

Processo di scelta del director di bilanciamento del carico VPN ASA

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Algoritmo di bilanciamento del carico](#)

[Processo di elezione del direttore](#)

[Avvertenze per gli scenari di riavvio](#)

[Processo di rielezione del direttore](#)

[Periferica Director rimossa dal cluster](#)

[Il dispositivo Director non risponde ai messaggi Hello del membro del cluster](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto il processo di selezione dei director in uno scenario di bilanciamento del carico VPN con Cisco serie 5500-X Adaptive Security Appliance (ASA).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per questo documento, è stato usato uno switch Cisco ASA 5500-X con software versione 9.2.

Nota: Questo documento è valido anche per tutte le versioni del software, poiché la funzione è stata introdotta per la prima volta nella versione 7.0(1).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il bilanciamento del carico VPN è un meccanismo utilizzato per distribuire in modo equo il traffico di rete tra i dispositivi di un cluster virtuale. Il bilanciamento del carico si basa sulla distribuzione semplice; non tiene conto dell'utilizzo della produttività o di altri fattori. Un cluster di bilanciamento del carico è costituito da due o più dispositivi, un director e uno o più dispositivi secondari, che non devono essere configurati in modo identico.

Algoritmo di bilanciamento del carico

Di seguito è riportata una panoramica dell'algoritmo di bilanciamento del carico:

- Il dispositivo director gestisce un elenco ordinato di membri del cluster secondario in ordine crescente di indirizzi IP interni.
- Il carico viene calcolato come percentuale intera (numero di sessioni attive/massime) fornita da ciascun membro secondario del cluster.
- Il dispositivo director reindirizza il tunnel VPN IPSec/Secure Sockets Layer (SSL) a un dispositivo con il carico più basso, finché non supera dell'1% quello degli altri dispositivi.
- Il dispositivo director esegue il reindirizzamento a se stesso solo quando tutti i membri del cluster secondario sono superiori dell'1% rispetto al dispositivo director.

Di seguito è riportato un esempio con un director e due membri secondari del cluster:

- Tutti i nodi iniziano con un carico dello 0% e tutte le percentuali vengono arrotondate al mezzo punto percentuale più vicino.
- Il dispositivo director stabilisce la connessione se tutti i membri hanno un carico superiore dell'1% rispetto al dispositivo director.
- Se la connessione non viene stabilita dal dispositivo director, la sessione viene eseguita dal dispositivo di backup con la percentuale di carico più bassa.
- Se tutti i membri hanno la stessa percentuale di carico, la sessione viene eseguita dal dispositivo di backup con il minor numero di sessioni.
- Se tutti i membri hanno la stessa percentuale di carico e lo stesso numero di sessioni, la sessione viene eseguita dal dispositivo di backup con il minor numero di indirizzi IP.

Processo di elezione del direttore

Il processo di selezione del director di bilanciamento del carico VPN viene eseguito nel cluster all'esterno della rete. Nella rete esterna sono disponibili due tipi di dati:

- I pacchetti ARP (Address Resolution Protocol) per l'indirizzo IP del cluster utilizzati per l'individuazione del director vengono scambiati. Il numero massimo di pacchetti ARP inviati per l'indirizzo IP del cluster per individuare il director è:

(10 - priorità) + 1

In questo caso, la *priorità* è configurata come nel sottocomando **priority** del comando CLI **vpn load-balancing**.

- I pacchetti UDP esterni per i messaggi di richiesta/risposta Hello vengono scambiati. Il numero di porta è specificato nel sottocomando **cluster port** load-balancing ed è il valore predefinito **9023**.

Ad esempio, se la *priorità* è cinque per un dispositivo di bilanciamento del carico, tenta di inviare fino a sei pacchetti ARP per verificare se un dispositivo director possiede l'indirizzo IP del cluster. Se viene rilevato un dispositivo director, l'ASA non invia altri messaggi ARP e attende 15 secondi prima di inviare la richiesta UDP Hello. Il dispositivo director risponde quindi con una risposta UDP Hello.

Avvertenze per gli scenari di riavvio

In una situazione di riavvio con due appliance ASA in un cluster di bilanciamento del carico:

- Il director era ASA-1 o ASA-2 prima del riavvio.
- ASA-1 viene riavviato.
- ASA-2 diventa il regista se non era lui in precedenza.
- ASA-1 si unisce semplicemente al cluster come membro dopo il riavvio.

L'algoritmo di bilanciamento del carico potrebbe essere interessato da una configurazione dello switch in cui è connessa anche l'interfaccia esterna dei dispositivi del cluster. Ad esempio, un algoritmo Spanning-Tree potrebbe causare un ritardo nella connettività quando il dispositivo connesso allo switch viene riavviato.

Suggerimento: Il comando [spanning-tree port fast](#) aiuta a velocizzare il processo.

In alcuni casi, un'appliance ASA appena riavviata con bilanciamento del carico abilitato potrebbe tentare di diventare il dispositivo director (anche se esiste già un dispositivo director) perché non è in grado di raggiungere il dispositivo director corrente a causa di un ritardo di connettività nello switch. Quando viene rilevato un conflitto di direzione a causa di una collisione ARP, prevale l'ASA con un indirizzo MAC (Media Access Control) basso, mentre l'ASA con un indirizzo MAC più alto rinuncia al ruolo di dispositivo del director.

Processo di rielezione del direttore

Esistono due situazioni che causano la rielezione del dispositivo director.

Periferica Director rimossa dal cluster

Quando si disabilita la funzione sull'appliance ASA, a tutti i membri del cluster viene inviato un messaggio broadcast per informare della modifica e viene eseguito il [processo di selezione](#) descritto in precedenza.

Il dispositivo Director non risponde ai messaggi Hello del membro del cluster

Se il dispositivo director non risponde al messaggio Hello di un membro del cluster, un membro del cluster ASA impiega circa 20 secondi per rilevare che il director non è più presente. I messaggi Hello vengono inviati ogni cinque secondi (non configurabile). Se i membri del cluster non ricevono una risposta dal dispositivo director dopo quattro messaggi Hello, viene attivato il processo di selezione.

Risoluzione dei problemi

Nota: consultare l'articolo [Informazioni importanti sui comandi di debug](#) in Cisco prima di usare i comandi di **debug**.

I comandi di debug seguenti possono essere utili con i tentativi di risolvere i problemi del sistema:

- **debug fsm 255** - Utilizzare questo comando per attivare il debug generale della macchina a stati finiti. Immettere il comando **no debug all** per disattivarlo.
- **debug menu vpnlb 3** - Utilizzare questo comando per attivare la traccia di debug di bilanciamento del carico VPN. Immettere nuovamente il comando **debug menu vpnlb 3** per disattivarlo.
- **debug menu vpnlb 4** - Utilizzare questo comando per attivare la traccia della funzione di bilanciamento del carico VPN. Immettere nuovamente il comando **debug menu vpnlb 4** per disattivarlo.

Informazioni correlate

- [Informazioni sul bilanciamento del carico](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)