BreakingPoint™
Find it before they do.™

1.866.352.6691 | INTL 1.

Demo | Contact | Su

Products Services Solutions Resources Blog

Blog Search Go

Most Recent Posts | Tech Talk | Tag Cloud

**Topics of Interest**

10/40/100 GigE
Application Protocol Fuzzing
Custom Applications and Attacks
Cyber Range
Cybersecurity
Data Loss Prevention
DDoS and Botnet Simulation
Deep Packet Inspection
IPv4/IPv6
Lawful Intercept
Mobile Network Security
Performance Measurement
Product Updates
Resiliency Score
Rethink Server Load Testing
Rethink Test Methodologies
VoIP

**Solutions**

Anti-Malware
Application Server Testing
Cloud Testing
Data Center Consolidation and Optimization
Firewall Testing
IDS/IPS Testing
Load Balancer Testing
LTE/4G Testing
Network Management Tools
Proxies
Routers and Switches
Unified Computing
Unified Threat Management
Virtualization Testing
Virus and Spam Filters
VPN Gateways
WAN Optimization

**Tech Talk**

MAY 17, 2011

# Lessons from the Amazon Outage: 5 Ways That Cloud Providers Must Take Responsibility for Service Levels

**By Tim Walker**

Common sense would dictate that when a Web site or application hosted through a cloud provider goes down, it's a violation of some service level agreement (SLA) — with the penalties to go along with it. The Amazon cloud service outage in April proves otherwise, however. Although several Amazon Elastic Compute Cloud (EC2) customer sites went down completely, this was, surprisingly, not considered a violation of any SLA. That fact is a sobering commentary on the state of the cloud industry.

To be fair, this is not an issue with Amazon alone. The Sony PlayStation Network and Yahoo! Mail also experienced cloud crashes in late April. Yet the negative impact of cloud performance failures goes well beyond these cloud providers: these incidents will have a profound effect on the industry as a whole if confidence in cloud solutions keeps declining. A New York Times headline on April 22 stated that "Amazon's Trouble Raises Cloud Computing Doubts." The article went on to say that "industry analysts said the troubles would prompt many companies to reconsider relying on remote computers beyond their control."

That's bad news for cloud providers. They want potential customers thinking "robust," not "risky," when they are considering the cloud. Because of that, fortifying cloud reliability, availability, and security could not be more important than it is right now.

## Five Steps to Restore Faith in the Cloud

The cloud industry is at a crossroads. Public cloud services could gain massive momentum . . . or remain a technology continuously on the fringe. It all depends on whether the cloud providers take to heart the lessons learned from the Amazon outage. What follows are five steps that cloud providers must take to avoid outages, strengthen customer confidence, and move to the next level in cloud evolution.

1. **Take Responsibility —** I have read several recent articles and blog posts that called the cloud industry "immature." If that's the case, it is time to grow up — and that means taking responsibility, being accountable. This responsibility should be the foundation upon which cloud providers build their infrastructures and implement the tools needed to ensure continued availability, performance, and security.
2. **Test Resiliency —** Cloud providers must assess the reliability of their virtual environments — and that means every component, from routers and switches to servers and firewalls — by simulating traffic loads, user behaviors, applications, and security strikes. There are only two ways to learn how the infrastructure will respond to a given set of conditions. The dangerous and expensive option is to take a chance that systems will work in the real world and then fix problems after the fact. The other option — the smart one — is to test cloud resiliency ahead of time by assaulting the components with the same stressful conditions they will face when deployed. Using that approach, cloud infrastructures can be fine-tuned to meet any challenge.
3. **Rethink SLAs —** As a cloud provider, you are your SLAs. Cloud providers must rethink SLAs and establish service levels that actually guarantee service **from the customer's perspective**. SLAs should be designed to protect the customer, not to shield the cloud provider from accountability.
4. **Automate Processes —** Unfortunately, any little manual action in the cloud could produce a disproportionate negative reaction. In its long postmortem on the EC2 outage, Amazon said "a network configuration change" was the official trigger for the problem. This is code for "human error." The key for eliminating these types of human errors is to automate processes — discovery, configuration, change management, monitoring, and systems management. Of course mistakes will still sometimes occur; when they do, go back to step #1: take responsibility, fix the problem, and explain what you're doing to prevent it from happening again.
5. **Communicate to Customers —** Probably the single greatest fear businesspeople have about the public cloud is the loss of control, which is manifested as the loss of visibility. That is why most companies still avoid sending their mission-critical apps into a public cloud. An extensive 2010 survey [PDF link] conducted by Vanson Bourne for HP found that almost half of the respondents considered the inability to monitor SLAs to be the top service management issue in the cloud. IT leaders will never truly trust the cloud unless they have clear visibility into their application availability, performance, and security, just as they would internally. Providers must open the lines of communication with customers to deliver an in-depth view of application performance across the cloud.

All five of these practices require work, and some of them will cost a bit more in the short run. But cloud providers must embrace them if they want to build a stable foundation for the future of the industry.

Related Content:

- Know the Score: Measuring the Performance and Capacity of

Videos

Interac
Twi
Fac
Em

Subsc

Type
q

Cloud and Virtualized Infrastructures
- Securing the High Performance Cloud
- BreakingPoint Application Load Evaluation Service

---

Posted by Tim Walker

Like Sign Up to see what your friends like.

SHARE Printer Friendly Create PDF

0 comments

Tags: Cloud Testing // Virtualization Testing //

**POST A COMMENT**

Name (Required)

Email

URL

Comment (Required)

Remember My Information □

Subscribe □

Submit