March
2009
Volume 1

SOFTWARE TESTING

New software testing technologies bring new challenges

TechTarget
The Technology Media ROI Experts

Testing challenges: The cloud and RIAs

EDITOR'S LETTER

CHAPTER 1 VIRTUAL TEST LABS MAKE MOST OF CLOUD

CHAPTER 2 TESTING RIAs FOR SECURITY HOLES

→ **WELCOME TO THE** inaugural edition of SearchSoftwareQuality.com's Software Testing E-zine. Throughout 2009, our e-zine's writers—all software testing experts—will deliver tactical how-to and in-depth trend and strategy articles on key issues including regression testing, service component architecture, mobile application testing, exploratory testing, SOA, agile development, virtualization, cloud computing and test management.

This first issue covers two new technology areas—virtualization and rich Internet applications (RIAs)—that are changing software testing approaches and presenting new challenges. Our writers, Colleen Frye and Kevin Beaver, each bring over 20 years of software industry experience to play in their analysis of these issues.

Industry veteran Colleen Frye opens the e-zine with a report called "Virtual test labs make most of cloud." The insights and technology updates in this article are timely, as the day when most test and development labs are virtualized is not far off. Already, 44% of software developers are testing in virtual environments and using virtualization technologies as part of their application development process, according to a recent SearchSoftwareQuality .com survey.

Frye explains how virtualization reduces test labs' hardware costs, increases server utilization rates, simplifies systems configuration, speeds setup and teardown of test configurations and more. Users of cloud-based development services can even bypass many traditional software configuration tasks.

In "Testing RIAs for security holes," information security expert Kevin Beaver makes it clear that new Web 2.0 and Ajax technologies haven't erased Web 1.0 security shortcomings. Sure, he writes, "there are many things to exploit with rich Internet applications," but he adds that he's had few security problems with them and explains why. Check out his advice on plugging security holes using automated scanning tools and when to use manual analysis on RIAs. ■

JAN STAFFORD
Executive Editor
jstafford@techtarget.com

Let Our Global Software Testing Community Help You Find Your Bugs

...So Your Customers Don't Have To.

uTest helps QA teams achieve maximum testing coverage and launch higher quality web, mobile and desktop apps.

Compliment your in-house QA team by tapping into our community of 14,000+ professional testers from 150 countries around the world. Build a virtual testing team based on location, language, application type, operating system and browser, and only pay for the bugs you approve.

Discover what QA teams from companies like Intuit, Thompson Reuters, Internet Brands, Second Rotation and Seesmic already know:

uTest helps QA teams meet their launch schedules and release higher quality:

» Web Applications
» Mobile Applications
» Desktop Applications

For more information, check out www.utest.com or call 1.800.445.3914

uTest® Software Testing Community

CHAPTER 1

Virtual test labs make most of cloud

QA and testing organizations are embracing the powers of virtualization and cloud-based computing to perform simpler testing at lower costs. **BY COLLEEN FRYE**

EDITOR'S LETTER

CHAPTER 1 VIRTUAL TEST LABS MAKE MOST OF CLOUD

CHAPTER 2 TESTING RIAs FOR SECURITY HOLES

→ **VIRTUALIZED TEST LABS** can make it faster and less expensive to set up and tear down test configurations, better utilize resources, and help to boost overall software quality. And now cloud computing brings the promise of even less infrastructure to worry about, which can help to further alleviate quality assurance (QA) bottlenecks due to resource issues.

"QA and testing organizations are increasingly embracing virtual test labs due to the efficiency and cost savings that can result," said Melinda-Carol Ballou, program director for application lifecycle management at IDC. According to Ballou, one of the barriers to QA is limited access to—and poor management of—physical infrastructure for test labs, as well as the effort involved in setting up and managing systems configurations for the labs.

"Groups tend to hoard the physical resources so that they will have access to them when needed, even when there is no immediate demand," she said. "This means that software can languish without being tested due to poor resource allocation and management."

This bottleneck can be costly, Ballou said—an issue that becomes even more critical in a down economy. "Virtual test lab management can help address these kinds of issues, as well as cutting the cost of infrastructure by augmenting or replacing physical systems."

