GRIDBYTE®
MULTI-DIMENSIONAL SOLUTIONS SM

✉ GRIDBYTE, Inc.
P.O. Box 6298
Laguna Niguel, CA 92607-6298
☎ 949.916.0799
☎ 800.634.0796
email: info@gridbyte.com

Title: **Business continuity in the age of software-as-a-service (SaaS)**
Case Studies: GridByte-WP2008-03
Created by: Sam O. George and H. Bola George, PhD., GridByte®
Release Date: 2008-Oct-27 (Revision 1.1)
URL: http://www.gridByte.com/Resources/Docoments/GridByte-WP2008-03.pdf
Keywords: Business continuity, Software-as-a-Service (SaaS), SaaS Escrow

Business continuity in the age of software-as-a-service (SaaS)[1] requires much work and proactive solutions as many companies have moved from relatively simple SaaS applications to more complex frameworks. These frameworks include platform-as-a-service (PaaS), integration-as-a-service (IaaS) and SaaS-mashups. The rush to adopt SaaS and its related cloud-computing technologies is inevitable because SaaS brings large total-cost-of-ownership (TCO)[2] savings over traditional software deployment/licensing models.

As client-companies[3] move forward with SaaS deployment, we find that many need robust business continuity strategies. For public companies, Sarbanes Oxley (SOX) financial accountability requirements are forcing critical thinking about SaaS business continuity issues. The renewed emphasis comes on the heels of notable outages at some of the largest SaaS companies this year; e.g., Amazon Web Services S3 in February 2008[4] and Google corporate enterprise email, Apps Premier Edition, in August 2008.[5] As many experts suggest, high profile outages are relatively infrequent. However, the cumulative effect of the lower-profile SaaS outages has an ongoing larger effect on business continuity. In many cases, the tools for monitoring and quantifying outages are in their infancy.

This paper discusses five strategies that address SaaS business continuity for corporations. Without robust SaaS business continuity strategies, the TCO promise of SaaS is lost. No doubt, SaaS will continue to demonstrate fast payoffs for many companies. However, as overall performance of SaaS becomes a firmer requirement in the next three years, business leaders must take a longer view to ensure that the great promise of SaaS is not jettisoned.

The overall solutions to SaaS business continuity can be found within the SaaS framework. To rehash, the TCO promise of SaaS results from elimination/reduction of in-house IT/IS hardware/software and specialized staff. Remaining (non-specialized) in-house staff thus refocuses on higher levels of value-creation combined with application management and configuration. The solutions discussed herein come from exploiting the SaaS model—as opposed to a general tendency to mitigate SaaS business continuity risk by utilizing traditional software licensing models as ad-hoc hedges.

In this presentation, we use the general definition of SaaS to frame our discussion. While there are many variations of SaaS within the Service Oriented Architecture (SOA), the underlying themes of business continuity are the same.

We define business continuity for SaaS as follows: SaaS applications must have the same (or better) speed (access, computation and low-latency), capacity, full-feature-sets and high-availability at all times ... as measured relative to applications installed on corporate servers.

What are the five SaaS business continuity critical risk factors and how do we mitigate them?

1. Availability: The SaaS application must maintain the same level of availability as software installed on a corporate server.

[1] Worldwide software-as-a-service (SaaS) revenue in the enterprise application markets* is on pace to surpass $6.4 billion in 2008, a 27 per cent increase from 2007 revenue of $5.1 billion, according to Gartner, Inc. The market is expected to more than double with SaaS revenue reaching $14.8 billion in 2012. –source: Gartner, Inc. Press Release, http://www.gartner.com/it/page.jsp?id=783212, 22 October 2008.

[2] Definition: Total Cost of Ownernership (TCO) is measured in years: It includes upfront costs such as acquisition, training and deployment. It also includes recurring costs associated with maintenance contracts, IT/IS and consulting, and software/hardware upgrades. In addition, TCO includes the significant costs associated with deployment of software, the cost of downtime and the cost of mobility.

