Cisco ISE Passive Identity Connector

目次

Cisco® ISE Passive Identity Connector は、認証データの複数のソースを単一の信頼できるソースに統合します。シスコのセキュリティ製品のインストールを簡素化し、主要なインフラストラクチャから作業をオフロードします。

製品の概要

ユーザー名は、ネットワークへのアクセスを決定する重要な要素です。また、ユーザー名は、ユーザーのデバイスに不審なアクティビティがあることを警告するのに役立ちます。誰がネットワークに接続しているのか、という重要な問題に答えます。

Cisco Identity Services Engine（ISE）Passive Identity Connector は、IP アドレス、MAC アドレス、ユーザー名などの ID 情報を一元化し、統合して配布します。同時に、Microsoft Active Directory などの主要なインフラストラクチャから作業をオフロードします。

ネットワーク上の多くのサーバーが、ユーザー認証に積極的に参加しています。ユーザーのログイン情報を取得し、それらを確認するか、Active Directory などの専用リポジトリで検索します。Passive Identity Connector は、ユーザー認証に積極的に関与するのではなく、ネットワーク上のさまざまな認証サーバーをリッスンします。認証情報が一元化されるので、信頼できる唯一の情報源がサブスクライバに提供されます。

Passive Identity Connector は、セッションアイデンティティ情報を、そのような情報の自然なコンシューマであるネットワーク上の他のデバイスに配布します。これらのデバイスには、ファイアウォール、Web セキュリティアプライアンス、トラフィックアナライザなどが含まれます。Cisco Platform Exchange Grid（pxGrid）を使用すると、Cisco ISE Passive Identity Connector で最大 20 のサブスクライバをサポートできます。

Cisco ISE 3.3 に含まれる pxGrid の機能強化により、ネットワーク管理者はネットワークをピアリングし、ネットワークを最適化して効率を高めるために必要なデータを見つけることができます。ネットワーク属性は、顧客が真に利用できる方法でデータを枠組みする方法で表示されるため、ネットワークセキュリティをより効果的に運用することができ、より安全なネットワークとデータ変換に必要な時間の短縮につながります。

さらに、Cisco ISE 3.4 リリースでの 2 つの新しい機能拡張により、Cisco ISE と pxGrid の間で相乗効果を高めることができます。

1. お客様は、pxGrid Direct コネクタからのデータを即時に同期できます。このリリースより前の Cisco ISE では、1 週間に 1 回以下（12 時間に 1 回以上）、増分更新は毎日（1 時間に 1 回以上）の頻度でデータベースの全更新を同期できます。即時に同期することで、1 週間に 1 回またはその日の終わりまで待機する必要がなくなります。すべての更新を待機せずすぐに実行できます。
2. サーバーには、更新を Cisco ISE に即時にプッシュする機能が付与されています。この新機能は pxGrid Direct プッシュと呼ばれ、遅延のない Cisco ISE の継続的な同期を実現します。つまり、レコードが 1 件調整されるたびに、サーバーは Cisco ISE へ即時に変更を送信します。

機能と利点

機能	利点
一元化された情報	複数の認証ソースからのデータを統合し、認証データを必要とするすべてのシステムがすべての認証ソースとやり取りする必要性を排除
パフォーマンスの向上	他の認証データコンシューマのデータをキャッシュする単一のシステムにより、過負荷になることが多いインフラストラクチャの負担を軽減
syslog サーバーのサポート	syslog をサポートするシステムから認証データを収集
Active Directory のサポート	Microsoft Windows Management Interface（WMI）を介して Active Directory から認証データを収集
Kerberos SPAN のサポート	Kerberos SPAN をサポートするスイッチからの Active Directory 認証データの収集
エンドポイントプローブ	エンドポイントがログオフするタイミングを把握
Active Directory エージェント	最大 10 の Microsoft Active Directory ドメインコントローラからの認証データの収集
カスタム API のサポート	カスタムインターフェイスをサポートするシステムから認証データを収集
Citrix Terminal Server のサポート	Citrix Terminal Server からの認証データの収集
ハイアベイラビリティ	アクティブ/パッシブ冗長性のサポート
移行のサポート	Cisco ISE Passive Identity Connector から Cisco ISE にアップグレードし、既存の Cisco ISE クラスタに Passive Identity Connector ノードを追加することが可能
仮想マシンのサポート	KVM、VMware、および Hyper-v のサポート
拡張性	組織に適合するよう、ライセンスに応じて 3,000 および 30 万のセッションをサポート

