CHAPTER 1

Context Directory Agent の概要

Cisco Context Directory Agent（CDA）は、Cisco Linux マシン上で実行され、Active Directory ドメイン コントローラ（DC）マシンの集合をリアルタイムにモニタして、一般にユーザ ログインを示す認証関連イベントの有無を確認し、データベース内の IP アドレスとユーザ ID のマッピングを認識、分析、キャッシュし、クライアント デバイスが最新のマッピングを使用できるようにするアプリケーションです。

クライアント デバイス（Cisco 適応型セキュリティ アプライアンス（ASA）や Cisco IronPort Web セキュリティ アプライアンス（WSA）など）は、最新の IP-to-user-identity マッピング セットを次のいずれかの方法で取得するために、RADIUS プロトコルを使用して Cisco CDA と通信します。

- **オンデマンド**：Cisco CDA は、特定のマッピングに対するクライアント デバイスからのオンデマンド クエリーに応答できます。
- **フル ダウンロード**：Cisco CDA は、現在キャッシュ内にあるマッピング セット全体を求めるクライアント デバイスからの要求に応答できます。

オンデマンド方式とフル ダウンロード方式の両方で、クライアント デバイスからの要求に、後続の更新に関連する登録も含んでいることを示すタグを特別に付けることができます。

たとえば、クライアント デバイスが基本的なオンデマンド クエリーを要求すると、Cisco CDA は応答してそのキャッシュ内で検出されている可能性のある特定のマッピングを提供しますが、そのマッピングに関するそれ以降の更新は送信しません。ただし、オンデマンド クエリーに登録も含まれている場合、Cisco CDA からの最初の応答は前述と同様ですが、後でこの特定のマッピングが変更される場合、Cisco CDA は要求元のクライアント デバイス（および通知登録しているその他のすべてのクライアント デバイス）に対し、この特定のマッピングの変更について事前に通知します。

同様に、クライアント デバイスが基本的なフル ダウンロードを要求する場合、Cisco CDA は現在キャッシュ内にあるすべてのマッピングを含むセッション データのスナップショットを転送しますが、それ以降の更新は送信しません。ただし、要求が複製登録の場合、Cisco CDA からの最初の応答は前述と同様です。後でマッピング セットに何か変更（新しいマッピングの追加または特定のマッピングの変更など）がある場合、Cisco CDA は要求元のクライアント デバイス（および複製登録しているその他のすべてのクライアント デバイス）に対し、この変更について以前に送信されたスナップショットを基準に事前に通知します。

Cisco CDA によって検出、管理、および提供される IP-to-user-identity マッピングには IPv4 アドレスだけでなく IPv6 アドレスも含めることができます。

Cisco CDA は、ログを 1 つ以上の Syslog サーバに送信できます。

いずれかの Active Directory ドメイン コントローラまたはクライアント デバイスで障害が発生しても、Cisco CDA は引き続き機能します。他のドメイン コントローラから情報を取得します。ただし、Cisco CDA のフェールオーバーは行われません。Cisco CDA 内蔵の「ウォッチドッグ」機能は、その内部の Linux プロセスを継続的にモニタし、プロセスがクラッシュしたことを検出すると自動的にそのプロセスを再起動します。CDA それ自体のフェールオーバーは行われませんが、全体としての解決策では、プライマリおよびセカンダリ CDA（プライマリおよびセカンダリ RADIUS サーバに類似）を設定する

機能を使用してフェールオーバー（コンシューマ デバイスによって制御される）をサポートし、プライマリが無応答の場合にはセカンダリ サーバにフェールオーバーします。プライマリおよびセカンダリ CDA は互いをまったく認識せず、ステート情報の交換も行いません。

