authentication/AccountLocked
platform:250	3	リモートマウントポイントを追加しました	/Platform/Storage/RFS/Add
platform:251	5	リモートマウントポイントを編集しました	/Platform/Storage/RFS/Edit

プラットフォームイベント (続き)

シグネチャ	緊急度	定義	カテゴリ
platform:252	7	リモートマウントポイントの作成に失敗しました	/Platform/Storage/RFS/Failure
platform:253	5	リモートマウントポイントを削除しました	/Platform/Storage/RFS/Remove
platform:260	5	静的経路が変更されました	/Platform/Configuration/Network/Route/Update
platform:261	5	静的経路が削除されました	/Platform/Configuration/Network/Route/Remove
platform:262	5	アプライアンスの時刻が変更されました	/Platform/Configuration/Time
platform:263		NIC設定が変更されました	/Platform/Configuration/NIC
platform:264		NTPサーバー設定が変更されました	/Platform/Configuration/NTP
platform:265	5	DNS設定が変更されました	/Platform/Configuration/Network/DNS
platform:266	5	Hostsファイルが変更されました	/Platform/Configuration/Network/Hosts
platform:267	5	SMTP設定が変更されました	/Platform/Configuration/SMTP
platform:268	5	静的経路が追加されました	/Platform/Configuration/Network/Route/Add
platform:269	5	プラットフォーム設定を更新しました	/Platform/Configuration
platform:280	7	アプライアンスのリブートが開始されました	/Appliance/State/Reboot/Initiate
platform:281	3	アプライアンスのリブートがキャンセルされました	/Appliance/State/Reboot/Cancel
platform:282	9	アプライアンスの電源オフが開始されました	/Appliance/State/Shutdown
platform:284	5	SANマルチパスを有効にしました	/Platform/Storage/Multipathing/Enable
platform:285	5	SANマルチパスを無効にしました	/Platform/Storage/Multipathing/Disable

プラットフォームイベント (続き)

シグネチャ	緊急度	定義	カテゴリ
platform:300	5	信頼済みの証明書をインストールしました	/Platform/Certificate/Install
platform:301	5	証明書取り消しリストをインストールしました	/Platform/Certificate/Revocation/Install
platform:302	5	信頼済みの証明書を削除しました	/Platform/Certificate/Delete
platform:303	5	証明書取り消しリストを削除しました	/Platform/Certificate/Revocation/Delete
platform:304	7	信頼済みの証明書のインストールに失敗しました	/Platform/Certificate/Install/Failure
platform:305	7	証明書取り消しリストのインストールに失敗しました	/Platform/Certificate/Revocation/Install/Failure
platform:306	5	プロセスの開始	/Platform/Process/Start
platform:307	5	プロセスの停止	/Platform/Process/Stop
platform:308	5	プロセスの再開	/Platform/Process/Restart
platform:310	5	FIPSモードを有効にしました	/Platform/Configuration/FIPS/Enable
platform:311	7	FIPSモードを無効にしました	/Platform/Configuration/FIPS/Disable
platform:312	7	Webサーバーの暗号強度が変更されました	/Platform/Configuration/WebServer/CipherStrength
platform:313	5	SSHの有効化	/Platform/Configuration/SSH/Enable
platform:314	7	SSHの無効化	/Platform/Configuration/SSH/Disable
platform: 315	7	起動/リブート時のみSSHを有効化	/Platform/Configuration/SSH/StartupOnly
platform:316	7	8時間のみSSHを有効化	/Platform/Configuration/SSH/Enable8Hours
platform: 320	3	アプライアンスの電源オフがキャンセルされました	/Appliance/State/Shutdown/Cancel
platform:371	5	OSサービスを再起動しました	/Platform/Service/Restart

プラットフォームイベント (続き)

シグネチャ	緊急度	定義	カテゴリ
platform:400	1	診断コマンドを実行しました	/Platform/Diagnostics/Command
platform:407	7	SSL証明書の有効期限に関する警告	/Platform/Certificate/SSL/Expiration
platform:408	5	アプライアンスの起動が完了しました	/Appliance/State/Startup
platform:409	3	ログイン警告バナーの設定	/Platform/Configuration/LoginBanner
platform:410	3	ネットワーク設定が変更されました	
platform:411	5	自動パスワードリセット	/Platform/Authentication/PasswordChange
platform:412	3	ロケールの設定	/Platform/Configuration/Locale
platform:440	3	SNMP設定が変更されました	Platform/Configuration/SNMP
platform:450	3	FTPサービスが有効化されました	
platform:451	3	FTPサービスが無効化されました	
platform:454	3	FTPサービス設定が変更されました	
platform:455	3	サブディレクトリを追加しました	
platform:456	3	サブディレクトリを削除しました	
platform:460	3	NICエイリアスが追加されました	/Platform/Network/Alias/Add
platform:462	3	NICエイリアスが削除されました	/Platform/Network/Alias/Remove
platform:500	5	メンバーをグループから削除	/Platform/Authorization/Groups/Membership/Remove
platform:501	5	グループメンバーが追加されました	/Platform/Authorization/Groups/Membership/Add
platform:502	5	ユーザーがグループから削除されました	/Platform/Authorization/Users/Groups/Remove
platform:503	5	ユーザーがグループに追加されました	/Platform/Authorization/Users/Groups/Add

プラットフォームイベント (続き)

シグネチャ	緊急度	定義	カテゴリ
platform:530	5	認証セッションの設定が正常に変更されました	/Platform/Configuration/Authentication/Sessions/Success
platform:540	5	パスワードロックアウトの設定が正常に更新されました	/Platform/Configuration/Authentication/Password/Lockout/Success
platform:550	5	パスワード有効期限の設定が正常に更新されました	/Platform/Configuration/Authentication/Password/Expiration/Success
platform:560	5	パスワード検証の設定が正常に更新されました	/Platform/Configuration/Authentication/Password/Validation/Success
platform:570	5	自動パスワードリセット許可の設定が正常に変更されました	/Platform/Configuration/Authentication/Password/AutomatedReset/Success
platform:590	5	RADIUS認証設定が正常に変更されました	/Platform/Configuration/Authentication/RADIUS/Success
platform:600	5	LDAP認証設定が正常に変更されました	/Platform/Configuration/Authentication/LDAP/Success
platform:610	5	グローバル認証設定が正常に変更されました	/Platform/Configuration/Authentication/Global/Success

システムヘルスイベント

システムヘルスイベントでは、次の4つのステータスインジケーターが提供されます。

- OK
- Degraded
- Rebuilding
- Failed

システムが正常に動作していることを示す**OK**イベントは、10分ごとに生成されます (1センサー、1時間あたり6つのイベントが生成されます)。**OK**以外のステータス (**Degraded**、**Rebuilding**、または**Failed**) の場合は、センサーが**OK**ステータスに変わるまで、イベントが1分ごとに送信されます。

SNMP関連のプロパティ

以下は、SNMPトラップ経由で送信されるシステムヘルスイベントのイベントフィールドです。SNMPトラップのセットアップの詳細な手順については、「SNMP」(237ページ)を参照してください。

• event.deviceReceiptTime	• event.endTime
• event.deviceVendor	• event.deviceProduct
• event.deviceVersion	• event.deviceEventClassId
• event.name	• event.deviceSeverity
• event.deviceEventCategory	• event.deviceCustomNumber1
• event.deviceCustomNumber1Label	• event.deviceCustomString1
• event.deviceCustomString1Label	• event.deviceCustomString2
• event.deviceCustomString2Label	• event.deviceCustomString3
• event.deviceCustomString3Label	• event.deviceCustomString4
• event.deviceCustomString4Label	• event.deviceCustomString5
• event.deviceCustomString5Label	• event.deviceCustomString6
• event.deviceCustomString6Label	• event.destinationAddress
• event.deviceAddress	

snmp.mib.versionは5.0に設定されます。

システムヘルスイベント

シグネチャ	緊急度	定義	カテゴリ
CPU			
cpu:100	1	CPU使用率	/Monitor/CPU/Usage
cpu:101	1	CPUごとのヘルス統計	/Monitor/CPU*n*/Usage
ディスク			
disk:101	1	残りのルートディスク容量	/Monitor/Disk/Space/Remaining/Data
disk:102	1	ディスク読み取りバイト数	/Monitor/Disk/*drive*/Read
disk:103	1	ディスク書き込みバイト数	/Monitor/Disk/*drive*/Write
disk:104	1	残りのディスク容量	/Monitor/Disk/Space/Remaining/Root
ハードウェア			
hardware:101	1	電流OK	/Monitor/Sensor/Current/Ok**

システムヘルスイベント (続き)

シグネチャ	緊急度	定義	カテゴリ
hardware:102	5	電流劣化	/Monitor/Sensor/Current/Degraded**
hardware:103	8	電流エラー	/Monitor/Sensor/Current/Failed**
hardware:111	1	電圧OK	/Monitor/Sensor/Voltage/Ok**
hardware:112	1	電圧劣化	/Monitor/Sensor/Voltage/Degraded**
hardware:113	1	電圧エラー	/Monitor/Sensor/Voltage/Failed**
hardware:121	1	バッテリOK	/Monitor/Sensor/Battery/Ok**
hardware:122	5	バッテリ劣化	/Monitor/Sensor/Battery/Degraded **
hardware:123	8	バッテリエラー	/Monitor/Sensor/Battery/Failed**
hardware:131	1	ファンOK	/Monitor/Sensor/Fan/Ok
hardware:132	5	ファン劣化	/Monitor/Sensor/Fan/Degraded
hardware:133	8	ファンエラー	/Monitor/Sensor/Fan/Failed
hardware:141	1	電源OK	/Monitor/Sensor/PowerSupply/Ok
hardware:142	5	電源劣化	/Monitor/Sensor/PowerSupply/Degraded
hardware:143	8	電源エラー	/Monitor/Sensor/PowerSupply/Failed
hardware:151	1	温度OK	/Monitor/Sensor/Temperature/Ok
hardware:152	1	温度劣化	/Monitor/Sensor/Temperature/Degraded
hardware:153	1	温度エラー	/Monitor/Sensor/Temperature/Failed
メモリ			
memory:100	1	プラットフォームのメモリ使用率	/Monitor/Memory/Usage/Platform
memory:101	1	JVMメモリのヘルス統計	/Monitor/Memory/Usage/Jvm
memory:102	1	プラットフォームのバッファーメモリのヘルス統計	/Monitor/Memory/Usage/Platform/Buffers
memory:103	1	プラットフォームのキャッシュメモリのヘルス統計	/Monitor/Memory/Usage/Platform/Cached
memory:104	1	プラットフォームの空きメモリのヘルス統計	/Monitor/Memory/Usage/Platform/Free
memory:105	1	JVMのヒープメモリのヘルス統計	/Monitor/Memory/Usage/Jvm/Heap
memory:106	1	JVMの非ヒープメモリのヘルス統計	/Monitor/Memory/Usage/Jvm/NonHeap

