



Hewlett Packard
Enterprise

HPE Security ArcSight Data Platform Event Broker

ソフトウェアバージョン: 2.02

管理者ガイド

2017年7月5日

ご注意

保証

Hewlett Packard Enterprise製品、またはサービスの保証は、当該製品、およびサービスに付随する明示的な保証文によってのみ規定されるものとします。ここでの記載は、追加保証を提供するものではありません。ここに含まれる技術的、編集上の誤り、または欠如について、Hewlett Packard Enterpriseはいかなる責任も負いません。

ここに記載する情報は、予告なしに変更されることがあります。

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

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

本書は機密情報です。

権利の制限

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

著作権について

© Copyright 2017 Hewlett Packard Enterprise Development, LP

著作権と承認の完全な表明については、以下のリンク先をご覧ください。

<https://www.protect724.hpe.com/docs/DOC-13026>

サポート

連絡窓口

電話	電話番号のリストは、HPE SecurityArcSightテクニカルサポートページに記載されています: https://softwaresupport.hpe.com/documents/10180/14684/esp-support-contact-list
サポートWebサイト	https://softwaresupport.hpe.com
Protect 724コミュニティ	https://www.protect724.hpe.com

目次

第1章: 概要	6
ADP Event Broker	6
Event Brokerの特長	6
Event Brokerのアーキテクチャー	8
ユーザー環境でのADP Event Brokerのセットアップ	9
Event Brokerの展開	10
第2章: イベントデータの作成と使用	11
SmartConnectorを使用したイベントの作成	11
ArcMCからJKSファイルをプッシュ	12
ArcSight InvestigateおよびHPE Verticalによるイベントの取得	13
ESMIによるイベントの取得	13
Loggerによるイベントの取得	13
LoggerへのEvent Brokerデータ送信	14
複数のLoggerでプールを設定する例	15
ArcSight以外のアプリケーションでのイベント取得	16
Apache Flumeによるイベント転送	16
Apache HadoopによるEvent Brokerイベントの取得	17
Hadoopデータ転送を行うKafkaのアーキテクチャー	18
HadoopとFlumeの接続設定	18
Flume設定ファイルのサンプル	20
Hadoopのセットアップ	21
第3章: Event Broker環境のセキュリティ保護	23
ファイアウォールの設定	23
Event Brokerのセキュリティモードの変更	23
第4章: Event Brokerトピックの管理	25
デフォルトのトピック	25
トピックの設定	26
データの冗長性とトピックのレプリケーション	26
ArcMCによるトピック管理	27

第5章: Event Brokerの管理	28
ArcMCによるEvent Brokerの管理	28
ArcMCによるEvent Brokerの管理の有効化	28
Event Broker Managerについて	28
Event Broker Managerへの接続	29
クラスターの管理	30
クラスター情報の表示	30
ブローカーの管理	31
ブローカーの詳細の表示	32
Summary	33
Metrics	33
Messages count	33
Per Topic Detail	33
トピックの管理	33
トピックの作成	35
トピックの詳細の表示	36
Topic Summary	37
Metrics	38
Operations	38
Partitions by Broker	39
Consumers consuming from this topic	40
Partition Information	40
コンシューマーの管理	40
コンシューマーの詳細の表示	41
優先レプリカの管理	42
パーティションの管理	42
第6章: トラブルシューティング	44
Event Brokerクラスターの稼働状態の確認	44
Event Brokerでよく発生する問題の診断	45
Event Brokerクラスターがダウンする	45
Podの起動順序	45
ZooKeeperのクエリを実行できない	46
ZooKeeperログでよく報告されるエラーと警告	46
Kafkaログでよく報告されるエラーと警告	46
Event Brokerのパフォーマンスチューニング	48
ストリームプロセッサEPSの追加	48
Kafkaの保存サイズ/期間の増加	49
Webサービスの管理者パスワードの変更	49

新しいワーカーノードの追加	49
付録A: installer.propertiesファイル	50
用語集	58
ドキュメントのフィードバックを送信	62

第1章: 概要

この章では、次の内容について説明します。

• ADP Event Broker	6
• Event Brokerのアーキテクチャー	8
• ユーザー環境でのADP Event Brokerのセットアップ	9
• Event Brokerの展開	10

ADP Event Broker

ArcSight Data Platform Event Brokerは、トピックの分類やイベントのルーティングにより、イベントを一元処理するソリューションです。ArcSight環境を拡張し、ArcSightイベントデータをサードパーティソリューションでも利用可能にします。

優れた拡張性と可用性を備えたマルチブローカークラスターを実装することで、イベントデータのパブリッシュとサブスクライブを行います。ADP Event Brokerは、ArcSightコネクター、Logger、ESMと統合されます。これによってArcMCによる管理と監視が可能になり、ArcSight Investigateを使用する基盤になります。

ArcSight Data Platform Event Brokerは、Confluent Kafkaのパッケージバージョンです。Event Brokerクラスターのインストールと設定が完了したら、ADP SmartConnectorを使用してデータをパブリッシュし、ADP Logger、ArcSight ESM、ArcSight Investigate、Apache Hadoop、独自のコンシューマーでデータをサブスクライブすることが可能になります。

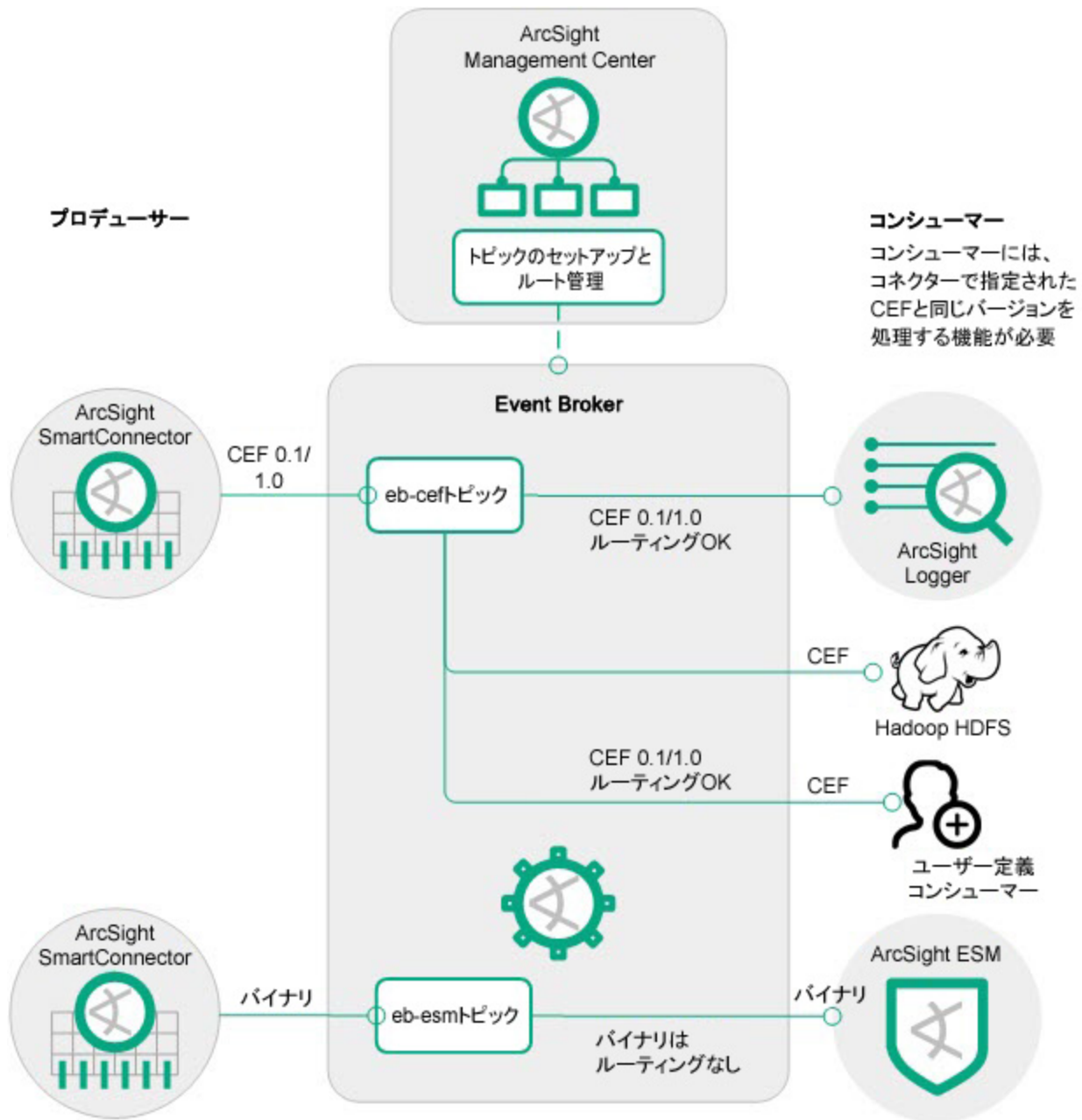
Event Brokerの特長

Event Brokerは、オープンソースの分散型高性能メッセージバスであり、復元力と冗長性を備えたメッセージパイプラインの構築に使用できます。Event Brokerは、オープンソースのKafkaを凌ぐ利点を数多く備えています。

- Event Brokerは、エンタープライズ対応のソリューションとして、以下の機能を備えています。
 - **コンテナベースの展開**: Kubernetesの展開を利用して、一元的な展開を高速実行できます。
 - **一元管理とローカル管理**: ArcSight Management Centerの一元管理機能と、Event Broker Managerのローカル管理機能を使用できます。
 - **システムとアプリケーションの監視**: 他のArcSightアプリケーションと同様に、Event BrokerのメトリックをArcSight Management Centerで監視します。

- Event Brokerは、展開に最適化されたソリューションとして、以下の機能を備えています。
 - **すぐに使用できるセキュリティ強化:** TLS、TLS-CA、FIPS、FIPS-CAをサポートします。
 - **イベントのフィルタリングとルーティング:** 必要に応じてイベントの分類とソートを実行します。
 - **形式変換エンジン:** CEFデータをAvro形式に効率的に変換します。
 - **すぐに使用できるトピック:** デフォルトトピックがインストールされているので、すぐに稼働を開始できます。

Event Brokerのアーキテクチャー



ArcSight SmartConnectorは、データをADP Event Brokerにパブリッシュするプロデューサーです。Event Brokerに送信されたデータ (CEFまたはバイナリ形式) は、Event Broker上のトピックに転送されます。

- CEFデータは、さらに分類用の特殊なトピックにルーティングされます。
- バイナリデータは、そのままの形式でArcSight ESMで使用されます。バイナリトピックはルーティングされないことがあります。

Event Brokerが処理したデータは、ArcSight Investigate (Verticaを使用)、ArcSight ESM、ADP Logger、Apache HDFSなどのコンシューマーや、サードパーティコンシューマーによるサブスクライブが可能です。

Event Brokerの管理には、Event Broker Manager、ArcMC、ArcSight一元管理および監視ソリューションを使用できます。

ユーザー環境でのADP Event Brokerのセットアップ

ステージング環境でEvent Brokerのセットアップとテストを行ってから、運用環境での展開に進みます。

ユーザー環境でEvent Brokerをセットアップする作業は、次の手順で行います。

1. **Event Broker要件のレビュー:** Event Brokerの技術的な要件を確認し、Event Brokerを展開するためのKubernetesノードを準備します。詳細については、『Event Broker展開ガイド』を参照してください。
2. **Event Brokerの展開:** 展開ガイドの説明に従って、Event BrokerをKubernetesノードに展開します。
3. **プロデューサーのセットアップ:** Event Broker向けのデータを生成する1つ以上のSmartConnector (バージョン7.6以降) をセットアップします。詳細については、『SmartConnectorユーザーガイド』を参照してください。
4. **ArcSight Management Center (ArcMC) のインストール:** Event BrokerをArcMCで管理する場合 (推奨)、ArcMCをインストールします。詳細については、『ArcSight Management Center管理者ガイド』を参照してください。
5. **ArcMCによる管理の設定:** ArcMCで管理する設定をEvent Brokerで行い、ホストとしてArcMCに追加します。手順については、『ArcSight Management Center管理者ガイド』を参照してください。
6. **コンシューマーのセットアップ:** イベントデータを使用する1つ以上のコンシューマーをセットアップします。
 - ArcSight Investigate、Logger (6.4以降)、ArcSight ESM (6.11.0以降)、Apache Hadoop、サードパーティコンシューマーのうち、1つ以上を展開します。
 - Event BrokerのKafkaクラスターからイベントを受信する設定をコンシューマーで行います。詳細については、「[Loggerによるイベントの取得](#)」(13ページ)、「[Apache HadoopによるEvent Brokerイベントの取得](#)」(17ページ)、「[ArcSight以外のアプリケーションでのイベント取得](#)」(16ページ) のいずれかを参照してください。