With the emergence of cloud-based offerings, the benefits of virtualization can be more immediate, Ballou said, "because you don't have to configure the software."

STARTUP GAINS CAPACITY, SAVINGS WITH VIRTUAL TEST LAB SOLUTION

For startup Apptio, a provider of on-demand IT cost transparency solutions, a virtualized infrastructure provided both affordability and the capacity to test more broadly.

EDITOR'S LETTER

CHAPTER 1 VIRTUAL TEST LABS MAKE MOST OF CLOUD

CHAPTER 2 TESTING RIAs FOR SECURITY HOLES

According to Colin Henry, senior software engineer at the Bellevue, Wash.-based company, Apptio is developing a data integration add-on for its primary product; the add-on will aggregate data from disparate data sources.

"We realized this portion of the product covered a broad range of systems—ERP, database, etc.—and the setup/teardown time for that would be costly," Henry explained. "We knew we needed a virtual infrastructure. Being a startup, we don't want to spend the world on getting three racks of servers or a huge box to throw five or six [virtual machines] on. I knew we wanted to go for virtualized space hosted on the cloud."

Henry said Apptio had performed manual testing on its primary product and did not have a traditional testing environment, "so we were starting from scratch."

The company researched on-premise and hosted virtual test labs, "but any kind of managed service on a local machine takes a lot of your administration time," he said. Provisioning a box can take three to four hours, according to Henry, and if you're adding application infrastructure on top of that, it could take up to eight. So Apptio decided that newcomer Skytap Inc. with its Skytap Virtual Lab product fit the bill. The result?

"Going from 12 hours to five minutes," Henry said. "That's a huge increase in productivity, because you're not slogged down in installing software."

Seattle-based Skytap describes itself as "serving up virtual machines over the Internet." According to CEO Scott Roza, "There is no infrastructure, no upfront expenditures, and it's delivered 100% as a service." Skytap Virtual Lab "is a multitenant model,"

"Being a startup, we don't want to spend the world on getting three racks of servers or a huge box to throw five or six VMs on. I knew we wanted to go for virtualized space hosted on the cloud."

—COLIN HENRY
Senior Software Engineer, Apptio

he said. "All you need to access it is a browser. With the browser you can get access to computing resources; you're not limited by the number of VMs you can run or the number of users you can have accessing [the environment]."

While QA and testing organizations have been early adopters of virtualization, Roza said, "very few QA organizations are all virtual" because "large database servers and databases historically don't work all that well in a virtualized environment." He said Skytap offers a hybrid model. "We have secure bidirectional VPN technology, so you can build part of your lab in the cloud and connect back to your own

EDITOR'S LETTER

CHAPTER 1 VIRTUAL TEST LABS MAKE MOST OF CLOUD

CHAPTER 2 TESTING RIAs FOR SECURITY HOLES

data center. The hybrid model can take advantage of the cloud as an extension of an in-house lab."

Roza likens the Skytap service to a family cell phone plan. Henry said Apptio has a plan for about 2,000 hours per month. "We don't have to keep the infrastructure running full-time," Henry said, "so we're not using unnecessary hours of their time. When you're done, you're done. To get rid of a VM you're not using anymore, you just delete and within a few minutes it's gone from the virtual lab. You can manage it relatively easily."

Roza added that pioneer Software as a Service (SaaS) companies like Salesforce.com broke down barriers of concern that SaaS might not be secure. For Henry, with their test cases, "we're not dealing with sensitive data, so in that regard it's not much of an issue. For long-lead VMs left on for monthly tests we have it set up over the VPN with Skytap."

AUTOMATION EASES TEST CONFIGURATION PROCESS

But testing organizations don't need a cloud-based service to reap benefits from virtualization, particularly for setting up and tearing down test configurations. "Automated testing took a lot of labor out of the process [before virtualization], but there was still a lot labor involved in setting up and tearing down the configurations," said Dave Malcolm, chief technology officer of Surgient Inc., an early pioneer in the virtualization space.

Surgient's QA/Test Solution (formerly VQMS) automates the deployment, configuration and teardown of complex software environments. Malcolm said to get started with virtualization, QA organizations need the physical infrastructure to support a virtual lab, a hypervisor platform like Microsoft's or VMware's, and test automation tools. Surgient integrates with HP's quality management suite and IBM Rational. "The testing tools will make the calls to the Surgient platform to automate test configurations," he explained.