システムヘルスイベント (続き)

シグネチャ	緊急度	定義	カテゴリ
ネットワーク			
network:100	1	ネットワーク使用状況—受信	/Monitor/Network/Usage/*iface*/In
network:101	1	ネットワーク使用状況—送信	/Monitor/Network/Usage/*iface*/Out
network:200	1	Apacheの接続数	
NTP			
ntp:100	1	NTP同期	
RAID			
raid:101	1	RAIDコントローラーOK	/Monitor/RAID/Controller/OK
raid:102	5	RAIDコントローラー劣化	/Monitor/RAID/Controller/Degraded
raid:103	8	RAIDコントローラーエラー	/Monitor/RAID/Controller/Failed
raid:111	1	RAID BBU OK	/Monitor/RAID/BBU/Ok
raid:112	5	RAID BBU劣化	/Monitor/RAID/BBU/Degraded
raid:113	8	RAID BBUエラー	/Monitor/RAID/BBU/Failed
raid:121	1	RAIDディスクOK	/Monitor/RAID/DISK/Ok
raid:122	5	RAIDディスク再構築中	/Monitor/RAID/DISK/Rebuilding
raid:123	8	RAIDディスクエラー	/Monitor/RAID/DISK/Failed

付録B: 通知先実行時パラメーター

設定可能な通知先パラメーターについて次の表で説明します。この表に示すパラメーターは、すべての通知先で使用できるわけではありません。ユーザーインターフェイスには、通知先で有効なパラメーターが自動的に表示されます。通知先の実行時パラメーターを更新するための順を追った説明については、「コネクターパラメーターの編集」(102ページ)を参照してください。

パラメーター	説明
一括転送処理	パフォーマンスを高めネットワーク帯域幅を最適化するため、コネクターはイベントを一括転送できます。有効にすると、コネクターはイベントのブロックを作成し、(1) ブロックが一定のサイズに達するか、(2) 時間ウィンドウが満了するかのうち、先に発生したタイミングで、ブロックを送信します。また、緊急度でバッチの優先順位を設定し、緊急度が最も高いイベントバッチを最初に送信し、緊急度が最も低いイベントバッチを後で送信するように、コネクターに指示することができます。
Enable Batching (per event)	指定したサイズのイベントバッチを作成します (5、10、20、50、**100**、200、300個のイベント)。
Enable Batching (in seconds)	コネクターは、この時間ウィンドウが満了するとイベントを送信します (1、5、10、15、30、60)。
Batch By	コネクターがバッチを受信したときにバッチを送信する場合は [**Time Based**] (デフォルト)、緊急度に基づいてバッチを送信する場合は [**Severity Based**] (緊急度が最も高いイベントのバッチを最初に送信)。
時間補正	これらのフィールドに設定する値は、前後の時刻制限を確立します。この制限を超えた場合、コネクターがデバイスから報告された時刻を自動的に補正します。
Use Connector Time as Device Time	デバイスが報告する時刻を無効にし、コネクターがイベント受信した時刻を使用します。このオプションは、コネクターの方が正確な時刻を報告する可能性が高いことを前提とします (**[No]** | [Yes])。
Enable Device Time Correction (in seconds)	コネクターは、デバイスの`Detect Time`で報告される時刻を、この設定を使用して調整できます。これは、リモートデバイスのクロックがArcSightマネージャーと同期されていない場合に有用です。これは一時的な設定とすることをお勧めします。Managerとデバイスでクロックを同期するための推奨される方法は、NTPプロトコルを使用することです。デフォルト値は**0**です。
Enable Connector Time Correction (in seconds)	コネクターは、この設定を使用して、コネクター自身が報告する時刻を調整できます。これは情報提供のみを目的としており、コネクターのローカル時刻を変更できます。これは一時的な設定とすることをお勧めします。マネージャーとコネクターでクロックを同期するための推奨される方法は、NTPプロトコルを使用することです。デフォルト値は**0**です。

パラメーター	説明
Set Device Time Zone To	通常は、元のデバイスが時刻とともにそのタイムゾーンを報告するものと見なされます。元のデバイスがタイムゾーンを報告しない場合は、コネクターがタイムゾーンを報告するものと見なされます。そのようになっていないか、デバイスが正しく報告していない場合は、このオプションをDisabledからGMTまたは特定のワールドタイムゾーンに切り替えることができます。そのタイムゾーンは、報告される時刻に適用されます。デフォルト値: **Disabled**。
デバイス時刻自動補正	
Future Threshold	コネクターは、検出時刻がコネクターの時刻よりも`Future Threshold`秒進んでいると内部アラートを送信します。
Past Threshold	コネクターは、検出時刻がコネクターの時刻よりも`Past Threshold`秒遅れていると内部アラートを送信します。
Device List	しきい値が適用されるデバイスのカンマ区切りのリスト。デフォルトは、全デバイスを意味する(`ALL`)です。
時刻チェック	これらのフィールドは、デバイス時刻の自動補正を行うための、時間範囲と頻度の要素です。
Future Threshold	コネクターの時刻チェックのための進みしきい値を延長する秒数。デフォルト値は**5分** (300秒)です。
Past Threshold	コネクターの時刻チェックのための遅れしきい値を延長する秒数。デフォルト値は**1時間** (3,600秒)です。
Frequency	コネクターはその進みまたは遅れしきい値を、この秒数で指定された間隔でチェックします。デフォルト値は**1分** (60秒)です。
キャッシュ	これらの設定を変更しても、キャッシュ済みのイベントに影響はなく、キャッシュに送信される新しいイベントのみに影響を与えます。
Cache Size	ArcSightマネージャーがダウンした場合、またはコネクターが大量のイベント(イベントバースト)を受信した場合、コネクターは圧縮ディスクキャッシュを使用して大量のイベントを保持します。このパラメーターは、使用するディスクスペースを指定します。デフォルト値は**1 GB**で、約1500万個のイベントを保持できますが(コネクターによって変わります)、**5 MB**まで減らすことができます。このディスクスペースが一杯になると、コネクターは最も古いイベントを破棄して、ディスクキャッシュスペースを空けます(5 MB、50 MB、100 MB、150 MB、200 MB、250 MB、500 MB、1 GB、2.5 GB、5 GB、10 GB、50 GB)。
Notification Threshold	通知を起動するキャッシュのコンテンツのサイズ。デフォルト値は**10,000**です。
Notification Frequency	Notification Thresholdに達した後で通知を送信する頻度(1分、5分、**10分**、30分、60分)。
ネットワーク	
Heartbeat Frequency	この設定は、コネクターが通知先にハートビートメッセージを送信する頻度を制御します。デフォルト値は**10秒**ですが、**5秒**～**10分**の間で設定できます。ハートビートは、コネクターとの通信にも使用されることに注意する必要があります。このため、ハートビートの頻度を[**10分**]に設定すると、設定情報またはコマンドをコネクターに送信するのに10分もかかってしまう可能性があります。

パラメーター	説明
Enable Name Resolution	コネクターは、必要かつイベントレートで許可される場合に、IPアドレスからホスト名、ホスト名からIPアドレスへの変換を試みます。この設定は、この機能を制御します。ソース、ターゲット、およびデバイスのIPアドレスとホスト名も、この設定により影響を受ける場合があります。デフォルトでは、名前解決は有効 (**Yes**) になっています。
Name Resolution Host Name Only	デフォルト値: **Yes**
Name Resolution Domain From E-mail	デフォルト値: **Yes**
Clear Host Names Same as IP Addresses	デフォルト値: **Yes**
Limit Bandwidth To	ネットワーク上でのコネクターの出力を抑制する一連の帯域幅オプション (**Disabled**、1 kbit/sec～100 Mbits/sec)。
Transport Mode	受信したすべての処理済みイベントをディスクにキャッシュするようにコネクターを設定できます。これは、コネクターを一時停止するのと同等です。ただし、この設定を使用して、特定の期間イベント送信を遅らせることができます。たとえば、この設定を使用して日中にイベントをキャッシュし、夜間に送信することができます。また、業務時間内は非常に高い緊急度付きのものを除いてすべてのイベントをキャッシュし、残りを夜間に送信するようにコネクターを設定することもできます (**Normal** | Cache | Cache (but send Very High severity events))。
Address-based Zone Population Defaults Enabled	このフィールドは、v3.0のArcSightマネージャーに適用されます。ESM v3.5ではシステムにゾーンマッピングが不可欠なため、このフィールドは該当しません。デフォルト値: **Yes**
Address-based Zone Population	このフィールドは、v3.0のArcSightマネージャーに適用されます。ESM v3.5ではシステムにゾーンマッピングが不可欠なため、このフィールドは該当しません。
Customer URI	指定した顧客URIを、コネクターから受信するイベントに適用します。顧客リソースが存在する限り、すべての顧客フィールドがArcSightマネージャー上で設定されます。この特定のコネクターが、複数の顧客に適用される可能性があるデータを報告している場合は、このフィールドでVelocityテンプレートを使用し、それらの顧客を条件に応じて識別することができます。
Source Zone URI	コネクターのソースアドレスに関連付けられたゾーンのURIを示します (ESM v3.0との互換性を確保するのに必要)。
Source Translated Zone URI	コネクターの変換後のソースアドレスに関連付けられたゾーンのURIを示します。変換は、NATが想定されています (ESM v3.0との互換性を確保するのに必要)。
Destination Zone URI	コネクターの宛先アドレスに関連付けられたゾーンのURIを示します (ESM v3.0との互換性を確保するのに必要)。
Destination Translated Zone URI	コネクターの変換後の宛先アドレスに関連付けられたゾーンのURIを示します。変換は、NATが想定されています (ESM v3.0との互換性を確保するのに必要)。