[3] Definition: The terms "client-company" and "SaaS client" means any company that uses SaaS software provided by SaaS vendors.

[4] Brad Stone, "As Web Traffic Grows, Crashes Take Bigger Toll," http://www.nytimes.com/2008/07/06/technology/06outage.html, The New York Times, 06 July 2008.

[5] Donna Scott and Matthew W. Cain, "Google E-Mail Outage Stresses SaaS/Cloud Services'Vulnerability," http://www.gartner.com/resources/161200/161217/google_email_outage_stresses_161217.pdf, ID Number: G00161217, Gartner, Inc., 03 September 2008.

✉ GRIDBYTE, Inc.
P.O. Box 6298
Laguna Niguel, CA 92607-6298
☎ 949.916.0799
☎ 800.634.0796
email: info@gridbyte.com

Title: **Business continuity in the age of software-as-a-service (SaaS)**
Case Studies: GridByte-WP2008-03
Created by: Sam O. George and H. Bola George, PhD., GridByte®
Release Date: 2008-Oct-27 (Revision 1.1)
URL: http://www.gridByte.com/Resources/Docoments/GridByte-WP2008-03.pdf
Keywords: Business continuity, Software-as-a-Service (SaaS), SaaS Escrow

2. What happens if the denial of service is due to Internet routing problems; e.g., extensive latency?
3. In light of fiducial and privacy regulatory issues, how does the company ensure that the SaaS vendor continues to meet the agreed-to-standard?
4. What exactly does an application uptime of 99.99% mean—and how do they prove that the problem to the SaaS vendor?
5. SaaS vendor selection does not favor the incumbent large software vendors.

The following sections address the five points outlined above.

#1 What happens if the SaaS application is unavailable to the client?

As documented in the August 18th 2008 edition of Information Week,[6] major SaaS vendors like Google Gmail, Apple MobileMe and Amazon S3 suffered critical outages, lasting up to 14 hours in some cases, between January and August 2008. From a business continuity perspective, such outages are the Achilles heel for SaaS. Let's consider:

- In the traditional software licensing model, the software application and data are usually controlled and housed on client-company infrastructure. So, if the software vendor goes offline for any reason, the client still has access to all their data and, in general, the software licenses remains active. In this model, the risk of a total application-outage is remote.
- In the SaaS deployment model, none (or very little) of the client's data and applications are housed on company resources. So outages leave the clients without business continuity options.

The prevailing reactive strategy: By far, the most widely used tools to address SaaS business continuity are corporate "legal" agreements. These include various redress language mostly in the form of Service Level Agreements (SLAs). Though functionally necessary, SLAs are reactive. The financial redress in most SLAs is not commensurate with business losses. If the SaaS application is unavailable for any length of time, the client-company incurs a significant loss in revenue—be it from inability to make money, inability to fulfill responsibilities to third parties or losses due to halted employee/machine production. As stand-alone SaaS applications morph into SaaS mashups, the probability and associated risks to business continuity expand dramatically.

Solution: To address availability, the best proactive SaaS business continuity solutions are SaaS Escrow and Offline Applications. While the current state of availability-solutions of both technologies is ad-hoc, these two methods offer mathematical and technical breath. These two methods are defined as follows:

- **SaaS Escrow**: In its most complete form, SaaS Escrow creates a live (or near real-time) replica of the SaaS application and associated databases on another third party system. In this context, data replication is considered a subset of escrow services. Interestingly, the third party escrow services are also SaaS services, such as Iron Mountain.
- **Offline Applications**: Some SaaS vendors offer offline editions. These are lightweight versions of the SaaS application that are installed on client-company assets. These offline applications allow business continuity during outages. The applications automatically resynchronize when the SaaS application come online.

Mathematically, SaaS escrow may be duplicated infinitely. As more SaaS escrow services are added to any system, the probability of business continuity disruption due to unavailability drops to near zero. SaaS Escrow goes

[6] J. Nicholas Hoover, "Outages Force Cloud Computing Users To Rethink Tactics," http://www.informationweek.com/story/showArticle.jhtml?articleID=210004236, InformationWeek, 16 August 2008.

GRIDBYTE, Inc.
P.O. Box 6298
Laguna Niguel, CA 92607-6298
☎ 949.916.0799
☎ 800.634.0796
email: info@gridbyte.com

Title: **Business continuity in the age of software-as-a-service (SaaS)**
Case Studies: GridByte-WP2008-03
Created by: Sam O. George and H. Bola George, PhD., GridByte®
Release Date: 2008-Oct-27 (Revision 1.1)
URL: http://www.gridByte.com/Resources/Docoments/GridByte-WP2008-03.pdf
Keywords: Business continuity, Software-as-a-Service (SaaS), SaaS Escrow

beyond technology. It defines a more complete SLA transactional framework similar to the fiducial and arbitration responsibility typical in financial transactions; e.g., the escrow transaction in purchasing a home is familiar to many readers. As is common, in the case of a billing dispute between the SaaS vendor and the client, the SaaS Escrow vendor must arbitrate without compromising the business continuity of the client or the SaaS vendor.

With application encryption, SaaS Escrow poses little risk of exposing SaaS vendor application codes or business methods to unauthorized third parties.

As SaaS applications become more complex (e.g., Mashups), the SaaS client needs to apply the same escrow requirement to all components of the mashup. The practice certainly poses some logistic difficulties but this needs to be considered part of the cost of doing SaaS business.

SaaS Offline Applications continue to be deployed in an ad-hoc manner. The general observation is that the offline applications must remain below some cost threshold. Otherwise, as many companies are discovering, the TCO-reduction-promise of SaaS rapidly dwindles.

#2 What happens if the denial of service is due to Internet routing problems; e.g., excessive latency?

SaaS applications depend on the Internet. Many corporate applications cannot tolerate high degrees of latency. For example, real-time processing of data may be compromised if the data feeds are severely delayed.

Solution: Latency, speed, bandwidth and throughput are functions of all the components of the network path from the client-company to the SaaS vendor(s) resources. The larger business continuity risk elements are latency, bandwidth and throughput. Latency is an inherent problem because of the way the Internet TCP/IP infrastructure is implemented. To control the quality of the network paths, many companies have started deploying network traffic management equipment and software. For example, Elastra Corporation private cloud server represents critical innovation in network traffic management. Selection of corporate-office premises is another critical factor. In many cases, mere T1 (and its fractional derivatives) does not satisfy many clients' needs. Ensuring that premises have optical fiber is becoming critical in eliminating latency from the matrix of SaaS business continuity factors.

SaaS is also forcing changes in the way computers are deployed. A SaaS hardware client needs to contain large network interface memory caches and buffers. SaaS applications must also use advanced levels of data synchronization technology to compensate for latencies. SaaS applications require advanced levels of network traffic and content management. In this regard, high performance Layer 4 (and higher) switches are critical components in SaaS deployments.

The application computation speed is a function of SaaS vendor's servers. With today's high-speed servers, speed of computation is not a business continuity problem for SaaS. However, the main challenge for SaaS is high bandwidth and throughput for delivery of data to the client-company. If the data contain high graphics content, the bandwidth requirements require fiber-optic links.

#3 In light of fiducial, performance, privacy and regulatory issues, how does the client-company ensure that the SaaS vendor continues to meet the agreed-to-standard?

The deployment nature of SaaS tends to reduce the in-house application knowledge-base of the client-companies. This is one of the reasons why SaaS is popular. Instead of relying on application specialists, e.g., database experts, the client-company relies on "application managers." These employees manage the software and its deployment, but are not specialists in any given area. The lack of in-house specialization creates vulnerabilities that may threaten business continuity.