Surgient customers can choose a hosted offering, but most install on-premise, Malcolm said, and build what he called an "internal or private cloud."

VIRTUAL TEST LABS IMPROVE UTILIZATION

Insuresoft, a software provider for the property and casualty insurance industry based in University Park, Ill., decided to install Surgient's QA/Test Solution on premise. "We wanted the flexibility to do what we wanted with our images and be able to troubleshoot ourselves and go through the process of learning about virtualization," said Hemanth Guttikonda, Insuresoft's QA manager. "We had some expertise in-house to do some of these things; also we're not a large enough organization to consider hosting."

Guttikonda said Insuresoft turned to virtualization to help with testing consistency first and foremost, and the company ultimately benefited

EDITOR'S LETTER

CHAPTER 1 VIRTUAL TEST LABS MAKE MOST OF CLOUD

CHAPTER 2 TESTING RIAs FOR SECURITY HOLES

from better resource utilization as well. He said the testing lab prior to Surgient was somewhat ad hoc, and they would set up and tear down software as new versions of their Diamond product, a hosted application, needed to be tested.

"We have 15 to 20 companies we service and have physical hardware for each company. We had about 30 to 40 physical servers, which mirrored our production environment." The process of installing and uninstalling software to test for each customer was tedious, he said.

While some testing was done in the lab, Guttikonda said other testing was done on individuals' physical machines, which he said wasn't mimicking what the product environment looked like. "The technology we were developing wasn't being fully tested."

Insuresoft was already utilizing automated testing tools from HP and saw Surgient, which supports HP, as a logical choice, he said.

Guttikonda said the company's test lab has been reduced from 30 to 10 servers. "In essence, we trimmed our physical servers by over 60%, and we're getting more utilization out of the 10 servers than with the 30 in the past," he said. "But it really means much more—it's the ability to tear down the environment and reuse the servers." Previously, he said, each server was dedicated to one customer and couldn't be used for any other purpose. "Now we can use [the server] for one company, and when we're done, tear down and deploy it for another, so hardware utilization is way up."

Consistency and quality are up as well, he said. "Now people see the benefits of how quickly we can get the environment available and ready for testing. In the past it sometimes took a day or more to get the testing environment set up, so people would abandon the idea of a central environment." Once the organization started using Surgient, "we started noticing that we were finding more defects." These were defects that weren't showing up when testing on local machines, he said. "People are starting to understand that [with Surgient] we're actually testing in a true production environment."

"People are starting to understand that [with Surgient] we're actually testing in a true production environment."

—HEMANTH GUTTIKONDA
QA Manager, Insuresoft

In addition to getting used to the cultural change, Insuresoft had to invest in more powerful servers than what Guttikonda called the "entry-level" ones they had in order to get the performance benefits of Surgient. However, Insuresoft is already seeing the cost savings of better resource utilization. "These servers are about $5,000, but in the past we would have had to purchase 15 to 20 desk-

top workstations at $30,000 a piece. Now we can serve the same number of employees with a lot less hardware."

CLOUD COMPUTING: THE NEW HYPERVISOR?

This type of capital expense will be one of the effects of cloud computing, according to Ravi Gururaj, CTO of virtualization provider VMLogix Inc. in Palo Alto, Calif. "You'll go from a CapEx to an OpEx," he said, as organizations are billed for usage. "The cloud is really the new hypervisor. Instead of an ESX [VMware hypervisor] box, you will have a cloud box. The cloud will give you the ability to provision infrastructure on demand, but the tools themselves will be the same, so the tools you're using on-premise will be available in the cloud."

Another benefit, he said, is that "the cloud can scale when you have a bursting situation." For instance, in the final stages of QA, scalability may need to be tested. The cloud will enable QA to extend its internal resources to provision from the cloud the amount of infrastructure required.

VMLogix is in the process of cloud-enabling its products, Gururaj said. The first stage will enable customers that have VMLogix on premise to burst to the cloud when necessary, and that will be followed by a pure cloud-based offering, he said.