パラメーター	説明
Connector Zone URI	コネクターのアドレスに関連付けられたゾーンのURIを示します (ESM v3.0との互換性を確保するのに必要)。
Connector Translated Zone URI	コネクターの変換後のアドレスに関連付けられたゾーンのURIを示します。変換は、NATが想定されています (ESM v3.0との互換性を確保するのに必要)。
Device Zone URI	デバイスのアドレスに関連付けられたゾーンのURIを示します (ESM v3.0との互換性を確保するのに必要)。
Device Translated Zone URI	デバイスの変換後のアドレスに関連付けられたゾーンのURIを示します。変換は、NATが想定されています (ESM v3.0との互換性を確保するのに必要)。
フィールドベースアグリゲーション	この機能は、基本的なコネクターアグリゲーションの拡張機能です。基本的なアグリゲーションは、2つのイベントのすべてのフィールドが同じ場合にのみ (唯一の違いは検出時刻) イベントを集約します。しかし、フィールドベースアグリゲーションは、より厳密でないアグリゲーションメカニズムを実装しており、選択したフィールドが両方のアラートで同じ場合にのみ2つのイベントが集約されます。フィールドベースアグリゲーションは、指定されたフィールドのみを含む新しいアラートを生成するため、残りのフィールドは無視されることに注意してください。 コネクターアグリゲーションは、受信データ量を大幅に減らし、イベントが提供される合計情報量よりも少ない情報を使用する場合にのみ適用します。たとえば、フィールドベースアグリゲーションを有効にして、ファイアウォールの「accepts」および「rejects」を集約することができますが、これは、ファイアウォールから提供されるすべての情報ではなく、これらのイベントの数に関心がある場合にのみ使用する必要があります。
Time Interval	コネクターが収集するイベントを集約するための基礎として使用する時間間隔を選択します (該当する場合)。これは、Event Thresholdと同時に使用できません (**Disabled**、1秒、5秒など、最大1時間)。
Event Threshold	コネクターが収集するイベントを集約するための基礎として使用するイベント数を選択します (該当する場合)。これは、アグリゲーションを実行できるイベントの最大数です。たとえば、選択した時間間隔内で150個のイベントが同じである (つまり、同じ選択したフィールドを含んでいる) ことが判明し、イベントしきい値として100を選択した場合、イベント数100のイベントとイベント数50のイベントの2つのイベントを受信することになります。このオプションは、Time Intervalと同時に使用できません (**Disabled**、10個のイベント、50個のイベントなど、最大10,000個のイベント)。
Field Names	コネクターが収集するイベントを集約するための基礎として使用する、1つ以上のフィールドを指定します (該当する場合)。結果は、監視対象のカンマ区切りのフィールドのリストになります。たとえば、「eventName,deviceHostName」を指定すると、イベント名とデバイスホスト名が同じイベントが集約されます。名前にはスペースを含めることができず、最初の文字は小文字にします。
Fields to Sum	コネクターが収集するイベントを集約するための基礎として使用する、1つ以上のフィールドを指定します (該当する場合)。
Preserve Common Fields	Yesを選択すると、各イベントの値が同じ場合に、集約後のイベントにフィールドが追加されます。デフォルトの**No**を選択すると、集約後のイベントでは、集約されていないフィールドが無視されます。

パラメーター	説明
フィルターアグリゲーション	フィルターアグリゲーションは、エージェントフィルターによって破棄されるイベントから集約されたイベントデータを取得するための手段です。フィルターで破棄されるイベントのみがフィルターアグリゲーションで考慮されます (すべてのイベントを参照するフィールドベースアグリゲーションとは違います)。 コネクターアグリゲーションは、受信データ量を大幅に減らし、イベントが提供される合計情報量よりも少ない情報を使用する場合にのみ適用します。
Time Interval	コネクターが収集するイベントを集約するための基礎として使用する時間間隔を選択します (該当する場合)。これは、Event Thresholdと同時に使用できません (**Disabled**、1秒、5秒など、最大1時間)。
Event Threshold	コネクターが収集するイベントを集約するための基礎として使用するイベント数を選択します (該当する場合)。これは、アグリゲーションを実行できるイベントの最大数です。たとえば、選択した時間間隔内で150個のイベントが同じである (つまり、同じ選択したフィールドを含んでいる) ことが判明し、イベントしきい値として100を選択した場合、イベント数100のイベントとイベント数50のイベントの2つのイベントを受信することになります。このオプションは、Time Intervalと同時に使用できません (**Disabled**、10個のイベント、50個のイベントなど、最大10,000個のイベント)。
Fields to Sum	(オプション) コネクターが収集するイベントを集約するための基礎として使用する、1つ以上のフィールドを選択します (該当する場合)。
処理	
Preserve Raw Event	デバイスによっては、生成されたアラートの一部としてrawイベントをキャプチャーできます。これが該当しない場合、ほとんどのコネクターは、ArcSightイベントを生成するために解析/処理されたシリアライズされたバージョンのデータストリームも生成できます。この機能を使用すると、コネクターは、このシリアライズされた「rawイベント」をフィールドとして維持できます。この機能はデフォルトで無効になっています。rawデータを使用すると、イベントサイズが増え、より多くのデータベース記憶領域が必要になるからです。この機能を無効にするには、**[Preserve Raw Event]**の設定を変更します。デフォルトは、[**いいえ**] です。[**はい**] を選択する場合、「ローイベント」のシリアル化された表現は通知先に送信され、ローイベントフィールドに保存されます。

パラメーター	説明
Turbo Mode	2つの「ターボ」(狭いデータ帯域幅)モードの1つを選択することで、コネクターを介したセンサーのイベント情報の転送を高速化できます。デフォルト転送モードは**Complete**と呼ばれ、追加データ(カスタム、ベンダー固有)を含め、デバイスから受信したすべてのデータを渡します。 **Complete**モードは、ArcSight ESM v3.xにおけるデータベースパフォーマンスの向上をすべて活用します。 最初のレベルのターボ高速化は**Faster**と呼ばれ、追加のデータのみを破棄し、他のすべての情報を維持します。**Fastest**モードでは、最高のスループットを達成するために、コアイベント属性を除くすべてのデータを破棄します。 企業でこれらのモードに適用される特定のイベント属性は、ArcSightマネージャーのセルフドキュメント化された`$ARCSIGHT_HOME/config/connector/agent.properties`ファイルで定義されます。これらのプロパティは各自のニーズに合わせて調整されている可能性があるため、このファイルで最終的なリストを参照してください。追加のデータをキャプチャーするために**Complete**モードで実行する必要があるのは、スキャナーコネクターのみです。 **注**: コネクターのターボモードは、そのイベントを処理しているArcSightマネージャーによって使用されるターボモードで上書きされます。たとえば、**Faster**に設定されたマネージャーは、デフォルトの**Complete**に設定されたコネクターにすべてのデータを渡さない可能性があります。

パラメーター	説明
Enable Aggregation (in seconds)	有効にすると、選択した時刻値に基づいて2つ以上のイベントを集約します (**Disabled**、1、2、3、4、5、10、30、60)。 アグリゲーションは、以下の固定されたフィールドのサブセットに対する1つ以上の一致に対して実行されます。 • エージェントID • 名前 • デバイスイベントカテゴリ • エージェントの緊急度 • 通知先アドレス • 通知先ユーザーID • 通知先ポート • リクエストURL • ソースアドレス • ソースユーザーID • ソースポート • 通知先プロセス名 • 転送プロトコル • アプリケーションプロトコル • デバイスインバウンドインターフェイス • デバイスアウトバウンドインターフェイス • 追加データ (存在する場合) • ベースイベントID (存在する場合) 集約されたイベントは、イベント数 (いくつのイベントが表示されたイベントに集約されたか) とイベントタイプを示します。集約されたイベントの残りのフィールドは、集約されたイベントのセットの中の最初のイベントの値をとります。
Limit Event Processing Rate	コネクターの処理レートを下げることで、そのCPU負荷を軽減することができます。これは、イベントバーストの影響に対処するための手段にもなります。 選択の範囲は、**Disabled** (CPU要求に対する制限なし) から**1 eps** (1秒間に1個のイベントのみを渡し、CPUに対する要求を最小にする) です。 注: このオプションの効果は、次のコネクター処理カテゴリの表に示すように、使用中のコネクターのカテゴリによって変わります。
Fields to Obfuscate	
Store Original Time in	**Disabled**またはFlex Date 1
Enable Port-Service Mapping	デフォルト値: **No**

パラメーター	説明
Enable User Name Splitting	デフォルト値: **No**
Split File Name into Path and Name	デフォルト値: **No**
Event Integrity Algorithm	**Disabled**、SHA-1、SHA-256、SHA-512、MD5
Generate Unparsed Events	デフォルト値: **No**
Preserve System Health Events	Yes、**No**、Disabled
Enable Device Status Monitoring (in minutes)	**Disabled**、1、2、3、4、5、10、30、60、120分
フィルター	
Filter Out	非該当
“Very High Severity” Event Definition	非該当
“High Severity” Event Definition	非該当
“Medium Severity” Event Definition	非該当
“Low Severity” Event Definition	非該当
“Unknown Severity” Event Definition	非該当
ペイロードサンプリング	(使用可能な場合)
Max. Length	Discard、128バイト、**256バイト**、512バイト、1キロバイト
Mask Non-Printable Characters	デフォルト値: **False**

付録C: 特別なコネクター設定

ArcSight Management Centerで使用する場合、一部のコネクターでは追加の設定が必要です。この付録では、追加の設定について説明します。コネクターのインストールに関する一般的な情報については、「コネクターの追加」(99ページ)を参照してください。

