How PaaS & Containerization Can Improve Government IT

redhat.

INDUSTRY PERSPECTIVE

INTRODUCTION

"What every agency wants to do is serve their constituents. We don't want IT to prevent that from happening, so problems are being solved by the marketplace and by the open source community, such that talented developers and agency personnel can actually do the work they're tasked to do."

JOHN KEESE
DIRECTOR OF GOVERNMENT CLOUD SERVICES FOR CSRA

Efficiency and security top the wish lists of government officials who want to migrate to the cloud. Since the Cloud First policy was issued in 2011, the federal government has made some headway in adopting cloud technology.

Fortified cloud technologies need to start with a sound foundational infrastructure, but building that groundwork is such a massive undertaking that most agencies can't do it alone. They need the guidance that comes through partnering with private companies that are experts in the continuously evolving cloud. To encourage such relationships, the government has made it easy for agencies to know at a glance which companies offer secure cloud products. Those companies that earn security certifications from the Federal Risk and Authorization Management Program (FedRAMP) and adhere to international computer security standards such as Common Criteria pave the way for agencies to feel confident that the solutions they're procuring are secure.

Increasingly, those solutions are based on the work of the open source community. "Open source" refers to code or technology that can be modified and shared by anyone because its design is publicly accessible. Instead of just a few people working on a solution, thousands of developers all over the world are able to make improvements collectively, which leads to innovation, improved code, and better products.

Open source technology and cloud have a long and solid relationship. Most of the largest cloud provider companies are built on open source technologies. Now, software firm Red Hat has made this consumable for enterprise users, enabling agencies to take that technology that they've been using as public cloud consumers and bring it to their own data centers. This offers end users plenty of benefits as well. Open source platforms improve cloud technology, help to end vendor lock-in and maximize efficiency.

For example, take OpenShift Enterprise, a Platform as a Service (PaaS) product from Red Hat, the world's leading provider of open source solutions. Based on OpenShift Origin, the platform plays a major role in solutions from FedRAMP-approved cloud provider BlackMesh and in ARCWRX, an open source PaaS cloud services platform from CSRA, formerly Computer Sciences Corp. (CSC).

PUTTING IT ALL TOGETHER

OpenShift makes use of three cloud tools to maximize security and drive productivity by enabling developers to focus on their main objective — writing code:

- Gartner's model of bimodal IT, defined by the market research firm as "the practice of managing two separate, coherent modes of IT delivery, one focused on stability and the other on agility. Mode 1 is traditional and sequential, emphasizing safety and accuracy. Mode 2 is exploratory and nonlinear, emphasizing agility and speed." That translates to a new way of organizing IT to meet agencies' needs.

- Linux containers, which are lightweight technical environments in which applications live

- Kubernetes, an open source project developed for container management and orchestration that automates the deployment, scaling, and operation of containers across clusters of hosts.

To better understand how these three tools go hand-in-hand, we talked with Adam Clater, Chief Cloud Architect with the Office of the Chief Technologist of Red Hat's North America Public Sector organization; John Keese, Director of Government Cloud Services for CSRA (formerly CSC government services) and BlackMesh Co-Founder Jason Ford.

Read on to learn how Red Hat's OpenShift can help government agencies, how companies are putting it to use in their solutions, what to ask yourself and your industry partners before moving to the cloud, and what best practices can help your agency deploy a secure cloud implementation.

Let's look at how technology has evolved to bring us to this technical trifecta. First, we need to understand the overall platform, PaaS. Until recently, cloud technology has been deployed in the form of Infrastructure as a Service (IaaS), which is essentially the virtualization of a physical server plus the ability for elastic compute, which lets users spin up and scale server types via a provisioning portal, Keese said. The PaaS environment, however, separates the IaaS stack into separate parts, orchestrated by Kubernetes. Overall, it enables the automatic expansion and contraction of computing power based on the demand on an application's containers.

"In an IaaS environment, your provisioning portal is the front end, where systems administrators go to create infrastructure," Keese said. "In PaaS, the underlying cloud platform then orchestrates the placement of those servers on what they call compute nodes." That orchestration happens through Kubernetes, an open source tool built for handling a large number of containers, which would be difficult to coordinate manually, Clater said. It takes care of the resources a containerized service or application needs and places them on nodes. When nodes go down for maintenance or need to be increased or decreased, Kubernetes helps the cloud provider put the containerized resource on a different compute node and move it as needed.