✉ GRIDBYTE, Inc.
P.O. Box 6298
Laguna Niguel, CA 92607-6298
☎ 949.916.0799
☎ 800.634.0796
email: info@gridbyte.com

Title: **Business continuity in the age of software-as-a-service (SaaS)**
Case Studies: GridByte-WP2008-03
Created by: Sam O. George and H. Bola George, PhD., GridByte®
Release Date: 2008-Oct-27 (Revision 1.1)
URL: http://www.gridByte.com/Resources/Docoments/GridByte-WP2008-03.pdf
Keywords: Business continuity, Software-as-a-Service (SaaS), SaaS Escrow

Solution: Similar to SaaS escrow, SaaS auditors are fast becoming a growth area in the software business. SaaS auditing is loosely similar to financial auditing. However, the former is tasked with constant monitoring of the SaaS vendor(s) and the communications links between the client-company and the SaaS vendor. SaaS audits utilize a combination of human and machine intelligence to ensure compliance and uncover blind spots in the entire SaaS infrastructure.

SaaS auditors are empowered to review critical code-features and change management practices. How do SaaS vendor infrastructures measure up to network and computation burst performance? SaaS audits must combine advanced levels of software testing with forensics.

Critically, and at a minimum, there is a strong push for SaaS vendors to show compliance with SAS[7] 70 (Levels I and II). SaaS 70 certifies SaaS vendor internal controls compliance (e.g., on change management), but it does not deal with performance issues of code or infrastructure.

At the very minimum all communications links must utilize the current state-of-the-art encryption standards; e.g., 256-bit SSL for communications over the http protocols. However, the vulnerabilities happen at the end-points. Client-company data needs to undergo additional *anonymizing* and encryption. When direct access to data is required, the SaaS vendor needs to exercise auditable security precautions.

The end-point vulnerabilities of SaaS manifest in a number of ways. For example, when users access data with clipboard functions (e.g., copy or cut), they potentially create a SaaS business continuity hazard because the data are not purged from the client-computer. The same applies to cached data. The solution to end-point vulnerabilities is for SaaS to evolve a set of self-cleaning functions to ensure that data storage on local hardware is eliminated. Alternatively, SaaS desktop encapsulation technologies (virtual desktops) that provide access to collections of business applications may be critical in mitigating these business risks.

Another vital end-point vulnerability of SaaS comes from mobile devices. For bandwidth and computation speed, mobile devices usually have light applications with stripped-down security functions. The solution is for mobile devices to include the same security functions possible on PCs. At the very least, the security links between mobile devices and SaaS vendor resources need to maintain the same high encryption standard as PCs.

[7] Statement on Accounting Standards #70 by the American Institute of Certified Public Accountants (AICPA).

GRIDBYTE, Inc.
P.O. Box 6298
Laguna Niguel, CA 92607-6298
☎ 949.916.0799
☎ 800.634.0796
email: info@gridbyte.com

Title: **Business continuity in the age of software-as-a-service (SaaS)**
Case Studies: GridByte-WP2008-03
Created by: Sam O. George and H. Bola George, PhD., GridByte®
Release Date: 2008-Oct-27 (Revision 1.1)
URL: http://www.gridByte.com/Resources/Docoments/GridByte-WP2008-03.pdf
Keywords: Business continuity, Software-as-a-Service (SaaS), SaaS Escrow

#4 What exactly does an application uptime of 99.9% mean—and how does the client-company prove the problem to the SaaS vendor?

In principle, SaaS applications cannot have uptimes that are better than the uptime of the network constituents. For example, the top-tier Internet Service Providers (ISP) guarantee uptimes better than 99.9%. SaaS vendor uptimes ranged from 95% to 99.9999%. How and where do these numbers factor in reducing the probability of outages in the matrix of SaaS business continuity issues? What tools do the client-company and the SaaS vendor use to verify uptime events?

Let's consider Table 1 below. This table relates uptimes of ISPs to SaaS vendors' uptimes to illustrate the total number of hours of outage a client-company may expect per year. For perspective consider this: Operating with a hypothetical ISP uptime of 100%, if the SaaS vendor is down for "routine maintenance" for thirty minutes once a week, their total outage hours amounts to a minimum of 26 hours a year. While the data and measurement metrics are spotty, the indications are that outages of most SaaS vendors exceed 26 hours a year.