ここでは、以下の内容について説明します。

Microsoft Windows Event Log - Unifiedコネクター

SmartConnector for Microsoft Windows Event Log - Unifiedは、FIPS準拠のソリューションには含まれていません。Windows Event Log - Unifiedコネクターを追加する場合、コネクターでイベントを収集するためには、コンテナーでFIPSが有効でないことが必要です。

Windows Event Log - Unifiedコネクターを追加する場合は、SmartConnectorの構成ガイドの手順に従って、パラメーターの入力、SSL使用時のセキュリティ証明書の入力、監査ポリシーの有効化、および標準ユーザーアカウントのセットアップを行います。

現在、Microsoft Windows Event Log - Unified SmartConnectorに対応した、2つのパーサーバージョンが存在します。

- パーサーバージョン0は、SmartConnectorの各リリースで一般に利用可能です。
- パーサーバージョン1は、Microsoft Windows Monitoringコンテンツで利用可能です。

初期設定時に設定したMicrosoft Windows Event Log - Unified SmartConnectorは、パーサーバージョン1を使用します。

このパーサーバージョンの詳細なセキュリティイベントマッピングは、『Security Event Mappings: SmartConnectors for Microsoft Windows Event Log - Unified with Parser Version 1』(MSWindowsEventLogUnifiedMappingsParserVersion1.pdf) に記載されており、HPE ArcSightのProtect724から入手できます。

追加のMicrosoft Windows Event Log Unifiedコネクターをインストールする場合は、一般に利用可能なベースパーサーバージョン (パーサーバージョン0) を使用してインストールします。

ベースパーサーバージョンのマッピングは、SmartConnectorの各リリース(『Security Event Mappings: SmartConnectors for Microsoft Windows Event Log』)で利用でき、SmartConnectorの構成ガイドと共に、Protect724で入手できます。デフォルトのWindows Monitoringコンテンツを使用する場合は、パーサーバージョン1を使用する必要があります。詳細については、『SmartConnector Configuration Guide for Microsoft Windows Event Log - Unified』または『SmartConnector Configuration Guide for Microsoft Windows Security Events - Mappings』を参照してください。

注: First Boot Wizardを使用してインストールされる事前にバンドル済みのSmartConnector for Microsoft Windows Event Log - Unifiedは、パーサーバージョン1を使用してインストールされます。コネクター設定ウィザードを使用してWindows Event Log - Unifiedコネクターを追加する場合、これらのコネクターはパーサーバージョン0 (ベースパーサー) を使用してインストールされます。

コンテナープロパティの更新によるパーサーバージョンの変更

パーサーは、デバイスのrawイベントに含まれる情報を解析する方法、およびその情報をHPE ArcSightのセキュリティイベントスキーマフィールドにマッピングする方法を指定するSmartConnectorコンポーネントです。パーサーは、プロパティファイル、マップファイル、またはCSVファイルの形で用いられます。各SmartConnectorには、1つまたは複数の独自のパーサーが存在します。

複数のパーサーバージョンにより、各SmartConnectorでrawイベントを異なる複数の方法で解析し、適切なマッピングでArcSightのセキュリティイベントを生成することが可能になります。SmartConnector for Microsoft Windows Event Log -- Unifiedは、ベースパーサーとパーサーバージョン1の2つのパーサーバージョンをサポートしています。

複数のパーサーバージョンに対応している場合:

- 1つのSmartConnectorビルドで複数のパーサーバージョンがサポートされます。
- ユーザーは、それぞれのイベントマッピング要件に応じてコネクターを設定することで、利用可能なパーサーバージョンを任意に使用できます。
- ユーザーは、必要に応じて適切なパーサーバージョンを使用するように、コネクターを再設定できます。

複数のパーサーバージョンは、現在、SmartConnector for Microsoft Windows Event Log -- Unifiedでのみサポートされています。この機能は、ユーザーが開発したArcSightのFlexConnectorではサポートされません。

各SmartConnectorには、現在のパーサーバージョンを表す個別の`fcp.version`内部パラメーター設定が含まれています。fcp.versionパラメーターのデフォルト値は、ベース(デフォルト)パーサーバージョンであるパーサーバージョン0です。各SmartConnectorは、合計8つのパーサーバージョンをサポートできます。`fcp.version`パラメーターの値の範囲は0～7です。

Microsoft Windows Unified SmartConnectorは、パーサーバージョン0および1をサポートしています。

マッピングの異なるコンテンツを使用する場合は、コンテンツに合わせてパーサーバージョンを変更する必要があります。

(agent.propertiesファイル内にある) コンテナープロパティを更新して、イベントのマッピング時に使用するパーサーバージョンを変更するには

1. 上部のメニューバーから **[Manage]** をクリックします。
2. ナビゲーションパスを選択します。
3. プロパティを更新するコンテナーを選択します。複数のコンテナーを選択できます。
4. **[Properties]**をクリックします。
5. ウィザードの指示に従ってコネクタープロパティを更新します。

   `fcp.version`パラメーター値0は、ベースパーサーを表します。パーサー1を使用するには、`fcp.version`パラメーターの値を1に変更します。次に例を示します。

   ```
   agents[0].fcp.version=1
   ```

SSL認証

SSLを接続プロトコルとして使用する場合は、Windowsドメインコントローラーサービスと Active Directoryサーバーの両方に対するセキュリティ証明書を追加する必要があります。ドメインコントローラーに有効な証明書をインストールすると、LDAPサービスで、LDAPとグローバルカタログトラフィックの両方のSSL接続をリスンし、自動的に受け入れることが可能になります。First Boot Wizardによるコネクターのインストールを使用する場合、証明書はすでにインポートされています。Windows Event Log - Unifiedコネクターを追加する場合は、『SmartConnector Configuration Guide for Microsoft Windows Event Log - Unified』の手順を参照してください。

データベースコネクター

次のデータベースコネクターは、ArcSight Expressを使用したインストール環境で使用できます。

- IBM SiteProtector DB*
- McAfee ePolicy Orchestrator DB*
- McAfee Vulnerability Manager DB*
- McAfee Network Security Manager DB*
- Microsoft SQL Server Audit Multiple Instance DB*
- Oracle Audit DB
- Symantec Endpoint Protection DB*

- Trend Micro Control Manager NG DB*
- Snort DB*

*これらのコネクターは、SQL ServerまたはMySQLのデータベースからイベントを抽出するため、JDBCドライバーが必要です。手順については「JDBCドライバーの追加」(310ページ)を参照してください。

これらのデータベースコネクターはいずれも、ArcSight Expressへの追加時に次の情報が必要です。また、一部のコネクターでは、イベントタイプやポーリング頻度などのパラメーターも必要になります。

パラメーター	説明
Database JDBC Driver	ODBCドライバーを使用する場合は、'sun.jdbc.odbc.JdbcOdbcDriver'ドライバーを選択します。JDBCドライバーの場合は、'com.microsoft.sqlserver.jdbc.SQLServerDriver'ドライバーを選択します。ODBCドライバーを使用する場合は、'sun.jdbc.odbc.JdbcOdbcDriver'ドライバーを選択します。JDBCドライバーの場合は、'com.microsoft.sqlserver.jdbc.SQLServerDriver'ドライバーを選択します。
Database URL	ODBCドライバーを使用する場合は、'jdbc:odbc:<ODBCデータソース名>'と入力します。ここで、<ODBCデータソース名>は、作成したODBCデータソースの名前です。JDBCドライバーを使用する場合は、'jdbc:sqlserver://<MS SQL Serverホスト名またはIPアドレス>:1433;DatabaseName=<MS SQL Serverデータベース名>'と入力します。<MS SQL Serverホスト名またはIPアドレス>および<MS SQL Serverデータベース名>は実際の値に置き換えます。
Database User	適切な権限を持つデータベースユーザーのログイン名を入力します。
Database Password	SiteProtectorデータベースユーザーのパスワードを入力します。

JDBCドライバーの追加

IBM SiteProtector DB、McAfee ePolicy Orchestrator DB、McAfee Vulnerability Manager DB、McAfee Network Security Manager DB、Microsoft SQL Server Audit Multiple Instance DB、Symantec Endpoint Protection DB、およびTrend Micro Control Manager NG DBコネクターは、SQL Serverデータベースからイベントを抽出します。MS SQL Server JDBCドライバーに関する情報およびダウンロード方法については、MicrosoftのWebサイトを参照してください。

注: SQL Serverデータベースのバージョンごとに異なるバージョンのJDBCドライバーが必要です。必ず使用しているデータベースのバージョンに対応した正しいドライバーを使用してください。JDBCドライバーのバージョンによっては、jarファイルの名前が異なる場合があります。

Snort DB用のSmartConnectorは、MySQLデータベースからイベントを抽出します。

JDBCドライバーをダウンロードして展開した後、次のようにして、ドライバーをリポジトリにアップロードし、該当する1つまたは複数のコンテナーに適用します。

1. ArcSight Expressから、**[Setup] > [Repositories]** を選択します。
2. 左側のペインから [**JDBC Drivers**] を選択し、[**JDBC Drivers**] タブをクリックします。
3. [**Upload to Repository**] をクリックします。
4. **Repository File Creationウィザード**で、[**Individual Files**] を選択してから、[**Next**] をクリックします。
5. デフォルトの選択内容を保持して、[**Next**] をクリックします。
6. [**Upload**] をクリックし、ダウンロードした.jarファイルを見つけて選択します。
7. [**Submit**] をクリックして指定したファイルをリポジトリに追加し、[**Next**] をクリックして次に進みます。
8. 必要なすべてのファイルを追加し、[**Next**] をクリックします。
9. [**Name**] フィールドに、zipファイルのわかりやすい名前を入力します (たとえば、`JDBCdriver`)。[**Next**] をクリックします。
10. [**Done**] をクリックして処理を完了します。新しく追加されたファイルが、[**Add Connector JDBC Driver File**] の下の [**Name**] フィールドに表示されます。
11. ドライバーファイルを適用するには、ドライバーの`.zip`ファイルを選択し、上向き矢印をクリックして、**Upload Container Files**ウィザードを起動します。[**Next**] をクリックします。
12. ドライバーをアップロードする1つまたは複数のコンテナーを選択し、[**Next**] をクリックします。
13. [**Done**] をクリックして、プロセスを完了します。