Microsoft Active Directory の統合

Cisco ISE Passive Identity Connector は、ネットワーク上の多数の認証サーバーからセッションデータを収集できますが、Microsoft Active Directory ほど重要なものはありません。Passive Identity Connector は、Microsoft Windows Management Interface（WMI）を使用するか、各ドメインコントローラにインストールされている Cisco Active Directory エージェント、Switched Port Analyzer（SPAN; スイッチドポートアナライザ）ポートの使用、または syslog を介して、最大 100 台のドメインコントローラから情報を収集できます。Microsoft WMI インターフェイスには、ドメインコントローラに追加のソフトウェアをインストールする必要がないという利点があります。Active Directory エージェントは、最大 10 台のドメインコントローラから情報を収集できます。ドメインコントローラでの設定変更は不要で、ドメインコントローラまたはメンバーサーバーのいずれかにインストールできます。

Active Directory インフラストラクチャの負荷を制限したい場合、または Active Directory を設定せずにデータをすばやく簡単に取得したい場合は、Cisco ISE Passive Identity Connector では SPAN ポートを使用してセッションデータを収集できます。SPAN はネットワークトラフィックをスニッフィングし、特に Kerberos メッセージを検査します。また、Active Directory によって保存されているユーザーアイデンティティ情報を抽出し、その情報を Passive Identity Connector に送信します。

定義済みおよびユーザー定義可能な syslog パーサー

ネットワーク上には多数のアイデンティティのソースがあり、それらとインターフェイスする方法は無数にあり、不可能な組み合わせも作成されます。Cisco ISE Passive Identity Connector は、汎用 syslog パーサーを提供することで、この課題を克服します。お客様は、認証サーバー上の syslog エージェントを Passive Identity Connector に接続し、アイデンティティ情報を解析することができます。

syslog パーサーは、正規表現を使用して認証情報を含む syslog メッセージを抽出することで、さまざまな syslog メッセージフォーマットをサポートできます。Passive Identity Connector では、ヘッダーに同じ正規表現機能を使用するため、ヘッダータイプが異なっていても問題ありません。Passive Identity Connector は、汎用の syslog パーサーに加えて、Cisco ISE、Cisco Secure Access Control System（ACS）、Cisco 適応型セキュリティアプライアンス（ASA）VPN、Aerohive、BlueCat、Blue Coat、F5 VPN、InfoBlox、Lucent QIP、Nortel VPN、および Safe Connect などの事前定義されたパーサーを提供します。

アプリケーション プログラミング インターフェイス

Cisco ISE Passive Identity Connector は、セッションデータを発行するが syslog を使用しないアプリケーション用のカスタム API を提供します。

ターミナルサーバーのサポート

Cisco ISE Passive Identity Connector は、ターミナルサーバーにインストールされているエージェントを使用して、Citrix ターミナルサーバー環境からセッション情報を収集する機能を提供します。

スタンドアロンおよび高可用性構成

Cisco ISE Passive Identity Connector は、スタンドアロンで動作することも、高可用性のために 2 番目の仮想マシンとペアリングすることもできます。アクティブ/パッシブ環境で動作する高可用性構成では、プライマリがセカンダリを更新します。

ハードウェアソリューション

シスコのハードウェアソリューションをお探しのお客様は、Cisco ISE バージョン 2.2 以降を搭載した Secure Network Server（SNS）3715、SNS 3755、または 3795 アプライアンスをご購入いただけます。SNS 3715 は専用 PSN によってサポートされる最大 25,000 の同時アクティブエンドポイント（共有 PSN によってサポートされる 12,500）、SNS 3755 は専用 PSN によってサポートされる最大 50,000 の同時アクティブエンドポイント（共有 PSN によってサポートされる 25,000）、SNS 3795 は専用 PSN によってサポートされる最大 100,000 の同時アクティブエンドポイント（共有 PSN によってサポートされる 50,000）をサポートできます。