Event Brokerの展開

Event Brokerの展開については、『ArcSight Installer Deployment Guide』で詳しく説明しています。このガイドは、[ArcSightソフトウェアコミュニティ](#)のArcSightドキュメントリポジトリで入手できます。

第2章：イベントデータの作成と使用

Event Brokerは、パブリッシュ/サブスクライブ型のメッセージングシステムを採用しています。イベントデータの生成にはArcSight SmartConnectorを使用し、コンシューマーとしてArcSight LoggerとArcSight ESM、さらにApache Hadoopなどのサードパーティコンシューマーをサポートします。

この章では、次の内容について説明します。

- SmartConnectorを使用したイベントの作成 11
- ArcSight InvestigateおよびHPE Verticalによるイベントの取得 13
- ESMによるイベントの取得 13
- Loggerによるイベントの取得 13
- ArcSight以外のアプリケーションでのイベント取得 16
- Apache HadoopによるEvent Brokerイベントの取得 17

SmartConnectorを使用したイベントの作成

ArcSight SmartConnectorは、Event Brokerトピックにイベントをパブリッシュできます。Event Brokerは、バージョン7.6.0以降のSmartConnectorタイプをすべてサポートします。

イベントをパブリッシュするには、Event Broker通知先を使用する設定をSmartConnectorで行う必要があります。イベントを複数のトピックに送信するには、同じEvent Brokerホストと異なるトピックで、複数の通知先を同時に設定することが可能です。

Event Broker通知先の設定が完了したら、SmartConnectorはEvent BrokerのKafkaクラスターにイベントを送信します。クラスターは、受信したイベントをさらにリアルタイム分析システムやデータウェアハウスシステムに配信します。他にも、ArcSight Investigate、ESM、Logger、あるいはKafkaからのデータ取得をサポートするサードパーティアプリケーション (Apache Hadoopなど) などのアプリケーションがイベントを受信できます。

ヒント: SmartConnectorは、想定されるスループットに基づいた調整が必要になる場合があります。

Event Brokerは、SmartConnectorが送信したイベントをトピック内のパーティションに均等に配信することで、ノード間でイベントを分散します。

Event Brokerがイベント受信の確認応答を行うと、SmartConnectorはそのイベントをローカルキューから削除します。確認応答は、無効化の設定、プライマリレプリカの確認応答のみを要求する設定、すべてのレプリカに確認応答を要求する設定が可能です (確認応答は、Loggerなどのコンシューマーがイベントを受信したことを示すものではなく、Event Brokerによる受信完了を示すものです)。

SmartConnectorは、自分自身のIPアドレスをエンコードし、Kafkaメッセージにメタデータとして格納します。これは、Loggerデバイスグループなど、その情報を必要とするコンシューマー向けのデータです。

SmartConnectorの詳細とEvent Broker通知先の設定方法については、『SmartConnector ユーザーガイド』の「CEF通知先」の章を参照してください。このガイドは、[Protect 724のArcSight製品ドキュメントコミュニティ](#)からダウンロードできます。

ArcMCからJKSファイルをプッシュ

ArcMCでは、JKS (Java Keystore) ファイルを複数の管理対象 SmartConnectorにプッシュできます。まず、ファイルをArcMCのファイルリポジトリにアップロードし、通知先となる SmartConnectorにプッシュします。次に、Kafka通知先をすべてのSmartConnectorで設定し、有効化します。

Java Keystoreファイルをアップロードするには

1. プッシュする.jksファイルを作成し、ネットワーク上の安全な場所に格納します。
2. ArcMCで、**[Administration] > [Repositories] > [New Repository]** をクリックします。
3. **[Name]**、**[Display Name]**、**[Item Display Name]** の各フィールドに「KAFKA_JKS」と入力します。
4. 必要に応じて他のフィールドにも値を入力し、**[Save]** をクリックします。
5. **[Upload to Repository]** をクリックします。
6. アップロードウィザードの指示に従って、最初の.jksファイルを選択します。注: 個別ファイルオプションを選択してください。
7. 複数のファイルをアップロードする場合は、アップロードウィザードを繰り返し実行します。

ファイルを複数のSmartConnectorにプッシュするには

1. ArcMCで、ファイルリポジトリ内にある.jksファイルを参照します。
2. **[Upload]** の矢印をクリックします。
3. ウィザードの指示に従い、通知先となるSmartConnectorを選択します。
4. ファイルが管理対象 SmartConnectorにプッシュされ、指定したSmartConnectorのフォルダーに保存されます。

Kafka通知先をすべてのSmartConnectorで設定するには

ArcMCで **[Node Management] > [Connectors]** タブをクリックします。

1. 設定の対象となるSmartConnectorを選択します。
2. **[Add a destination]** を選択し、通知タイプとしてKafkaを選択します。
3. 通知先の詳細、.jksのパスとパスワードを追加し、変更内容を保存します。

ArcSight InvestigateおよびHPE Verticaによるイベントの取得

デフォルトトピックeb-internal-avroで変換されたイベント (Avro形式) は、HPE Verticaデータベースによって読み取られます。イベントデータがVerticaストレージに格納されると、ArcSight Investigate検索でのアクセスが可能になります。

Event BrokerでArcSight Investigateを使用する設定を行う場合、Verticaインストーラーの一部で、VerticaがサブスクライブするデフォルトのAvroトピックの場所を指定できます。詳しい手順については、HPE Verticaインストーラーのドキュメントを参照してください。

ESMによるイベントの取得

ArcSight ESMバージョン6.11.0以降は、Event Brokerイベントのサブスクライブに対応しています。ESMによるEvent Brokerトピックのサブスクライブには、SmartConnectorリリース7.6以降が必要です。

Event Brokerのパブリッシュ/サブスクライブ型メッセージングシステムにおいて、ESMエージェントはコンシューマーとして動作します。ESMエージェントはArcSight Event Brokerに接続し、サブスクライブしているトピックのすべてのイベントをバイナリ形式で取得します。

さらに、ESMはデータモニター機能により、Event Brokerのヘルスを監視します。

ESM 6.11.0以降をコンシューマーとして設定する方法については、『ESM Administrator's Guide』を参照してください。

Loggerによるイベントの取得

LoggerでEvent Brokerトピックをサブスクライブするには、Logger 6.4以降でEvent Brokerレシーバーを設定する必要があります。Event Brokerのパブリッシュ/サブスクライブ型メッセージングシステムにおいて、LoggerのEvent Brokerはコンシューマーとして動作します。Event Brokerのトピックから、イベントを共通イベントフォーマット (CEF) 形式で受信します。Event BrokerレシーバーはArcSight Event Brokerに接続し、サブスクライブしているトピックのすべてのイベントを取得します。

Event Brokerレシーバーの設定では、コンシューマーグループとトピックを指定します。コンシューマーグループ内の複数のLoggerが、同じトピックからイベントを取得する設定も可能です。

Loggerの詳細とEvent Brokerレシーバーの設定方法については、『ArcSight Logger管理者ガイド』の「設定」>「レシーバー」のセクションを参照してください。このガイドは、[Protect 724のArcSight製品ドキュメントコミュニティ](#)からダウンロードできます。

LoggerへのEvent Brokerデータ送信

LoggerでEvent Brokerイベントを取得するには、LoggerのEvent Brokerレシーバーで、Event Brokerホスト、コンシューマーグループ、イベントトピックリストを設定する必要があります。Event Brokerにデータを送信するSmartConnectorには、Event Broker通知先が必要です。

複数のLoggerをグループ化したプールを作成し、イベントの受信と分散を行うことも可能です。その動作は、SmartConnector上のArcSight Logger Smart Message Pool通知先を使って作成したLoggerプールに類似しています。ただし、SmartConnectorにArcSight Logger Smart Message Pool通知先がある場合には、SmartConnectorがイベント負荷を分散するのに対して、SmartConnectorにEvent Broker通知先がある場合には、Loggerが負荷分散を行う点が異なります。

プールにLoggerを追加するには、Loggerを新しく作成して、Event Brokerレシーバーで同じEvent Brokerホスト、コンシューマーグループ、イベントトピックリストを設定します。既存のLoggerやSmartConnectorの再設定は必要ありません。

Loggerプールが取得したイベントは、プール内のLoggerに分散されます。いずれかのLoggerがダウンすると、イベントは残りのLogger間で再分散されます。Loggerをコンシューマーグループに追加または削除すると、イベント負荷はLoggerプール全体に分散されます。

SmartConnectorグループからLoggerプールにイベントを送信するには、Loggerプールの取得先トピックにイベントを送信する設定をEvent Broker通知先で行う必要があります。

特定のSmartConnectorのイベントデータをサブスクライブする設定をLoggerで行うには、次のいずれかを実行します。

- すべてのSmartConnectorで、イベントを同じトピックにパブリッシュする設定を行います。次に、LoggerのEvent Brokerレシーバーで、そのイベントトピックをサブスクライブする設定を行います。
- SmartConnectorごとに、イベントを異なるトピックにパブリッシュする設定を行います。次に、LoggerのEvent Brokerレシーバーで、複数のイベントトピックをサブスクライブする設定を行います。

ヒント: 同じプール内のLoggerは同じコンシューマーグループに所属するので、同じイベントを取得することはありません。高可用性が求められる環境では、2つの異なるLoggerにイベントを保存する必要があります。同じイベントを2つのLoggerに保存するには、Loggerで異なるコンシューマーグループ名を指定してから、同じイベントトピックをサブスクライブします。

プール内のLoggerの数は、イベントトピックパーティションの数によって制限されます。たとえば、パーティションが5つしかない場合、イベントを受信できるLoggerの数は5つだけとなります。

す。コンシューマーグループ内にLoggerが6つ以上ある場合、一部のLoggerは通常はイベントを受信しませんが、ホットスペアとしては使用可能です。レシーバーを追加する場合は、イベントトピックパーティションの数を増やしてください。詳細については、「[トピックの管理](#)」を参照してください。

LoggerへのEvent Brokerデータ送信 (概要):

1. SmartConnectorを設定します。
 - SmartConnectorで、特定のイベントトピックに対してパブリッシュする設定を行います。コネクタで送信先として指定できるのは、1つの通知先で1つのトピックのみです。1つのイベントを複数のトピックに送信する場合には、通知先を追加設定してください。イベントトピック内のパーティション数を記録しておきます。
 - SmartConnectorで、Event Broker通知先の設定を行います。Loggerでは、Event Broker通知先を使用します。
 - SmartConnectorの詳細とEvent Broker通知先の設定方法については、『SmartConnectorユーザーガイド』の「CEF通知先」の章を参照してください。このガイドは、[Protect 724のArcSight製品ドキュメントコミュニティ](#)からダウンロードできます。
2. Loggerを設定します。
 - Loggerプール内のLoggerごとに、Event Brokerレシーバーを作成します。
 - SmartConnectorのデータパブリッシュ先となるイベントトピックをサブスクライブする設定を、各レシーバーで行います。複数のトピックをサブスクライブするには、Event Brokerレシーバーの設定で、イベントトピックリストパラメーター (カンマ区切り値のリスト) でトピックを指定します。
 - 各レシーバーを同じコンシューマーグループに所属させる設定を行います。
Event Brokerを使ってKafkaイベントを受信する設定をLoggerで行う方法については、「[Loggerによるイベントの取得](#)」(13ページ) と、『Logger管理者ガイド』の「設定」の章の「レシーバー」セクションを参照してください。ガイドは、[ArcSight製品ドキュメントコミュニティ](#)からダウンロードできます。

