ASA VPN負載平衡導向器選擇過程

目錄

簡介

本檔案介紹使用Cisco 5500-X系列調適型安全裝置(ASA)的VPN負載平衡方案中的導向器選舉過程。

必要條件

需求

本文件沒有特定需求。

採用元件

本文檔中的資訊基於運行軟體版本9.2的Cisco ASA 5500-X。

> **附註**：本檔案也適用於所有軟體版本，因為這個功能是在版本7.0(1)中首次匯入。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

VPN負載平衡是一種機制，用於在虛擬集群中的裝置之間公平地分配網路流量。負載均衡基於簡單分配；它沒有考慮吞吐量利用率或其他因素。負載平衡集群由兩台或多台裝置、一台控制器和一個或多個輔助裝置組成，這些裝置不必進行相同的配置。

負載均衡演算法

以下是負載均衡演算法的概述：

- 控制器裝置維護按內部IP地址升序排序的輔助集群成員清單。
- 負載的計算方式為每個輔助集群成員提供的整數百分比（活動/最大會話數）。
- 導向器裝置首先將IPSec/安全套接字層(SSL)VPN隧道重定向到負載最低的裝置，直到其比其它裝置高1%。
- 僅當所有輔助集群成員都比導向器裝置高1%時，導向器裝置才會重定向到自己。

以下是一個具有一個導向器和兩個輔助群整合員的示例：

- 所有節點以零百分比負載開始，所有百分比都四捨五入到最接近的半百分比。
- 如果所有成員的負載都比導向器裝置高1%，則導向器裝置將接通。
- 如果指揮交換機裝置沒有建立連線，會話將由當前負載百分比最小的備份裝置建立。
- 如果所有成員都具有相同的負載百分比，則會話數量最少的備份裝置將使用該會話。
- 如果所有成員都具有相同的負載百分比和相同的會話數，則IP地址數量最少的備份裝置將使用該會話。

董事選舉程式

VPN負載平衡導向器選舉過程在群集外部網路上執行。在外部網路上交換的資料有兩種型別：

- 交換用於控制器發現的群集IP地址的地址解析協定(ARP)資料包。為了發現控制器，為群集IP地址傳送的ARP資料包的最大數量為：

  （10 — 優先順序）+ 1

  這裡的*priority*設定方式與**vpn load-balancing** CLI命令的**priority**子命令相同。

- 交換Hello請求/響應消息的外部的UDP資料包。埠號在**cluster port** load-balancing子命令中指定，預設為**9023**。

例如，如果負載均衡裝置的*優先順序*為5，它會嘗試傳送多達六個ARP資料包，以便檢視是否有任何控制器裝置擁有群集IP地址。如果檢測到導向器裝置，則ASA不再傳送任何ARP消息，並等待15秒後傳送UDP Hello請求。然後，指揮裝置會使用UDP Hello響應進行響應。

重新引導方案的警告

在負載平衡集群中有兩個ASA的重新啟動情況下：

- ASA-1或ASA-2在重新啟動前是控制器。

- ASA-1已重新啟動。
- 如果以前不是導向器，則ASA-2將成為導向器。
- ASA-1隻需在重新啟動後作為成員加入群集。

負載均衡演算法可能受同時連線集群裝置的外部介面的交換機配置的影響。例如，當連線到交換器的裝置重新開機時，跨距樹狀目錄演演算法可能會導致連線延遲。

> **提示：**spanning-tree port fast命令有助於加快處理速度。

在某些情況下，新重新啟動且已啟用負載平衡的ASA可能會嘗試成為控制器裝置（即使控制器裝置已存在），因為它由於交換機中的連線延遲而無法到達當前控制器裝置。當由於ARP衝突而檢測到導向器衝突時，具有低媒體訪問控制(MAC)地址的ASA將獲勝，而具有較高MAC地址的ASA將放棄導向器裝置角色。

董事重選程式

有兩種情況會導致控制器裝置重新選擇。

從群集中刪除導向器裝置

當您在ASA上禁用該功能時，將向所有集群成員傳送廣播消息以通知更改，並執行前面介紹的選擇過程。

導向器裝置不響應集群成員Hello消息

如果指揮交換機裝置不響應集群成員Hello消息，則ASA集群成員大約需要20秒才能檢測到指揮交換機不再存在。Hello消息每五秒傳送一次（不可配置）。 如果群整合員在傳送了四個Hello消息後沒有收到來自控制器裝置的響應，則會觸發選舉過程。

疑難排解

> **附註**：使用**debug**指令之前，請先參閱有關Debug指令的重要資訊Cisco一文。

以下debug指令可用於嘗試解決系統問題：

- **debug fsm 255** — 使用以下命令以啟用常規有限狀態機器調試。輸入**no debug all**命令以停用。
- **debug menu vpnlb 3** — 使用此命令啟用VPN負載平衡調試跟蹤。再次輸入**debug menu vpnlb 3**命令以停用。
- **debug menu vpnlb 4** — 使用此命令啟用VPN負載平衡功能跟蹤。再次輸入**debug menu vpnlb 4**命令以取消啟用。

相關資訊

- 瞭解負載平衡
- 技術支援與文件 - Cisco Systems