Active Directoryコネクタのパフォーマンスについて

内容

はじめに

このドキュメントでは、Umbrella DNSのActive Directoryコネクタのパフォーマンスについて説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Umbrella DNSに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要

Umbrellaコネクタサービスは、UmbrellaのActive Directory統合の一部としてユーザ/コンピュータのログインイベントを監視するために使用されます。OpenDNSコネクタサービスは、そのサイトの各ADドメインコントローラのセキュリティイベントログからログイン情報を読み取ります。

ユーザログインイベントの頻度が高い環境では、これらのパフォーマンスガイドラインを確認することが重要です。正確なユーザ識別のために、コネクタサービスはログイン情報を迅速に取得できる必要があります。

最大イベント/秒

処理できるイベントの数に大きな制限はありません。Umbrellaコネクタサービスは、「サイト」内のすべてのドメインコントローラで1秒間に850イベントを継続的にサポートすることがテストされています。 これは、サードパーティ製ソフトウェアが実行されていない専用のラボ環境に基づいています。実際の結果は、ネットワーク遅延やその他のボトルネックによって異なります。

お客様は、この記事の後半にある「1秒あたりのイベント数」のセクションを参照して、おおよそのイベント数を確認できます。

新しい機能

ログインイベントの頻度が高い大規模な導入のお客様には、Umbrellaのパフォーマンス指向の新機能をご利用いただけます。一般的なパフォーマンスに関する推奨事項に加えて、ロードバランシング、パラレル通信、および直接イベントログリーダー接続に関するこの記事で後述するガイドラインも参照してください。

パフォーマンスの推奨事項

コネクタのサイズ

Active Directory Connectorサービスを実行するサーバには、Umbrellaのマニュアルのサイジングガイドで指定されているCPUおよびメモリリソースが必要です。

専用コネクタ

コネクタサービスはドメインコントローラに直接インストールできますが、Cisco Umbrellaでは

、コネクタサービス専用のメンバサーバにコネクタをインストールすることをお勧めします。このメンバサーバには、他のサードパーティ製ソフトウェアがインストールされていない必要があります。インストールプロセスの詳細については、Umbrellaのドキュメントを参照してください。

包括サイト

可能な限り、Umbrellaの導入は、ネットワーク上で通信するコンポーネントを制限する「サイト」に分離する必要があります。コネクタサービスは、同じUmbrellaサイト内のコンポーネントとのみ通信できます。この機能は、ユーザが地理的に広いエリアに分散して配置されている場合に必ず使用する必要があります。

通常、Umbrellaサイトは物理的な場所ごとに作成されます。Umbrellaサイトは、Umbrellaのドキュメントに次のルールが必要です。

Umbrellaサイトを適切に使用すると、展開が大幅に改善され、ワイドエリアネットワーク経由でコンポーネントが通信できなくなります。

ネットワーク遅延

ログインイベントは、ネットワークを介してコネクタに転送できます。 ネットワーク関連の遅延を減らすために、コネクタと各ドメインコントローラの間に高速接続を確立することが重要です。コネクタは、ドメインコントローラと仮想アプライアンスにできるだけ近い場所に配置できます。

コネクタの数

Umbrellaサイトごとに1つのコネクタが必要です。 Umbrellaサイトに複数のコネクタを配置することは可能ですが、冗長化の目的でのみ必要となります。追加のコネクタを使用すると、最初のコネクタと同じ機能を複製するため、ドメインコントローラに余分な負荷がかかります。Umbrellaでは、Umbrellaサイトごとに最大2つのコネクタを推奨しています。

イベントログのサイズ

Windowsセキュリティイベントログが大きいと、このWMI操作のパフォーマンスに悪影響を及ぼす可能性があります。 Umbrellaでは、イベントログのサイズを制限することを推奨しています。ログファイルのサイズが512 MB未満の場合に最適なパフォーマンスが得られますが、ログ保存要件に合わせて調整できます。ログファイルのサイズは、次の手順を使用して調整できます。

