Getting Started with Splunk for F5

Jason Rahm, 2011-26-04

Pete Silva & Lori MacVittie both had blog posts last week featuring the F5 Application for Splunk, so I thought I'd take the opportunity to get Splunk installed and check it out. In this first part, I'll cover the installation process. This is one of the easiest installions I've ever written about--it's almost like I'm cheating or something.

Installing Splunk

My platform of choice for this article is Ubuntu, so I downloaded the 4.2.1 Debian package for 64-bit systems from the Splunk site. Installation is a one step breeze:

> dpkg –i /var/tmp/splunk-4.2.1-98165-linux-2.6-amd64.deb

After installation (defaulting to /opt/splunk) start the Splunk server:

> /opt/splunk/bin/splunk start

I had to accept the license agreement during the startup process. Afterwards, I was instructed to point my browser to http:<server>:8000. I logged in with the default credentials (admin / changeme) and then was instructed to change my password, which I did (you can skip this step if you prefer). Pretty easy path to an completed installation. The browser should now be in the state shown below in Figure 1.
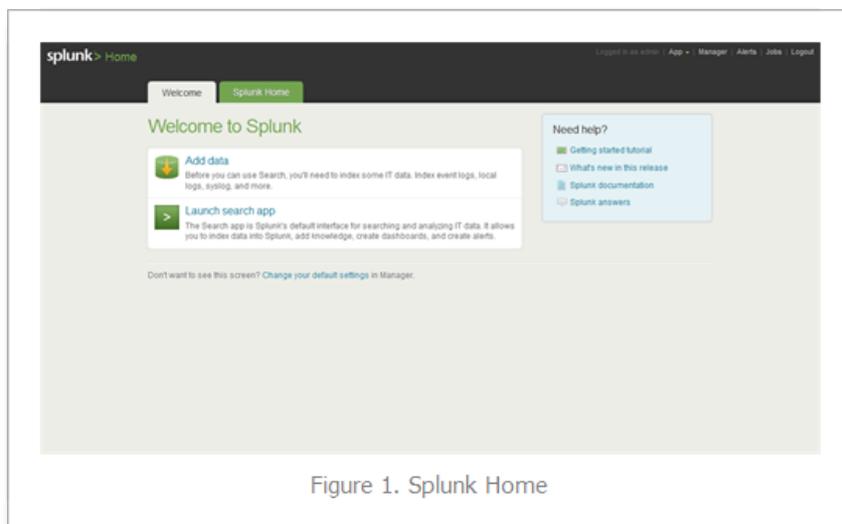

Figure 1. Splunk Home

Installing Splunk for F5

Click on Manager in the upper right-hand corner of the screen, which should take you to the screen shown below in Figure 2.
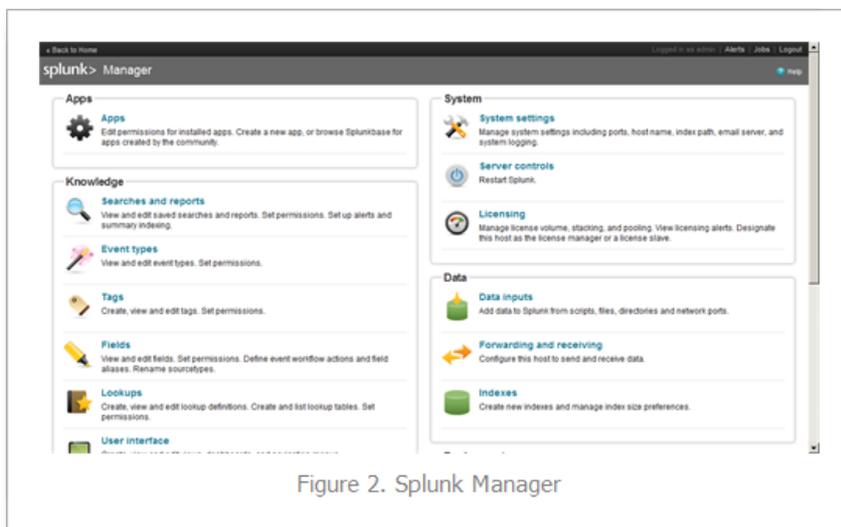
Figure 2. Splunk Manager
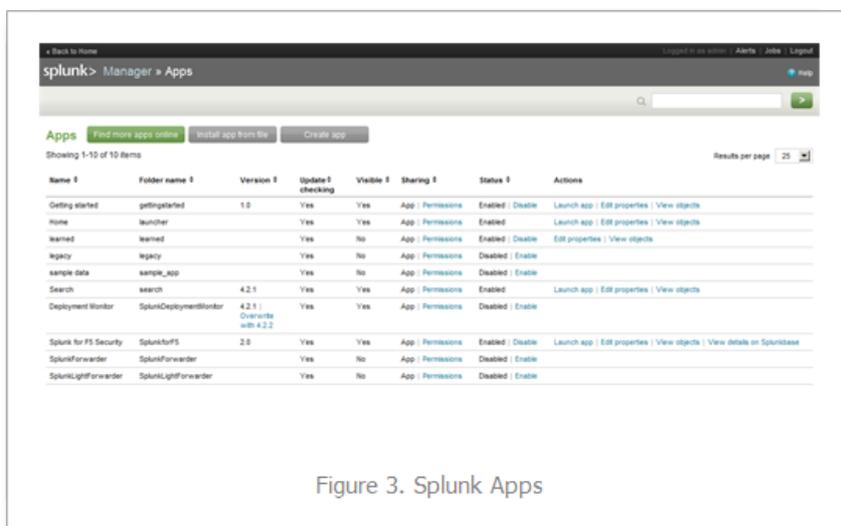
Next, click on Apps as shown below in Figure 3.

