

Configurar o balanceamento de carga GTM F5 de dispositivos virtuais usando grupos de prioridade

Contents

[Introdução](#)

[Overview](#)

[Como fazer](#)

[Verificação](#)

Introdução

Este documento descreve como configurar um Balanceador de Carga F5 executando GTM para conexões de balanceamento de carga para Umbrella Virtual Appliances.

Overview

Essa solução utiliza grupos de prioridade e uma verificação de integridade que monitora a conectividade DNS para dispositivos virtuais e redireciona o tráfego com base na disponibilidade do dispositivo virtual.

Mais informações sobre os Balanceadores de Carga F5 podem ser encontradas aqui:

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

Como fazer

F5 tem a noção de grupos de prioridade. Ao configurar um pool, você pode fazer com que todos os dispositivos virtuais tenham uma prioridade mais alta do que seus resolvedores DNS locais normais.

1. Atribua um grupo Prioridade a cada membro do seu pool Umbrella. Os VAs devem ter o mesmo número de prioridade mais alto; seus resolvedores locais de backup devem ter uma prioridade mais baixa.
2. Crie uma verificação de integridade que faça uma pesquisa DNS. Esta etapa garante que o servidor DNS esteja funcionando e desabilita um do pool se não estiver funcionando. Para isso, estamos usando a verificação de integridade externa "dnsmonitor" disponível aqui: <https://devcentral.f5.com/codeshare?sid=390>.
3. Faça o download do código do link e salve-o como um arquivo local, "dnsmonitor"
4. Importe "dnsmonitor" em System > File Management > External Monitor Program File List.

5. Crie um novo monitor de verificação de integridade em Tráfego local > Monitores > Novo monitor. Aqui estamos fazendo uma pesquisa de registro DNS A para a.rootservers.net, que esperamos que seja sempre 198.41.0.4. Nos argumentos, especificamos o que estamos procurando, "a.rootservers.net"; que tipo de registro, "A"; o que esperamos que seja, "198.41.0.4"; e quanto tempo leva, 2 segundos. Sinta-se à vontade para alterar o endereço de pesquisa para algo que seja adequado ao seu ambiente ou adicionar mais verificações de integridade, se necessário
6. Agora adicionamos este exame de saúde à nossa piscina. Em Local Traffic > Pools > "umbrella (ou qualquer pool criado na Etapa 1) > Properties, altere o Health Monitor para nosso novo dns-monitor-a.rootservers.net. Você pode selecionar vários monitores de integridade conforme sugerido acima. Você também precisará acessar a guia avançado para selecionar o requisito de disponibilidade. Por enquanto, vamos manter tudo básico com um único monitor de saúde.
7. Crie um servidor virtual E uma porta para o F5 ouvir. Esse é o BigIP ou IP virtual que seus clientes consultam. Ele usa o pool de "guarda-chuvas".

Verificação

Você pode verificar se está acessando um Virtual Appliance fazendo uma consulta TXT para debug.opendns.com.

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

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

Isso gera informações com relação à sua conta Umbrella. Procure um campo chamado "id do equipamento". O número depois disso é exclusivo para cada dispositivo virtual. Você pode verificar se ele está balanceando a carga executando a pesquisa TXT e copiando a ID do dispositivo, depois desconecte o primeiro VA no pool e execute o comando novamente para obter uma ID de um dos outros VAs em seu pool.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.