In a containerized environment, each part of the computing stack — the database and middleware — is abstracted from the underlying operating system and put in its own container. Coupled with PaaS, the containers have a semblance of the OS, freeing developers from having to worry about this.

"They only have to worry about the types of applications that would typically sit on a virtualized server, and deploy those in the containers," Keese said. "As demand on that entire compute environment expands — for instance, with heavy database activity — Kubernetes works with the broker, the OpenShift broker in this case, and creates multiple containers of PostgreSQL databases, multiple containers of Apache, or multiple containers of JBoss [Red Hat middleware], and it does so in an auto-scaling feature."

Think of it this way, Keese said: "Those components are like Legos that can be stacked on top of each other. In a containerized world, each one of those Legos is essentially decoupled from the others, but they're all interrelated so if one Lego needs to get bigger, it gets bigger, and then it contracts again."

The decoupling of the IaaS stack by PaaS increases the security of the underlying OS because IT managers no longer have to install patches to it and each application to harden the whole system, Keese said. In this approach, IT workers can leave the patching to Red Hat. This also removes the potential for human error.

"That's a significant advance in security. Typically, vulnerabilities occur because people have to do the work to secure those things on an ongoing basis, and if they're not applying security appropriately or forget to apply the security or aren't keeping up with the security, then you'll have vulnerabilities that occur naturally," Keese said. "When you automate these processes, you increase the level of assurance that it's done consistently. … These are consistent builds every time. You don't have the possibility of human error, or you decrease the amount of human intervention, which means you can ensure that the process is repeated over and over and over again in exactly the same way, and humans can't do that as well as machines."

This also increases productivity and efficiency because developers can focus on writing application code, not spinning up each element of the stack and closing security holes, Keese said.

"Code helps solve agency and mission problems. Applications help agencies become more productive, opening up things to the constituent taxpayers and solving problems of logistics," Keese said. "What every agency wants to do is serve their constituents. We don't want IT to prevent that from happening, so these problems are being solved by the marketplace, by the open source community, such that talented developers and agency personnel can actually do the work they're tasked to do."

CASE STUDY

HOW BLACKMESH USES RED HAT

Managed services provider BlackMesh began using Red Hat's open source cloud building platform OpenStack about five years ago, OpenShift v2 about three years ago, and is currently using OpenShift v3. This has enabled BlackMesh to become early adopters of containerization, Ford said.

Containerization has been around for a while via Linux containers, but "no one knew how to leverage it at scale," he said. "Once Docker [a platform for running containerized applications in the cloud] emerged about three years ago, a popular movement grew in support of using it. Containers are just a way to stack more and more workloads on top of a single host. At the end of the day, containers still share the compute resources below them – no matter what."

BlackMesh works with multimodal IT, which Gartner says is necessary because as workloads change, organizations need to be able to build infrastructure and applications that are symbiotic and responsive to each other from a technology perspective – this entails Mode 1 and Mode 2 applications. Examples of Mode I applications include systems of record, while Mode 2 would be systems of engagement and innovation. Though BlackMesh deploys more Mode 1 applications, customers are beginning to move towards Mode 2 applications as market trends occur. Interestingly, as Ford explains it, modes that are somewhat intermittent do exist. For example, legacy applications that reside on mainframes and systems such as legacy units are not particularly Mode 1 applications – they are pre-Mode 1, and are focused on that mode.

It sounds simple, but bimodal IT isn't as straightforward as it sounds. "It's an interesting concept to try to put Mode I applications into a containerized model," Ford said. "It's somewhat difficult at times because those applications aren't used to having underlying infrastructure removed in the way a container can do."

He cited containerization expert Google, which recommends treating computing resources like cattle — "just slaughter and create more," Ford said. The idea with containers is that agencies shouldn't plan on infrastructure staying put, so if it fails, it has a way to heal itself.

"Mode 2 applications used to put up multiple containers, so if any of them fail, it is inconsequential. A number of containers would still exist and permit continuous operation," Ford said. "Some applications aren't meant for that, however – especially persistent web applications and Enterprise Resource Planning (ERP) systems. ERP systems that require a large amount of dedicated resources are often hard to containerize. Services that are good for containerization efforts entail tiered services such as splitting web servers and database servers apart, for example. Splitting traffic load with an application that is able to scale horizontally is perfect for containerization because they can spread user requests out over a large multi–data center set."

BlackMesh opted to leverage OpenStack and OpenShift as part of its focus on PaaS when the Energy Department sponsored it through the FedRAMP certification process in early 2015.

