User AgentからIdentity Services Engineへの移行

内容

はじめに

このドキュメントでは、User Agent(UA)からFirepower User Agent用のIdentity Services Engine(ISE)に移行する方法について説明します。

背景説明

今後のリリースでは、Firepowerユーザエージェントは使用できなくなります。 代わりに、ISEまたはIdentity Services Engine - Passive ID Connector(ISE-PIC)が使用されます。現在User Agentを使用していて、ISEへの移行を検討している場合は、このドキュメントで移行に関する考慮事項と戦略を説明します。

ユーザアイデンティティの概要

現在、既存のアイデンティティインフラストラクチャからユーザID情報を抽出するには、ユーザエージェントとISEの統合の2つの方法があります。

ユーザエージェント

ユーザエージェントは、Windowsプラットフォームにインストールされるアプリケーションです。Windows Management Instrumentation(WMI)プロトコルを使用して、ユーザログオンイベント

（イベントタイプ4624）にアクセスし、データをローカルデータベースに保存します。ユーザエージェントがログオンイベントを取得する方法には、ユーザのログイン時にリアルタイムで更新する方法（Windows Server 2008および2012のみ）と、設定可能なすべての間隔でデータをポーリングする方法の2つがあります。同様に、ユーザエージェント(UA)はActive Directory(AD)から受信したデータをFirepower Management Center(FMC)にリアルタイムで送信し、ログオンデータのバッチを定期的にFMCに送信します。

User Agentが検出できるログインのタイプには、ホストへの直接またはリモートデスクトップ経由のログイン、ファイル共有ログイン、コンピュータアカウントログインなどがあります。Citrix、ネットワークログオン、Kerberosログインなどの他のタイプのログインは、ユーザエージェントではサポートされません。

User Agentには、マッピングされたユーザがログオフしたかどうかを検出するオプション機能があります。ログオフチェックが有効な場合、マップされた各エンドポイントでプロセスが実行されているかどうか`explorer.exe`が定期的にチェックされます。実行中のプロセスを検出できない場合は、72時間後にこのユーザのマッピングが削除されます。

Identity Services Engine

ISEは、ユーザのネットワークログインセッションを管理する堅牢なAAAサーバです。ISEは、スイッチやワイヤレスコントローラなどのネットワークデバイスと直接通信するため、ユーザのアクティビティに関する最新のデータにアクセスでき、ユーザエージェントよりも優れたアイデンティティソースとなります。ユーザがエンドポイントにログオンすると、通常は自動的にネットワークに接続されます。ネットワークでdot1x認証が有効になっている場合、ISEはこれらのユーザの認証セッションを作成し、ユーザがネットワークからログオフするまでアクティブな状態を維持します。ISEがFMCと統合されている場合、ISEはユーザIPマッピング（およびISEによって収集されたその他のデータ）データをFMCに転送します。

ISEはpxGridを介してFMCと統合できます。pxGridは、ISEサーバ間および他の製品との間でセッション情報の配布を一元化するように設計されたプロトコルです。この統合では、ISEがpxGridコントローラとして機能し、FMCはセッションデータを受信するためにコントローラにサブスクライブし（後で説明する修復中を除き、FMCはデータをISEに発行しません）、ユーザ認識を実現するためにそのデータをセンサーに渡します。

Identity Services Engine：パッシブIDコネクタ(ISE-PIC)

Identity Services Engine(ISE):Passive Identity Connector(ISE-PIC)は、基本的に制限付きライセンスを持つISEのインスタンスです。ISE-PICは認証を実行しませんが、代わりにネットワーク内のさまざまなアイデンティティソースの中央ハブとして機能し、アイデンティティデータを収集して加入者に提供します。ISE-PICは、ADからログインイベントを収集するためにWMIを使用する点ではユーザエージェントに似ていますが、パッシブIDと呼ばれるより堅牢な機能を備えています。また、pxGridを介してFMCと統合されています。

移行の考慮事項

ライセンス要件

FMCには追加ライセンスは必要ありません。ISEがインフラストラクチャにまだ導入されていない場合は、ライセンスが必要です。詳細については、『Cisco ISEライセンスモデル』を参照してください。 ISE-PICは完全なISE導入にすでに存在する機能セットであるため、既存のISE導入がある場合は追加のライセンスは必要ありません。ISE-PICの新規または個別の導入については、『Cisco ISE-PICライセンス』ドキュメントを参照してください。

シスコ内部情報
注：ユーザエージェントからISE-PICに移行するお客様には、無料のライセンスオプションがあります。ただし、無償オプションは、アプライアンス（ハードウェア）FMC、FMCv25、およびFMCv300でのみ使用できます。つまり、FMCv2とFMCv10は対象外です。 お客様にシスコのアカウントチームに連絡するようアドバイスします。

SSL証明書

User AgentはFMCおよびADとの通信に公開キーインフラストラクチャ(PKI)を必要としませんが、ISEまたはISE-PICの統合では、認証の目的でのみISEとFMCの間で共有されるSSL証明書が必要です。サーバ認証とクライアント認証拡張キー使用法(EKU)の両方が証明書に追加されている場合、統合では認証局署名付き証明書と自己署名付き証明書がサポートされます。

