

Software as a service—a step by step guide



John Rowell

Software companies should set up a Software as a Service (SaaS) delivery model.

Faced with intensifying competition as well as a desire for more stable revenue streams and stronger customer relationships, software companies are increasingly turning to the Software as a Service (SaaS) delivery model.

The obvious question is why SaaS? Adoption of SaaS is driven in by the end-users who benefit from access to any application, from anywhere, on virtually any Web-enabled device, better licensing and cost control, and assurance that the most recent version of the application is in use.

As a strategic offering, SaaS has already shown that it can open new markets, revenue streams, and distribution channels. It provides a stable, recurring revenue model and affords consolidation of development and support around a single version of code.

Software companies are now facing complex issues involved with building service delivery capabilities necessary to support SaaS offerings. Building a SaaS infrastructure is a complex undertaking, requiring a committed team and a focussed effort. End-users demand a 100 percent uptime, appropriate Service Level Agreements, and a 24x7 call centre support. Meeting those demands requires 24x7 application and systems management, hosting, networking and security infrastructures, disaster recovery capabilities, change management policies and procedures, and more.

In this article we describe a high-level, step-by-step methodology for successfully starting operations with SaaS.

? **Understand the objectives for your SaaS offering**

To successfully deploy Software as a Service offering, you must be guided by clearly defined business requirements, objectives, and timelines. It is critical that these objectives are identified before starting the process. Therefore, detailed investigation of how is the on-demand application designed to run, to access; is the on-demand application designed to handle multiple users and is it designed to meet scalability, security, and failover requirements?

? **Designate the operations team**

The SaaS task force then designates the operations team to design the scalable architecture for hosting the SaaS platform based on the application's requirements. To be successful, the operations team will need to have expertise in multiple technologies. Some of these include system and application management, network and security management, change control expertise, infrastructure design and deployment experience.

Conceive and design scalable infrastructure and services

With a clear understanding of the application(s) and the service offering, the next step for the operations team is to architect a comprehensive infrastructure and its supporting components. These infrastructure components include the data centre, network components and connectivity, security, hardware systems and storage, tape backup, monitoring tools and systems management tools.

Final decisions must include strategies for Service Level Agreement (SLA) creation and management, scalable 24x7x365 systems and application management, end-user call centre support, disaster recovery, scalability of Web, application and database servers, performance and availability commitments, network and bandwidth capacities, security and security management, monitoring management and reporting.

? **Determine bandwidth requirements and select hosting facility**

Hosting your infrastructure behind the appropriate public connectivity and with the facility that is best suited to your needs is the key to a consistently positive end-user experience. When reviewing bandwidth, you must understand the demographics related to your application(s) by identifying where the majority of your network connections come from. End-users who will access your application from home-based desktop computers will require a different approach, compared to those in corporate offices with dedicated high-speed Internet connections.

If you determine that you will host your infrastructure in a third-party data centre, there are some key components to review. Questions include—are the data centres staffed 24x7x365, are there redundant systems for power and cooling, what is the testing frequency, what physical security measures are in place and how many Internet Service Providers (ISPs) are available for purchasing connectivity?

? **Procure the infrastructure components**

With the overall infrastructure design complete, components with proven reliability and functionality are selected for the actual production infrastructure. A core set of these components will include firewall/IDS devices, VPN and SSL acceleration units, load balancers, servers, storage devices, software and support contracts.

? **Deploy the SaaS delivery infrastructure**

With the arrival of infrastructure components, the operations team enters the build phase, deploying the infrastructure in accordance with set specifications. During this hands-on effort, network equipment is racked, burned in and updated with the latest firmware versions, prior to being configured. Configurations are placed on the networking infrastructure that appropriately manage multiple ISP connections for redundancy and segment traffic from public and private networks. Security devices are updated with the most current versions of intrusion detection software (IDS) and firewall rule-sets are established that allow customers access to the systems while keeping unwanted intruders out.

Servers are racked and configured to support overall application(s) requirements. Operating systems are installed and brought to the appropriate patch levels. Systems and networks will then need to be tied to your disaster recovery solution.

? **Implement disaster recovery and business continuity planning**

With a live application now ready for delivery via SaaS, the task force must focus on business continuity issues. Key questions include what happens in the event of a disaster and how quickly can the application be up and running, following such an event?

? **Integrate a monitoring solution**

To ensure that all infrastructure components are both working and working with each other, a monitoring solution is essential. Key components that must be periodically

checked include hardware: memory, CPU, hard drives; operating systems: event logs, process lists, key services; and the application layer: process, TCP ports, Web service checks.

? **Establish a Network Operations Centre (NOC), client call centre, and ticketing system**

Always focussed on your service delivery infrastructure, the NOC is the central monitoring station that performs correlations between triggered alerts and appropriate responses. Fully-staffed and on alert 24x7x365, the NOC is also your product's eyes and ears for monitoring system health and performance.

End-user support is a key component in successfully deploying SaaS. End-users that encounter application-related issues must have a primary point of contact for escalating issues. Responsible for receiving and processing all support calls 24x7x365, a call centre must have policies and procedures in place, designed to help end-users who call in with issues and a clear path for escalating the issue to an appropriate resource for resolution.

To support the infrastructure, a ticketing system is required that connects the human components across the organisation (NOC, operations delivery team, etc.) to issues management. A robust ticketing system provides the organisation with a consistent view into the issues impacting SaaS delivery, from end-user support to application development.

? **Design and manage an SLA**

Based on the components that comprise your SaaS offering, the task force should then work with the marketing team to develop a comprehensive SLA that meets end-user expectations. Key SLA elements include application availability, infrastructure alert response time and call centre response time.

? **Document and manage the solution**

Once deployed, the operations team must document the entire infrastructure, noting any nuances or areas of concern related to custom components. The documentation should take advantage of automated tools and be available within a centralised knowledge base.

Once your infrastructure is in place, all components are working together, and your SaaS offering is bringing in revenues every day, ongoing success will result from diligent management. To that end, daily, weekly, and monthly maintenance task lists should be produced for every device in the infrastructure.

Summing it up

This high-level overview describes a proven methodology for successfully starting operations with SaaS. It is important to note, however, that there is no substitute for domain expertise. Therefore, the most critical element to have in place before taking on this challenge is a team of experts in operations and engineering who have previously designed, built and managed complex infrastructures.

The author is Senior Vice-president, Operations and Engineering, OpSource Inc. He can be reached at john@opsource.net