ASA VPN ロード バランシング マスター選択プロセス

目次

概要

このドキュメントでは、Cisco 5500-X シリーズ適応型セキュリティ アプライアンス (ASA) を使用した VPN ロード バランシング シナリオのマスター選出プロセ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

このドキュメント内の情報は、ソフトウェア バージョン 9.2 を実行している Cisco ASA 5500-X に基づきます。

> **注:** このドキュメントは、この機能がバージョン 7.0(1) で初めて導入されて以降のすべてのソフトウェア バージョンにも適用されます。

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たものです。 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。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

VPN ロード バランシングは、ネットワーク トラフィックを仮想クラスタ内のデバイス間で均等に分散させるために使用されるメカニズムです。 ロード バランシングは単純な分散に基づいており、 アカウントのスループット使用率などの要素を考慮しません。 ロード バランシング クラスタは 1 つのマスター デバイスと 1 つ以上のセカンダリ デバイスの複数のデバイスで構成され、これらのデバイスは同じに設定する必要がありません。

ロード バランシング アルゴリズム

ロード バランシング アルゴリズムの概要を以下に示します。

- マスター デバイスは、内部 IP アドレスの昇順にソートされたセカンダリ クラスタ メンバーのリストを維持します。
- 負荷は、各セカンダリ クラスタ メンバーから提供される整数パーセンテージ（アクティブ セッション数/最大セッション数の値）として計算されます。
- マスター デバイスは、最初に、IPsec/セキュア ソケット レイヤ（SSL）VPN トンネルを負荷が最も低いデバイスにリダイレクトしますが、そのデバイスの負荷が他のデバイスより 1% 以上高くなるまでです。
- マスター デバイスは、すべてのセカンダリ クラスタ メンバーがマスター デバイスより 1% 以上高い場合にのみ、それ自体にリダイレクトします。

1 つのマスター クラスタ メンバーと 2 つのセカンダリ クラスタ メンバーを使用した例を以下に示します。

- すべてのノードが 0% の負荷で始まり、すべてのパーセンテージが最も近い 0.5% に丸められます。
- マスター デバイスは、すべてのメンバーの負荷がマスター デバイスより 1% 以上高い場合に接続を取得します。
- マスター デバイスが接続を取得しなかった場合は、最も負荷パーセンテージの低いバックアップ デバイスがセッションを取得します。
- すべてのメンバーの負荷パーセンテージが同じ場合は、セッション数が最も少ないバックアップ デバイスがセッションを取得します。
- すべてのメンバーの負荷パーセンテージが同じでセッション数も同じ場合は、IP アドレスが最も低いバックアップ デバイスがセッションを取得します。

マスター選出プロセス

VPN ロード バランシング マスター選出プロセスは、クラスタ外部ネットワーク上で実行されます。 次の 2 種類のデータが外部ネットワーク上で交換されます。

- マスターの検出に使用されるクラスタ IP アドレスの Address Resolution Protocol（ARP）パケットが交換されます。 マスターを検出するためにクラスタ IP アドレス宛てに送信される ARP パケットの最大数は、

  ((10 - priority) + 1 です。

  ここで、*priority* は **vpn load-balancing** CLI コマンドの **priority** サブコマンドで設定されます。

- Hello 要求/応答メッセージの外部で UDP パケットが交換されます。 ポート番号は、**cluster port** load-balancing サブコマンドで指定され、デフォルトで **9023** に設定されます。

たとえば、ロード バランシング デバイスの *priority* が 5 の場合は、マスター デバイスがクラスタ IP アドレスを所有しているかどうかを確認するために最大 6 回の ARP パケットの送信が試みられます。 マスター デバイスが検出されると、ASA は ARP メッセージの送信を停止し、15 秒待ってから UDP Hello 要求を送信します。 その後で、マスター デバイスが UDP Hello 応答を返します。

リブート シナリオに関する警告

ロード バランシング クラスタ内に 2 つの ASA が存在するリブート状況では：

- リブート前は ASA-1 と ASA-2 のどちらかがマスターでした。
- ASA-1 がリブートされます。
- ASA-2 が以前はマスターでなかった場合にマスターになります。
- ASA-1 はリブート後にスレーブとしてクラスタに参加するだけです。

ロード バランシング アルゴリズムは、クラスタ デバイスの外部インターフェイスが接続されるスイッチの設定の影響も受ける可能性があります。 たとえば、スイッチに接続されたデバイスがリブートされると、スパニングツリー アルゴリズムが接続の遅延を引き起こす可能性があります。

ヒント： spanning-tree port fast コマンドがプロセスの高速化に役立ちます。

新しくリブートした ASA は、ロード バランシングが有効になっていれば、スイッチ内の接続遅延が原因で現在のマスター デバイスに到達できないため、マスター デバイスになろうとします（マスター デバイスがすでに存在する場合でも）。 ARP コリジョンの結果としてマスターシップの競合が検出された場合は、Media Access Control（MAC）アドレスの低い ASA が選出されますが、MAC アドレスの高い ASA はマスター デバイスの役割を放棄します。

マスター再選出プロセス

マスター デバイスの再選出が次の 2 つの状況で発生します。

クラスタから削除されたマスター デバイス

ASA 上の機能を無効にすると、ブロードキャスト メッセージがすべてのクラスタ メンバーに送信されて変更が通知され、前述の選出プロセスが実行されます。

マスター デバイスがクラスタ メンバーの Hello メッセージに応答しない

マスター デバイスがクラスタ メンバーの Hello メッセージに応答しない場合は、ASA クラスタ メンバーがマスターが存在しないことを検出するのに約 20 秒かかります。 Hello メッセージは 5 秒ごとに送信されます (設定不可)。 クラスタ メンバーが 4 つの Hello メッセージの後にマスター デバイスからの応答を受信しなかった場合は、選出プロセスがトリガーされます。

トラブルシューティング

> **注: debug コマンド**を使用する前に、「debug コマンドの重要な情報」を参照してください。

次の debug コマンドは、システムに伴う問題をトラブルシューティングする場合に役に立つ可能性があります。

- **debug fsm 255**：このコマンドは、一般的な有限状態マシン デバッグをアクティブにするために使用します。 非アクティブにするには、**no debug all コマンド**を入力します。
- **debug menu vpnlb 3**：このコマンドは、VPN ロード バランシングのデバッグ トレースをアクティブにするために使用します。 非アクティブにするには、**debug menu vpnlb 3** コマンドを再度入力します。
- **debug menu vpnlb 4**：このコマンドは、VPN ロード バランシング関数トレースをアクティブにするために使用します。 非アクティブにするには、**debug menu vpnlb 4** コマンドを再度入力します。

関連情報

- **ロード バランシングの概要**
- **テクニカルサポートとドキュメント - Cisco Systems**