For organizations considering a cloud-based solution, Skytap's Roza said it will require a mindshift. "We're in the early adopter phase around cloud computing. There are going to be some changes to processes, and you have to embrace that and look at the upside of the cost savings versus having 10 servers next to my desk. We find a lot of VPs of IT say it's a threat to [their] way of life, in terms of headcount, budget, etc. We try to do as much as we can to make it feel like a lab in your data center, with better collaboration."

The cloud will enable QA to extend its internal resources to provision from the cloud the amount of infrastructure required.

IDC's Ballou said organizations also need to examine how the vendor has structured its cloud strategy. First and foremost, she said, organizations need to evaluate the stability and reliability of the vendor and the service. For example, she said, is there a plan for disaster recovery? Secondly, organizations need to look at how the pricing model is structured and determine whether it is cost-effective: "Do I have the resources to run this internally, versus do I have the time? You have to balance that." ■

COLLEEN FRYE is a freelance writer and editor in Bridgewater, Mass. She has been covering the IT industry for more than 20 years.

EDITOR'S LETTER

CHAPTER 1 VIRTUAL TEST LABS MAKE MOST OF CLOUD

CHAPTER 2 TESTING RIAs FOR SECURITY HOLES

Accelerate the Application Lifecycle and Reduce Costs with Virtual Automation and Lab Management from Surgient

Surgient Virtual Automation Platform
Patented Virtualization and Private Cloud Technology Used by 60+ of the World's Largest Companies

The industry's most comprehensive solution for automating the rapid deployment, configuration and teardown of complex environments, Surgient's patented 6th-generation platform supports initiatives across the enterprise, ranging from Dev and QA/Test to IT Ops.

Dramatically reduce CapEx and OpEx costs

Manage test resources across distributed teams

Maintain a library of known-good test configs and environments

"Snapshot" environments to capture defects and share for diagnosis

Download a Free Virtualization Dev & QA/Test Resource Pack

SURGIENT®

1-877-SURGIENT (1-877-787-4436)

www.surgient.com

CHAPTER 2

Testing RIAs for security holes

Rich Internet applications bring their own set of vulnerabilities to software testing, but you can address security problems by looking at apps from the hacker's point of view.

BY KEVIN BEAVER

EDITOR'S LETTER

CHAPTER 1 VIRTUAL TEST LABS MAKE MOST OF CLOUD

CHAPTER 2 TESTING RIAs FOR SECURITY HOLES

→ **WE'RE NOT OUT** of the woods yet with the old-school Web flaws.

In the days of Web 1.0, Web applications were chock-full of flat HTML, CGI and the like. Anyone armed with modest vulnerability scanners and some technical know-how could find practically every Web security hole left unplugged.

Skip ahead to Web 2.0, Ajax and client-side processing, a new world of rich Internet applications (RIAs) that have their own slew of vulnerabilities and, of course, new tools and skill sets to evaluate and learn to use.

In my work, I still see more of the old and less of the new, but things are changing pretty quickly. I do see a lot of development shops revamping their sites and apps, implementing Ajax like it's going out of style. If you're serious about Web security, it's probably time to take things up a couple of notches. Get on board with the ins and outs of this stuff so you don't get burned by hackers.

THE SAME OLD ISSUES

One thing has *not* changed with these new client-centric RIA technologies: how the bad guys work. They're still examining your Web applications with a malicious eye, seeing what they can exploit in the simplest manner to provide the highest payoff for ill-gotten gains. That formula will never change, and that's why you have to use the same approach if you're going to find the right Web vulnerabilities.

So whether you're a developer, a tester or a security professional, your ultimate goal is finding and fixing Web security flaws before the bad guys exploit them. You have to step into the attacker's mindset, looking at your applications from that point of view. This requires using an ethical hacking approach, which includes these processes:

1. Mapping the application
2. Scanning for common vulnerabilities

③ Exploiting the vulnerabilities
④ Penetrating the system

In each step, apply the right tools and techniques as both an untrustworthy outsider and a trusted user of the application. Delving into your Web application in this way, you go beyond typical black box security testing and checklist audits and actually see what else can be exploited in the application.