ISE へのアップグレード

Cisco ISE Passive Identity Connector から Cisco ISE にアップグレードし、既存の Cisco ISE クラスタに Passive Identity Connector ノードを追加することができます。適切なライセンスを使用して、Passive Identity Connector をスタンドアロン Cisco ISE インスタンスにアップグレードすることもできます。これはすべてライセンスのインストールによって実現され、追加のソフトウェアをインストールする必要はありません。そのため、ビジネスニーズの拡大に合わせて投資を保護することができ、IT スタッフによる多額の投資は不要です。

製品仕様

WMI または Active Directory エージェントを使用してサポートされる Microsoft Active Directory ドメインコントローラの最大数	100
Microsoft Active Directory ドメインコントローラにインストールした場合、Active Directory エージェントごとにサポートされる Microsoft Active Directory ドメインコントローラの最大推奨数	1
メンバーサーバーにインストールした場合、Active Directory エージェントごとにサポートされる Microsoft Active Directory ドメインコントローラの最大推奨数	10
pxGrid サブスクライバの最大数	20
Cisco ISE Passive Identity Connector クラスタあたりのノードの最大数	2
REST API プロバイダーの最大数	50
syslog クライアントの最大数	50
SPAN ポートの最大数	1 台のスタンドアロンマシンで 1 つ、高可用性クラスタで 2 つ

システム要件

ハイパーバイザ	ESXi 5.x の場合は VMware バージョン 8、ESXi 6.x の場合は VMware バージョン 11（デフォルト）、Red Hat Enterprise Linux 7.0 の KVM、または Microsoft Hyper-V
CPU	6 コア。2.0 GHz 以上：最大 100,000 セッション 8 コア。2.0 GHz 以上：最大 300,000 セッション
メモリ	16 GB：最大 100,000 セッション 64 GB：最大 300,000 セッション
ディスク	最小 200 GB

発注情報

Passive Identity Connector Q&A は、ISE パッシブアイデンティティ と、組織のニーズに最適なライセンスタイプを理解するのに役立ちます。購入方法については、「購入案内」を参照してください。ISE Passive Identity Connector ソフトウェアをダウンロードするには、Cisco Software Center にアクセスしてください。

部品番号	製品の説明
R-ISE-PIC-VM-K9=	ISE Passive Identity Connector 3,000 セッション仮想マシン
L-ISE-PIC-UPG=	ISE Passive Identity Connector：最大 30 万セッションにアップグレード

保証情報

Cisco ISE Passive Identity Connector には、90 日間の限定保証が付属しています。保証に関する情報については、https://www.cisco.com/go/warranty [英語] を参照してください。

シスコおよびパートナーの提供サービス

シスコでは、多様なサービスプログラムをご用意しています。これらの画期的なプログラムは、さまざまな人材、プロセス、ツール、パートナーを組み合わせて提供されるものであり、お客様からも高い評価を受けています。シスコのサービスは、お客様のネットワーク投資を保護してネットワーク運用を最適化するだけでなく、ネットワーク インテリジェンスの強化や事業拡張に向けた新しいアプリケーションの導入準備という面でもサポートします。シスコのサービスの詳細については、シスコ テクニカル サポート サービスまたはシスコセキュリティサービスを参照してください。詳細については、https://www.cisco.com/jp/go/warranty を参照してください。

Cisco Capital

目的達成に役立つ柔軟な支払いソリューション

Cisco Capital® により、目標を達成するための適切な技術を簡単に取得し、ビジネス変革を実現し、競争力を維持できます。総所有コスト（TCO）の削減、資金の節約、成長の促進に役立ちます。100 ヵ国あまりの国々では、ハードウェア、ソフトウェア、サービス、および他社製製品を購入するのに、シスコの柔軟な支払いソリューションを利用して、簡単かつ計画的に支払うことができます。詳細はこちらをご覧ください。

購入方法

購入オプションを確認し、シスコの営業担当者に問い合わせるには、https://www.cisco.com/c/ja_jp/buy.html にアクセスしてください。

詳細情報

Cisco ISE ソリューションの詳細については、https://www.cisco.com/go/ise を参照するか、最寄りの代理店までお問い合わせください。

文書の変更履歴

新規トピックまたは改訂されたトピック	説明箇所	日付
Cisco ISE Passive Identity Connector	3 ページ「製品の概要」	2024 年 5 月

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices）をご覧ください。

Printed in USA C78-3740518-01 05/24