As Public Cloud OS Instances Grow, So Do Security Admin Challenges

AUTHOR | DANIEL P. DERN, THE LINUX FOUNDATION

"Some cloud vendors tout that systems deployed within their framework require little or no administration: You create an image with the software and applications that you want it to provide services for, spin it up in a management console, and Voila! you have an entirely new system online; with minimal cost, no hassle, little work. However, even with newer models for virtualization appearing on the horizon, this is not exactly how things are actually used today."

THE EVER EXPANDING ENTERPRISE

As companies move or extend IT from private to public clouds, and from virtual machines (VMs) to system images, they often use a number of different operating system versions. They run different Linux distributions, different distro releases, and perhaps also non-*nix OSes, along with multiple templates, and the total number of instances can grow.

Some cloud vendors tout that systems deployed within their framework require little or no administration: You create an image with the software and applications that you want it to provide services for, spin it up in a management console, and Voila! you have an entirely new system online; with minimal cost, no hassle, little work. However, even with newer models for virtualization appearing on the horizon, this is not exactly how things are actually used today, according to David Dingwall, Architect and VP of Product Marketing at Fox Technologies.

With this growth in complexity, says Dingwall, comes greater administration for areas not well covered by the current generation of cloud provisioning tools.

"Having more concurrent OS vendors, versions and instances than you have been used to in your private cloud can have security consequences that aren't necessarily obvious," Dingwall says, "and that can be more onerous to address, particularly for SMBs, where IT staff are likely already over-tasked."

QUIS CUSTODIET THE OPERATING SYSTEMS?

While virtualization, the cloud, and more recently containers reduce much of the headline administrative load — particularly in terms of provisioning and maintaining hardware, facilities, power and cooling — "a company's system administrators are still responsible for building and configuring the virtual machines or system images and their contents," says Dingwall. "This includes 'hardening' the security for the operating system, even if the higher app and related service layers already include adequate security from the cloud vendor."

When you obtain an OS directly from its vendor, e.g., Microsoft, Red Hat, or SUSE, "the default image is set up with a rather generic security policy," says Dingwall, "What you've downloaded isn't tailored to any security policy that your company would need in order to run it safely in your own private cloud. Work needs to be done."

This is also particularly true when building within a public Platform-As-A-Service (PaaS) cloud, stresses Dingwall. "The system image isn't something you typically build and construct yourself, you tend for convenience to pick it up from the public cloud's app store. For web-facing instances — the part that may take your order — your organization may spin up as many as needed, and discarded them like a used paper plate when idle."

For instances that preserve or process data (middleware, databases, live interfaces to business partners) that actually run your business, these act a lot more like the traditional servers that your business used to depend on, according to Dingwall. "For the OSes that are the initial building block of these transactional instances, again, there's usually only a generic level of OS security in place — and worse, nothing to stop developers from picking up a pre-packaged combined OS/App images from the store, linking them together and going directly to start working on the apps."

Part of the reason, suggests Dingwall, is that "cloud vendors want SMBs to engage as fast as possible, so they want to make the on-boarding experience go quickly, and make the experience as 'sticky' as possible."

Yes, public cloud providers do spend time on their own security, Dingwall readily acknowledges. "For example, Amazon provides pre-hardened versions of apps and data stores. You can be guaranteed the apps are already secure, and logos are splashed all over presentations with compliance certifications, providing assurances to the business management holding the checkbook."

But, Dingwall cautions, "Being told how your data and applications are pre-delivered secure and certified may blind you to the reality that the operating systems that your secured apps and data are running on are still relatively poorly configured compared to what you'd have enforced if they were running in your own private cloud."

"When you try to pin down the Cloud security directors at shows, and ask specifically whether their cloud service provides assurance that the OS is secure, the answer is , 'That's always the customer's responsibility,'" says Dingwall. "Looking at the small print, the OS vendor says something like 'we provide this OS for use in this Portal/Channel, however it comes with no warranty' and the public cloud vendor says 'We take no responsibility for the operating system, that's your problem.'"

And, says Dingwall, "That blanket lack of warranty for that OS image you've picked from the App store isn't usually highlighted, since calling attention to it conflicts with the on-boarding experience their marketing, sales, and consulting teams want to promote their cloud services to net new customers – SMBs."

SECURE THAT OS

"On a technical side, the click-and-drop experience of 'I need an OS, here's the app to go on top of it,' doesn't typically include a 'now go harden your OS image — have an IT admin log on and do some work on it' step," says Dingwall. "The danger of moving your environment to the public cloud, if you are a smaller organization, and/or being led by a small consulting house, there's a chance that this step could be bypassed or omitted completely, because it isn't part of the workflow provided by the admin and provisioning tool they use."

"Never deploy into production with an as-delivered system image from a public cloud's app store," stresses Dingwall. "Copy it, harden it, and then add any other security software or configuration changes to the image by involving your security admins. Deploy from your copy, which has become your organization's template, just like you would in a private cloud."

Using operating system images 'out of the box' is a problem, Dingwall points out, "because operating systems typically have rather liberal security policies when you install them out of the box. "It's up to the system or security admin to do things like change the passwords and maybe add two-factor authentication for some account access. And all this configuration work has to be done before the template is accepted and released to production."

Doing this for an image straight from a Linux distro provider (e.g. Red Hat, SUSE or Ubuntu) could take a few hours to harden the system to meet a company's existing standards, according to Dingwall. "Plus it needs to go through release testing, and,

depending on a company's policies, it may have to go to production testing for verification.

"Secure the OS" to-do's, according to Dingwall, "have not changed much from the time where we were securing a single OS on a single server," and include:

- don't allow the root account to be directly logged into
- control which support teams can log into the server, using SSH
- do correct allocation and group set-up
- do file monitoring and alerting, associated with particular groups
- if appropriate, add two-factor authentication, (in the public cloud typically as one-time codes sent to mobile devices, rather than smart cards and tokens in private clouds)
- reset factory-default passwords
- set password expiration, complexity
- define SUDO groups and program options

"If you already have a private cloud running virtual machines, and if you plan to move these VMs to the pubic cloud, start with replicating those templates and then harden them and make them secure to meet your company standards and deal with any additional wrinkles presented by the PaaS cloud," says Dingwall. And, he points out, this work needs to be repeated in other technology stacks, like using containers in the future.

"Regardless of where the operating system came from — a vendor or an app store — you still 'own' — are responsible for — the security model inside it," Dingwall says. "You have to set up security and make sure it works. No one else is going to do that for you."

ABOUT FOXT

Fox Technologies, Inc. helps companies protect corporate information assets with network security and access management software as well as striving to simplify compliance and streamline administration with an award-winning access management and privileged account control solution. Our access management software centrally enforces granular access entitlements in real time across diverse server environments.

To learn more about Fox Technologies, please visit us at: **www.foxt.com**

CONTACT INFO

North America
3300 Eagle Run Drive NE, Suite 202
Grand Rapids, MI 49525
+1 877 818 3698 (Toll Free)

Sweden
FoxT Sweden AB
Kungsängsgatan 18A
SE-753 22, Uppsala
+46 18 16 00 00 (Main)

United Kingdom
400 Thames Valley Park
Reading , Berkshire RG6 1PT
+44 1189 637 681 (Main)

www.foxt.com I info@foxt.com

foxtechnologies.

You may also be interested in: Best Practices for Unix/ Linux Privileged Identity and Access Management