複数のLoggerでプールを設定する例

Loggerプールの設定では、特定のデバイスタイプ (この例では「Firewall」) のイベントをサブスクライブすることが可能です。これを行うには、次の手順を実行してください。

1. ArcMCでKafkaトピックを作成し、「Firewall」という名前を付けます。
2. ファイアウォールイベントを処理するすべてのSmartConnectorで、「Firewall」トピックにイベントをパブリッシュする設定を行います。

3. Loggerプール内でLoggerを設定します。
 - プール内のLoggerごとに、Event Brokerレシーバーを作成します。
 - このレシーバーで「Firewall」トピックをサブスクライブする設定を行い、「Logger_Firewall」コンシューマーグループに追加します。

設定がすべて完了すると、Loggerプールはデバイスタイプ「Firewall」のサブスクライブを開始します。

ArcSight以外のアプリケーションでのイベント取得

Event Brokerは、サードパーティツールをサポートするように設計されています。標準的なKafkaコンシューマーを作成し、Event Brokerトピックをサブスクライブする設定が可能です。これにより、取得したEvent Brokerイベントを、ArcSight以外の独自のデータレイクに保存できるようになります。

注: コンシューマーの作成には、バージョン0.10以降のKafkaクライアントライブラリを使用してください。

- Event Brokerノード、コンシューマー、プロデューサーをすべてDNS/リバーズDNS向けに正しく設定し、NTPなどのタイムサーバーで時刻も正しく設定する必要があります。
- イベントは、標準CEF (CEFテキストおよびCEFバイナリ、ESMの取得専用) で送信されます。Kafkaからのデータを取得でき、CEFテキストを認識できるアプリケーションであれば、どのようなアプリケーションでもイベントを処理できます。
- 複数のコンシューマーグループを設定し、各グループが各イベントのコピーを取得することも可能です。これにより、LoggerとApache Hadoopがそれぞれ同じトピックから各イベントのコピーを取得することができます。これにより、SmartConnectorを再設定したり、CPUまたはネットワークリソースを追加したりしなくても、複数のイベントコピーを展開できます。

Apache Flumeによるイベント転送

Event Brokerイベントをデータレイクに転送するアプリケーションの1つに、Apache Flumeがあります。Flumeは、大量のソースからデータを収集し、HDFSやHBaseといったHadoopエコシステム内の各種ストレージシステムにプッシュすることを目的に設計されたサービスです。このセクションでは、Apache Flumeをデータ転送チャンネルとして使用し、Event BrokerからApache Hadoopなどのストレージシステムにイベントを転送する方法について説明します。

前提条件

- Event Brokerがインストール済みであること。詳細については、『Event Broker展開ガイド』を参照してください。

- Flumeがインストール済みであること。Flumeのインストールおよび設定方法については、Flumeのドキュメント (<https://flume.apache.org/releases/content/1.6.0/FlumeUserGuide.pdf>) を参照してください。
- ストレージシステムがインストール済みであること。ストレージシステムのドキュメントを参照してください。

手順

Flumeの制御には、エージェント設定ファイルを使用します。このファイル内で、Event Brokerをソースエージェント、ストレージシステムをシンクエージェント、ZooKeeperをチャネルエージェントとして指定します。

Event Brokerをソースとして設定するには

エージェント設定ファイルを編集し、次の表で示す必須プロパティを指定します。お使いの環境で必要なプロパティが他にもあれば設定してください。

Kafkaソースで必要な設定

プロパティ	説明
type	org.apache.flume.source.kafka.KafkaSourceに設定します。
topic	このソースがメッセージを読み出すイベントトピック。Flumeは、1つのソースに対して1つのトピックのみをサポートします。
ZooKeeperConnect	Kafkaが使用するZooKeeperサーバーまたはクラスターのURI。 POCシングルノードの例: zk01.example.com:332181 ZooKeeperクラスターのノードを指定するカンマ区切りリストの例: zk01.example.com:32181,zk02.example.com:32181,zk03.example.com:332181

シンクを設定するには

必要な設定はストレージシステムによって異なります。詳細については、Flumeのドキュメントを参照してください。「[Apache HadoopによるEvent Brokerイベントの取得](#)」(17ページ)には、例としてApache Hadoopをシンクとして設定する方法が記載されています。

Apache HadoopによるEvent Brokerイベントの取得

Apache Hadoopは、大量のデータセットをコンピュータークラスターで分散処理するためのソフトウェアフレームワークです。HadoopへのEvent Brokerイベント送信には、Apache Flumeを

使用できます。

このセクションでは、Apache Flumeエージェントをセットアップして、共通イベントフォーマット(CEF) イベントをEvent Broker KafkaクラスターからHadoop分散ファイルシステム(HDFS)に転送する方法について説明します。

次の項目について説明します。

- [Hadoopデータ転送を行うKafkaのアーキテクチャー](#) 18
- [HadoopとFlumeの接続設定](#) 18
- [Flume設定ファイルのサンプル](#) 20
- [Hadoopのセットアップ](#) 21

Hadoopデータ転送を行うKafkaのアーキテクチャー

Apache Flumeは、ソースモジュールを使用して、RAW CEFイベントを含むKafkaトピックを読み取ります。読み取ったイベントはメモリチャネルを使用して転送され、シンクモジュールを使用してHDFSに永続化されます。CEFファイルはHDFS上で、「年/月/日/時」形式のディレクトリ構造で保存されます。



HadoopとFlumeの接続設定

概要:

最も簡単な展開モデルでは、Apache FlumeエージェントをHadoopノードに展開してイベントをプルし、Hadoop分散ファイルシステム(HDFS)に送信します。

前提条件:

HadoopをFlumeに接続するには、Hadoopをインストールしておく必要があります。Hadoopをまだ展開していない場合、HadoopをRed Hat Enterprise Linux 7.2マシンに展開してください。詳細については、「[Hadoopのセットアップ](#)」(21ページ)を参照してください。

手順:

1. Hadoopサーバーにユーザー名「hadoop」でログインします。
2. Flumeを[Apacheダウンロードサイト](#)からダウンロードします。
3. ".gz" ファイルを解凍し、任意のディレクトリに展開します。
4. 設定ファイルを開き、ZooKeeperアドレスとポート、Kafkaトピック、HDFSアドレスとポートを追加します。

デフォルトでは、この設定によってCEFファイルが1時間に1回永続化されます。または、イベント数またはファイルサイズを使用する方法もあります。イベントが大量に発生する環境では、HPE ArcSightは、メモリ不足を回避するために時間ではなくイベント数オプションの使用を推奨します。詳細については、『Flume Users' Guide』の「[Flume HDFS sink](#)」を参照してください。

5. 次のコマンドを実行し、HadoopのcefEventsディレクトリを作成します。

```
hadoop fs -mkdir /opt
hadoop fs -mkdir /opt/hadoop
hadoop fs -mkdir /opt/hadoop/cefEvents
```

6. 「[Flume設定ファイルのサンプル](#)」(20ページ)のテンプレートに従って、Flumeのconfディレクトリ(bin/flume/conf/)に設定ファイルを作成します。ここではkafka.confというファイル名を使用しますが、任意のファイル名にすることができます。

- a. flume-env.sh.templateをコピーし、flume-env.shという名前になります。
- b. flume-env.shファイルを編集し、次のように変更します。
 - JAVA_HOMEを設定し、システム上でJavaがインストールされているディレクトリに指定します。
 - JAVA_OPTSの行のコメントを解除します。

```
export JAVA_OPTS="-Xms100m -Xmx2000m -Dcom.sun.management.jmxremote"
```

- FLUME_CLASSPATH=<Flumeのインストールディレクトリ>/libを設定します。

- c. 共通のjarファイルを、HadoopのインストールディレクトリからFlumeのlibディレクトリにコピーします。

```
cp <Hadoopのインストールディレクトリ>/share/hadoop/common/*.jar /<Flumeのインストールディレクトリ>/lib
```

```
cp <Hadoopのインストールディレクトリ>/share/hadoop/common/lib/*.jar /<Flumeのインストールディレクトリ>/lib
```

- d. hadoop-hdfs-2.7.2.jarを、HadoopのインストールディレクトリからFlume libディレクトリにコピーします。

```
cp <Hadoopのインストールディレクトリ>/share/hadoop/hdfs/hadoop-hdfs-2.7.2.jar /<Flumeのインストールディレクトリ>/lib
```

7. 次のコマンドを実行し、Flumeをホームディレクトリから起動します。
`bin/flume-ng agent --conf conf/ --conf-file conf/kafka.conf --name tier1 -Dflume.root.logger=INFO,console`
8. Flumeが起動したら、次のコマンドを実行し、HDFS上でファイルを検索します。
`hadoop fs -ls -R /opt/hadoop/cefEvents`
このパスは、Hadoopの設定で作成したHDFSディレクトリと一致する必要があります。
ファイルは「年/月/日/時」の形式で保存されています。

Flume設定ファイルのサンプル

Apache Flumeを起動する前に、以下のテンプレートに沿って設定ファイルを作成します。

作成した設定ファイルは、`bin/flume/conf/`に保存します。この例で使用するファイルの名前は`kafka.conf`ですが、設定ファイルは任意の名前にすることができます。

```
#####  
#Sample Flume/Kafka configuration file  
#####  
#defines Kafka Source, Channel, and Destination aliases  
tier1.sources = source1  
tier1.channels = channel1  
tier1.sinks = sink1  
  
#Kafka source configuration  
tier1.sources.source1.type = org.apache.flume.source.kafka.KafkaSource  
tier1.sources.source1.ZooKeeperConnect = <ZooKeeperAddress>:Port  
# Example Address of ZooKeeper on an Event Broker master node, with port  
32181:  
# masterNodeIP:32181  
tier1.sources.source1.topic = <Kafka_topic>  
tier1.sources.source1.groupId = flume  
tier1.sources.source1.channels = channel1  
tier1.sources.source1.interceptors = i1  
tier1.sources.source1.interceptors.i1.type = timestamp  
tier1.sources.source1.kafka.consumer.timeout.ms = 150
```

```
tier1.sources.source1.kafka.consumer.batchsize = 100
#Kafka Channel configuration
tier1.channels.channel1.type = memory
tier1.channels.channel1.capacity = 10000
tier1.channels.channel1.transactionCapacity = 1000

#Kafka Sink (destination) configuration
tier1.sinks.sink1.type = hdfs
tier1.sinks.sink1.channel = channel1
tier1.sinks.sink1.hdfs.path = hdfs://localhost:9000/opt/\
hadoop/cefEvents/year=%y/month=%m/day=%d
tier1.sinks.sink1.hdfs.rollInterval = 360
tier1.sinks.sink1.hdfs.rollSize = 0
tier1.sinks.sink1.hdfs.rollCount = 0
tier1.sinks.sink1.hdfs.fileType = DataStream
tier1.sinks.sink1.hdfs.filePrefix = cefEvents
tier1.sinks.sink1.hdfs.fileSuffix = .cef
tier1.sinks.sink1.hdfs.batchSize = 100
tier1.sinks.sink1.hdfs.timeZone = UTC
```

Hadoopのセットアップ

ここでは、Apache Hadoop 2.7.2をインストールし、単一ノードクラスターとしてセットアップする手順について簡単に説明します。詳細については、<https://hadoop.apache.org/docs/r2.7.2/hadoop-project-dist/hadoop-common/SingleCluster.html>、または使用しているバージョンのHadoopのドキュメントを参照してください。