関連項目

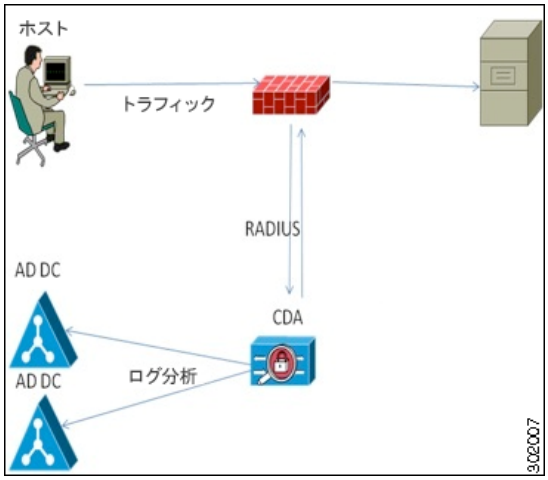
「機能の概要」（P.1-2）

機能の概要

図 1-1 は、Cisco CDA ソリューションを表した簡略図です。この例では、ユーザはコンピュータからログインして、サーバへのアクセスを要求することによって Web トラフィックを生成します。クライアント デバイスは Web トラフィックをインターセプトし、コンピュータにログインしたユーザを求めている Cisco CDA に RADIUS 要求を送信します。Cisco CDA は最新の IP-to-user-identity マッピング セットを管理しており、ユーザ情報をクライアント デバイスに送信します。クライアント デバイスはユーザ ID 情報を使用して、エンド ユーザにアクセス権を付与するかどうかを決定します。

ASA がネットワークに VPN コンセントレータとして導入された場合、Cisco CDA は、Active Directory から受信したログイン イベントに加えてマッピングの更新イベントを受け入れます。

図 1-1　　Cisco CDA のアーキテクチャ



Cisco CDA は次を行います。

- コンシューマ デバイスへの IP-to-user-identity マッピングの提供（プッシュおよびプル、単一およびバルク）。
- コンシューマ デバイスから IP-to-user-identity マッピングに関する通知の受信。
- 各種コンポーネント（Cisco CDA およびドメイン コントローラ）のステータスを取得するインターフェイスの提供。
- IP-to-user-identity マッピングのセッション ディレクトリの管理。
- セッション情報のキャッシュ。
- マッピングのリアルタイム学習とコンシューマ デバイスへの変更通知。
- 履歴ログ データの読み取りによる既存の IP-to-user-identity マッピングに関する学習。

- GUI を使用して Cisco CDA を設定する設定メカニズムの提供、同時マッピング リストおよびログ イベントの表示。
- 期限切れマッピングの定期的なクリーニング。有効期限はユーザ ログイン TTL によって定義されます。

Cisco CDA はネットワーク内の次のコンポーネントと対話します。

- コンシューマ デバイス
- Active Directory ドメイン コントローラ マシン
- Syslog サーバ

コンシューマ デバイス

クライアント デバイスは Cisco CDA から最新の IP-to-user-identity マッピングをアクティブに取得（およびパッシブに受信）します。コンシューマ デバイスは次を行います。

- Cisco CDA から IP-to-user-identity マッピングの取得。
- Cisco CDA から IP-to-user-identity マッピングの通知の受信。
- ファイアウォール ポリシーに基づく ID の実施。
- Cisco CDA 経由での Active Directory 接続の基本モニタリング。
- グループ情報の Active Directory からの直接取得。
- Cisco CDA が ID にマッピングしなかった IP の Web 認証フォールバック。
- コンシューマ デバイスにより明らかになった新しいマッピングの Web 認証経由での Cisco CDA への転送。
- VPN セッションの IP-to-user-identity マッピングの転送。
- NetBIOS プローブの実行と切断通知の Cisco CDA への転送。

これらの更新は RADIUS Accounting-Request メッセージとして送信されます。

関連項目

- 「Active Directory ドメイン コントローラ マシン」（P.1-3）
- 「Syslog サーバ」（P.1-4）

Active Directory ドメイン コントローラ マシン

Cisco Context Directory Agent は、ユーザ ログインに関する情報を取得し、このデータをコンシューマ デバイスに提供するために、Active Directory ドメイン コントローラのセキュリティ イベント ログをモニタします。