ArcSight Expressでサポートされている各データベースコネクター用の構成ガイドは、Protect 724コミュニティで入手できます。以下に示すアプリケーションのセットアップ情報とマッピングが記載された個別の構成ガイドは、Protect 724で入手できます。

- IBM SiteProtector DB
- McAfee ePolicy Orchestrator DB
- McAfee Vulnerability Manager DB (従来のFoundScan)
- McAfee Network Security Manager DB
- Microsoft SQL Server Multiple Instance Audit DB
- Oracle Audit DB
- Symantec Endpoint Protection DB
- Trend Micro Control Manager DB
- Snort DB

APIコネクター

次のAPIコネクターは、ArcSight Expressを使用したインストール環境で使用できます。これらのAPIコネクターでは、クライアントと認証の資格情報が必要です。また、デバイスからコネクターに送信されるイベントタイプを設定する必要があります。

- Cisco Secure IPS SDEE
- Sourcefire Defense Center eStreamer

Cisco Secure IPS SDEEの場合、SmartConnectorでCisco IPSセンサーの認証証明書を検証するには、IPSセンサーから認証証明書を取得して、アプライアンスにインポートする必要があります。

Sourcefire Defense Center eStreamerの場合は、eStreamerクライアントを追加し、認証証明書を作成して、コネクターに送信するイベントタイプを選択します。

手順については、各コネクターの個別の構成ガイドを参照してください。

『Connector Management for ArcSight Express 4.0 User's Guide』の「Uploading Certificates to the Repository」の手順に従って、信頼済みの証明書をArcSight Expressにインポートします。

ArcSight Expressでサポートされ ているAPIコネクターの構成ガイドは、Protect 724コミュニティで入手できます。以下に示すアプリケーションのセットアップ情報とマッピングが記載された個別の構成ガイドは、Protect 724で入手できます。

- Cisco Secure IPS SDEE
- Sourcefire Defense Center eStreamer

ファイルコネクター

ファイルベースのコネクターは、NFS (Network File System) またはCIFS (Common Internet File System) を使用します。

次のファイルコネクターは、ArcSight Expressを使用したインストール環境で使用できます。

- Blue Coat Proxy SG Multiple Server File

Blue Coat Proxy SG Multiple Server Fileに対するSmartConnectorのデバイスセットアップ、パラメーター設定、およびマッピング情報については、構成ガイドを参照してください。

ファイルベースのコネクターは、NFS (Network File System) またはCIFS (Common Internet File System) を使用します。Windowsシステム上のファイルベースのコネクターの場合は、コネクターを追加する前にCIFS共有を設定します。

CIFSマウントまたはNFSマウントの作成については、『Connector Management for ArcSight Express 4.0 User's Guide』の「Managing a Remote File System」を参照してください。

Syslogコネクター

First Boot Wizardによる初期インストール時にSyslog Daemonを選択した場合、Syslog Daemonコネクターはすでにインストールされています。

新しいコンテナーには、Syslog File、Syslog Pipe、またはSyslog Daemonコネクターを追加できます。以下のデバイスのSyslogコネクターは、ArcSight Expressで使用できます。

- Cisco PIX/ASA Syslog
- Cisco IOS Router Syslog
- Juniper Network and Security Manager Syslog
- Juniper JUNOS Syslog
- UNIX OS Syslog

syslogイベントを送信するようにデバイスをセットアップしてください。デバイスの設定については、デバイスのドキュメントまたはSmartConnectorの構成ガイドを参照してください。このガイドには、ArcSightのイベントフィールドへの特定のデバイスのマッピングや、PipeまたはFileコネクターをインストールする場合の設定に必要な追加情報も記載されています。
『SmartConnector for UNIX OS Syslog Configuration Guide』のマッピングは、すべてのSyslogコネクターに適用されます。デバイスごとのマッピングは、デバイスの構成ガイドに記載されています。

ArcSight Expressでサポートされている次のSyslogコネクターの構成ガイドは、Protect 724コミュニティで入手できます。

- Cisco PIX/ASA Syslog
- Cisco IOS Syslog
- Juniper JUNOS Syslog
- Juniper Network and Security Manager Syslog
- UNIX OS Syslog

付録D: ArcSight Management Centerアプライアンスのセットアップ

この付録では、初めて使用する場合のArcSight Management Centerアプライアンスのセットアップ手順について説明します。

準備

ArcSight Management Centerアプライアンスを初めて使用する場合は、以下の準備を行います。

1. アプライアンスと付属のアクセサリを梱包から取り出します。
2. アプライアンスに同梱されている指示、使用上の注意および警告をよく確認します。確認しないと、人身傷害やアプライアンスの故障の原因となる可能性があります。
3. 同梱されているラック取り付け手順をなくさないように取っておきます。
4. ドキュメント『Hewlett Packard Enterpise Entitlement Certificate』の手順に従い、管理アプライアンスのライセンスキーを取得します。このキーは、管理アプライアンスの機能にアクセスする際に必要です。
5. HPE ArcSightのユーザーコミュニティであるProtect 724にアカウントを登録します。このアカウントは、HPE ArcSight製品のドキュメントやその他のコミュニティベースのリソースにアクセスする際に必要になります。
6. ラック取り付け手順 (アプライアンスに同梱) に従い、アプライアンスをラックにしっかりと取り付けて、背面パネルの接続を行います。
7. 次のいずれかの方法で、アプライアンスへのローカルアクセスが利用できるようにします。
   - キーボード、モニター、マウスをアプライアンスのポートに接続します。
   - DB-9コネクター付きのヌルモデムケーブルを使用して、アプライアンスのシリアルポートにターミナルを接続します。このシリアルポートには、標準のVT100互換のターミナルが必要です。設定は9600 bps、8ビット、パリティなし、1ストップビット (8N1)、フロー制御なしとします。
8. アプライアンスの電源をオンにします。
9. 必要に応じて、アプライアンスでアウトオブバンドリモートアクセスが利用できるようにします。http://www.hpe.com/go/iLOから『HPE ProLiant Integrated Lights-Outユーザーガイド』をダウンロードして、手順を確認してください。

準備ができたら、アプライアンスのセットアップを開始します。

セットアップ

アプライアンスのセットアップでは、以下の手順を実行します。

1. CLIでアプライアンス用に新規のIPアドレスを設定します。
2. エンドユーザーライセンス契約に同意し、アプライアンスにログインします。
3. ArcSight Management Centerアプライアンスを初期設定します。

以下では、各ステップの内容について詳しく説明します。

新規IPアドレスを設定する

アプライアンスのコマンドラインインターフェイス (CLI) を使用して、新規のIPアドレスを設定します。ArcSight Management Centerアプライアンスは、Eth0にデフォルトIPアドレス 192.168.35.35 (サブネットマスク255.255.255.0) が設定された状態で出荷されます。また、デフォルトゲートウェイ、ホスト名、DNSサーバー、およびNTPサーバーを指定する必要があります。

作業を始める前に、以下の情報を用意しておく必要があります。

- 新規のIPアドレス (およびプレフィックスまたはサブネットマスク)。
- デフォルトゲートウェイのアドレス。
- 完全修飾ドメイン名。
- DNS解決用の1つ以上の名前検索ドメインとサーバーアドレス。
- 1つ以上のNTPサーバーアドレス。

CLIで新規IPアドレスを設定するには

1. CLIで、次のデフォルトの資格情報を使用して、アプライアンスに接続します。

```
Login:admin
Password:password
```

2. 次のいずれかのコマンドを使用して、新規のIPアドレスを設定します。

- `set ip eth0 <ip>/<prefix>`、ここで、`<ip>`は新規のIPアドレスで、`<prefix>`はお使いのプレフィックスです。 または、
- `set ip eth0 <ip> <subnetmask>`、ここで、`<ip>`は新規のIPアドレスで、`<subnetmask>`はお使いのサブネットマスクです。

3. `set defaultgw <address>`と入力します。`<address>`は、お使いのデフォルトゲートウェイのIPアドレスに置き換えます。

4. set hostname <FQDN>と入力します。<FQDN>は、ホストの完全修飾ドメイン名に置き換えます。
5. set dns <search_domain_1>, <search_domain_2>...<search_domain_N> <nameserver1> <nameserver2>...<nameserver_N>と入力します。<search_domain_N>はそれぞれ検索ドメインに置き換え、<nameserver_N>はそれぞれDNSで使用するネームサーバーのIPアドレスに置き換えます。
6. set <ntp_server_1> <ntp_server_2>...<ntp_server_N>と入力します。<ntp_server_N>はそれぞれアプライアンスの時刻を設定するためのNTPサーバーのIPアドレスに置き換えます。
7. show configと入力して、設定内容を確認します。正しくない設定内容がある場合は、前のステップの説明に従って設定を修正します。

続いて、エンドユーザーライセンス契約に同意します。

エンドユーザーライセンス契約に同意する

ブラウザー経由でアプライアンスに初めて接続すると、エンドユーザーライセンス契約 (EULA) に同意するかどうかを確認するプロンプトが表示されます。

EULAに同意するには

1. ブラウザーで、https://<IP>のArcSight Management Centerアプライアンスに接続します。ここで、<IP>は先ほど設定した新規のIPアドレスです。
2. ライセンスの内容を確認します。
3. [**I accept the terms of the License Agreement**] チェックボックスを選択し、[**Accept**] をクリックします。
4. 次のデフォルトの資格情報を使用して、管理者としてログインします。

Login:admin

Password:password

続いて、アプライアンスを初期設定します。

ArcSight Management Centerアプライアンスを初期設定する

続いて、アプライアンスを初期設定するため、ライセンスファイルをアップロードします。また、必要に応じて、日付と時刻を設定し、管理者ログインの資格情報をデフォルト以外の値に変更します。

アプライアンスを初期設定するには

1. [**ArcSight Management Center Appliance Configuration**] ページの [**License**] フィールドで、現在のライセンスを参照してアップロードします。
2. [**Save**] をクリックします。
3. アプライアンスの日付と時刻を設定します。
4. 管理者ログインの資格情報をデフォルト値から変更します。「パスワードの変更」(280 ページ) の説明を参照してください。

