Servers, SUSE, Red Hat and Fedora

By *Roy Schestowitz*
Created *09/08/2019 - 2:29am*
Submitted by Roy Schestowitz on Friday 9th of August 2019 02:29:13 AM Filed under GNU [1] Linux [2] Red Hat [3] Server [4] SUSE [5]

- **My Favorite Infrastructure [6]**

  PCI policy pays a lot of attention to systems that manage sensitive cardholder data. These systems are labeled as "in scope", which means they must comply with PCI-DSS standards. This scope extends to systems that interact with these sensitive systems, and there is a strong emphasis on compartmentation?separating and isolating the systems that are in scope from the rest of the systems, so you can put tight controls on their network access, including which administrators can access them and how.

  Our architecture started with a strict separation between development and production environments. In a traditional data center, you might accomplish this by using separate physical network and server equipment (or using abstractions to virtualize the separation). In the case of cloud providers, one of the easiest, safest and most portable ways to do it is by using completely separate accounts for each environment. In this way, there's no risk that a misconfiguration would expose production to development, and it has a side benefit of making

it easy to calculate how much each environment is costing you per month.

When it came to the actual server architecture, we divided servers into individual roles and gave them generic role-based names. We then took advantage of the Virtual Private Cloud feature in Amazon Web Services to isolate each of these roles into its own subnet, so we could isolate each type of server from others and tightly control access between them.

By default, Virtual Private Cloud servers are either in the DMZ and have public IP addresses, or they have only internal addresses. We opted to put as few servers as possible in the DMZ, so most servers in the environment only had a private IP address. We intentionally did not set up a gateway server that routed all of these servers' traffic to the internet?their isolation from the internet was a feature!

Of course, some internal servers did need some internet access. For those servers, it was only to talk to a small number of external web services. We set up a series of HTTP proxies in the DMZ that handled different use cases and had strict whitelists in place. That way we could restrict internet access from outside the host itself to just the sites it needed, while also not having to worry about collecting lists of IP blocks for a particular service (particularly challenging these days since everyone uses cloud servers).

[...]

Although I covered a lot of ground in this infrastructure write-up, I still covered only a lot of the higher-level details. For instance, deploying a fault-tolerant, scalable Postgres database could be an article all by itself. I also didn't talk much about the extensive documentation I wrote that, much like my articles in Linux Journal, walks the reader through how to use all of these tools we built.

As I mentioned at the beginning of this article, this is only an example of an infrastructure design that I found worked well for me with my constraints. Your constraints might be different and might lead to a different design. The goal here is to provide you with one successful approach, so you might be inspired to adapt it to your own needs.

- **A Blunt Reminder About Security for Embedded Computing [7]**

  The ICS Advisory (ICSA-19-211-01) released on July 30th by the Cybersecurity and Infrastructure Security Agency (CISA) is chilling to read. According to the documentation, VxWorks is ?exploitable remotely? and requires ?low skill level to exploit.? Elaborating further, CISA risk assessment concludes, ?Successful exploitation of these vulnerabilities could allow remote code execution.?
  The potential consequences of this security breech are astounding to measure, particularly when I look back on my own personal experiences in this space, and now as an Account Executive for Embedded Systems here at SUSE.

  [...]

At the time, VxWorks was the standard go-to OS in the majority of the embedded production platforms I worked with. It was an ideal way to replace the legacy stove-piped platforms with an Open Architecture (OA) COTS solution. In light of the recent CISA warning, however, it is concerning to know that many of those affected systems processed highly-classified intelligence data at home and abroad.

- **Red Hat Recognized as a Leader by Independent Research Firm in Infrastructure Automation Platforms Evaluation [8] [Ed: Forrester is not ?Independent Research Firm?; It?s taking bribes to lie [9].]**

- **Why Red Hat can take over the cloud sooner than you think [10]**

- **Red Hat Enterprise Linux 7.7: Final Full Support Update [11]**

- **Transport Layer Security version 1.3 in Red Hat Enterprise Linux 8 [12]**

  TLS 1.3 is the sixth iteration of the Secure Sockets Layer (SSL) protocol. Originally designed by Netscape in the mid-1990?s to serve the purposes of online shopping, it quickly became the primary security protocol of the Internet. Now not limited just to web browsing, among other things, it secures email transfers, database accesses or business to business communication.

  Because it had its roots in the early days of public cryptography, when public knowledge about securely designing cryptographic protocols was limited, the first two iterations: SSLv2 and SSLv3 are now quite thoroughly broken. The next two iterations, TLS 1.0 and TLS 1.1 depend on the security of Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA1).

- **Cute Qt applications in Fedora Workstation [13]**

  Fedora Workstation is all about Gnome and it has been since the beginning, but that doesn?t mean we don?t care about Qt applications, the opposite is true. Many users use Qt applications, even on Gnome, mainly because many KDE/Qt applications don?t have adequate replacement written in Gtk or they are just used to them and don?t really have reason to switch to another one.

  For Qt integration, there is some sort of Gnome support in Qt itself, which includes a platform theme reading Gnome configuration, like fonts and icons. This platform theme also provides native file dialogs, but don?t expect native look of Qt applications. There used to be a gtk2

style, which used gtk calls directly to render natively looking Qt widgets, but it was moved from qtbase to qt5-styleplugins, because it cannot be used today in combination with gtk3.

For reasons mentioned above, we have been working on a Qt style to make Qt applications look natively in Gnome. This style is named adwaita-qt and from the name you can guess that it makes Qt applications look like Gtk applications with Adwaita style. Adwaita-qt is actually not a new project, it?s been there for years and it was developed by Martin B?íza. Unfortunately, Martin left Red Hat long time ago and since then a new version of Gnome?s Adwaita was released, completely changing colors and made the Adwaita theme look more modern. Being the one who takes care of these things nowadays, I started slowly updating adwaita-qt to make it look like the current Gnome Adwaita theme and voilà, a new version was released after 3 months of intermittent work.

- **Fedora Community Blog: Friday with Infra** **[14]**

  Friday with Infra is a new event done by CPE (Community Platform Engineering) Team, that will help potential contributors to start working on some of the applications we maintain. During this event members of the CPE team will help you to start working on those applications and help you with any issue you may encounter. At the end of this event you should be able to maintain the application by yourself.

GNU Linux Red Hat Server SUSE

Source URL: http://www.tuxmachines.org/node/126767

Links:
[1] http://www.tuxmachines.org/taxonomy/term/144
[2] http://www.tuxmachines.org/taxonomy/term/63
[3] http://www.tuxmachines.org/taxonomy/term/142
[4] http://www.tuxmachines.org/taxonomy/term/147
[5] http://www.tuxmachines.org/taxonomy/term/117
[6] https://www.linuxjournal.com/content/my-favorite-infrastructure
[7] https://www.suse.com/c/a-blunt-reminder-about-security-for-embedded-computing/
[8] https://www.redhat.com/en/about/press-releases/red-hat-recognized-leader-independent-research-firm-infrastructure-automation-platforms-evaluation
[9] http://techrights.org/wiki/index.php/Forrester
[10] https://www.zdnet.com/video/from-linux-to-cloud-why-red-hat-matters-for-every-enterprise/
[11] https://adtmag.com/articles/2019/08/08/red-hat-linux.aspx
[12] https://www.redhat.com/en/blog/transport-layer-security-version-13-red-hat-enterprise-linux-8
[13] https://jgrulich.cz/2019/08/07/cute-qt-applications-in-fedora-workstation/
[14] https://communityblog.fedoraproject.org/friday-with-infra/