Servers and Proprietary Software Leftovers

By Roy Schestowitz
Created 21/11/2021 - 12:14am

- OpenHPC Announces Release of OpenHPC 2.4 [3]
  This is an update release for the OHPC 2.x branch targeting support for RHEL8 variants and OpenSUSE Leap 15. In addition to a number of component version updates, this release updates previous CentOS8-based recipes to leverage Rocky8.

- Docker really did change the world | InfoWorld [4]
  In 2013, Docker was the ?it? company. Docker made headlines for the critical role it played in bringing containers to the mainstream, and in many ways displaced PaaS as the hotness of the time (Heroku anyone?). Now, the company is back in the press with the introduction of a new model for Docker Desktop that requires larger organizations to buy a paid subscription for the tools. There?s been a vocal reaction to this announcement, one that reminds me of the important role Docker played in popularizing a model we know, love, and now use on a mainstream basis: containers.

  [...]

  By 2009, the value of using virtualization was well understood and it was widely deployed. Most organizations had already garnered the benefits of virtualization or had a roadmap to get there. The marketing machine was tired of virtualization. People were hungry for the next innovation in IT and software development. It came in the form of Heroku. In fact, PaaS in general and Heroku specifically became wildly popular. So much so that it looked like PaaS
was going to take over the world.

At that time, Heroku was huge. You just go out to this portal and develop your apps and deliver them as a service? What?s not to like? Why wouldn?t you develop apps on Heroku?

As it turned out, there were a couple of good reasons not to use Heroku and PaaS platforms of its ilk. For example, applications built on Heroku were not portable; they were available only within Heroku. Developers had to work remotely on the PaaS platform if they wanted to collaborate. Unlike Netflix, it turns out, developers love to develop locally. If a developer wanted to work on their local box, they were still left to manually build the environment themselves.

In addition, although the Heroku model was extremely powerful if you used what was provided out of the box, it was complex behind the scenes. As soon as your team built something more complex than a simple web app, or they needed to customize the infrastructure for security or performance reasons, it became a difficult, very ?real? engineering problem.

---

**SD Times news digest: Databricks launched Partner Connect; OpenAI?s API now available with no waitlist; Logz.io unveils observability updates - SD Times** [5]

The Linux Foundation, the nonprofit enabling innovation through open source, and The Cloud Native Computing Foundation, which builds sustainable ecosystems for cloud native software, have announced that the Kubernetes and Cloud Native Associate (KCNA) exam, originally announced last month, is now generally available for enrollment and scheduling.

In addition, a new online training course, Kubernetes and Cloud Native Essentials, has been released to both prepare individuals for entry level cloud roles and to sit for the KCNA exam. KCNA is made up of a multiple-choice certification exam designed to test entry-level knowledge and skills in Kubernetes as well as the wider cloud native ecosystem.

The KCNA exam is broken up into different sections, including Kubernetes fundamentals, container orchestration, cloud native architecture, cloud native observability, and cloud native application delivery.

---

**NCSC on rise in ransomware attacks** [6] [Ed: A Windows problem [7]]

Over the past 12 months the UK official National Cyber Security Centre (NCSC) has responded to a rise in ransomware attacks, and a range of services have been provided to businesses over the year to help protect them from ransomware. That?s according to the NCSC?s annual report on its fifth year of working, to August 2021.
Security of the software supply chain has gained significant attention over the past year. Two major cybersecurity attacks—SolarWinds and Kaseya—proved sharp reminders to reexamine every component of software development and deployment, including what they are and where they came from.

The first signs of major supply chain vulnerability actually showed up over four years ago when the malware wiper NotPetya was launched against Ukraine in 2017. NotPetya attackers, believed to be threat actors in the Russian military, allegedly injected malicious code into accounting software owned by a Ukrainian company. The result was an estimated $10 billion in damages that impacted organizations across Asia, Europe and the Americas.

Source URL: http://www.tuxmachines.org/node/158194

Links: