CEF エクストラクタ

この章は、次のセクションで構成されています。

CEF エクストラクタ サービスについて

Advanced Web Security Reporting（AWSR）アプリケーションで実行される共通イベント フォーマット（CEF）エクストラクタ サービスによって、1 つまたは複数の WSA から受信したアクセス ログを CEF 形式の出力データに変換して、ArcSight アプリケーションなど、他のサードパーティ製セキュリティ情報管理（SIM）システムに転送できます。

（注） CEF エクストラクタ サービスは分散環境のみで動作するため、少なくとも 2 つの個別の AWSR インスタンスを異なるホストで実行する必要があります。一方の AWSR インスタンスが「マスター」または「検索ヘッド」として機能し、専用の検索機能やライセンス共有機能を提供します。さらに、他方の「リスナー」または「ピア」インスタンスはインデクサとして機能し、AWSR データベースに変換後の Syslog データを送信します。

CEF エクストラクタ サービスの設定

Advanced Web Security Reporting の CEF エクストラクタ サービスは、次の手順で設定します。

- 1 つまたは複数のピア インスタンスを「リスナー」として設定し、リンクした Web セキュリティ アプライアンスからの syslog データの受信と変換、および syslog データへのインデックス作成を行えるようにします。詳細については、「CEF ピアの設定」を参照してください。
- マスター AWSR インスタンスまたは「検索ヘッド」を設定します。「AWSR マスターの設定」を参照してください。

- すべてのマスターおよびピア システムでライセンスを設定します。「ライセンスの設定」を参照してください。
- マスター システムで CEF サービスを設定します。「CEF エクストラクタの初期設定」を参照してください。
- マスター システムの再起動
- CEF 出力フィールドへのアクセス ログのマッピング設定
- CEF サービスのデータ入力を設定します。「CEF エクストラクタ サービスのデータ入力の設定」を参照してください。

はじめる前に

- 必要なすべてのホストで、AWSR ソフトウェアをインストールし、基本的な稼働と通信に関する設定を行います。

CEF ピアの設定

以下の手順に従って、インデックス ピアのホスト サーバで、インデックス ピアを「リスナー」として設定します。これには、受信側の新しいエントリを作成し、Web セキュリティ アプライアンスの syslog データをリッスンするポートを指定します。

始める前に

- AWSR ピアを起動し、管理者ユーザとしてログインします。

ステップ 1 **[設定（Settings）] > [データ（Data）] > [転送と受信（Forwarding and Receiving）]**を選択します。

ステップ 2 [転送と受信（Forwarding and Receiving）] ページで、[データを受信（Receive data）] セクションの [受信を設定（Configure receiving）] 行の [新規追加（Add new）] リンクをクリックします。

目的のリスナー ポートがすでに設定されている場合、[受信を設定（Configure receiving）] リンクをクリックして、[データを受信（Receive data）] ページに直接移動し、ポートを有効化できます。

ステップ 3 [新規追加（Add new）] > [受信を設定（Configure receiving）] ページで、リッスンするポートの番号を入力します。

ステップ 4 [保存（Save）] をクリックします。

[データを受信（Receive data）] ページに戻り、リッスンする利用可能なポートが表示されます。ここでは、個々のポートの有効化/無効化および削除を行えます。このページから新しいポートを追加することもできます。

AWSR マスターの設定

マスター（または検索ヘッド）システムで分散検索を有効にして、1 つまたは複数の検索ピアをピアのリストに追加する必要があります。

始める前に

- AWSR マスターを起動し、管理者ユーザとしてログインします。

ステップ 1 分散検索を有効にするには、次のコマンドを実行します。

1. **[設定（Settings）] > [分散環境（Distributed Environment）] > [分散検索（Distributed Search）]**を選択します。
2. [分散検索（Distributed search）] ページで、[分散検索の設定（Distributed search setup）] をクリックします。
3. **[分散検索の設定（Distributed search setup）]** ページで、[分散型の検索を有効にしますか（Turn on distributed search?）] オプションに対して [はい（Yes）] を選択します。
4. [保存（Save）] をクリックします。

[分散検索（Distributed search）] ページに戻ります。

ステップ 2 検索ピア（インデクサ）を追加するには、以下の手順を実行します。

1. [分散検索（Distributed search）] ページの [検索ピア（Search peers）] 行にある [新規追加（Add new）] をクリックします。
2. [新規追加（Add new）] ページの [検索ピアを追加（Add search peers）] で、[ピアID（Peer ID）] に *server_name:management_port* または *IP_address:management_port* のいずれかの形式で入力します。
3. ピアに接続するために、以下の分散検索認証パラメータを指定します。
   - [リモートユーザ名（Remote username）]：リモート検索ピアの管理者ユーザのユーザ名を指定します。
   - [リモートパスワード（Remote Password）]：そのユーザの接続パスワードを入力します。
   - [パスワードの確認（Confirm password）]：パスワードを再入力します。
4. [保存（Save）] をクリックします。