アイデンティティソースカバレッジ

User Agentは、ポーリングベースのログアウト検出を使用して、Windowsデスクトップからの Windowsログインイベントのみを対象とします。ISE-PICは、Windowsデスクトップログインに加えて、ADエージェント、Kerberos SPAN、Syslogパーサー、ターミナルサービスエージェント(TSA)などの追加のアイデンティティソースを対象とします。フルISEでは、すべてのISE-PICに加え、Windows以外のワークステーションやモバイルデバイスからのネットワーク認証など、さまざまな機能をカバーしています。

	ユーザエージェント	ISE-PIC	ISE
Active Directoryデスクトップログオン	Yes	Yes	Yes
ネットワークログオン	いいえ	いいえ	Yes
エンドポイントプローブ	Yes	Yes	Yes
InfoBlox/IPAM	いいえ	Yes	Yes
[LDAP]	いいえ	Yes	Yes
セキュアなWebゲートウェイ	いいえ	Yes	Yes

REST APIソース	いいえ	Yes	Yes
Syslogパーサー	いいえ	Yes	Yes
ネットワークSpan	いいえ	Yes	Yes

ユーザエージェントのサポート終了

User Agentをサポートするfirepowerの最新バージョンは6.6です。このバージョンでは、User Agentを無効にしてから新しいリリースにアップグレードする必要があることを示す警告が表示されます。6.6以降のバージョンへのアップグレードが必要な場合は、アップグレード前にユーザエージェントからISEまたはISE-PICへの移行を完了する必要があります。詳細については、『ユーザエージェント設定ガイド』を参照してください。

互換性

Firepower製品の互換性ガイドを確認し、統合に含まれるソフトウェアバージョンに互換性があることを確認します。将来のFirepowerリリースでは、それ以降のバージョンのISEのサポートには特定のパッチレベルが必要であることに注意してください。

移行戦略

User AgentからISEまたはISE-PICへの移行では、FMCのユーザIDソースのスムーズな移行を保証し、ユーザトラフィックへの影響を回避するために、慎重な計画、実行、およびテストが必要です。このセクションでは、この課題のベストプラクティスと推奨事項について説明します。

移行の準備

ユーザエージェントからISE統合に切り替える前に、次の手順を実行できます。

ステップ 1：PassiveIDを有効にし、Active DirectoryとのWMI接続を確立するようにISEまたはISE-PICを設定します。『ISE-PICアドミニストレーションガイド』を参照してください。

ステップ 2：FMCのID証明書を準備します。これは、プライベートまたはパブリックの認証局(CA)によって署名されるように、FMCによって発行された自己署名証明書、またはFMCで生成された証明書署名要求(CSR)のいずれかになります。CAの自己署名証明書またはルート証明書がISEにインストールされている必要があります。詳細については、『ISEおよびFMC統合ガイド』を参照してください。

ステップ 3：ISEのpxGrid証明書（自己署名の場合はpxGrid証明書）に署名したCAルート証明書をFMCにインストールします。詳細については、『ISEおよびFMC統合ガイド』を参照してください。

カットオーバープロセス

FMCとISEの統合は、FMCのユーザエージェント設定を無効にしないと設定できません。これは、この2つの設定が相互に排他的であるためです。これは、変更中にユーザに影響を与える可能性があります。これらの手順は、メンテナンスウィンドウ中に実行することを推奨します。

ステップ 1：FMC-ISE統合を有効にして確認します。詳細については、『ISEおよびFMC統合ガイド』を参照してください。

ステップ 2：FMCのページに移動して、ユーザアクティビティがFMCに報告されAnalysis > User > User Activitiesていることを確認します。

ステップ 3：ユーザとIPのマッピングおよびユーザグループのマッピングがで管理対象デバイスで使用できることを確認Analysis > Connections > Events > Table View of Connection Eventsします。

ステップ 4： ユーザ名またはユーザグループの条件に応じて、トラフィックをブロックするルールに対するアクションを一時的にMonitorに変更するには、アクセスコントロールポリシーを変更します。発信側のユーザまたはグループに基づいてトラフィックを許可するルールの場合は、ユーザ基準を使用せずにトラフィックを許可する重複ルールを作成してから、元のルールを無効にします。このステップの目的は、メンテナンス期間後のテスト段階でビジネスクリティカルなトラフィックに影響が及ばないようにすることです。

ステップ 5：メンテナンスウィンドウの後、通常の営業時間中に、ユーザとIPのマッピングを監視するためにFMCの接続イベントを確認します。接続イベントでユーザー情報が表示されるのは、ユーザーデータを必要とするルールが有効になっている場合のみです。これが、前述の手順でモニタアクションが推奨される理由です。

手順 6：望ましい状態が達成されたら、アクセスコントロールポリシーに対して行った変更を元に戻し、ポリシーの導入を管理対象デバイスにプッシュするだけです。

関連情報

- ビデオチュートリアル：ユーザエージェントのISE-PICへの移行
- Cisco ISE 2.4管理ガイド：ライセンス
- ユーザエージェント設定ガイド
- Cisco Firepower 互換性ガイド
- ISE 2.4およびFMC 6.2.3 pxGrid統合の設定
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。