



Can an Enterprise Email Backbone Infrastructure be Moved to the Cloud?

Overview

Moving data center infrastructure and business applications “to the cloud” continues to be the hot topic amongst senior executives and IT professionals—in fact the hype has some executives thinking that everything but the office kitchen sink can be moved to the cloud. Contrary to this, Gartner indicates in their recent hype cycle research¹ “Cloud Computing has reached the peak of its hype cycle and is poised to drop in the ‘trough of disillusionment.’” This is certainly the case when it comes to email infrastructure—many Fortune 1000 IT professionals are becoming disillusioned as their messaging infrastructure cloud initiatives stall. Why? Simply put, they are discovering it’s not only about migrating end-user email, it’s also about supporting myriad departmental email-generating applications and SMTP-based programs—many of which they did not know existed. When all is said and done they discover that in addition to having to keep the email backbone on-premises and under their control, they also need to modernize their existing email backbone in order to take advantage of the cloud at all. This may seem counter intuitive, so let’s break down the messaging infrastructure into logical layers to see why this is the case.

“This (the move to cloud) is happening in a very fragmented, ad hoc way because of real business needs—the problem is these ad hoc projects often go in place without a strong focus on security and no attention to longer-term architectural issues resulting in a mess of systems that do not work well with one another.”

— John Hagel, co-chairman Deloitte
Center for the Edge Research Center

Messaging Infrastructure Overview

The typical enterprise messaging infrastructure has some combination of the following three layers:

1. **Gateway Layer** — inbound malware filtering, simple routing and security
2. **Groupware Layer** — mail stores with simple policy and user-user message delivery
3. **Email Backbone Layer** — Directory-driven policy and security enforcement, intelligent routing, and core infrastructure for SMTP-based applications

The first two layers of the infrastructure have proven to give enterprises the best ROI for moving to the cloud.

The Gateway Layer which filters inbound email is the easiest to migrate. Spam and virus filtering technologies have become commoditized and there is minimal security risk in having a third-party filter inbound email before delivering it to the end-user groupware mailbox. From an OPEX perspective, the hardware required to manage the Gateway filtering function can be eliminated along with the costly maintenance, support, and management of those systems.

The Groupware Layer (Microsoft Exchange, IBM Lotus Notes, etc.) has proven to be more technically challenging to migrate to the cloud, but it also provides the greatest ROI—some enterprises dedicate up to 95 percent of their IT messaging support team to manage this layer. The ROI that can be achieved by moving this layer to the cloud often outweighs some of the perceived security implications.

This leaves the question:

Can an Enterprise Email Backbone Infrastructure be Moved to the Cloud?

The third layer, sometimes referred to as the email backbone, email middleware, or the messaging fabric, is the core infrastructure that glues the on-premises departmental SMTP-based applications together as well as the layers of the infrastructure that have moved to the cloud. Virtually all enterprise IT managers who thought they could migrate this layer to the cloud first discovered that, in practice, the ROI was just not compelling and there was very little to gain in doing so—on average only 5 percent of IT messaging support resources are used to manage this layer as compared to the Gateway and Groupware Layers. Secondly, and possibly more importantly, they are discovering the potential high cost of re-configuring or re-coding the

departmental SMTP-based applications to interface with the cloud. The sheer number of applications along with performance, security, and technical limitations—such as applications being hardwired to specific IP addresses and to other departmental systems—often makes it impractical to even consider moving this layer to the cloud. To illustrate, empirical data shows us that the level of effort to migrate from 10 SMTP-based applications to 100 can be 1000 times greater (EID)?

So the answer to our question is yes, you could move your email backbone to the cloud, but why would you want to?

- Is it technically feasible?
- Is it secure?
- Is it practical?
- Is there an ROI?

Departmental Email-generating Applications and SMTP-based Programs

It's well understood that virtually all businesses rely on groupware email systems for human-to-human communications, and is the most compelling part of the email infrastructure to move to the cloud. What comes as a surprise to many IT organizations during their cloud-sourcing projects is just how many different departmental applications there are that rely on the email infrastructure—in some cases literally thousands of different systems and applications. To illustrate, let's look at some real world examples.

Application-to-Application Communications

A bank receives requests for wire transfers from other banks, trading firms, and other institutions via email. The email messages are received by the corporate mail system, but contain special coding that tells the system to bypass mail filtering and to route the message via SMTP to the correct backend ERP system. The backend system handles the validation and verification and automatically releases the funds over the wire—all without human intervention.

Failure to complete the transaction within the agreed upon time limits between banks carries a significant financial penalty, therefore it is critical that wire messages don't get caught in spam filters or be delayed by human intervention. This SMTP-based approach to wire fulfillment gives bank personnel an easy method for manually verifying wire transactions without interfering with the time sensitive transaction.

Another good example is an ordering system that generates email messages and sends them to a warehouse fulfillment application. The warehouse application receives the message and prints a "pick sheet" so the warehouse personnel can fulfill the order. Let's look at the message flow of the application below to illustrate inefficiencies the cloud can sometimes impose on the infrastructure.

1. An order comes into the organization and is processed by an order processing application.
2. The order processing application emails a pick sheet to the warehouse application. If the email backbone infrastructure is in the cloud, then the pick sheet message leaves the organization into the cloud email infrastructure
3. The cloud infrastructure determines that the message should be routed to the warehouse application. The message is routed back into the organization to the warehouse application, which then prints the pick list.
4. The picker confirms the order is being picked which generates a message back to the order system (an acknowledgement).
5. That acknowledgement goes back out to the cloud infrastructure, only to be routed back to the organization.