Hadoopをインストールするには

1. インストールする環境が、オペレーティングシステムとJavaの前提条件を満たしていることを確認してください。
2. hadoopユーザーを追加します。
3. Hadoopをダウンロードして解凍します。
4. Hadoopを疑似分散モードに設定します。

- 環境変数を設定します。
 - パスフレーズなしのSSHを設定します。
 - オプションで、Yarnをセットアップします (Hadoopを処理用には使用せず、ストレージ専用で使用する場合は、Yarnは不要です)。
 - Hadoopの設定ファイルを編集し、コアの場所、Hadoop分散ファイルシステム (HDFS) の場所、レプリケーション値、NameNode、DataNodeを指定します。
 - NameNodeをフォーマットします。
5. 付属のツールでHadoopサーバーを起動します。
 6. ブラウザーでHadoopサービスにアクセスし、「hadoop」ユーザーでログインします。
 7. 次のコマンドを実行し、HadoopのcefEventsディレクトリを作成します。

```
hadoop fs -mkdir /opt
hadoop fs -mkdir /opt/hadoop
hadoop fs -mkdir /opt/hadoop/cefEvents
```
 8. 次のコマンドを実行し、このHDFSへの書き込み権限をApache Flumeに割り当てます。

```
hadoop fs -chmod 777 -R /opt/hadoop
hadoop fs -ls
```
 9. 次のコマンドを実行し、Hadoopのシステムステータスをチェックします。

```
hadoop dfsadmin -report
```
 10. 次のコマンドを実行し、FlumeがHadoopに転送したファイルを表示します。

```
hadoop fs -ls -R /
```

第3章: Event Broker環境のセキュリティ保護

Event Broker環境は、ビジネスニーズや要件に沿ってセキュリティ保護する必要があります。Event Brokerでは、セキュリティ機能としてトランスポートレイヤーセキュリティ (TLS) をサポートします。ビジネスニーズと環境に適した方法でファイアウォールを設定しておいてください。

この章では、次の内容について説明します。

- [ファイアウォールの設定](#) 23
- [Event Brokerのセキュリティモードの変更](#) 23

ファイアウォールの設定

ファイアウォールでは、必要なサービスのみへのアクセスを許可するルールを設定する必要があります。

Event Broker環境では、次のアクセスが必要です。

- Kafkaはポート9093を使用します。このポートではTLSが有効になっています。顧客データはすべてTLSでセキュリティ保護されます (Verticaデータベースを使用している場合、すべてのEvent Brokerノード、コンシューマー、プロデューサーにポート9092へのアクセスを許可してください。ただし、9092ではTLSは有効になっていません)。
- ZooKeeperはポート332181を使用します。このポートは、すべてのEvent Brokerノード間でアクセス可能にしてください。
- Event Broker ManagerはKafkaの監視にポート9999と10000を使用します。この2つのポートは、すべてのEvent Brokerノード間で相互にアクセス可能にしてください。

デフォルトでは、Kafka ZooKeeperの相互通信にTLSまたはFIPSは使用されません。この通信には顧客データは含まれません。

Event Brokerのセキュリティモードの変更

展開とセットアップの前に、セキュリティモードを決定する必要があります。一般的に、Event Brokerに接続するシステム (コンシューマーとプロデューサー) では、Event Brokerと同じセキュリティモードを設定してください。

TLSがデフォルト設定です。 [installer.properties](#) ファイルを編集し、TLS+CAとFIPSを有効化します。

Event Brokerのセキュリティモードの変更は展開後でも可能ですが、Event Brokerと関連システムでダウンタイムが発生します。また、すべてのEvent Broker関連システムで再設定が必要になります。

注: Vertica SchedulerはTLSをサポートしていません。Verticaに接続する場合には、ポート9092 (非 TLSポート) をすべてのEvent Brokerノードで開き、Verticaノードからのアクセスのみを許可してください。

セキュリティモードを変更するには (概要)

1. SmartConnectorのイベント送信を停止します。これにより、接続が閉じます。SmartConnectorのイベント送信を停止する方法については、『SmartConnectorユーザーガイド』を参照してください。
2. すべてのコンシューマー (ArcSight Logger、ArcSight ESM、Vertica Scheduler) で、Event Brokerのトピックからの取得を停止します (既存のメッセージをトピックから消去する必要はありません)。
3. セキュリティモードの変更によってEvent BrokerコンシューマーまたはEvent Brokerプロデューサーの再起動が必要になる場合には、まずEvent Brokerから切断してください。詳細については、コンシューマーまたはプロデューサーのドキュメントを参照してください。Vertica Schedulerは、セキュリティモードの変更をサポートしていません。
4. Event Brokerコンテナの展開を解除します。
5. テキストエディターで`installer.properties`を開き、次のように設定を変更します。
 - `predeploy.eb.init.client-auth=false`。trueに設定してTLS+CAを有効化します。
 - `predeploy.eb.init.fips=false`。trueに設定してFIPSを有効化します。

注: `installer.properties`設定の一覧については、[付録](#)を参照してください。

6. Event Brokerコンテナを再度展開します。
7. コンシューマーとプロデューサーのドキュメントの手順に従ってアプリケーションを再設定し、Event Brokerと同じセキュリティモードにします。
8. コンシューマーとプロデューサーを再度接続します。詳細な手順については、各製品のドキュメントを参照してください。

第4章: Event Brokerトピックの管理

Event Brokerトピックの管理には、Event Broker ManagerまたはArcMCを使用します。

この章では、次の内容について説明します。

- デフォルトのトピック 25
- トピックの設定 26
- データの冗長性とトピックのレプリケーション 26
- ArcMCによるトピック管理 27

デフォルトのトピック

Event Brokerの展開では、デフォルトトピックがいくつか用意されています。デフォルトのトピックをそのまま使用する方法と、ユーザーが独自のトピックを設定する方法があります。トピック名は、大文字と小文字が区別されます。

デフォルトのトピック名	説明
eb-esm	ESMをコンシューマーとしてサポートします。すべてのESMイベントで使用できます。ESMイベント用に他のトピックを追加することが可能ですが、ルートを作成はできません。
eb-cef	CEF 0.1イベントまたはCEF 1.0イベントで使用できます。ルートを作成し、このトピックのイベントのフィルター処理に適用することが可能です。
eb-other	カスタマイズしたコンシューマーで使用します。
eb-internal-stream-processor-metrics	内部使用のみです。SmartConnector通知先で、このトピックにイベントを送信する設定は行わないでください。
eb-internal-avro	内部使用のみです。SmartConnector通知先で、このトピックにイベントを送信する設定は行わないでください。
__consumer_offsets	内部使用のみです。SmartConnector通知先で、このトピックにイベントを送信する設定は行わないでください。
_schemas	内部使用のみです。SmartConnector通知先で、このトピックにイベントを送信する設定は行わないでください。
eb-internal-datastore	内部使用のみです。SmartConnector通知先で、このトピックにイベントを送信する設定は行わないでください。

トピックの設定

HPE ArcSightでは、カテゴリ別に異なるトピックを使用することをお勧めします。たとえば、ファイアウォールイベントとアンチウイルスイベントには、それぞれ別のトピックを使用します。

- データの分割や分類の要件に基づいてトピックを設定します。分類されたトピックのみにルーティングする場合、イベントはVerticalに送信されないため、ArcSight Investigateでは使用できません。
- スループットとコンシューマー数に基づいて、トピックのパーティション数を設定します。パーティション数には、現在の(および将来的な)コンシューマーの総数以上の数値を設定してください。
- イベントの重要度に基づいて、レプリケーション係数を設定します。新規トピックで推奨されるレプリケーション係数は2です。クラスター内のすべてのノードにすべてのトピックを複製することは可能ですが、トラフィックの増大によってスループットが低下し、ディスク容量が大量に消費される可能性があるためにお勧めしません。

データの冗長性とトピックのレプリケーション

Event Brokerの設定では、Event Brokerが配信する各トピックのコピー数(レプリカ数)を指定できます。

Kafkaは、Event Brokerで設定したトピックレプリケーションレベルが示す数のブローカーノードに、トピック内の各イベントを自動配信します。レプリケーションによってスループットは若干低下しますが、HPE ArcSightではレプリケーション係数を2以上に設定することをお勧めします。各レプリカにはノードが1つ以上必要です。たとえば、トピックのレプリケーションレベルが5の場合、5つ以上のノードが必要です。各ノードにレプリカが1つ格納されます。

トピックのレプリケーションレベルが1の場合、イベントを受信するブローカーは1つのみです。そのブローカーがダウンすると、イベントデータは失われてしまいます。それに対して、レプリケーションレベルが2であれば、2つのブローカーノードが同じイベントを受信します。1つがダウンしても、稼働中のもう1つのノードにイベントデータが存在します。ダウンしたノードが復帰した時点でデータは復元されます。データが失われるのは、両方のブローカーノードが同時にダウンした場合だけです。トピックのレプリケーションレベルが3の場合、イベントを受信するブローカーは3つになります。イベントデータが失われるのは、3つのブローカーノードがすべて同時にダウンした場合だけです。

新しいコンシューマーを追加する際、プロデューサーを更新する必要はありません。配信とレプリケーションは、Event Brokerによって自動調整されます。

詳細については、[Apache Kafkaのドキュメント](#)を参照してください。

ArcMCによるトピック管理

ArcMCを使用して、ルーティング用のトピックの表示や作成、ルートを作成を行うことにより、イベントを適切なトピックに転送できます。

ルートとは、Event Brokerに対して、特定の条件を満たすイベントをソーストピックからルートの宛先トピックに複製するよう指示するルールです。ルールは、イベントフィールドの名前と想定される値で定義します。

ArcMCを使用することで、CEFフィールドとイベントメタデータに基づいて、ルートを表示、作成、編集、削除することが可能になります (イベントのルーティングを行う前にトピックを作成する必要があります)。

詳細については、『ArcSight Management Center管理者ガイド』を参照してください。

第5章: Event Brokerの管理

ArcMCでは、トピックのルーティングとEvent Brokerインフラストラクチャーの管理を実行できます。また、ArcSight Event BrokerにはEvent Broker Managerが付属しています。これは、Yahoo Kafka Managerバージョンの1つであり、Kafkaサービスの監視と管理を実行できます。

Yahoo Kafka Managerの詳細については、<https://github.com/yahoo/kafka-manager>を参照してください。

Kafkaの監視機能の詳細については、[Apache Kafkaのドキュメントにある監視のセクション](#)を参照してください。

この章では、次の内容について説明します。

- [ArcMCによるEvent Brokerの管理](#)28
- [Event Broker Managerについて](#)28

ArcMCによるEvent Brokerの管理

ArcSight Management Center (ArcMC) を使用すると、トピックやルーティングルールを作成、Event Brokerメトリックの監視、Event Brokerステータスに関する通知の受信を行うことができます。

監視できるEvent Brokerパラメーターには、CPU使用率、メモリ、ディスク使用率、スループット、EPS (1秒あたりのイベント数)、イベント解析エラー、ストリーム処理EPS、ストリーム処理遅延などがあります。

ArcMCによるEvent Brokerの管理の有効化

ArcMCでEvent Brokerの管理を有効にするには、Event BrokerをホストとしてArcMCに追加します。Event Brokerをホストとして追加する手順については、『ArcSight Management Center管理者ガイド』を参照してください。このガイドは、[ArcSightソフトウェアコミュニティ](#)で入手できます。またこのガイドでは、トピック、ルーティングルール、監視対象メトリック、通知を管理する手順についても詳しく説明しています。

Event Broker Managerについて

Event Broker Managerは、クラスター、トピック、パーティションを管理する機能を備えています。次のような監視および管理オプションが提供されています。

