Configurazione del bilanciamento del carico F5 GTM delle appliance virtuali tramite gruppi di priorità

Sommario

[Introduzione](#)

[Panoramica](#)

[Istruzioni](#)

[Verifica](#)

Introduzione

In questo documento viene descritto come configurare un load balancer F5 che esegue GTM per il bilanciamento del carico delle connessioni alle appliance virtuali Umbrella.

Panoramica

Queste soluzioni utilizzano gruppi di priorità e un controllo dello stato che controlla la connettività DNS alle appliance virtuali e reindirizza il traffico in base alla disponibilità dell'appliance virtuale.

Per ulteriori informazioni sui load balancer F5, visitare il sito Web all'indirizzo <https://www.f5.com/glossary/load-balancer>.

Istruzioni

F5 ha la nozione di gruppi di priorità. Quando si configura un pool, è possibile assegnare a tutte le appliance virtuali una priorità più alta rispetto ai normali resolver DNS locali.

1. Assegnare un gruppo di priorità a ogni membro del pool Umbrella. I VA devono avere lo stesso numero di priorità più alta. I resolver locali di backup devono avere una priorità più bassa.
2. Crea un controllo di integrità che esegue una ricerca DNS. Questo passaggio assicura che il server DNS funzioni e ne disattiva uno dal pool se non funziona.
A tale scopo, viene utilizzato il controllo esterno dello stato di salute "dnsmonitor" disponibile qui: <https://devcentral.f5.com/codeshare?sid=390>.
3. Scaricare il codice dal link e salvarlo come file locale, "dnsmonitor"
4. Importare "dnsmonitor" in Sistema > Gestione file > Elenco file programma monitor esterno.
5. Creare un nuovo monitoraggio di controllo dello stato in Traffico locale > Monitor > Nuovo

monitoraggio. Qui stiamo facendo una ricerca di record A DNS per a.rootservers.net, che si spera sia sempre 198.41.0.4. Nelle argomentazioni specifichiamo ciò che stiamo cercando, "a.rootservers.net"; che tipo di documento, "A"; come ci aspettiamo che sia, "198.41.0.4"; e quanto tempo ci vuole, "2" secondi. Sostituire l'indirizzo di ricerca con un indirizzo adatto all'ambiente in uso o aggiungere altri controlli di integrità, se necessario

6. Ora aggiungiamo questo controllo alla nostra piscina. In Traffico locale > Pool > "ombrella (o il pool creato nel passaggio 1) > Proprietà, modificare Health Monitor con il nuovo dns-monitor-a.rootservers.net. È possibile selezionare più monitor di stato come suggerito in precedenza. Sarà inoltre necessario passare alla scheda Avanzate per selezionare i requisiti di disponibilità. Per ora, lo manterremo basico con un singolo monitor.
7. Creare un server virtuale e una porta per l'F5 su cui eseguire l'ascolto. Si tratta del BigIP o dell'IP virtuale interrogato dai client. Utilizza la piscina "a ombrello".

Verifica

È possibile verificare se si sta colpendo un'appliance virtuale eseguendo una query TXT per debug.opendns.com.

OSX/Linux - digita testo debug.opendns.com <IP VIP>

Windows - nslookup -type=txt debug.opendns.com <IP VIP>

Questo produce informazioni relative al vostro conto Umbrella. Cercare un campo denominato "ID accessorio". Il numero che segue è univoco per ciascuna appliance virtuale. È possibile verificare il bilanciamento del carico eseguendo la ricerca TXT e copiando l'ID dell'accessorio, quindi disconnettere la prima VA del pool ed eseguire di nuovo il comando. Si ottiene un ID da una delle altre VA del pool.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).