"It has helped us become more focused on cutting-edge enterprise technologies," Ford said of OpenShift. "We're not afraid of trying implement new technologies. But at the same time, we see the market going towards containers; that has allowed us to focus our team on Kubernetes, Docker, and OpenShift. BlackMesh still wants to push private clouds, Red Hat OpenStack, and different JBoss technologies to support those still emerging markets."

"What containers are giving those agencies and organizations is the ability to rapid-deploy and rapid-develop," Ford added. "The ability to let the developers provision their own infrastructure to test out code changes is the best productivity point that we're seeing right now."

While some BlackMesh clients are using OpenShift for development and staging, many are getting accustomed to the idea of using the solution for production workloads, Ford said. "The cloud has been out for several years and enterprises are still moving physical into virtualized assets," Ford added." Making use of OpenShift for production workloads is becoming more acceptable."

"Still, virtualization shows real results. One federal organization went from paying as much as $8 million a year for a website to about $300,000 a year once they switched to BlackMesh services. "That's the cost savings we're talking about," Ford said. "That's taxpayer money, so why not use the most cost-effective solution possible?"

BEST PRACTICES FOR USING RED HAT–BASED SOLUTIONS

Despite the clear benefits of cloud migration and PaaS environments, a cultural shift is necessary to introduce them into agencies. It's not easy for IT managers to let go of what they've traditionally controlled and see industry as a partner. To get a better sense of an agency's readiness to try this new technology, Ford recommends asking the following questions:

Are developers spending more time with contractors developing tools than doing actual development themselves? "That is an excellent sign to say, 'We should probably look at an OpenShift-style product,' because that will save administration resources."

Are applications coming up for redevelopment that need to meet cloud or open source mandates? If so, this is a great time to make the switch.

Once it's clear that this technology is the way to go, it won't magically appear. The following steps can help agencies on the path to choosing the right commercial cloud partner, Keese said:

Define the problems that impede the IT staff from meeting the agency's mission.

Map those problems to what solutions in the marketplace offer, and determine whether those solutions can get the job done better, faster, cheaper, and more securely.

When you have a correlation between government challenges and industry solutions, you've got a match.

CONCLUSION

"Agencies must know how to procure services from a contracting vehicle and firmly understand their technical requirements," Ford added. "While most agencies may have their technical requirements properly defined, they may not know their security requirements. Developers are often shocked to find out from their security team what they actually need before searching for providers."

To further ease the shift to containers, it's important to note that they are less disruptive than traditional cloud technologies, Clater added. "Often, implementing cloud technologies can be very disruptive from an organizational perspective. If I'm implementing a new Infrastructure as a Service, like OpenStack, it can be fairly disruptive and it can want to take over a lot of the data center," he said.

One of the nice things about Platform as a Service and containerized infrastructure in general is that you can continue to have a lot of those same types of characteristics of being a cloud technology while being a lot less disruptive."

Containers let organizations start at a smaller scale and without changing much infrastructure. They can divide an application into many components called micro services, containerize those and then redeploy the application. "That's a very isolated way of going about how you change the entire paradigm of how you build and host applications, and because it's not disruptive, it's a lot easier for a government agency to adopt that," Clater said. "PaaS lends itself very well to developing in a microservices mode."

A solid infrastructure foundation is crucial to building a secure, efficient cloud environment. Despite the newness of the technology, the underlying practices are tried and true. What's more, the benefits are real, and just like the architecture, one feeds off the other: When developers can spend more time on mission-critical code, agencies solve problems better, faster and cheaper — and more securely.

ABOUT RED HAT

Red Hat® is the world's leading provider of open source solutions, using a community-powered approach to provide reliable and high-performing cloud, virtualization, storage, Linux® and middleware technologies. Today, Red Hat is at the forefront of open source software development for enterprise IT, with a broad portfolio of products and services for commercial markets. That vision for developing better software is a reality, as CIOs and IT departments around the world rely on Red Hat to deliver solutions that meet their business needs. Solutions that provide technology leadership, performance, security, and unmatched value to more than 90 percent of Fortune 500 companies.

Learn more: http://www.redhat.com/en/technologies/industries/government

redhat.

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 200,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

govloop

1152 15th Street NW, Suite 800 Washington, DC 20005
Phone: (202) 407-7421 | Fax: (202) 407-7501
www.govloop.com
@GovLoop