[検索ピア（Search peers）] ページに戻ります。

[検索ピア（Search peers）] ページに、現在設定されているすべてのピアが一覧表示されます。個々の検索ピアを有効化/無効化および削除できます。このページから新しい**検索ピア**を追加することもできます。**[設**

定（**Settings**）] > **[分散環境（Distributed Environment）]** > **[分散検索（Distributed Search）]** を選択し、[検索ピア（Search peers）] をクリックして、このページにいつでもアクセスできます。

ライセンスの設定

マスターシステムでは、1つのライセンスを各インデクサで使用できます。つまり、インデクサピアごとに個別のライセンスは必要ありません。次の項では、すべての AWSR インスタンスにライセンスを設定する方法について説明します。

- ピアのライセンス
- マスター ライセンス

ピアのライセンス

各インデクサは、マスター システムによって維持されるライセンス プールのライセンスにアクセスするように設定します。

ステップ 1 インデクサシステムで**[設定（Settings）]** > **[システム（System）]** > **[ライセンス（Licensing）]**を選択し、[ライセンス（Licensing）] ページを開きます。

このページの上部に、このサーバのライセンスのロールに関する通知が表示されます。サーバのロールは、[リモートマスターライセンスサーバへ関連付け（associated with a remote master license server）] または [マスターライセンスサーバとして動作（acting as a master license server）] のいずれかになります。

ステップ 2 このピアについて表示されているロールが [マスターライセンスサーバとして動作（acting as a master license server）] の場合は、[スレーブへ変更（Change to slave）] ボタンをクリックします。

ステップ 3 [マスターの関連付けを変更（Change master association）] ページで、[マスターライセンスサーバとして異なるAWSRインスタンスを指定（Designate a different AWSR instance as the master license server）] を選択します。

ステップ 4 マスターのライセンスサーバのアクセス情報として、目的のサーバの *server_name :management_port* または *IP_address:management_port* を入力します。

ステップ 5 [保存（Save）] をクリックします。

マスター ライセンス

マスターシステムでは、1つのライセンスを各インデクサで使用できます。以下の手順に従って、すべての設定済みインデクサ システムで共有するライセンス プールを指定します。

ステップ 1 検索ヘッドで **[設定（Settings）]** > **[システム（System）]** > **[ライセンス（Licensing）]**を選択し、[ライセンス（Licensing）] ページを開きます。

このページの上部に、このサーバのライセンスのロールに関する通知が表示されます。サーバのロールは、[リモートマスターライセンスサーバへ関連付け（associated with a remote master license server）] または [マスターライセンスサーバとして動作（acting as a master license server）] のいずれかになります。

ステップ 2 このピアについて表示された権限が [リモートマスターライセンスサーバへ関連付け（associated with a remote master license server）] の場合は、[マスターへ変更（Change to master）] ボタンをクリックし、[マスターの関連付けを変更（Change master association）] ダイアログ ボックスでこのサーバをマスター ライセンス サーバとして指定します。このダイアログ ボックスで [保存（Save）] をクリックして、[ライセンス（Licensing）] ページに戻ります。

ステップ 3 [ライセンスのスタック（License stack）] セクションで、インデクサ ピアと共有するライセンス プールを表す行の [編集（Edit）] をクリックします。

ステップ 4 [ライセンスプールの管理（Manage license pool）] ページで、[このプールから取得できるインデクサを指定（Which indexers are eligible to draw from this pool?）] オプションの [特定のインデクサ（Specific indexers）] を選択します。

使用可能なインデクサの一覧が表示されます。

ステップ 5 [関連付けられたインデクサ（Associated indexers）] リストに追加するために、目的のインデクサの前に表示された緑色の [追加（Add）] ボタンをクリックします。必要に応じてこの手順を繰り返します。

ステップ 6 [送信（Submit）] をクリックします。

ステップ 7 [更新（Update）] の通知で [OK] をクリックします。

[ライセンス（Licensing）] ページに戻ります。このページで、ライセンスを追加したり、ライセンス プールを追加、編集、および削除したりできます。

CEF エクストラクタの初期設定

AWSR CEF エクストラクタ マスターおよびインデクサ システムを設定したら、CEF エクストラクタ サービスを設定する必要があります。

始める前に

- AWSR マスター システムを起動し、管理者ユーザとしてログインします。

ステップ 1 **[設定（Settings）] > [サードパーティサービス（Third Party Services）] > [CEFエクストラクタ（CEF Extractor）]**を選択し、[CEFエクストラクタ（CEF Extractor）] ページを開きます。