これで、ArcSight Management Centerアプライアンスを使用する準備が整いました。

付録E: 工場出荷時設定の復元

概要

アプライアンスに内蔵されたユーティリティを使用して、ArcSight Management Centerを工場出荷時設定に復元することができます。復元は、最新モデルのArcSight Management Centerに加えて、ArcSight Management Centerに移行済みの従来のコネクターアプライアンスにも適用されます。

ArcSight Management Centerアプライアンスを工場出荷時設定に戻すと、すべての設定内容が完全に削除されます。工場出荷時設定への復元を行う際には、前もって設定内容をバックアップしておいてください。

工場出荷時設定への復元に使用するユーティリティ(および復元後のアプライアンスイメージ)は、復元を行うアプライアンスのタイプによって異なります。以下の表を参照して、使用するユーティリティを確認してください。

アプライアンスモデル	システム復元ユーティリティ	復元後のアプライアンスイメージ
C6600	HPE System Restore	ArcSight Management Center
すべてのCX500 (C6500を含む)	HPE System Restore	ArcSight Management Center
CX400 (RHEL 5.x、移行前)	HPE System Restore	ArcSight Management Center
CX400 (RHEL 6.x、移行前)	Acronis True Image	コネクターアプライアンス

HPE System Restoreを使用した工場出荷時設定の復元

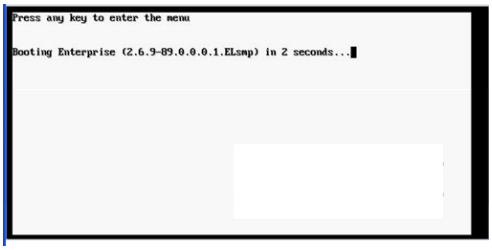
HPE System Restoreを使用して復元したアプライアンスは、ArcSight Management Centerのイメージになります。

HPE System Restoreを使用して工場出荷時設定を復元するには

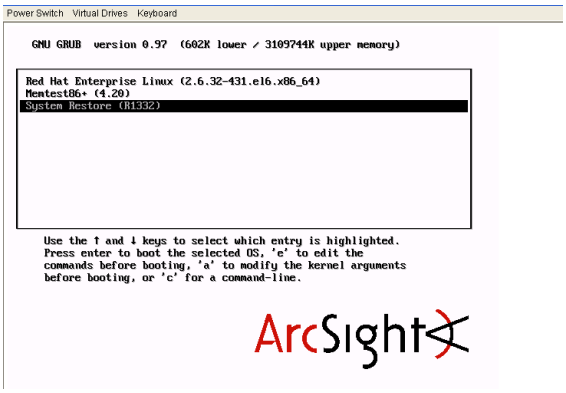
1. アプライアンスのIPアドレス、デフォルトゲートウェイ、およびサブスクライブをメモします。
2. キーボード、モニター、マウスをアプライアンスに直接接続します。

3. GUIからArcSight Management Centerをリブートします。[**Setup**] > [**System Admin**] > [**Reboot**] をクリックしてから、[**Start Reboot Now**] ボタンをクリックします。コマンドラインインターフェイスを使用してリブートすることもできます。
4. 以下の画面が表示されたら、キーボードの任意のキーを押します。

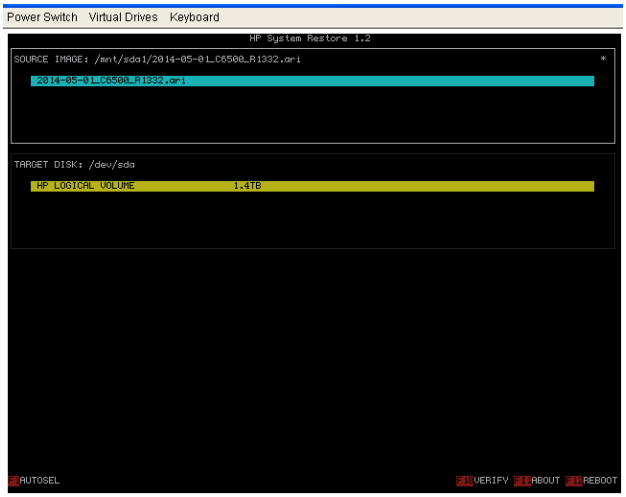
   注: この画面は、非常に短時間しか表示されません。キーボードのキーを素早く押してください。そうしないと、アプライアンスは通常の起動を続行します。



5. 下に示すような画面が、接続したモニター上に表示されます。マウスまたは矢印キーを使用して**[System Restore]**を選択し、**Enter**を押します。HPE System Restoreユーティリティが起動します。



6. **F1 (自動選択)** キーを押します。



7. **F2**キーを押して、アプライアンスを**復元**します。

8. [**Proceed with restore?**] というプロンプトが表示されたら、**y**を押します。復元が開始されます。
9. 復元ユーティリティの手順に沿ってプロセスを完了します。
10. 完了したら、**Enter**キーを押します。
11. **F12**キーを押して、アプライアンスをリブートします。
12. [**Reboot appliance?**] というプロンプトが表示されたら、**y**を押します。アプライアンスがリブートします。

復元が完了すると、工場出荷時設定に復元されたArcSight Management Centerになります。

使用する場合は、復元を行う前にメモしたIPアドレス、デフォルトゲートウェイ、およびネットマスクを使用して、アプライアンスを設定する必要があります。設定の手順については、HPE ArcSightのオンラインコミュニティであるProtect724から入手可能なドキュメント『Getting Started with ArcSight Management Center Appliance』を参照してください。

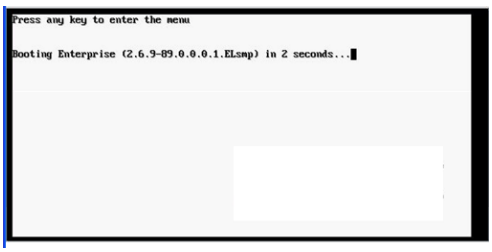
Acronis True Imageを使用した工場出荷時設定の復元

Acronis True Imageを使用して復元したアプライアンスは、コネクターアプライアンスのイメージに復元されます。

Acronis True Imageを使用して工場出荷時設定に復元するには

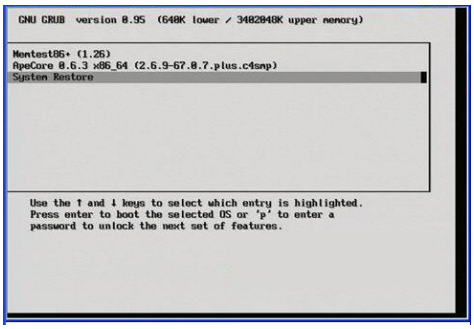
1. アプライアンスのIPアドレス、デフォルトゲートウェイ、およびサブスクライブをメモします。
2. キーボード、モニター、マウスをアプライアンスに直接接続します。
3. GUIからArcSight Management Centerをリブートします。[**Setup**] > [**System Admin**] > [**Reboot**] をクリックしてから、[**Start Reboot Now**] ボタンをクリックします。コマンドラインインターフェイスを使用してリブートすることもできます。
4. 以下の画面が表示されたら、キーボードの任意のキーを押します。

   注: この画面は、非常に短時間しか表示されません。キーボードのキーを素早く押してください。そうしないと、アプライアンスは通常の起動を続行します。



5. 下に示すような画面が、接続したモニター上に表示されます。マウスまたは矢印キーを

使用して [**System Restore**] を選択し、Enterを押します。



6. [**Acronis True Image Server**] をクリックして続行します。
7. [**Acronis True Image Echo Server**] ダイアログボックスで、[**Pick a Task**] リストから [**Recovery**] を選択し、Enterを押します。
8. Restore Data Wizardが起動したら、[**Next**] をクリックして続行します。
9. **[Backup Archive Selection]**ページで**[Acronis Secure Zone]**を選択し、**[Next]**をクリックします。
10. **[Restoration Type Selection]**ページで**[Restore disks or partitions]**を選択し、**[Next]**をクリックします。
11. **[Partition or Disk to Restore]**ページで、**cciss/c0d0**または**sda** (アプライアンスモデルによって異なります) というラベルが付けられたドライブ全体を選択し、**[Next]**をクリックします。
12. **[NT Signature selection for image restoration]**ページで、復元したディスクからのNTシグネチャーを処理する方法を選択し、**[Next]**をクリックします。
13. **[Restored Hard disk Location]**ページで、復元するドライブ (**cciss/c0d0**または**sda**) を選択し、**[Next]**をクリックします。
14. **[Non-empty Destination Hard Disk Drive]**ページで、**[Yes, I want to delete all partitions on the destination hard disk drive before restoring]**を選択し、**[Next]**をクリックします。
15. **[Next Selection]**ページで**[No, I do not]**を選択し、**[Next]**をクリックします (復元する他のパーティションやディスクはありません)。
16. アプライアンスをリセットする前にアーカイブを検証する場合は、**[Restoration Options]** ページで、**[Validate backup archive for the data restoration process]** を選択します。アプライアンスを自動的に再起動するには**[Reboot the computer automatically after the restoration is finished]**を選択します。**[Next]**をクリックします。
17. 実行する操作のチェックリストを確認し、**[Proceed]**をクリックしてファクトリーリセットを開始します。前のページに戻るには**[Back]**をクリックします。

注意: リセット処理の間は、ArcSight Management Centerを中断したり、電源をオフにしないでください。リセット処理を中断すると、システムが回復不能な状態に陥る可能性があります。

進行状況バーに現在の処理のステータスと全体の進行状況が表示されます。

18. データが正常に復元されたことを示すメッセージが表示されたら、**[OK]**をクリックします。
19. 自動的な再起動を以前に指定した場合、リセットが完了するとアプライアンスが再起動します。自動的な再起動を指定しなかった場合は、手動で再起動します。