Figure 3. Splunk Apps

At this point you have a choice. If you downloaded the Splunk for F5 app from splunkbase, you can click the "install app from file" button. I chose to install from the web, so I clicked the "find more apps online" button. This loaded a listing from splunkbase, with the Splunk for F5 app shown at the bottom of Figure 4 below.
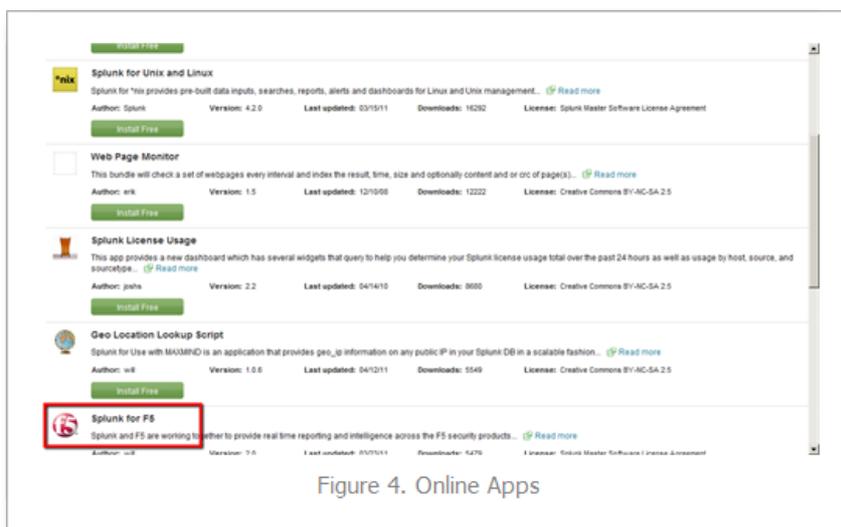

Figure 4. Online Apps

After clicking the "install Free" button, I had to enter my splunk.com credentials, then the application installed. Splunk requested a restart, so I restarted and then logged back in. My new session was returned to the online apps screen, so to get to my new F5 app, I clicked "back to search" in the upper left corner, which took my to the Search app home page. Finally, in the upper right corner I selected App and then clicked "Splunk for F5 Security". This resulted in the screen show below in Figure 5.
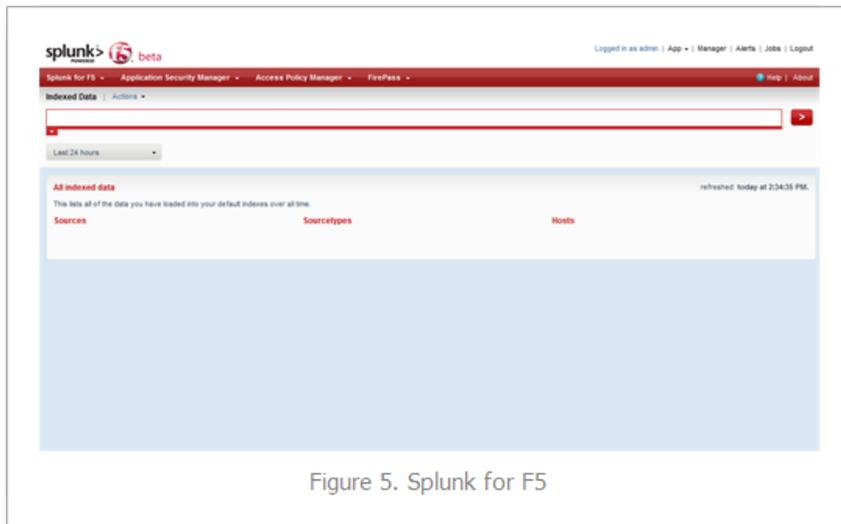
Figure 5. Splunk for F5

Success! Now…what to do with it? How is this useful? Check back for part two next week… For some hints, check out the blogs I mentioned at the top of this article from Pete and Lori:

- Spelunking for Big Data
- Do You Splunk 2.0

Other Related Articles

- Do you Splunk?
- ASM & Splunk integration - DevCentral - F5 DevCentral > Community ...
- F5 Networks Partner Spotlight - Splunk
- f5 ltm dashboard in splunk - DevCentral - F5 DevCentral ...
- Logging HTTP traffic to Splunk - DevCentral - F5 DevCentral ...
- Client IP Logging with F5 & Splunk - DevCentral - F5 DevCentral ...

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc. Corporate Headquarters info@f5.com	F5 Networks Asia-Pacific apacinfo@f5.com	F5 Networks Ltd. Europe/Middle-East/Africa emeainfo@f5.com	F5 Networks Japan K.K. f5j-info@f5.com