DevCentral Top 5: Nov 3, 2014

John Wagnon, 2014-03-11

Make sure you grab a tissue, because you will literally weep when you read the awesome content so prominently and consistently delivered in our community. And, even if you don't weep uncontrollably, you'll at least work up a couple of tears. And, for that one guy who has no viable tear ducts in his face...you won't physically create tears while reading these articles, but you will undoubtedly learn something new and amazing. With that, I proudly present this edition of the DevCentral Top 5:

The Top Ten Hardcore F5 Security Features in BIG-IP 11.6

I couldn't resist highlighting a "top ten" article inside a "top 5" article. It just makes sense. David Holmes does a great job of picking out 10 of the 29 new security features available in the upcoming BIG-IP 11.6 release. I won't list them all here (since that's kind of the whole point of David's article), but I will tell you that the list includes things like DNS firewall features, hardware DDoS integration, geo-location anomaly detection, flow table sweeper enhancements, and external crypto offloading. What's more, David shows how these new features are built into several different BIG-IP modules (GTM, vCMP, ASM, APM, AFM, LTM). F5 takes security very seriously, and it shows by the way these security features are baked into the core of so many BIG-IP modules. Upgrade to 11.6 and enjoy all these rock-star security features!

F5 Proudly Optimizing the Network for Microsoft's Cloud Platform System

Ryan Korock reminds us that the single largest transformation of the traditional data center in recent history is the concept of the "Private Cloud". We all want it, and we want it now! Well, guess what? It's not always that easy to move the "Private Cloud" from vision to reality. A true "Private Cloud" includes aspects of compute, storage, and network...all of which are probably delivered by different vendors who adopted different APIs and management toolsets. It doesn't take long to see how this "Private Cloud" orchestration can get very complex and expensive. Microsoft recently announced a "converged infrastructure" that delivers pre-built offerings that are designed to have all the necessary pieces working together before they ever reach the customer's data center. Microsoft delivered a completely automated solution (called the Cloud Platform System) that includes best of breed technologies on the compute, storage, and network components. The other good news is that Microsoft partnered with F5 to make all this happen. The BIG-IP's RESTful API provides the ability to automate both configuration and device management while the traffic management engine allows flexibility for workflow traffic. It's a match made in heaven!

SSLv3 POODLE mitigation recommendations

If you need to mitigate a recent security vulnerability (or any security vulnerability for that matter), Jeff Costlow is your guy. In this article, Jeff builds on his discussion of the recent POODLE vulnerability. The best solution to POODLE is to disable SSLv3. Unfortunately, many legacy clients can't disable SSLv3. What to do, right? Well, Jeff and his team of super-smart security experts have investigated the use of RC4 in mitigating POODLE on legacy clients. While RC4 does have a known weakness (an attacker could recover plaintext after several hundred million messages), the POODLE vulnerability allows an attacker to recover plaintext after a few thousand messages. So, if you *can't disable SSLv3*, it makes more sense to enable RC4-SHA *only for use in SSLv3 sessions*. This article shows you how to configure your virtual server to do exactly what we just talked about. Jeff reminds us at the end of his article that it is still recommended to disable SSLv3 and RC4 once you are able to remove all legacy clients. Thanks for keeping us safe, Jeff!

SDN is important to the Internet of Things if it covers the entire network

When it comes to a good debate on SDN and IoT, no one can go more rounds than Lori MacVittie. In this article, Lori discusses SDN as a major enabler of IoT...and she notes that SDN must include the entire network (layers 2-7). The SDN tendency is to remain stuck in the stateless layers 2-4 with a focus on routing and switching and basic forwarding. While that piece works great for dealing with bandwidth issues and peak traffic, it doesn't address scaling out access or security services, or scaling out the apps themselves. For that, you need to reach up the stack and look to stateful layers 4-7. Let's be honest...if/when you're gonna deploy SDN, you need to do it correctly (and completely)!

LineRate Performance Tip: Logging in Node.js

Andrew Jenkins hits a home run with this technical article on logging behaviors in Node.js (he even includes a classic "Bob Newhart" clip from yesteryear). As you may or may not know, LineRate's Node.js engine lets you program in the datapath with JavaScript. Once you embed business logic in your proxy, you'll need to debug this logic and report on the actions your proxy is taking. Whether your service scales to millions of requests per second, or just a trickle, there are some simple performance considerations that you should keep in mind. Andrew does a great job of outlining several logging tips to consider...things like using log levels, deferring string concatenation, considering stdout/stderr differences, and getting counters on demand. Knowing these tips up front prevents you from learning expensive habits that are harder to fix later. Thanks for the great tips, Andrew!