起動時に、CDA はすでにログインしているユーザの時間ベースのウィンドウ（履歴）を読み取ります。CDA を起動し、実行すると、CDA はユーザ ログインをリアルタイムでモニタし、取得します。ユーザ ログイン イベントを取得するために、CDA と Active Directory ドメイン コントローラ間に接続が必要です。

Active Directory ドメイン コントローラに接続するために、CAD は Active Directory ユーザを使用します。

CAD で使用される Active Directory ユーザは、Active Directory ドメイン コントローラに接続し、モニタするために必要な権限が付与されている必要があります。

CAD で使用される Active Directory ユーザは、Domain Admin グループのメンバーであることができます。ただし、Cisco CDA パッチ 1（将来、CDA パッチはパッチ 1 の機能も含むようになります）をインストールしている場合は必須ではありません。

CDA と Active Directory ドメイン コントローラ間の接続は、MS NTLM プロトコルを使用しても認証されます。CDA パッチ 1 は NTLMv1 と NTLMv2 をサポートします。

関連トピック

- 「Active Directory ユーザが Domain Admin グループのメンバーである場合に必要な権限」（P.2-7）
- 「Active Directory ユーザが Domain Admin グループのメンバーでない場合に必要な権限」（P.2-7）

Syslog サーバ

Cisco CDA は、管理とトラブルシューティングに関する情報が含まれているログを 1 つ以上の Syslog サーバに転送できます。また、IP-to-user-identity マッピング情報の更新も行います。これらのログの内容は、Cisco CDA マシンでローカルに使用可能なカスタマー ログと同じです。Syslog メカニズムにより、Syslog サーバが実行されており、Syslog メッセージを受信できるターゲット マシンにこの情報がリモート配信されます。

関連項目

- 「コンシューマ デバイス」（P.1-3）
- 「Active Directory ドメイン コントローラ マシン」（P.1-3）

Cisco CDA のパフォーマンスとスケーラビリティ

Cisco CDA は最大 80 のドメイン コントローラ マシンに対応でき、また最大 64,000 の IP-to-user-identity マッピングを内部にキャッシュできます。最大 100 個の Identity コンシューマ デバイスに対応します。Cisco CDA は、最大 1000 の IP-to-user-identity マッピングを毎秒処理します（入力と出力）。

Cisco CDA は、3 台の Syslog サーバ、20 名の管理者、および 5 つの同時ドメイン管理 GUI セッションに対応することがテスト済みです。

CDA 導入に関する推奨事項

CDA を導入する際に、次の側面を考慮することを推奨します。

- Cisco CDA は、UDP プロトコルを使用してコンシューマ デバイスと相互運用できます。したがって、コンシューマ デバイスと地理的に近い場所に CDA を配置することを推奨します。これは、主に CDA が WAN 経由では時間がかかる可能性があるコンシューマ デバイスに大量のデータを送信するときに重要です。
- 導入時に、CDA ノードが Active Directory ドメイン コントローラからユーザ ログイン情報をすべて受け取ることを推奨します。これにより、コンシューマ デバイスは、すべてのユーザ ログイン データに対してローカルの CDA と相互運用できるようになります。さらに、Active Directory ドメイン コントローラを CDA と地理的に近い場所に配置することで信頼性が向上します。

- ハイ アベイラビリティを実現するために、両方の CDA が同じ Active Directory ドメイン コントローラから同じユーザ ログイン情報を取得するように設定された同じコンフィグレーションを持つ 2 つの CDA を使用することができます。最初の CDA が応答しない場合、2 番目の CDA に切替えるのはコンシューマ デバイスの役割です。

図 1-2　推奨される Cisco CDA の導入タイプ