1. Event Viewerアプリケーション(eventvwr.msc)を開きます。

2. Windows Logs > Systemの順に移動します。

3. システムログを右クリックして、Propertiesを選択します。

4. 必要に応じて最大ログ・ファイル・サイズを調整し、OKを選択します。

サードパーティのソフトウェア

WMIを利用するソフトウェア製品は他にも多数あり、ドメインコントローラのWMIにボトルネックを発生させる可能性があります。これには次のものが含まれます。

- イベントログを監視するサードパーティ製のセキュリティ/分析ソフトウェア
- Windowsイベントログ転送
- SIEM統合と、イベントログを監視するその他のソフトウェア

このソフトウェアが不要になった場合は、無効にすることを推奨します。 または、付録に記載されている「イベントログリーダーの直接接続」を使用して、この問題を軽減することもできます。

アンチウイルスソフトウェア

アンチウイルススキャンから、このフォルダと次の実行可能ファイルを除外します。

```
C:\Program Files (x86)\OpenDNS\OpenDNS Connector
C:\Program Files (x86)\OpenDNS\OpenDNS Connector\OpenDNSAuditService.exe
C:\Program Files (x86)\OpenDNS\OpenDNS Connector\<VERSION>OpenDNSAuditClient.exe
```

追加のドメインコントローラ

ドメインコントローラのWMI通知システムは、各イベントログエントリをキューに入れて処理し、WMIサブスクライバに送信します。これは、イベントがDCによって送信されるプッシュメカニズムです。したがって、イベントの送信速度に影響を与えるパフォーマンスのボトルネックがドメインコントローラ自体に存在する可能性があります。

このボトルネックは、AD環境にドメインコントローラを追加することで軽減できます。Umbrellaでは、1台のドメインコントローラで最大850イベント/秒のテストを実施しました。

サービスアカウントの例外

サービスアカウントを除外することにより、Umbrellaで検出されるADログインの数を減らします。これらのアカウントは、正しいポリシーを適用するために除外する必要があります。 また、ADユーザポリシーを使用していないが、大量のユーザログオンを持つ可能性があるサーバやその他のデバイスを除外することもできます。

WMIパッチ

ドメインコントローラとコネクタサーバーが最新のMicrosoftパッチで最新であることを確認してください。既知のWMIパフォーマンスの問題を解決するホットフィックスの例を次に示します。

WMIメモリとハンドルの制限

WMIには、ボトルネックを発生させる可能性のある独自の内部制限が含まれています。これは、他のソフトウェアが集中的なWMI操作を実行している場合に特に当てはまります。これらの制限

を増やす方法の例については、Microsoftのドキュメントを参照してください。

Umbrellaサポートでは、お客様の環境に適した制限をアドバイスすることはできません。Microsoftにお問い合わせください。

DCロードバランシング

Umbrellaでは、ロードバランシング機能がサポートされるようになりました。この機能は、サイトに複数のドメインコントローラがあり、多数のログオンイベントがある場合に便利です。このシナリオでは、追加のコネクタがインストールされ、ロードバランシンググループを介してドメインコントローラがコネクタに割り当てられます。

単純な環境では、ロードバランシングは次のように機能します。

- DC_AとDC_Bは、Connector_1で処理されるロードバランシングGroup_1に割り当てられます。
- DC_CとDC_Dは、Connector_2で処理されるロードバランシングGroup_2に割り当てられます。
- 仮想アプライアンスは両方のコネクタからイベントを受信し続けるため、すべてのログオンイベントを認識し続けます。
- 冗長性が必要な場合、追加のコネクタを各ロードバランシンググループにインストールできます。

この機能には、次のような利点があります。

- 各コネクタの作業負荷が大幅に軽減されます。各コネクタが処理するドメインコントローラの数が少ない。
- これは通常、DCから受信するイベントの遅延が大きいシナリオで役立ちます。

ロードバランシングは、多数のドメインコントローラを持つ複雑なマルチサイト環境で使用できるように拡張できます。追加のコネクタを設置する以外に、ロードバランシングを使用する欠点はありません。