↘ EDITOR'S LETTER

↘ **CHAPTER 1** VIRTUAL TEST LABS MAKE MOST OF CLOUD

↘ **CHAPTER 2** TESTING RIAs FOR SECURITY HOLES

FINDING THE FLAWS

When getting started with testing, I recommend running an automated scanning tool against your rich Internet applications. A good way to get things kicked off is by mapping the applications and finding the low-hanging fruit. Automated scanners are especially good at throwing thousands of similar requests at applications to see how they hold up—very tedious work we just can't do manually. When using vulnerability scanners, I've found it to be both important and beneficial to use the latest version of reputable commercial tools. Commercial tools tend to find more of the important flaws—especially client-side flaws such as cross-site scripting and cross-site request forgery—and

Wary developers reduce Web 2.0 security risks

AJAX AND WEB 2.0 technologies have gotten a bad reputation for being riddled with security holes. The general consensus is that client-side code is more accessible to the bad guys and thus more easily exploited. While there are many things to exploit with rich Internet applications, I've had few security problems with them, and here's why.

Most RIAs I've encountered have been well-coded with only a minimal set of vulnerabilities, especially compared to older Web technologies. These RIAs aren't just more secure because they're using new technologies. Instead, applications are being developed securely up front, with good support from management. It's obvious that Web 2.0 developers have learned a lesson from Web 1.0 security disasters. That's half the battle.

Project managers have learned from past mistakes, too. More and more, I see managers asking consultants and their own teams for extra security checks of their applications. That's going to result in more secure systems. I expect these double-checks will be a common practice, as more developers use Web 2.0 technologies and systems become more complex. —K.B.

they're also continually updated with support readily available in most cases.

There is one problem with automated scanners. When testing RIAs you can't rely on Web vulnerability scanners to find every weakness. This is true with previous generation websites and applications, but it's even more important now with client-side code. That's been the biggest letdown for me in testing RIAs with traditional tools. Although I've had a good experience overall, it seems the client intervention required in rich Internet applications is sometimes more than automated scanners can handle. In fact, my experience has shown that quite often vulnerability scanners won't know where to go and what to do within the application, especially when logged in as a trusted user. Sometimes they just hang up altogether.

Automation tools have gotten better over the past year, and I'm confi-

↘ EDITOR'S LETTER

↘ **CHAPTER 1** VIRTUAL TEST LABS MAKE MOST OF CLOUD

↘ **CHAPTER 2** TESTING RIAs FOR SECURITY HOLES

Set these must-have controls on RIAs

AT A MINIMUM, ensure your RIAs have the following controls in place:

- **Reasonable input validation so the application only accepts what is expected.**
- **Strong password requirements beyond easy-to-guess words and number combinations.**
- **Intruder lockout that disables accounts after five to 10 failed login attempts.**
- **Generic errors displayed during failed authentications, improper data submissions, etc.**
- **Strong multifactor authentication that can't be easily manipulated.**
- **Strong session keys and nonpersistent cookies.**
- **Minimal use of hidden fields and related client-side data that's easy to abuse.**
- **SSL usage throughout the entire site.**

These controls won't guarantee Web security, but they create a foundation upon which good security and solid risk management can be built. —K.B.

EDITOR'S LETTER

CHAPTER 1 VIRTUAL TEST LABS MAKE MOST OF CLOUD

CHAPTER 2 TESTING RIAs FOR SECURITY HOLES

dent the vendors will make more improvements soon. But, even with all the scanning tools in the world, they still only represent half of the Web security testing equation. This is where manual analysis comes into play.

USING MANUAL ANALYSIS

Some things can only be tested for and exploited using manual analysis:

- Can forms be manipulated so that junk data is appended to a default user selection and sent back to the server?
- Can client-side form data be manipulated altogether using a Web proxy tool?
- Is sensitive information such as the username and password being passed back and forth between the client and server in every HTTP request?
- How are errors handled? Are detailed messages being generated by the server or is client code generating pop-up messages? Can this be further abused?
- Is random JavaScript or XML code (e.g., via RSS) blindly published and reflected back to the user with no complaints or errors?
- Are persistent cookies being stored on the client, which can lead to further abuse?
- Is autocomplete enabled for form fields, allowing the Web browser to store potentially sensitive information on the local computer for others to access?
- With the bigger findings, do certain Web browsers behave differently than others? While it's next to impossible to test all versions of all browsers, the reality is that users will employ their own browser version whether you support it or not.