復元が完了すると、工場出荷時設定に復元されたコネクターアプライアンスになります。

使用する場合は、復元を行う前にメモしたIPアドレス、デフォルトゲートウェイ、およびネットマスクを使用して、アプライアンスを設定する必要があります。設定の手順については、HPE ArcSightのオンラインソフトウェアコミュニティであるProtect724から入手可能なドキュメント『Getting Started with Connector Appliance』を参照してください。

付 録F: スーパースキーマ

以 下 は、Event BrokerのCEF-to-Avro (c2a) ストリームプロセッサーで使 用 されるスーパースキーマで構 成 されています。

フィールド名	データ型	長さ
agentAddress	VARCHAR	16
agentDnsDomain	VARCHAR	255
agentHostName	VARCHAR	1023
agentId	VARCHAR	40
agentMacAddress	VARCHAR	デフォルトを定 義
agentReceiptTime	DATE	
agentSeverity	VARCHAR	デフォルトを定 義
agentTimeZone	VARCHAR	255
agentTranslatedAddress	VARCHAR	デフォルトを定 義
agentTranslatedZoneURI	VARCHAR	2048
agentType	VARCHAR	63
agentVersion	VARCHAR	31
agentZoneURI	VARCHAR	2048
applicationProtocol	VARCHAR	40
baseEventCount	INT	
bytesIn	Long	
bytesOut	Long	
categoryDeviceGroup	VARCHAR	1023
categoryDeviceType	VARCHAR	1023
categoryObject	VARCHAR	1023
categoryOutcome	VARCHAR	1023
categorySignificance	VARCHAR	1023
categoryTechnique	VARCHAR	1023
cryptoSignature	VARCHAR	512
customerURI	VARCHAR	2048

フィールド名	データ型	長さ
destinationAddress	VARCHAR	16
destinationDnsDomain	VARCHAR	255
destinationGeoLocationInfo	VARCHAR	1023
destinationHostName	VARCHAR	1023
destinationMacAddress	VARCHAR	デフォルトを定義
destinationNtDomain	VARCHAR	255
destinationPort	INT	
destinationProcessId	INT	
destinationProcessName	VARCHAR	1023
destinationServiceName	VARCHAR	1023
destinationTranslatedAddress	VARCHAR	16
destinationTranslatedPort	INT	
destinationTranslatedZoneURI	VARCHAR	2048
destinationUserId	VARCHAR	1023
destinationUserName	VARCHAR	1023
destinationUserPrivileges	VARCHAR	1023
destinationZoneURI	VARCHAR	2048
deviceAction	VARCHAR	63
deviceAddress	VARCHAR	16
deviceAssetId	VARCHAR	デフォルトを定義
deviceCustomDate1	DATE	
deviceCustomDate1Label	VARCHAR	1023
deviceCustomDate2	DATE	
deviceCustomDate2Label	VARCHAR	1023
deviceCustomDescriptorId	VARCHAR	デフォルトを定義
deviceCustomFloatingPoint1	FLOAT	
deviceCustomFloatingPoint1Label	VARCHAR	1023
deviceCustomFloatingPoint2	FLOAT	
deviceCustomFloatingPoint2Label	VARCHAR	1023
deviceCustomFloatingPoint3	FLOAT	

フィールド名	データ型	長さ
deviceCustomFloatingPoint3Label	VARCHAR	1023
deviceCustomFloatingPoint4	FLOAT	
deviceCustomFloatingPoint4Label	VARCHAR	1023
deviceCustomIPv6Address1	VARCHAR	デフォルトを定義
deviceCustomIPv6Address1Label	VARCHAR	1023
deviceCustomIPv6Address2	VARCHAR	デフォルトを定義
deviceCustomIPv6Address2Label	VARCHAR	1023
deviceCustomIPv6Address3	VARCHAR	デフォルトを定義
deviceCustomIPv6Address3Label	VARCHAR	1023
deviceCustomIPv6Address4	VARCHAR	デフォルトを定義
deviceCustomIPv6Address4Label	VARCHAR	1023
deviceCustomNumber1	LONG VARCHAR	
deviceCustomNumber1Label	VARCHAR	1023
deviceCustomNumber2	LONG VARCHAR	
deviceCustomNumber2Label	VARCHAR	1023
deviceCustomNumber3	LONG VARCHAR	
deviceCustomNumber3Label	VARCHAR	1023
deviceCustomString1	VARCHAR	4000
deviceCustomString1Label	VARCHAR	1023
deviceCustomString2	VARCHAR	4000
deviceCustomString2Label	VARCHAR	1023
deviceCustomString3	VARCHAR	4000
deviceCustomString3Label	VARCHAR	1023
deviceCustomString4	VARCHAR	4000
deviceCustomString4Label	VARCHAR	1023
deviceCustomString5	VARCHAR	4000
deviceCustomString5Label	VARCHAR	1023
deviceCustomString6	VARCHAR	4000
deviceCustomString6Label	VARCHAR	1023
deviceDirection	VARCHAR	デフォルトを定義

フィールド名	データ型	長さ
deviceDnsDomain	VARCHAR	255
deviceDomain	VARCHAR	1023
deviceEventCategory	VARCHAR	1023
deviceEventClassId	VARCHAR	100
deviceExternalId	VARCHAR	255
deviceFacility	VARCHAR	1023
deviceHostName	VARCHAR	100
deviceInboundInterface	VARCHAR	128
deviceMacAddress	VARCHAR	デフォルトを定義
deviceNtDomain	VARCHAR	255
deviceOutboundInterface	VARCHAR	128
devicePayloadId	VARCHAR	128
deviceProcessId	INT	
deviceProcessName	VARCHAR	1023
deviceProduct	VARCHAR	100
deviceReceiptTime	DATE	
deviceSeverity	VARCHAR	63
deviceTimeZone	VARCHAR	255
deviceTranslatedAddress	VARCHAR	デフォルトを定義
deviceTranslatedZoneURI	VARCHAR	2048
deviceVendor	VARCHAR	100
deviceVersion	VARCHAR	16
deviceZoneURI	VARCHAR	2048
endTime	VARCHAR	デフォルトを定義
eventId	Long	デフォルトを定義
eventOutcome	VARCHAR	63
externalId	VARCHAR	40
fileCreateTime	DATE	
fileHash	VARCHAR	255
fileId	VARCHAR	1023

フィールド名	データ型	長さ
fileModificationTime	DATE	
fileName	VARCHAR	1023
filePath	VARCHAR	1023
version		
filePermission	VARCHAR	1023
fileSize	LONG	
fileType	VARCHAR	1023
flexDate1	DATE	
flexDate1Label	VARCHAR	128
flexNumber1	LONG	
flexNumber1Label	VARCHAR	128
flexNumber2	LONG	
flexNumber2Label	VARCHAR	128
flexString1	VARCHAR	1023
flexString1Label	VARCHAR	128
flexString2	VARCHAR	1023
flexString2Label	VARCHAR	128
locality	VARCHAR	デフォルトを定義
message	VARCHAR	1023
name	VARCHAR	デフォルトを定義
oldFileCreateTime	DATE	
oldFileHash	VARCHAR	255
oldFileId	VARCHAR	1023
oldFileModificationTime	DATE	
oldFileName	VARCHAR	1023
oldFilePath	VARCHAR	1023
oldFilePermission	VARCHAR	1023
oldFileSize	LONG	
oldFileType	VARCHAR	1023
rawEvent	VARCHAR	4000

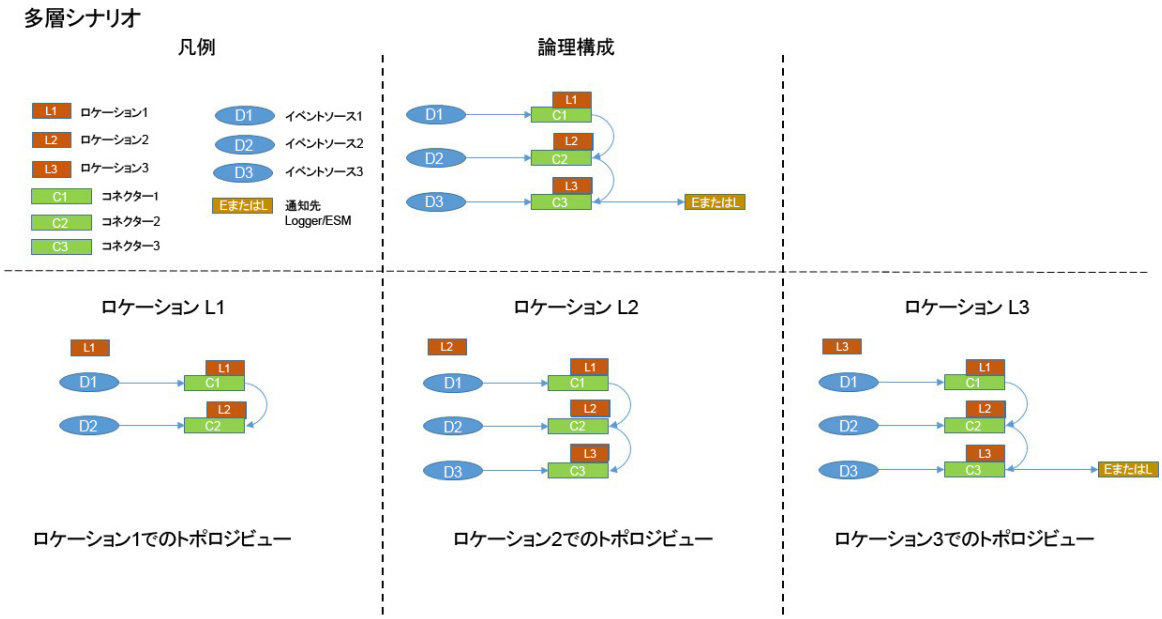
フィールド名	データ型	長さ
reason	VARCHAR	1023
requestClientApplication	VARCHAR	1023
requestContext	VARCHAR	2048
requestCookies	VARCHAR	1023
requestMethod	VARCHAR	1023
requestUrl	VARCHAR	1023
requestUrlFileName	VARCHAR	1023
requestUrlQuery	VARCHAR	1023
severity	INT	
sourceAddress	VARCHAR	デフォルトを定義
sourceDnsDomain	VARCHAR	255
sourceGeoLocationInfo	VARCHAR	1023
sourceHostName	VARCHAR	1023
sourceMacAddress	VARCHAR	デフォルトを定義
sourceNtDomain	VARCHAR	255
sourcePort	INT	
sourceProcessId	INT	
sourceProcessName	VARCHAR	1023
sourceServiceName	VARCHAR	1023
sourceTranslatedAddress	VARCHAR	デフォルトを定義
sourceTranslatedPort	INT	
sourceTranslatedZoneURI	VARCHAR	2048
sourceUserId	VARCHAR	1023
sourceUserName	VARCHAR	1023
sourceUserPrivileges	VARCHAR	1023
sourceZoneURI	VARCHAR	2048
startTime	DATE	
transportProtocol	VARCHAR	31
type	VARCHAR	デフォルトを定義