Does it make sense to have all of this traffic between the cloud and the internal infrastructure for two applications that might be down the hall from each other?

Application-to-Human Communications

There are literally thousands of examples of departmental applications and systems that communicate via email to humans—copiers, scanners, and office printers can all send email to end-users and are some of the more obvious examples. Internal alarm systems of various types send urgent alerts via SMTP to personnel responsible for maintaining those systems. Billing, invoicing, and alert systems that automatically notify customers via email when account transactions take place, is common place today. The number of these types of applications found in the enterprise can be staggering, and the complexity and effort to migrate them to the cloud may not provide sufficient payback.

Human-to-Application Communications

There are hundreds of these types of applications found in the enterprise as well. For example, banks give ATM customers the option to have their transaction receipts sent via email. The ATMs are on private and secure networks that communicate via SMTP to the backend customer systems which handle transaction data and customer notifications. CRM and ERP systems, help-desk, and IT support applications are additional examples of SMTP-based applications that humans (your customers and employees) interact with on a daily basis. Some of these applications may be easier to migrate to the cloud than others, but are you willing to give up control of these types of applications?

Message Security and Policy Requirements

Above and beyond the requirements to support myriad departmental email applications, there are a number of other risks, challenges, and business-specific requirements that should also be considered before embarking on a project to outsource enterprise email infrastructure to the cloud—for example:

- What types of regulatory compliance laws require your company's compliance?
- Does your company have stringent corporate governance policies that must be followed?
- What are your encryption requirements—user-to-user, application-to-user, gateway-to-gateway?
- Does your organization have requirements for complex message handling that requires custom message header rewriting, stripping, and manipulation?
- Does your email system need to interface with corporate directories (which contain sensitive information) for policy enforcement, intelligent message routing, and custom message handling?
- What are your message archiving and data retention requirements?
- Do IT personnel require access to message logs and control over message tracking?

Future Proofing and Enabling Enterprise Email Infrastructure for the Cloud

The promises of cloud computing can be realized by migrating certain layers of the messaging infrastructure to the cloud, however, enterprise IT organizations need to be cautious and take a strategic and incremental approach. Virtually all large companies and government agencies are discovering that to effectively enable cloud computing for their messaging infrastructure, a hybrid architecture with a modern on-premises email backbone is required. A well architected modern messaging infrastructure gives businesses the agility required to adapt quickly to changing application requirements without being hindered by the constraints of cloud providers. Those enterprises that take this type of pragmatic approach to cloud computing will reap the benefits not only today, but also well into the future.

“The most common misperceptions about cloud computing are about security—it is often believed that the cloud is a lawless wasteland where data and programs float across the globe vulnerable to predators and user naivety, however, an equally prevalent misconception is that the cloud is secure and ready for use by any application—both are wrong.”

—Lynette Ferrera,
CSC

Sendmail Messaging Architecture Review

To help enterprises properly plan an email infrastructure cloud migration project, Sendmail offers a comprehensive Messaging Architecture Review. A Messaging Architecture Review is comprised of a thorough review and assessment involving input from your company's messaging team and other key business units. To support this, Sendmail Messaging Architects review your existing architecture and implementation, as well as current issues and concerns, to develop the following:



- Business objectives
- Short-term recommendations
- Long-term recommendations
- Recommended roadmap
- A comprehensive report and presentation, delivered to the organization for review and analysis.

Additional information:

White Paper: Moving to the Cloud—

Important Things to Consider before Migrating your Messaging infrastructure to the Cloud

http://sendmail.com/pdfs/whitepapers/wp_moving_to_the_cloud.pdf

Internet Research Group Market Report—

A Messaging Fabric: The Case for a Messaging Infrastructure Layer

<http://www.irg-intl.com/whitepapers.html>

Footnotes

1. Gartner Hype Cycle for Cloud Computing, July 2010
2. Empirical Infrastructure Data (EID): The effort for on-premises to cloud conversion is directly related to the number of SMTP applications involved. The approximate transfer function is: $\text{Effort} = A e^{\sqrt{N}}$ where A is a constant and N is the number of SMTP applications.

About Sendmail, Inc

Sendmail provides message processing appliances, applications, and services that enable enterprises to modernize their messaging infrastructures resulting in optimal email systems and lowered operating costs. Since 1982, thousands of customers around the globe have relied on Sendmail open source and commercial products for intelligent email backbones that solve the complex problems of policy-based message handling and routing between email systems such as Microsoft Exchange or IBM Lotus Notes and the Internet. The award-winning Sentrion Message Processors provide enterprises with a core messaging platform available in hard appliance, virtual appliance, and blade server configurations that can be customized with add-on applications available from the Sentrion App Store. Sentrion Message Processors and applications address the challenges of gateway management, inbound threat protection, outbound data leak prevention, full email content scanning for regulatory compliance, and intra-company message management all on a single, yet powerful, messaging infrastructure platform. Sendmail is headquartered in Emeryville, CA with sales and support offices throughout the Americas, Europe, and Asia.



Sendmail, Inc.

6475 Christie Avenue, Suite 350, Emeryville, CA 94608 USA

Tel: +1-888-594-3150 | Fax: +1-510-594-5429

Email: info@sendmail.com

www.sendmail.com