I cannot stress enough that manual analysis has to be a part of the Web security equation. The more client-side code we have, the more manual testing needs to be done.

STAYING SECURE

Web 2.0 has introduced what's arguably the equivalent of open source software into the World Wide Web. Rich Internet applications are often free and open, and the possibilities are endless. With Web-centric malware generation toolkits such as MPack and Webattacker, there's even more reason to be concerned with these new technologies.

Given this new frontier of Web interaction, how do you ensure your RIAs are not left vulnerable to both current and forthcoming attacks? You can take the easy route and invest in a Web application firewall (WAF). Just set it up and forget about it. Unfortunately, that would be like using duct tape to hold your house together, all the while knowing it was built on a shaky frame and foundation. It may work for now, but it's not the right way to go about things long-term.

Don't get me wrong. WAFs have their place, but only after your security policies and development stan-

↘ EDITOR'S LETTER

↘ **CHAPTER 1** VIRTUAL TEST LABS MAKE MOST OF CLOUD

↘ **CHAPTER 2** TESTING RIAs FOR SECURITY HOLES

dards have been solidified and your codebase is relatively secure. This means, at the very least, your Web applications need to have reasonable input filtering that keeps the junk out, solid login mechanisms that aren't easily broken, and application logic that can't be easily abused. In addition, you need to patch and harden Web servers running underneath. RIAs or not, I still see these silly, inexcusable oversights in Web-based systems. Vendors, analysts and certain pundits scream about how scary the Web 2.0 world is, but they'd have less to scream about if these basics were addressed.

Vendors, analysts and certain pundits scream about how scary the Web 2.0 world is, but they'd have less to scream about if these basics were addressed.

At the end of the day, rich Internet applications are nice for users and great for business. If you focus on using sound development and QA practices—combined with periodic, consistent and proper security testing—you'll set your business up for success, even when the next new wave comes crashing in. ■

KEVIN BEAVER is an independent information security consultant, keynote speaker and expert witness with Atlanta-based Principle Logic LLC. He has over 20 years of experience in the industry and specializes in performing independent information security assessments revolving around compliance and information risk management. Kevin has authored or co-authored seven books on information security, including the ethical hacking books *Hacking For Dummies* and *Hacking Wireless Networks For Dummies* (Wiley). He's also the creator of the *Security On Wheels* information security audio books and blog, providing security learning for IT professionals on the go.

ABOUT OUR SPONSORS

- **Surgient Platform Overview**
- **Insuresoft Webinar**
- **Sisters of Mercy Case Study**

About Surgient: Headquartered in Austin, Texas, Surgient is the market leader in self-service virtualization automation and lab management. The company's flagship, award-winning product, the Surgient Virtual Automation Platform,™ is a powerful, flexible and mature solution that optimizes IT's ability to support critical business initiatives, effectively manage diverse virtual resources and eliminate physical server and VM sprawl. Using the Surgient Virtual Automation Platform,™ world-class companies including IBM, Merck, Raymond James, HP, Halliburton, EMC, CA, Iron Mountain, Target, GE, SAP, Microsoft, Siemens, Intuit and others are accelerating their growth and profitability by automating virtual infrastructure in support of their business initiatives.

- **Ten Things Every QA Manager Should Know About Building & Leading a World-Class Testing Team**
- **Six Benefits of Using Community-Driven Testing to Compliment Your In-House QA Efforts**
- **Eight Essentials of Crowdsourcing the Design, Development and Testing Of Your Application**
- **Watch A Free Online Demo of uTest**

About uTest: uTest is the world's largest marketplace for software testing services. The company enables in-house QA teams to maximize real-world testing coverage through its community of 14,000+ professional testers from 150 countries around the world.

More than 400 QA and development organizations—including those from Intuit, Thompson Reuters, Internet Brands and Gazelle—have signed up with uTest to get their web, mobile and desktop apps tested. And because uTest is on-demand, customers pay only for the bugs that they approve.