

Configurer l'équilibrage de charge F5 GTM des appareils virtuels à l'aide de groupes de priorités

Table des matières

[Introduction](#)

[Aperçu](#)

[Méthode](#)

[Vérification](#)

Introduction

Ce document décrit comment configurer un équilibreur de charge F5 exécutant GTM pour équilibrer la charge des connexions aux appareils virtuels Umbrella.

Aperçu

Cette solution utilise des groupes de priorité et un contrôle d'intégrité qui surveille la connectivité DNS aux appliances virtuelles et redirige le trafic en fonction de la disponibilité de l'appliance virtuelle.

Pour plus d'informations sur les équilibreurs de charge F5, consultez le site :

<https://www.f5.com/glossary/load-balancer>.

Méthode

F5 a la notion de groupes prioritaires. Lors de la configuration d'un pool, vous pouvez faire en sorte que tous les appareils virtuels aient une priorité supérieure à celle de vos résolveurs DNS locaux normaux.

1. Attribuez un groupe Priorité à chaque membre de votre piscine Umbrella. Les VA doivent avoir le même numéro de priorité plus élevé, vos résolveurs locaux de sauvegarde doivent avoir une priorité plus faible.
2. Créez un contrôle d'intégrité qui effectue une recherche DNS. Cette étape permet de s'assurer que le serveur DNS fonctionne et d'en désactiver un dans le pool s'il ne fonctionne pas.
Pour cela, nous utilisons le contrôle d'intégrité externe « dnsmonitor » disponible ici :
<https://devcentral.f5.com/codeshare?sid=390>.
3. Téléchargez le code à partir du lien et enregistrez-le dans un fichier local, « dnsmonitor »
4. Importez « dnsmonitor » sous System > File Management > External Monitor Program File List.

5. Créez un nouveau moniteur de contrôle d'intégrité sous Trafic local > Moniteurs > Nouveau moniteur. Ici, nous faisons une recherche d'enregistrement DNS A pour a.rootservers.net, qui est toujours, espérons-le, 198.41.0.4. Dans les arguments, nous spécifions ce que nous recherchons, «a.rootservers.net»; quel type d'enregistrement, «A»; ce que nous attendons de lui, «198.41.0.4»; et combien de temps cela prend, « 2 » secondes. N'hésitez pas à remplacer l'adresse de recherche par une adresse adaptée à votre environnement ou à ajouter d'autres contrôles d'intégrité si nécessaire
6. Nous ajoutons maintenant ce bilan de santé à notre pool. Sous Local Traffic > Pools > «umbrella (ou le pool que vous avez créé à l'étape 1) > Properties, remplacez Health Monitor par votre nouveau dns-monitor-a.rootservers.net. Vous pouvez sélectionner plusieurs moniteurs d'intégrité comme suggéré ci-dessus. Vous devez également accéder à l'onglet Avancé pour sélectionner les exigences en matière de disponibilité. Pour l'instant, nous allons simplement garder la base avec un seul moniteur d'état.
7. Créez un serveur virtuel ET un port d'écoute pour le F5. Il s'agit du BigIP ou de l'adresse IP virtuelle que vos clients recherchent. Il utilise la piscine « parapluie ».

Vérification

Vous pouvez vérifier que vous accédez à une appliance virtuelle en effectuant une requête TXT pour debug.opendns.com.

OSX/Linux - dig txt debug.opendns.com <IP VIP>

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

Cette commande fournit des informations relatives à votre compte parapluie. Recherchez un champ appelé « ID d'appareil ». Le numéro suivant est unique pour chaque appliance virtuelle. Vous pouvez vérifier qu'il s'agit d'un équilibrage de charge en exécutant la recherche TXT et en copiant l'ID de l'appliance, puis déconnectez la première appliance virtuelle du pool et exécutez à nouveau la commande pour obtenir un ID de l'une des autres appliances virtuelles de votre pool.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.