- トピック、コンシューマー、オフセット、ブローカーノード、レプリカ配置、パーティション割り当てなど、クラスターの状態を表示および管理します。
- トピックを作成して更新します。
- パーティションを生成してトピックに追加します。
- パーティションを別のブローカーノードに再割り当てします (障害が発生したノードを新しいノードと置換する場合など)。
- ノードが一時的にクラスターから除外された後 (リブートの発生など)、パーティションリーダーを優先ブローカーノードに再割り当てします。
- ブローカーレベルメトリックとトピックレベルメトリックについて、JMXポーリングを管理します。

Event Broker Managerへの接続

Event Broker Managerにアクセスできるのは、Event Brokerサーバーにログインできるユーザーのみです。Event Broker Managerへのアクセスには、Event BrokerノードからローカルなWebブラウザを使用して直接アクセスする方法と、Kafkaが稼働しているKubernetesワーカーノードからSSH転送を使用してアクセスする方法があります。

Event Broker Managerへの接続には、Chrome、Firefox、Internet Explorerなど、ほとんどのブラウザを使用できます。本リリースでサポートされるブラウザのリストについては、[ArcSight Protect 724の製品ドキュメントコミュニティ](#)からダウンロードできるADPサポートマトリクスを参照してください、

Event Broker Managerにアクセスするには

1. Event Brokerノードで`kubectl get service`コマンドを実行し、サービスのリストを取得します。
2. Event Broker Managerサービスの`eb-kafkamgr-svc`を検索し、IPとポート番号を確認します。

Event Brokerサーバーノードから直接接続するには

1. Event Brokerサーバーにログインします。
2. サポートされているブラウザを使用し、Event Broker ManagerのIPとポートで接続します (上記を参照)。

`http://<Event BrokerのIP:ポート>`

接続すると、[Clusters] ページが表示されます。詳細については、「[クラスターの管理](#)」(30ページ)を参照してください。

ローカルマシンから接続するには

1. ローカルシステムで次のコマンドを実行し、SSH転送および接続の設定を行います。

```
ssh -L <Event Brokerのポート>:<Event BrokerのIP:ポート> eb1.example.com
```

2. サポートされているブラウザで、次のURLに接続します。

```
http://<127.0.0.1:ポート>
```

接続すると、[Clusters] ページが表示されます。詳細については、「[クラスターの管理](#)」(30ページ)を参照してください。

クラスターの管理

[Clusters] ページは、Event Broker Managerのホームページです。このページでは、Event Broker Managerのビューでクラスターを変更、無効化、削除できます (クラスター自体が削除されることはありません)。また、クラスターにドリルダウンして詳細情報を表示することも可能です。

場所: Clusters

[<クラスター名>] リンクをクリックします。Event Broker Managerで [Cluster Summary] ページが表示されます。詳細については、「[クラスター情報の表示](#)」(30ページ)を参照してください。

クラスターを編集するには

1. [Modify] をクリックします。Event Broker Managerで [Update Cluster] ページが表示されます。
2. 必要なフィールドを変更し、[Save] をクリックします。

クラスターの編集には高度な知識が必要です。通常はクラスターを編集しないでください。

クラスターを無効にするには

[Disable] をクリックします。クラスターが無効化されると、[Delete] ボタンが表示されます。

クラスターを削除するには

[Delete] をクリックします。

クラスター情報の表示

[Summary] ページには、クラスター内のZooKeeperプロセスが表示されます。ここからトピックやブローカーノードにドリルダウンして、詳細情報を表示することができます。

場所: Clusters > <クラスター名> > Summary

The screenshot shows the 'Summary' page for an Event Broker cluster. At the top, there is a navigation bar with 'Event Broker' and 'event-broker' highlighted, followed by 'Cluster', 'Brokers', 'Topic', 'Preferred Replica Election', 'Reassign Partitions', and 'Consumers'. Below this is a breadcrumb trail: 'Clusters / event-broker / Summary'. The main content is divided into two sections: 'Cluster Information' and 'Cluster Summary'. 'Cluster Information' includes 'Zookeepers' (with three placeholder links) and 'Version' (0.10.0.0). 'Cluster Summary' is a table with two columns: 'Topics' with a value of 8 and 'Brokers' with a value of 3. Below the table, there are two boxes: 'トピックのリンク' (Topic Link) with an arrow pointing to the 'Topics' cell, and 'ブローカーのリンク' (Broker Link) with an arrow pointing to the 'Brokers' cell.

クラスター情報を表示するには

- クラスターが開いていない場合は、ナビゲーションバーの **[Cluster] > [List]** をクリックします。次に、**[<クラスター名>]** リンクをクリックします。
- クラスターがすでに開いている場合は、**[Clusters] > [<クラスター名>] > [Summary]** をクリックします。

クラスター内のトピックを表示または編集するには

[Topics] リンクをクリックします。詳細については、「[トピックの管理](#)」(33ページ)を参照してください。

クラスター内のブローカーノードを表示または編集するには

[Brokers] リンクをクリックします。詳細については、「[ブローカーの管理](#)」(31ページ)を参照してください。

ブローカーの管理

[Brokers] ページには、全ブローカーノードに関する概要情報が表示されます。ここから各ブローカーにドリルダウンして、詳細情報を表示することができます。

注: ArcMCでは、「ブローカー」という用語は「Event Brokerノード」を指します。どちらの用語も、Kafkaを実行する単一のノードを意味します。

場所: Clusters > <クラスター名> > Brokers

クラスター内のブローカーノードを表示するには

ナビゲーションバーの [Brokers] をクリックします。[Brokers] ページが開きます。

特定のブローカーに関する情報を表示するには

ブローカーの [<ID>] リンクをクリックします。<ブローカー名>のIDが開きます。詳細については、「[ブローカーの詳細の表示](#)」(32ページ)を参照してください。

ブローカーの詳細の表示

ブローカーの詳細情報は、[<ブローカー名>] 詳細ページで確認できます。

場所: Clusters > <クラスター名> > Brokers > <ブローカー名>

特定のブローカーに関する情報を表示するには

1. ナビゲーションバーの [Brokers] をクリックします。
2. [<ブローカー名>] リンクをクリックします。[<トピック名>] ページが開きます。

このページには、次の情報が表示されます。

- 「[Summary](#)」(33ページ)
- 「[Metrics](#)」(33ページ)
- 「[Messages count](#)」(33ページ)
- 「[Per Topic Detail](#)」(33ページ)

Summary

[Summary] セクションには、ブローカーの概要 (トピック数 やパーティション数など) が表示されます。

Metrics

[Metrics] セクションには、データフローに関する情報が表示されます。

Messages count

[Messages count] セクションには、メッセージビューチャートが表示されます。

Per Topic Detail

[Per Topic Detail] セクションには、トピックのレプリケーションとパーティションに関する情報が表示されます。各トピックにドリルダウンして、詳細情報を表示することが可能です。

特定のトピックに関する情報を表示するには

[Per Topic Details] セクションで [トピック名] リンクをクリックします。詳細については、「[トピックの詳細の表示](#)」(36ページ) を参照してください。

トピックの管理

[Topics] ページでは、パーティションの割り当てを実行または生成したり、新規パーティションを追加したり、各トピックにドリルダウンして詳細情報を表示したりすることができます。

場所: Clusters > <クラスター名> > Topics

Topic	# Partitions	# Brokers	Brokers Spread %	Brokers Skew %	# Replicas	Under Replicated %	Producer Message/Sec
7864-connector	10	3	100	0	3	0	0.00
__consumer_offsets	50	3	100	0	2	0	0.00
firewall	10	3	100	0	3	0	0.00
syslog-topic	30	3	100	0	2	0	0.00

注: 次のトピックはデフォルトでインストールされます。

- `__consumer_offsets`
- `_schemas`
- `eb-internal-datastore`
- `eb-internal-stream-processor-metrics`

これらはEvent Brokerが内部的に使用するトピックなので、変更しないでください。

クラスター内のトピックを管理するには

ナビゲーションバーの [Topic] > [List] をクリックします。

トピックに関する情報を表示するには

[<トピック名>] リンクをクリックします。 [<トピック名>] ページが開き、トピックのサマリー、メトリック、コンシューマー、パーティションが表示されます。詳細については、「[トピックの詳細の表示 \(36ページ\)](#)」を参照してください。

パーティションの割り当てを生成するには

1. **[Generate Partition Assignments]** をクリックします。
2. 再割り当てを行うトピックとブローカーノードを選択します。
3. **[Generate Partition Assignments]** をクリックします。

生成したパーティションを割り当てるには

1. **[Run Partition Assignments]** をクリックします。
2. 再割り当てするトピックを選択します。
3. **[Run Partition Assignments]** をクリックします。

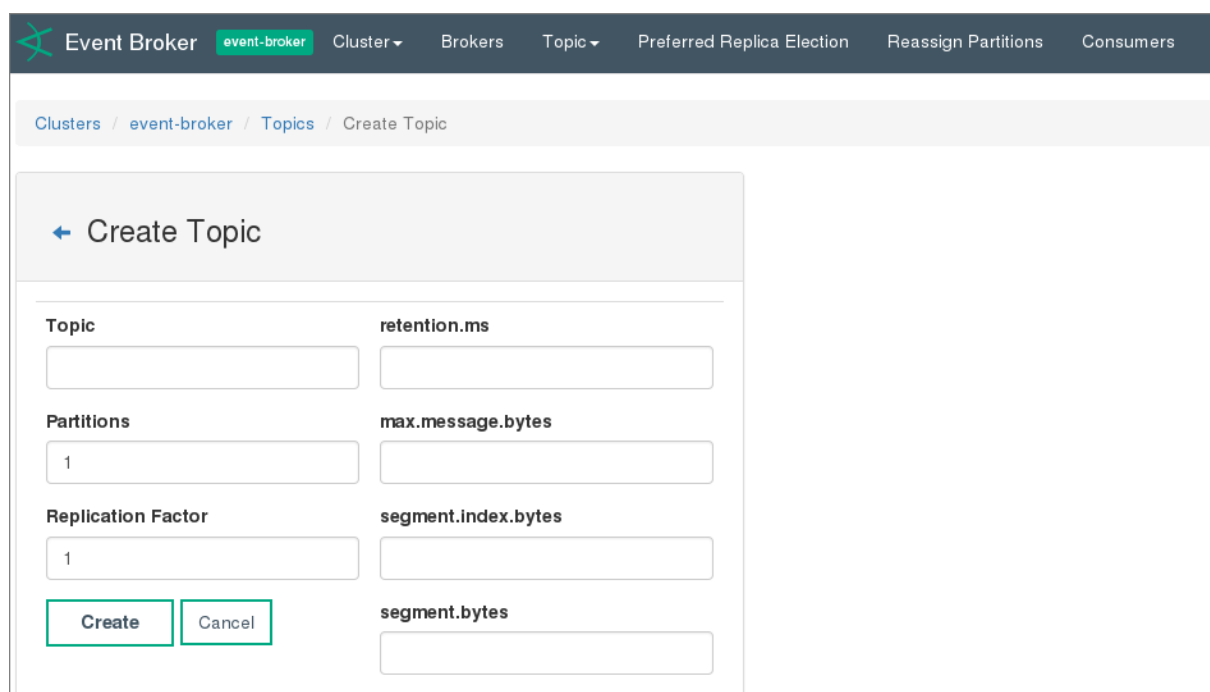
パーティションを追加するには

1. **[Add Partition]** をクリックします。
2. 新しいパーティション数を入力します。
3. トピックとブローカーノードを選択します。
4. **[Add Partitions]** をクリックします。

トピックの作成

トピックの新規作成は、**[Create Topic]** ページで行います。

場所: Clusters > <クラスター名> > Topics > Create Topic



The screenshot shows the 'Create Topic' page in the Event Broker management interface. The page has a dark header with navigation links: Event Broker, event-broker, Cluster, Brokers, Topic, Preferred Replica Election, Reassign Partitions, and Consumers. Below the header is a breadcrumb trail: Clusters / event-broker / Topics / Create Topic. The main content area is titled 'Create Topic' and contains a form with the following fields:

Topic	retention.ms
<input type="text"/>	<input type="text"/>
Partitions	max.message.bytes
<input type="text" value="1"/>	<input type="text"/>
Replication Factor	segment.index.bytes
<input type="text" value="1"/>	<input type="text"/>
<input type="button" value="Create"/> <input type="button" value="Cancel"/>	segment.bytes
	<input type="text"/>

注: いったん作成したトピックは削除できません。

[Add Topic] ページを開くには

ナビゲーションバーの **[Topic]** > **[Create]** をクリックします。

新しいトピックを作成するには

必要な情報をフィールドに入力し、**[Create]** をクリックします。

トピックの詳細の表示

トピックの詳細は、[<トピック名>] 詳細ページで確認できます。このページには、サマリー、メトリック、コンシューマー、パーティションなどの情報が表示されます。

場所: Clusters > <クラスター名> > Topics > <トピック名>

特定のトピックに関する情報を表示するには

1. ナビゲーションバーの **[Topic]** > **[List]** をクリックします。
 2. [<トピック名>] リンクをクリックします。 [<トピック名>] ページが開きます。
- このページには、次の情報が表示されます。

- 「Topic Summary」(37ページ)
- 「Metrics」(38ページ)
- 「Operations」(38ページ)
- 「Partitions by Broker」(39ページ)
- 「Consumers consuming from this topic」(40ページ)
- 「Partition Information」(40ページ)

Topic Summary

[Topic Summary] セクションには、トピックのレプリカ、パーティション、ブローカーノードなどの情報が表示されます。

Topic Summary	
Replication	3
Number of Partitions	10
Sum of partition offsets	0
Total number of Brokers	3
Number of Brokers for Topic	3
Preferred Replicas %	100
Brokers Skewed %	0
Brokers Spread %	100
Under-replicated %	0
Config	Value
cleanup.policy	delete

Metrics

[Metrics] セクションには、データフローに関する情報が表示されます。

Metrics				
Rate	Mean	1 min	5 min	15 min
Messages in /sec	23.14	28.80	28.80	28.80
Bytes in /sec	2.1k	2.6k	2.6k	2.6k
Bytes out /sec	6.4k	10k	10k	10k
Bytes rejected /sec	0.00	0.00	0.00	0.00
Failed fetch request /sec	0.00	0.00	0.00	0.00
Failed produce request /sec	0.00	0.00	0.00	0.00

Operations

[Operations] セクションでは、パーティションの再割り当て、パーティションの割り当ての生成、パーティションの追加、トピック設定の更新、トピックをブローカーノードに手動で割り当てる操作を実行できます。

Operations		
Reassign Partitions	Generate Partition Assignments	
Add Partitions	Update Config	Manual Partition Assignments

パーティションを再割り当てするには

[Reassign Partitions] をクリックします。

パーティションの割り当てを生成するには

1. [Generate Partition Assignments] をクリックします。
2. 再割り当てを行うトピックとブローカーノードを選択します。

3. **[Generate Partition Assignments]** をクリックします。

パーティションを追加するには

1. **[Add Partitions]** をクリックします。
2. 新しいパーティション数を入力します。
3. トピックとブローカーノードを選択します。
4. **[Add Partitions]** をクリックします。

トピックの設定を更新するには

1. **[Update Config]** をクリックします。
2. 設定フィールドを編集します。
3. **[Update Config]** をクリックします。

パーティションの割り当てを指定するには

1. **[Manual Partition Assignment]** をクリックします。
2. 割り当てを選択します。
3. **[Save Partition Assignment]** をクリックします。

Partitions by Broker

[Partitions by Broker] セクションには、トピックのパーティション情報が表示されます。ドリルダウンして各ブローカーの詳細情報を表示することもできます。

Partitions by Broker			
Broker	# of Partitions	Partitions	Skewed?
1 ← ブローカーのリンク	10	(0,1,2,3,4,5,6,7,8,9)	false
2	10	(0,1,2,3,4,5,6,7,8,9)	false
3	10	(0,1,2,3,4,5,6,7,8,9)	false

ブローカーの詳細情報を表示するには

ブローカーのリンクをクリックします。[Topic Summary] ページが開き、トピックの遅延、パーティション、コンシューマーオフセットなどの情報が表示されます。

Kafka Managerでは、バイナリ (ESM) トピックとCEF (InvestigateまたはLogger) トピックで異なるオフセット値が表示されます。CEFトピックの場合、オフセット値は、トピック経由で渡され

たイベント数に関連しています。メッセージはそれぞれ個別のイベントです。一方、バイナリトピックにはこのような関連はありません。

Consumers consuming from this topic

[**Consumers consuming from this topic**] セクションでは、各コンシューマーにドリルダウンして詳細情報を表示できます。

新しいコンシューマーの表示には、若干時間がかかる場合があります。正しいデータが表示されるまで、しばらくお待ちください。

コンシューマーの詳細情報を表示するには

[<トピック名>] リンクをクリックします。[Topic Summary] ページが開き、トピックの遅延、パーティション、コンシューマーオフセットなどの情報が表示されます。

Partition Information

[**Partition Information**] セクションには、トピックのパーティションに関する情報が表示されます。各リーダーにドリルダウンして詳細情報を表示できます。

リーダーの詳細情報を表示するには

リーダーのリンクをクリックします。<ブローカー名>のIDページが開き、ブローカーのサマリー、メトリック、メッセージ件数、トピックの詳細情報が表示されます。詳細については、「[ブローカーの詳細の表示](#)」(32ページ)を参照してください。

コンシューマーの管理

[**Consumers**] ページには、コンシューマーのリストが表示され、コンシューマーのタイプと使用するトピックを確認できます。コンシューマーとトピックにドリルダウンして、詳細情報を表示することもできます。

場所: Clusters > <クラスター名> > Consumers

Consumer	Type	Topics it consumes from
firewall-consumer	KF	firewall : (100% coverage, 0 lag)
console-consumer-6395	ZK	console : (100% coverage, 22638 lag)
OS-consumer	KF	RHEL72 : (100% coverage, 0 lag) WIN : (100% coverage, 1041 lag)
systems	KF	7816-topic : (100% coverage, 0 lag) 6418-topic : (100% coverage, 985 lag)

クラスター内のコンシューマーを表示または編集するには

ナビゲーションバーの [Consumers] をクリックします。

特定のコンシューマーの詳細情報を表示するには

[<コンシューマー名>] リンクをクリックします。 [<コンシューマー名>] ページが開き、コンシューマーの詳細情報が表示されます。ドリルダウンすると、詳細情報が表示されます。

コンシューマーが使用するトピックの詳細情報を表示するには

[<トピック名>] リンクをクリックします。 [<トピック名>] ページが開き、トピックの詳細情報が表示されます。ドリルダウンすると、詳細情報が表示されます。

コンシューマーの詳細の表示

[<コンシューマー名>] 詳細ページには、コンシューマーに関する情報が表示されます。コンシューマーが使用するトピックにドリルダウンすることも可能です。

場所: Clusters > <クラスター名> > Consumer > <コンシューマー名>

コンシューマーの情報を表示するには

1. [Clusters] > [<クラスター名>] > [Consumer] をクリックします。
2. [<コンシューマー名>] をクリックします。

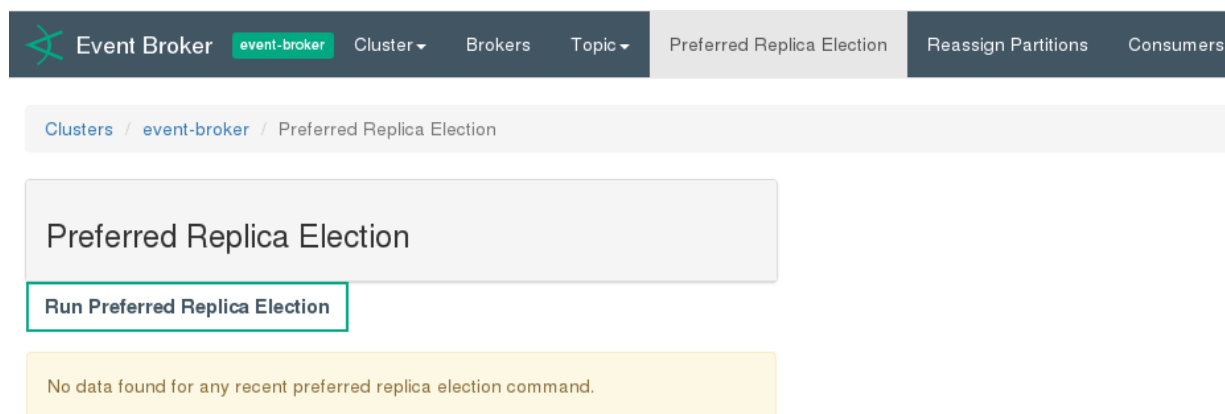
コンシューマーが使用するトピックに関する情報を表示するには

1. [**<トピック名>**] をクリックします。[Consumed Topic Information] ページが開き、トピックに関する情報が表示されます。トピック名をクリックすると、詳細情報が表示されます。

優先レプリカの管理

各クラスターのレプリカの更新は、[Preferred Replica Election] ページで行います。

場所: Clusters > <クラスター名> > Preferred Replica Election



[Preferred Replica Election] ページを開くには

ナビゲーションバーの [Preferred Replica Election] をクリックします。

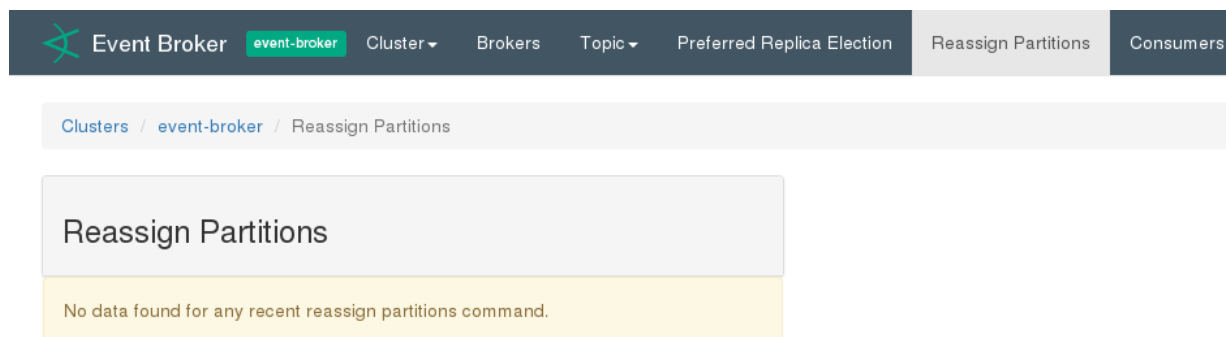
トピックで [Preferred Replica Election] を実行するには

[Run Preferred Replica Election] をクリックします。

パーティションの管理

クラスターのパーティションの再割り当ては、[Reassign Partitions] ページで行います。

場所: Clusters > <クラスター名> > Reassign Partitions



[Reassign Partitions] ページを開くには
ナビゲーションバーの **[Reassign Partitions]** をクリックします。

トピックのパーティションを再割り当てするには
[Reassign Partitions] をクリックします。

第6章: トラブルシューティング

Event Brokerの問題解決に役立つトラブルシューティングのヒントをご紹介します。

この章では、次の内容について説明します。

- Event Brokerクラスターの稼働状態の確認 44
- Event Brokerでよく発生する問題の診断 45
- Event Brokerのパフォーマンスチューニング 48

Event Brokerクラスターの稼働状態の確認

各コンテナの稼働状態の確認: `kubectl get pods -o wide`を実行し、Podとそのステータスを一覧表示します。

各コンテナのKubernetesログの表示: `kubectl logs`を実行します。

```
# kubectl logs [POD ID/名前]
```

```
# kubectl logs [WebサービスのPOD ID/名前] -c atlas-web-service
```