Table 1: The Full Cost of Uptime Metrics

ISPs in mon.itor.us Network Providing 99% + uptime from USA in July 2008[8]	SaaS Vendor Uptime	Effective Probability of outage (%)	# of hours of outage in 1 year (365.25 days)
Best → 99.77	95	5.005287205	438.7634764
	97	3.008803749	263.7517366
	99	1.026109156	89.94872861
	99.9	0.250798724	21.98501615
	99.99	0.230217289	20.18084752
	99.999	0.230002174	20.16199056
	99.9999	0.230000022	20.16180191
	99.99999	0.23	20.16180002
Worst → 99.56	95	5.019322663	439.9938247
	97	3.032094985	265.7934464
	99	1.092520023	95.77030519
	99.9	0.451220567	39.5539949
	99.99	0.440113622	38.58036008
	99.999	0.440001136	38.57049961
	99.9999	0.440000011	38.570401
	99.99999	0.44	38.57040001

Solution: The first order of selection requires that only SaaS vendors that guarantee five-nines (99.99999%) be considered. As shown in the above table, increasing SaaS vendor uptime ensures that the outage limiter is strictly Internet/ISP based.

In the best case, there is a probability that outages are short (lasting seconds to minutes) and distributed throughout the year. In the worst case, SaaS outages may be longer (lasting hours) and concentrated in a short time window; e.g., the

[8] Mon.itor.us, "ISPs in mon.itor.us Network Providing 99% + uptime from USA in July 2008," http://isp-ranking.blogspot.com/2008/08/monitorus-and-isp-uptime-ranking-for.html, last accessed 03 August 2008.

GRIDBYTE, Inc.
P.O. Box 6298
Laguna Niguel, CA 92607-6298
☎ 949.916.0799
☎ 800.634.0796
email: info@gridbyte.com

Title: **Business continuity in the age of software-as-a-service (SaaS)**
Case Studies: GridByte-WP2008-03
Created by: Sam O. George and H. Bola George, PhD., GridByte®
Release Date: 2008-Oct-27 (Revision 1.1)
URL: http://www.gridByte.com/Resources/Docoments/GridByte-WP2008-03.pdf
Keywords: Business continuity, Software-as-a-Service (SaaS), SaaS Escrow

outage of Amazon S3 lasting 14 hours (sometime between July and August 2008). Uptime needs to be defined appropriately for the business. For some businesses, a typical nine-to-five work day may suffice. However, SaaS clients increasingly require 24-hour uptime metrics.

Client-companies need to apply automatic continuous SaaS and network monitoring agents (software or hardware). These agents can be simple synchronous or more complex asynchronous monitors. Both the client-company and SaaS vendor(s) must agree on the performance metrics and algorithms for such monitors. Details aside, these agents are effective concurrently or as forensic tools to help diagnose network outage issues.

#5 SaaS vendor selection does not favor the incumbent larger software vendors.

By modest counts, the number of SaaS start-up vendors will continue to grow by twenty to thirty percent for the next 3 years. In many cases, these SaaS vendors bring serious innovation and competitive diversity to the marketplace. Unfortunately, start-up companies also have high failure rates. The failure-rate is one of the most critical risk factors in SaaS business continuity. The opportunities for new vendors comes from a general recognition that for many reasons the larger established software vendors do not provide leadership positions in the arena of SaaS.

Solution: Basically, a client-company cannot discount a SaaS vendor solely because it is a start-up. This is because the SaaS model engenders a "best-of-breed" concept. This means that SaaS offers the possibility for companies to utilize the best software components from different vendors – as opposed to being tied to a vertical software platform of an incumbent software company. However, the following considerations must then enter the selection criteria.