付 録 G: トポロジビューと管 理 対 象 でない デバイス

ここでは、ArcMCで管 理されていないデバイスがネットワーク内 に存 在 する場 合 のさまざまなシナリオと、ArcMCのトポロジビューへの影 響 について説 明します。特 に、コネクターが多 層 構 成 でチェーン接 続されている場 合 には、管 理 対 象 でない製 品 によって、隣 接 する下 位 階 層 からのビューがブロックされることがあります。

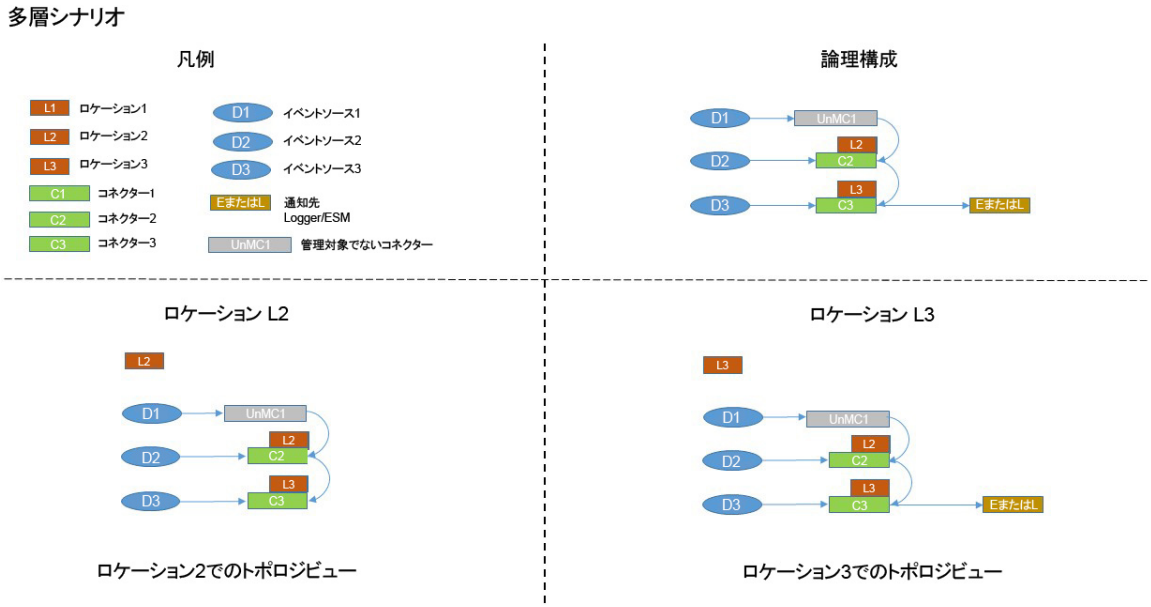
シナリオ1: 管 理 対 象 でないデバイスが存 在 しない

このシナリオでは、ネットワーク内 に管 理 対 象 でない製 品 が存 在 しません。そのため、ArcMCのトポロジビューが制 限 されることはなく、任 意 のロケーションから見 た論 理トポロジが正 確 に表 現されます。



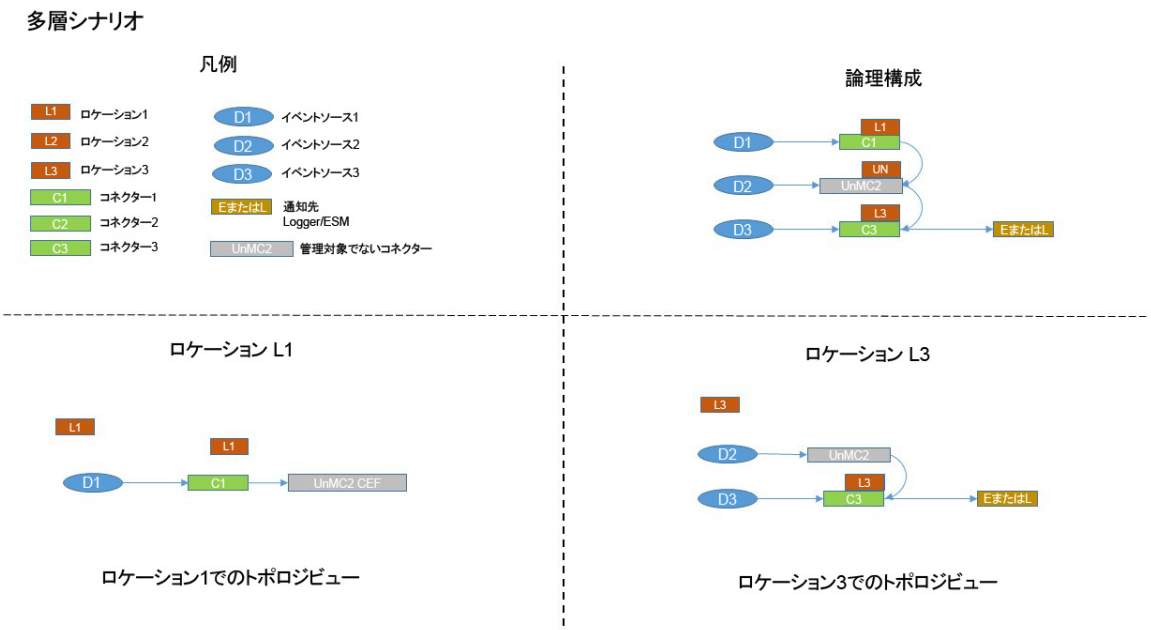
シナリオ2: ロケーションL1に管理対象でないコネクターが存在する

このシナリオでは、ロケーションL1に管理対象でないコネクターが表示され、ロケーションL2およびL3から見た結果がトポロジビューに表示されます。L1には管理対象ノードが存在しないため、L1から見たビューはありません。他の下位階層のロケーションのビューは期待どおりです。



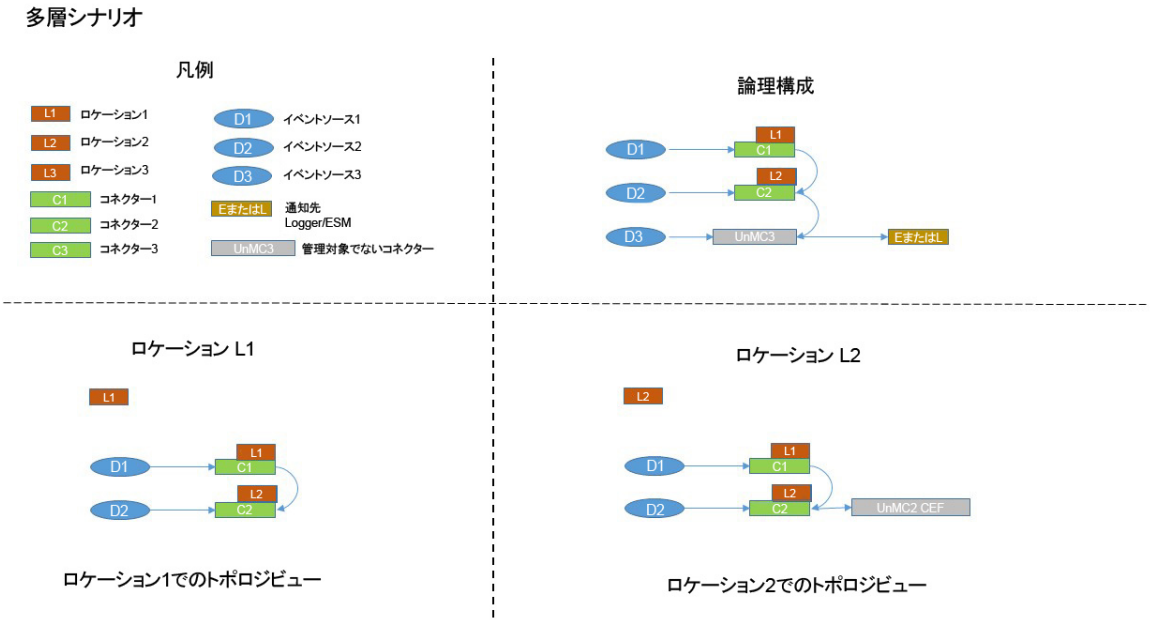
シナリオ3: ロケーションL2に管理対象でないコネクターが存在する

このシナリオでは、管理対象でないコネクターがロケーションL2に存在し、ロケーションL1およびL2のコネクターと接続されています。このため、L3から見たL1のトポロジビューがブロックされます。また、通知先LoggerまたはESMに、L1からのトラフィックが表示されません。



シナリオ4: ロケーションL3に管理対象でないコネクターが存在する

このシナリオでは、ロケーションL3に管理対象でないコネクターが存在します。このため、ロケーションL3の正確なトポロジビューが分かりません。実際、通知先Logger/ESMでは、ロケーションL1およびL2からのトラフィックが表示されません。



論理ビューを詳細かつ正確に把握するには、ArcMCを使用して論理トポロジ内にあるサポートされるすべてのコネクターを管理することを強く推奨します。

ドキュメントのフィードバックを送信

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

管理者ガイド (ArcSight Management Center 2.6x) に関するフィードバック

本文にご意見、ご感想を記入の上、[送信] をクリックしてください。

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

お客様からのご意見、ご感想をお待ちしています。