この時点で、Umbrellaサポートによってロードバランシング機能を有効にする必要があります。要件については、Umbrellaサポートにお問い合わせください。

仮想アプライアンスパラレル通信

コネクタは、デフォルトのシリアル方式を使用する代わりに、複数の仮想アプライアンスにログインイベントを同時に送信できるようになりました。 これは、サイトに複数の仮想アプライアンスがあり、多数のログオンイベントがある場合に便利です。

この機能には、次のような利点があります。

- 複数のアプライアンスが存在する場合に、ログイン情報の送信の遅延を最小限に抑えます。 イベントはすべてのアプライアンスに同時に送信できます。
- 1台のアプライアンスが他のアプライアンスに対して電源投入機能を持つことで、通信の問題や停止が発生することを防ぎます。 それぞれに対して個別のイベントキューが維持され

ます。

この機能は自動的に有効になりますが、サーバがCPUとメモリの推奨事項を満たしている場合に限られます。

ユーザログインイベントの転送の高速化

コネクタは、ユーザログインイベントをバッチで送信できるようになりました。これにより、仮想アプライアンスに送信できる1秒あたりのイベント数（1秒あたり）が大幅に増加します。 これは、コネクタがリモートロケーションの仮想アプライアンスと通信する場合に特に重要です。

この機能は自動的に有効にできますが、次の要件があります。

- パラレル通信（上記）を有効にする必要があります。 サーバは、CPUとメモリの推奨事項を満たしている必要があります。
- ADCバージョン1.8+が必要
- コネクタバージョン3.2.0+が必要

イベントログリーダーの直接接続

Active Directoryコネクタのバージョン1.4+では、WMIクエリを使用せずにドメインコントローラのセキュリティイベントログに直接接続する新しい方法がサポートされています。これにより、WMIは「中間者」ではなくなり、WMIがボトルネックになっている場合のパフォーマンスが大幅に向上します。これは、個々のドメインコントローラが多数のログインイベントを処理している場合に特に役立ちます。

この機能は、正しいユーザが識別されるのに短い（たとえば5秒）遅延が生じるように、コネクタが5秒ごとに新しいイベントをプルするプルメカニズムを使用して動作します。

この最適化はデフォルトで有効になっています。 この機能の詳細については、Umbrellaサポートにお問い合わせください。

イベント/秒

1秒あたりのイベント数を推定するために、ドメインコントローラの最近のイベント数をカウントすることができます。Umbrellaは、ピーク時に次の手順を実行することを推奨しています。

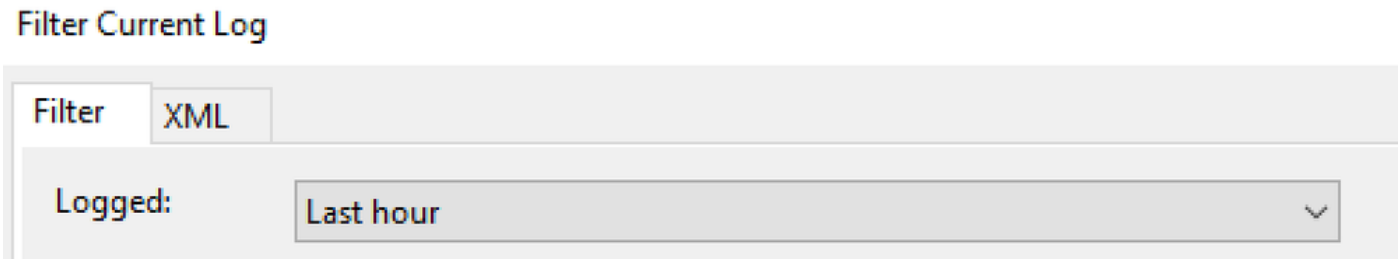
1. Event Viewerアプリケーション(eventvwr.msc)を開きます。

2. Windows Logs > Systemの順に移動します。

3.「現在のログをフィルタ」を選択し、「過去1時間に記録されたイベント」を選択します。

4.「OK」を選択します。

フィルタがロードされると、イベントログに過去1時間のイベント数が表示されます。この値を3600で除算すると、1秒あたりのイベント数を推定できます。



360024901511

360024894112

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。