システム内のデータフローの確認: 次のいずれかをチェックします。

- ArcMCでEPSグラフを確認します。これにより、イベントがストリームプロセッサを通過しているかどうかを確認できます (ルーティングと変換)。
- VerticaサーバーでKafka Schedulerのステータスをチェックし、イベント数と拒否された数を確認します。時間の経過とともにイベント数は増加しているはずです。

```
# ./install-vertica/kafka_scheduler status
```

- Verticaで、Kafka Managerオフセットを `Select Count(*)` でチェックします。時間の経過とともにカウントは増加しているはずです (たとえば、`SELECT COUNT (*) FROM investigation.events`)。
- すべてのトピック: Event Broker Manager内の各トピックのオフセットをチェックします。時間の経過とともに値が増加しているはずです。

WebサービスAPIの稼働状態の確認:

- Webサービスコンテナのログをチェックします (上記コマンドを参照)。
- ポートのバインドを確認します。

```
# netstat -lntp | grep 38080
```

- Vertica Schedulerが稼働中であることを確認します。
- Kafka Schedulerのステータスをチェックします。

```
# watch ./root/install-vertica/kafka_scheduler status
```

- ステータス出力で、オフセットの値が増加していることを確認します。増加していない場合、Avroトピックにデータがない可能性があります。データがある場合は、問題が発生している可能性があります。
- トピックパーティションの数と分散状態を確認します。
- 設定したパーティション数が、想定される値と一致することを確認します。
- Event Broker Managerで、トピックのパーティション数またはレプリケーション係数を確認します。

Event Brokerでよく発生する問題の診断

Event Brokerでよく発生する問題を診断する方法を説明します。

Event Brokerクラスターがダウンする

Event Brokerクラスターの動作に必要なノード数は、レプリケーション係数によって異なります。レプリケーション係数を1に設定することはお勧めしませんが、この場合、EBクラスター内のすべてのKafkaノードが稼働状態でないと、EBクラスターは正常に機能しません。一般的に、レプリケーション係数がNの場合、N-1件までのサーバー障害に対処できるトランスが実現され、ログにコミットされたレコードが失われることはありません。

Podの起動順序

展開の完了後、Podは次の順序で起動するように設定されます (ダウンストリームPodは、依存関係が確立されるまでは起動しません)。

1. クラスター内のZooKeeper Podのクォーラムが稼働状態になる必要があります (3つのうち2つ、または5つのうち3つ)。ZooKeeperの総数は奇数である必要があります。
2. Kafka Podがすべて稼働状態になる必要があります。
3. スキーマレジストリPodが稼働状態になる必要があります。
4. ブートストラップWebサービス、Event Broker Manager。
5. 変換ストリームプロセッサ、ルーティングストリームプロセッサ。

ZooKeeperのクエリを実行できない

この問題は、`kubectl get pods`コマンドを実行してPodのステータスを取得する際に発生します。ダウンストリームPod (Podの起動順序で定義) が稼働状態を維持できず、ステータスとして「CrashLoop」タイプのエラーが報告されます。

- ZooKeeper Podが稼働していることを確認します。
- ZooKeeper Podのステータスが保留の場合、ノードにラベルがない可能性があります (zk=yes)。`kubectl get nodes -L=zk`コマンドを実行し、ノードにラベルがあることを確認してください。
- `installer.properties`の`predeploy.eb.zookeeper.count`属性で、ZooKeeperの数が奇数に設定されていることを確認します。
- `kubectl logs <Pod名>`を使用して、ZooKeeper Podログにエラーが記録されていないかチェックします。

ZooKeeperログでよく報告されるエラーと警告

- **クォーラム例外:** リーダーを選択できません。このタイプのエラーが記録されている場合、上記の条件をチェックしてください。
- **ソケットエラー:** 接続数が多すぎる場合に発生します。`kubectl delete <pod名>`を実行し、Podを再起動してください。Podは自動的に再作成されます。

Kafkaログでよく報告されるエラーと警告

IDを登録できない: ブローカーノードでIDを登録できなくなることがあります。これは、同じIDを使った複数のブローカーノードが存在することが原因です。これはほとんど発生しない問題であり、クラスターでノードの追加や削除を行う際に、クラスターが正しく定義されていない場合に発生することがあります。Kafkaブローカーを実行している各システムに接続し、`/opt/arcsight/k8s-hostpath-volume/eb/kafka/meta.properties`でそれぞれの`broker.id`値をチェックしてください。Kafkaノードの`broker.id`には、一意の値を定義する必要があります。

SSL接続エラー: Kafkaとコンシューマーまたはプロデューサー間の接続に問題が発生すると、この警告が報告されます。

他のブローカーと通信できない: ホスト名が正しく設定されていない可能性があります。ノードがリバースルックアップを実行できないか、DNSが正しく設定されていない可能性があります。

最初の展開でEvent Brokerのデフォルトピックが作成されていない: この場合、ブートストラップWebサービスのログに500の応答コード (スキーマレジストリからの応答) が記録

され、トピックが作成されません。Event Brokerコンテナの展開を解除してから、再度展開を行ってください。

1つまたは複数のコネクターがKafkaにデータを送信できない: 次の項目をチェックしてください。

- コネクターの接続が正しく設定されている。
- コネクターとEvent Brokerの暗号化モード (TLS、TLS+FIPS、TLS+CA、TLS+FIPS+CA) が同じ。
- システム上のKafkaポートへの接続が可能であり、ネットワーク障害は発生していない。

接続時に、証明書の取得でエラーが発生する: データパイプライン内の全システムの時刻が同期していることを確認します。

Kafka Podがダウンしているかどうかをチェックします。コネクターの設定でブローカーアドレスを1つのみ指定した場合、そのブローカーがダウン状態になっていないかチェックします。ブローカーが複数存在する場合は、すべてカンマ区切りのリストとしてコネクターで設定する必要があります。

• レプリケーション係数が1でKafkaブローカーがダウンしている場合、データはEvent Brokerに送信されません。ブローカーの問題を修正し、動作を再開させます。一般的に、トピックの設定でレプリケーション係数を2以上に指定することで、この問題を回避できます。

Kafkaの再同期に時間がかかっている: これによってイベントスループットが低速になる可能性はありますが、イベントフローが停止することはありません。

VerticaがKafkaからイベントを読み出せない: Event Brokerが稼働状態であることを確認したら、次の項目をチェックします。

- 新規セットアップの場合: Kafka Schedulerで、通信ポートとしてKafkaポート9092が設定されていることを確認します。また、ネットワーク接続もチェックします。
- 既存のセットアップの場合 (Verticaコンシューマー): オフセットが認識されていない可能性があります。この場合、Kafka Schedulerはトピック内のメッセージのオフセットIDを認識できなくなります。原因としては、Kafka Schedulerがトピックからの読み出しを突然停止して、その後再起動されたことが考えられます。

解決策: kafka_scheduler deleteコマンドを実行し、メタデータを削除します。コマンドの実行後、すぐにkafka_scheduler createコマンドを実行して、Schedulerをセットアップします。

• 既存のセットアップの場合: コンシューマーの接続先のトピックを含むすべてのブローカーを設定している状態で、そのコンシューマー用に設定されているブローカーがダウンしています。

EBコンポーネントがクラッシュする: 次の項目をチェックしてください。

- コンテナの起動順序 (上記を参照)。起動していない依存Podやクラッシュしている依存Podがないか。
- JVMが必要とするメモリ容量がシステムに実装されているか。
- 空きソケットの数。

Event Broker EPSが想定値よりも小さい: CPU、メモリ、ディスク容量など、Event Brokerノードのリソースに制限がないかチェックします。また、ArcMCで使用率をチェックします。

ネットワークボトルネック: ストリームプロセッサが変換処理に対応しきれていないか、リソースに制限が発生しています。ArcMCで確認すると、ストリームプロセッサのメトリックがコネクタのEPSよりも小さくなっています。リソース、メモリ、CPUが十分に提供されているか確認してください。

ネットワーク障害が続く: TCP/IPリソースの管理に関する問題です。TIME_WAITは、ノードが接続の終了を完了するのにかかる時間と、古い接続を強制終了するまでの時間を示すパラメーターです。デフォルト値よりも小さい値に設定してください。

/etc/sysctl.confファイルを編集し、末尾に以下の行を追加します (または既存の値を編集します)。

TIME_WAITの秒数を減らします。

```
net.ipv4.tcp_fin_timeout = 10
```

TIME_WAITソケットのリサイクルと再利用までの時間を短縮します。

```
net.ipv4.tcp_tw_recycle = 1
```

```
net.ipv4.tcp_tw_reuse = 1
```

ファイルの編集が完了したら、次のコマンドを実行します。

```
$ sysctl --system
```

Event Brokerのパフォーマンスチューニング

Event Brokerのパフォーマンスを向上するヒントをご紹介します。

ストリームプロセッサEPSの追加

ArcSightインストーラーの設定UIでストリームプロセッサインスタンスを追加することにより、Stream Processor EPSを追加することが可能です。ArcSightインストーラーの設定UIを使って行った設定内容は、変換ストリームプロセッサ (c2av) にのみ適用されません。ルーティングストリームプロセッサの設定は変更されません。ルーティングストリームプロセッサのストリーム数は変更できません。

この値を変更する際、Event Brokerの再展開は必要ありません。ただし、変更によってPod数が増える点に注意してください。Pod数の違いは、`kubectl get pods`コマンドを実行すると確認できます。

Kafkaの保存サイズ/期間の増加

Event Brokerコンテナの展開後、Event Broker Managerから、トピックの保存サイズ/期間を変更できます。変更内容はすぐに有効になります。イベントがトピックへを通過している状態でも変更は可能です。

展開の前にデフォルト値を変更するには、`installer.properties`ファイルを変更します。

Webサービスの管理者パスワードの変更

展開の前に、`installer.properties file`に格納されているWebサービスの管理者パスワードが変更されます。

新しいワーカーノードの追加

新しいワーカーノードを追加するには、新しいノードにラベルを割り当てます (既存のラベルを削除または新しいラベルでオーバーライド)。古いノードからラベルを削除します。Kubernetesにより、新規ノード上でKafkaが起動します。次に、新規ノードでパーティションが再割り当てされます。データコピーが開始されます。この処理には若干時間がかかることがあります。

付録A: installer.propertiesファイル

installer.propertiesは、Event Brokerのインストールで重要な設定を管理するファイルです。ここでは、設定値について詳しく説明します。

installer.propertiesファイルを編集するには、テキストエディターでファイルを開き、必要な変更を行います。

設定の変更内容を有効にするには、Event Brokerの展開を解除してから、再度展開を行う必要があります。

設定	説明
<pre>## All Event Broker components will use FIPS-certified encryption algorithms</pre>	
<pre>predeploy.eb.init.fips=false</pre>	FIPSを有効にします。展開後には変更しないことをお勧めします。展開を解除してから、再度展開を行ってください。
<pre>## Event Broker Kafka will use TLS Client Authentication to verify client connections</pre>	
<pre>predeploy.eb.init.client-auth=false</pre>	TLS-CAを有効にします。展開後には変更しないことをお勧めします。展開を解除してから、再度展開を行ってください。
<pre>## Number of partitions for Event Broker default topics in Kafka</pre>	

設定	説明
<pre>predeploy.eb.init.noOfTopicPartitions=5</pre>	<p>デフォルト値。新規作成したトピックにのみ適用されます (Event Broker Managerで、既存のトピックに新しいパーティションを追加します)。</p>
<pre>## Replication factor for Event Broker default topics in kafka</pre>	
<pre>predeploy.eb.init.topicReplicationFactor=2</pre>	<p>デフォルト値。新規作成したトピックにのみ適用されます (レプリケーション係数を変更するには、古いトピックを削除する必要があります)。</p>
<pre>## kafka log retention size</pre>	
<pre>predeploy.eb.init.kafkaRetentionBytes=10737418240</pre>	<p>各トピックのパーティションごとのデフォルト値。非常に小さな値であり、ユーザーの調整が必ず必要になります。ユーザーのために計算を行ってください。EBで継続時間または保持バイト数のいずれかに達した時点で削除が発生します。</p>
<pre>## kafka log retention size for the vertica Avro topic.This is uncompressed and requires more space to hold events for the same duration.</pre>	