CEF アプリケーションがまだ完全に構成されていないことが通知されます。

ステップ 2 [アプリの設定ページに進む（Continue to app setup page）] ボタンをクリックして、AWSR CEF の設定ページに進みます。

ステップ 3 [リアルタイムのインデックス作成を有効にする（Enable Indexed Realtime）] をオンにして、リアルタイムでインデックスの作成と検索ができるようにします。

パフォーマンスを向上させるには、このオプションを有効にすることをお勧めします。

ステップ 4 [インデクサの設定（Indexer Setup）] セクションの [インデクサ（Indexers）] フィールドに、各ピアのアクセス ID 情報を *server_name:listener_port* または *Ip_address:istener_port* のいずれかの形式で入力します。

（注） インデクサエントリごとに、「CEF ピアの設定」で説明されているように、そのインデクサシステム用に設定されたリスナーポートの番号を使用してください。

ステップ 5 [保存（Save）] をクリックします。

マスター システムの再起動

Advanced Web Security Reporting マスター システム、ピア ライセンス共有、および CEF エクストラクタ サービスを構成したら、マスター サーバを再起動する必要があります。

ステップ 1 **[設定（Settings）] > [システム（System）] > [サーバコントロール（Server Controls）]** を選択し、[サーバコントロール（Server controls）] ページを開きます。

ステップ 2 [AWSRを再起動（Restart AWSR）] ボタンをクリックし、指示に従ってシステムを再起動します。

ステップ 3 再起動が完了したら、再度ログインします。

CEF 出力フィールドへのアクセス ログのマッピング設定

次のタスクでは、Web セキュリティ アプライアンスのアクセス ログのマッピングを CEF エクストラクタ サービスの CEF 出力フィールドに設定し、この情報の出力先を定義します。

ステップ 1 **[設定（Settings）] > [サードパーティサービス（Third Party Services）] > [CEFエクストラクタ（CEF Extractor）]**を選択し、[CEFエクストラクタ（CEF Extractor）] ページを開きます。

ステップ 2 [新規（New）] をクリックして、**CEF エクストラクタデータ検索設定**ウィザードを起動します。

ステップ 3 データを取得する [データモデル（Data Model）] を選択します。この場合は、[Web_Access_Data] を選択します。

ステップ 4 [オブジェクト（Object）] ドロップダウン リストから [Web_Access_Event] を選択することにより、Web セキュリティ アプライアンスの Web アクセス ログからデータ フィールドを取得するように指定します。

ステップ 5 [次へ（Next）] をクリックして、ウィザードの [マップフィールド（Map Fields）] ページに進みます。

このページには、[CEF出力フィールド（CEF Output Fields）] と [データモデル属性（Data-model attributes）] の 2 つの列が表示されます。各行の [出力フィールド（Output Fields）] 列は、すべての CEF 出力形式を含むドロップダウンリストです。また、[データモデル属性（Data-model attributes）] 列にはデータモデルで使用できる属性のハードコードされたリストが表示されます。

ステップ 6 必要に応じて、**CEF 出力**フィールドを Web Access のデータモデル属性にマップします。

一部のフィールドは自動的にマッピングされます（たとえば、データモデルの属性 `host` は自動的に CEF フィールドの `syslog_host` にマッピングされます）。このページには、自動的なマッピングとデフォルトのマッピングの両方が表示され、それぞれを変更できます。

マッピングを追加または変更するには、更新対象の出力フィールドから属性へのマッピングを表す行のドロップダウンリストを開き、このデータモデル属性にマッピングする **CEF 出力**フィールドを選択します。

ステップ 7 [次へ（Next）] をクリックして、ウィザードの [静的フィールドの作成（Create Static Fields）] ページに進みます。

このページのフィールドを使用して、対応するデータモデル属性がない CEF 出力フィールドに、状況依存の静的値を指定します。

ステップ 8 一覧表示された **CEF 出力**フィールドに対する静的なフィールド値を入力します。

たとえば、CEF 出力フィールド `dvc_vendor` にフィールド値の CISCO を入力し、`dvc_product` に `AWSR_CEF` を入力できます。