- **Business Models**: SaaS vendor business strategy and models may be of critical concern to the client-companies. What assumptions has the SaaS vendor made about its underlying technologies? In the case of mashups like Twitter, their underlying reliance on other SaaS vendors like AWS S3 poses a business continuity risk that needs to be understood by the client-companies.
- **Data Standards**: As mentioned earlier, client-companies need to ensure that their SaaS vendors participate in SaaS escrow services and compliant with SAS 70, HIPAA and other standards. At a very elemental level, SaaS vendors can hasten adoption of their technologies by subscribing to open access data standards; e.g., adoption of XML. SaaS Mashups are clearly showing the way in this regard.
- For more complex data and application frameworks, client-companies may reduce their business continuity risk exposure by applying some macro strategies. They may consider taking partnerships and other equity stake holding in the innovative SaaS vendors. This may include consortiums, etc. This point may seem opposed to the freedom-notion that SaaS seems to espouse, but it really isn't. The reality is that data and software applications are not fungible by design or competitive circumstance. Therefore, some element of captive models should remain part of the macro solution to deploying SaaS.

Conclusion

We have restricted our discussion to five critical areas in the SaaS business continuity framework. However, there are additional areas in which SaaS demonstrates higher business continuity risks when compared to traditional software licensing models. Some of these are:

GRIDBYTE, Inc.
P.O. Box 6298
Laguna Niguel, CA 92607-6298
☎ 949.916.0799
☎ 800.634.0796
email: info@gridbyte.com

Title: **Business continuity in the age of software-as-a-service (SaaS)**
Case Studies: GridByte-WP2008-03
Created by: Sam O. George and H. Bola George, PhD., GridByte®
Release Date: 2008-Oct-27 (Revision 1.1)
URL: http://www.gridByte.com/Resources/Docoments/GridByte-WP2008-03.pdf
Keywords: Business continuity, Software-as-a-Service (SaaS), SaaS Escrow

- **Price control**—To the extent that SaaS has not evolved to the same degree of stability as, say, public utilities—changing your SaaS vendor remains one of the most effective price-control mechanisms. There seems to be a de facto thinking that suggests that this is an easy proposition. This is far from the truth. For complex software/data frameworks, the SaaS implementations will closely couple the client-company to the SaaS vendor. For example, let us consider Hosted Exchange services. As we recently found, migrating from one vendor to another is complicated and expensive. These experiences contain many opportunities for data loss. Data escrow and replication services may provide a solution to portability.
- **Competence gap**—SaaS platforms are relatively new. In its purest form, client-companies should not need to develop expert knowledge about the working of the SaaS software. However, in the interest of self preservation, expert knowledge will continue to be required in the near term. Client-companies must position critical staff to fill this void. Unfortunately, the SaaS landscape needs to be more open to facilitate client-employee competence.

As a foundation, SaaS client-companies need to approach SaaS with a performance and Quality-of-Service checklist similar to what they would have if they hosted their applications and data in-house. Business leaders must factor that today's SaaS does not enjoy the same stability, reliability and ubiquity of, say, public utilities. Thus, especially in terms of SOX requirements, client-companies must concurrently solve the business continuity risk factors of SaaS before deployment. All assumptions about stability of SaaS vendors need to be questioned and evaluated for potential business continuity risk exposures.

SaaS business continuity needs to evolve at the same pace as SaaS application development. This effort needs to be driven by client companies as well as SaaS vendors because the interests of both segments is very closely coupled. The good thing is that this understanding of the SaaS business landscape is driving new innovation.

The solutions outlined in this paper should be part of SaaS implementation frameworks. Availability, uptime and Internet issues are critical aspects of SaaS business continuity as discussed above. Business continuity Service Level Agreements must include the provisions specified in #1 through #5 above. However, business continuity requires both the SaaS client and vendor(s) to engage at a deeper proactive level. SaaS business continuity requires, at a minimum, inclusion of auditing standards like SAS 70.

Citation

Sam O. George and H. Bola George, Ph.D., "Business continuity in the age of software-as-a-service (SaaS)," http://www.gridbyte.com/Resources/Documents/GridByte-WP2008-03.pdf, GridByte®, Version 1.1, 27 October 2008.