設定	説明
predeploy.eb.init.kafkaRetentionBytesForVertica=10737418240	各トピックのパーティションごとのデフォルト値。非常に小さな値であり、ユーザーの調整が必ず必要になります。ユーザーのために計算を行ってください。データは圧縮されないため、他のトピックよりも大きな領域が必要になる場合があります。他のトピックと同じレベルのデータ保持を設定するには、他のトピックよりも非常に大きな領域(7倍以上)が必要になる場合があります。EBで継続時間または保持バイト数のいずれかに達した時点で削除が発生します。
## kafka log retention duration	

設定	説明
<pre>predeploy.eb.init.kafkaRetentionHours=672</pre>	<p>環境に応じて設定します。ユーザーのために計算を行ってください。ArcMCで作成したトピックを含め、すべてのトピックに適用されます。EBで継続時間または保持バイト数のいずれかに達した時点で削除が発生します。</p>
<pre>## kafka inter-broker protocol version</pre>	
<pre>predeploy.inter.broker.protocol.version=0.10.1.0</pre>	<p>アップグレード専用の設定です。</p>
<pre>## The message format version the broker will use to append messages to the logs.</pre>	
<pre>predeploy.log.message.format.version=0.10.1.0</pre>	<p>アップグレード専用の設定です。</p>
<pre>## Size of kafka and ZooKeeper pet-sets</pre>	
<pre>predeploy.eb.kafka.count=3</pre>	<p>Kafkaで使用するクラスターサイズを指定します。K8sでkafka=yesというラベルが付いたワーカーノードの数と同じ数値を指定してください。1ホストに対して1ノードです。</p>

設定	説明
predeploy.eb.zookeeper.count=3	クラスターサイズを指定します。最大値は7です。K8sでzk=yesというラベルが付いたワーカーノードの数と同じ数値を指定してください。必ず奇数を指定します。
## Host path to store data persistently	
predeploy.eb.kafka.path=/opt/arcsight/k8s-hostpath-volume/eb/kafka	大きなサイズになります。サイジングのガイドラインを参照してください。設定が存在しない場合は作成されます。
predeploy.eb.zookeeper.path=/opt/arcsight/k8s-hostpath-volume/eb/zookeeper	設定が存在しない場合は作成されます。
## ArcMC hostname	
predeploy.eb.arcmc.hosts=localhost:443	無視してください。
## The endpoint identification algorithm to validate the server hostname using the server certificate.	
predeploy.ssl.endpoint.identification.algorithm=https	リバーズDNSが正しく設定されていない場合、空白であることがあります。Kafka接続に対して、Kafkaのホスト名が検証されます。
## The number of stream threads	

設定	説明
predeploy.stream.num.threads=6	パフォーマンスに問題がある場合を除き、変更しないでください。
## Log level for each EB container	
predeploy.level=info	サポート設定のみ。
predeploy.kafka.log.level=\${predeploy.level}	
predeploy.zookeeper.log.level=\${predeploy.level}	
predeploy.schema.log.level=\${predeploy.level}	
predeploy.web.service.log.level=\${predeploy.level}	
predeploy.c2av.stream.processor.log.level=\${predeploy.level}	
predeploy.eventbroker.routing.processor.log.level=\${predeploy.level}	
## Host path directory for ArcMC certificates	
predeploy.arcmc.certs.path=/opt/arcsight/k8s-hostpath-volume/eb/arcmmcerts	

設定	説明
##truncate fields in c2av	
predeploy.c2av.field.truncate=false	<p>trueの場合、長すぎるフィールドは SuperSchema に合わせて切り捨てられます。SuperSchema の詳細については、『ArcSight Management Center 管理者ガイド』を参照してください。</p> <p>false (デフォルト)の場合、長いフィールド内のデータは検索できなくなります。</p>

用語集

A - Z

Apache Avro

データをシリアル化するシステムです。Avroは、非常に効率的な方法でイベントを保存します。

Apache Flume

大量のログデータの収集、集約、移動を効率化するサービスです。

Apache Hadoop

大量のデータセットをコンピュータークラスターで分散処理するためのソフトウェアフレームワークです。単一サーバーから数千台のマシンまで対応できる優れた拡張性を備え、それぞれローカルに演算処理機能とストレージを実装しています。Hadoopは、Event Brokerコンシューマーとして設定可能です。

Apache Kafka

オープンソースの分散パブリッシュ/サブスクライプ型のメッセージングシステムであり、Event Brokerの一部としてインストールされます。

Apache ZooKeeper

設定情報の管理、名前付け、分散型の同期、グループサービスの提供を行う集中管理サービスです。ZooKeeperは、冗長サービスによって優れた可用性をサポートするアーキテクチャーを採用しています。ZooKeeperはEvent Brokerの一部としてインストールされ、Kafkaクラスターと連携します。

ArcMC

ArcSight Management Center (ArcMC) は、ArcSightの製品です。

CEF

Common Event Format (共通イベントフォーマット) の略。拡張性に優れたテキストベース

の高性能フォーマットであり、複数のデバイスタイプを非常に簡単な方法でサポートします。さまざまなメッセージ構文に、単一のArcSight Enterprise Security Manager (ESM) 正規化で対応します。特に、CEFは標準ヘッダーとさまざまな拡張要素で構成されるログレコード用の構文を定義し、キー値のペアとしてフォーマットします。このフォーマットには、最も関連性の高いイベント情報が格納されており、コンシューマーがイベントを簡単に解析および使用できるようになっています。

ESM

Enterprise Service Management (ESM) は、ArcSightの製品です。

Event Broker Manager

Event Brokerに付属する管理ツールです。Yahoo Kafka Managerと同等の機能を備えています。

FIPS

Federal Information Processing Standards (連邦情報処理規格) の略。非軍事政府機関と政府委託業者が使用するコンピューターシステムについて、米国政府が策定した標準規格です。特にFIPS PUB 140-2は、暗号化モジュールの承認に使用される、米国政府のコンピューターセキュリティ標準規格です。

HDFS

Hadoop Distributed File System (Hadoop分散ファイルシステム) の略。Javaベースのファイルシステムであり、拡張性と信頼性に優れたデータストレージです。コモディティサーバーで構成される大規模クラスター向けに設計されています。

installer.properties

さまざまなEvent Broker設定を管理するプロパティファイル。

Investigate

Investigateは、ArcSightの製品です。

Logger

ArcSightの製品の1つであり、イベントデータを取得して、検索や分析が行えるように保存します。Loggerは、Event Brokerコンシューマーとして設定可能です。詳細については、『Logger管理者ガイド』を参照してください。

SmartConnector

ArcSight製品の1つであり、ネットワーク上のオブジェクトからイベントデータを収集します。データの正規化には、値(重要度、優先度、タイムゾーンなど)を共通フォーマットに正規化する方法と、データ構造を共通スキーマに正規化する方法の2種類があります。SmartConnectorは、Event Brokerプロデューサーとして設定可能です。詳細については、『SmartConnectorユーザーガイド』を参照してください。

SOC

Security Operations Centerの略。

TLS

Transport Layer Security (トランスポートレイヤーセキュリティ)の略。Event Brokerではデフォルトで有効化されます。

Vertica

HPE Verticaは、高度な機能を備えたSQLデータベースアナリティクスポートフォリオです。Hadoop上でSQLを実行し、スケーラブルな予測的アナリティクスや、組み込み解析機能で構成される包括的なライブラリの活用を可能にします。

Yahoo Kafka Manager

Apache Kafkaを管理するオープンソースツール。Event Brokerには、Yahoo Kafka Managerが付属しています。

あ

オフセット

パーティション内のメッセージの場所を識別するシーケンシャルな番号。パーティションオフ

セットの合計は、トピック内のイベント総数と一致します。

か

クォーラム

特定のパーティションについて、同期状態にあるレプリカのセット。レプリカとリーダーが同じ状態にあると、レプリカは同期状態と見なされます。リーダーはレプリカの過半数がデータを取得するまで待機し、その後データを「コミット済み」と見なします。リーダーに障害が発生すると、フォロワーの過半数によって新たなリーダーが選出されます。レプリカの数が多い場合、過半数を確保することが可能になります。クォーラム内のレプリカであれば、どのレプリカもリーダーになることができます。その結果、障害が発生した場合でも、プロデューサーはメッセージのパブリッシュを継続し、コンシューマーは正しいメッセージの取得を継続できます。

クラスター

ブローカーのグループであり、連携することでスループットと耐障害性を向上します。

コンシューマー

1つまたは複数のトピックをサブスクライブし、メッセージフィードを処理するプロセスです。

コンシューマーオフセット

コンシューマーが使用するパーティション内の読み取り位置。

コンシューマーグループ

複数のコンシューマーを論理的にまとめたグループです。グループ内でメッセージを処理するコンシューマーは1つのみです。

さ

サブスクライブ

トピックにパブリッシュされたイベントをコンシューマーが取得するアクション。アクティブなサブスクライバーは、パブリッシュされたイベントを取得

できます。また、コンシューマーグループが初めて認識された時点で、イベントを「最初から」リクエストすることができます。それ以降は、グループのコンシューマーが前回イベントを取得した時点からのイベントを取得します。

シンク

Apache Flumeでは、シンクはターゲットとなるストレージにイベントを送信します。

スケジューラー

Kafka向けにジョブプロセスの管理と追跡を行います。

ストリームプロセッサ

受信したイベントを処理し、CEFからAVROへデータ形式を変換するEvent Brokerの機能です。c2avとも呼ばれます。

ソース

Apache Flumeでは、ソースはイベントをFlumeに送信します。

た

チャネル

Apache Flumeでは、シンクがイベントの書き込みを完了するまで、イベントを格納しておくバッファを指します。

デバイスグループ

Loggerでは、デバイスは名前付きソースIPアドレスを指します。デバイスグループは、ストレージルールに関連付けることができます。ストレージルールでは、特定のデバイスからのイベントを格納するストレージグループが定義されています。詳細については、Loggerのドキュメントを参照してください。

トピック

同じカテゴリに関連するメッセージのフィード。

な

ノード

Kafkaインスタンスが稼働するマシン。

は

パーティション

トピックのセグメント。1つのトピックに、1つまたは複数のパーティションを作成できます。パーティション数によって、コンシューマーグループ内のコンシューマーの最大数が決まります。

パブリッシュ

Event Brokerにトピックを送信するアクション。プロデューサーは、所定のトピックでイベントをパブリッシュします。

プール

Loggerの論理的なグループ。プール内のLoggerは、同じコンシューマーグループに所属し、同じトピックをサブスクライブします。

ブローカー

Kafkaサーバーソフトウェアのインスタンスです。

プロデューサー

メッセージをトピックにパブリッシュするプロセス。Event Brokerでは、ArcSight SmartConnectorを指します。

変換

データの形式を別の形式に変換する処理。たとえば、Event BrokerはCEFイベントをAvro形式に変換します。これにより、Verticaでの格納が可能になります。

ら

リーダー

パーティションのオリジナルレプリカを保持し、そのデータを管理するブローカー。

ルート

Event Brokerはこのルールに従って、特定の条件を満たしたイベントをターゲットトピックにコピーします。ルートによって、ソースとターゲットの両方のトピックにイベントのコピーが保持されます。

レシーバー

Loggerでは、イベントの受信、イベントデータのキャプチャー、各イベントへの送信元情報の格納を行うプロセスを指します。詳細については、『Logger管理者ガイド』を参照してください。

レプリカ

パーティションのコピー。1つのパーティションに、1つまたは複数のレプリカが存在します。冗長化を行わない場合でも、オリジナルはレプリカと呼ばれます。

レプリケーション係数

トピックをKafkaノードに複製する際の回数を指します。レプリケーション係数が3の場合、トピックは3つのKafkaノードにコピーされます。

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 (Event Broker 2.02) 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。