ステップ 9 [次へ（Next）] をクリックして、ウィザードの [出力を定義（Define Outputs）] ページに進みます。

このページでは、CEF データの送信先の出力グループを作成または選択します。

ステップ 10 [新規出力グループの作成（Create new output group）] をクリックします。

ステップ 11 [新規出力グループ（New Output Group）] ダイアログボックスで、以下の新しい出力グループパラメータを指定します。

- [名前（Name）]：この出力グループの識別子。
- [データの出力先のホスト（Hosts to output data to）]：CEF 出力データを送信する出力サーバ。*server_namereceive_port* または *IP_address:receive_port* のいずれかの形式で入力します

（注） syslog データを出力する予定がある場合は、TCP ポート 514 はすでに使用されているため使用できません。「Web セキュリティアプライアンス Syslog のデータ入力の設定」を参照してください。

ステップ 12 [保存（Save）] をクリックして、[新規出力グループ（New Output Group）] ダイアログボックスを閉じます。

ステップ 13 [次へ（Next）] をクリックして、ウィザードの [検索を保存（Save Search）] ページに進みます。

ステップ 14 このマッピングまたは検索の設定を指定します。

- [検索名（Search Name）]：この CEF 情報の検索設定の識別子またはマッピング名。
- [検索の説明（Search Description）]（任意）：この CEF 情報検索の簡単な説明。

ステップ 15 [保存（Save）] をクリックして、ウィザードを終了します。

[CEFエクストラクタ（CEF Extractor）]ページに、定義済みのデータセットのマッピングが一覧表示されます。新しいデータセットを追加したり、既存のデータセットを有効化、無効化、または削除したりできます。

CEF エクストラクタ サービスのデータ入力の設定

次のタスクでは、CEF エクストラクタ サービスのデータ フィールドを設定します。

（注） この項では、CEF エクストラクタ サービスのデータ入力として Web セキュリティ アプライアンスのアクセス ログを設定する方法について説明します。また、FTP プッシュおよび syslog プッシュをサービスのデータ入力として設定することもできます。詳細については、「継続的なデータ転送の設定」と「Umbrella のログの更新」を参照してください。

ステップ 1 **[設定（Settings）]** > **[データ（Data）]** > **[データ入力（Data inputs）]**を選択して、[データ入力（Data inputs）] ページを開きます。

ステップ 2 [データ入力（Data inputs）]ページの [ファイルとディレクトリ（Files & directories）]行の [新規追加（Add new）]をクリックして、新しいデータ フォルダのフィールドのマッピングと監視を設定するウィザードを起動します。

ステップ 3 [ファイルまたはディレクトリ（File or Directory）] フィールドの横にある [参照（Browse）] ボタンをクリックします。

ステップ 4 [ソースの選択（Select source）] ダイアログ ボックスで、目的の Web セキュリティ アプライアンスのアクセス ログ フォルダを参照して選択します（たとえば、`home/logger/incoming/wsa_test/accesslogs`）。

ステップ 5 [選択（Select）] をクリックして [ソースの選択（Select source）] ダイアログ ボックスを閉じます。

ステップ 6 [ソースの選択（Select Source）] ウィザード ページで [次へ（Next）] をクリックして [入力設定（Input Setting）]ページに移動します。

ステップ 7 ソースの種類については、[選択（Select）] をクリックし、[ソースの種類を選択（Select Source Type）] をクリックして `wsa_accesslogs` を選択します（[ソースの種類の選択（Select Source Type）] ドロップダウン リストの一番上にあるフィルタ フィールドに `wsa_accesslogs` を 1 文字ずつ入力することで、エントリをすばやく見つけることができます）。

ステップ 8 アプリ コンテキストについては、[アプリコンテキスト（App context）] ドロップダウンリストから [Advanced Web Security Reporting 6.1.0] を選択します。

ステップ 9 [ホスト（Host）] エントリまで下にスクロールして、[パス内のセグメント（Segment in path）] をクリックし、[セグメント番号（Segment number）] に入力します。

[ホスト（Host）] エントリは、ソースのイベントに対してホスト フィールドの値を決定する方法を指定します。[パス内のセグメント（Segment in path）] オプションは、先に指定した [ソースパス（Source path）] のセグメントから決定されることを意味します。セグメント番号は、パスのどのセグメントがホスト値であるかを示します。たとえば、前のサンプルのソース パス

`home/logger/incoming/wsa_test/accesslogs` の場合、ホスト名 `wsa_test` はパスの 4 番目のセグメントなので、ここに入力するセグメント番号は 4 になります。

ステップ 10 [レビュー（Review）] をクリックして、ウィザードの [レビュー（Review）] ページに進みます。

ステップ 11 入力した情報を確認し、[送信（Submit）] をクリックして新しいデータ入力インスタンスを作成します。