Noah Built The Ark Before The Flood

Why proactive monitoring of your services architecture is critical and cost efficient.

This white paper is sponsored by GSX Groupware Solutions

and was written independently **by Paul Mooney**

Overview

During the last four months of 2008, the global business community has undergone the largest economic crisis in a generation, possibly the largest in over seventy years. In this time of mergers, consolidations, takeovers, and economic instability, the last thing any business of any size desires is the loss of critical information services. Now is not the time to radically change any of your system architectures already in place. Instead, you should be looking to ensure that the systems you have in place are operating as reliably and efficiently as possible.

Since 2004, Bill Buchan (www.billbuchan.com), a long suffering colleague of mine in the Lotus community, and myself have collected stories related to large scale outages on Lotus Domino sites, ranging in size from 50 users to 128,000 users. For instance, there is a story about simple code changes applied directly to a production environment on a critical business application. These changes "accidently" executed and started replicating globally, effectively shutting down business for three days as the IT department had to repair the damage.

These horrific events, which would scare any IT service engineer or manager, have been collected on the Worst Practices website (www.theworstpractices.com), as well as becoming a conference session. "The Worst Practices: Learning From The Mistakes Of Others" has become a mainstay and "must-see" session at IBM's premier conference, Lotusphere.

Although presented in a very "tongue in cheek" fashion, the presentation conveys a serious message: simple mistakes can happen very easily. Effective prevention, monitoring, and education are essential to ensure it doesn't happen to you.

The cost of downtime

Call-logging statistics give us some insight into the causes of critical errors over a wide array of companies. Where I work, we track and monitor all support calls logged. From the standpoint of prevention, over 40% of the critical errors logged could have been prevented by simple monitoring. With monitoring software, that percentage could easily increase to 60%.

These critical errors caused downtime and revenue loss for companies, along with the associated levels of panic and fire fighting that comes with these situations. These errors are caused by two main issues. First, the companies did not have adequate system monitoring in place. Second, they did not have written and/or updated contingency plans for system recovery.

Critical system downtime is a costly process. Placing a currency value on that cost is difficult, but it is widely understood that it always costs more than you think. Consider an email outage in your company. For better or worse, email is used as a file server by many people and can be their storage location for important files. At one point, it was estimated that approximately 60% of business process data was

retained in email systems as opposed to document management systems. When email is not accessible due to an outage there are numerous cost points:

- Cost of IT Operations staff working to get services back online
- Cost of lost productivity for business staff (This is often underestimated)
- Loss of revenue linked to unavailable systems

There are numerous other intangible costs, including morale, trust in the services, and reputation. Although they may not be associated with a hard currency cost, they need to be recognised and acknowledged.

Size doesn't matter…

Every business is cost intolerant. Downtime costs money, sometimes a lot of money. With relation to companies and costs, size doesn't matter. It's a fair case to say that larger enterprise companies sometimes move at such a glacial pace that downtime may not visibly affect their bottom line. On the other hand, small businesses (SMB's) and fast-moving companies can have their profit margin severely impacted by an incident. One particular automotive company experienced downtime of one application in 2007. The outage lasted for a single day. The estimated cost of this downtime was estimated at 300,000USD. SMB's have lost revenue for a quarter, or even longer, in a single, critical outage.

New systems by acquisition

With the current global economic woes, companies are merging at a feverish pace to stay solvent and avoid bankruptcy. When this occurs, they suddenly have two or more different work environments that have to play well together. This is critical if the systems are to assist in the business merging process. The idea of "rip and replace", a wholesale replacement of technology platforms, on one side of the merge is typically not an option. There are already financial constraints in place, as well as requirements to minimise changes in process. System stability is even more important in this situation, as services cannot seem to have worsened due to business change. That would affect morale and trust in the new structure of the company. Customer morale, witnessing mergers may already be shaken. Loss of service in these times, or worsening responses, cannot help a sometimes precarious situation.

Mobile technologies

The evolution of mobile technologies in business has been fascinating to watch over the past 15 years. The industry has gone from Apple Newtons to Palm PDAs to Windows Mobile devices, Blackberries and iPhones. Blackberry set the bar for email communication and basic Personal Information Management, or "PIM", four years ago, and they still lead the field for secure and reliable products for business. The irony is that mobile devices are only now living up to the advertising from ten years ago. While Blackberries have been the product of choice for business email during the last four years, applications on mobile devices are coming to the market, and are being adopted at a rapid pace. At one time it could be argued that mobile email was a "non critical frill". Now it is a business necessity.

Another reality is that mobile email devices have established themselves with senior management in all industries and government. From sales staff to senior executives to CEOs, not to mention presidents of

entire countries, mobile devices are almost always in the hands of the boss. And the boss does not like to live without their mobile email and applications when a critical system is down.

Effective monitoring reduces fire fighting

All too often, good *monitoring* skills and technologies are mistaken for good *troubleshooting* skills and technologies. Being great at locking the barn door after the horse has bolted is useful to any business, but monitoring prevents the issue from happening in the first place.

The approach to monitoring the environment

Different companies deal with system monitoring in different ways, Generally, they can be grouped into the following categories:

1. **Do Nothing**

The highest risk option for any company is to do no monitoring whatsoever. In this situation, notification of an issue is triggered by a customer complaint. Immediately, the business is on a defensive footing, fire fighting their way into discovering the cause and a remedy as quickly as possible. Once resolved, the company returns to not monitoring the services at all, tempting fate to bring the next outage.

Although the obvious cost of the "do nothing category" is in the loss of service and fire fighting costs, morale is a serious issue here. Due to the lack of proactive monitoring, skilled technicians have to fire fight and deal with frequent customer complaints. They will quickly lose morale and enthusiasm in their job. Conversely, the business users and customers will quickly lose faith in the IT Services department. This leads to a high turnover of skilled staff, and constant hiring and training of new hires.

2. **Reactive Monitoring**

This category of system monitoring typically occurs when a business has been affected by a serious outage of a service. They decide to monitor that service in the future, and the monitoring process is put in place. Although resources and processes are assigned to monitoring that particular service, related services are not monitored. Although the same technical outage may not happen again, the same service outage caused by a related service failure is easily possible.

3. **Typical Monitoring**

The standard monitoring in business utilises native tools within specific technical products. This allows knowledgeable staff to monitor the services on a scheduled basis, checking for errors and potential issues. Although this is a substantial improvement on the earlier categories, there are numerous downsides to this approach:

- Skilled staff with knowledge of the systems is required to monitor the services. They need to specifically know and understand each monitoring tool in order to effectively utilise it.
- Typically the native monitoring tools in any service product (e.g. MS Exchange, Lotus Domino, or Blackberry Enterprise Server) are limited in nature.

- Time required to actively monitor services is required.

4. Proactive Monitoring

Proactive monitoring is the safest method of monitoring the services, and it negates the need for specialised staff and scheduled monitoring. This method uses dedicated software to monitor the services in a straight-forward fashion. Dashboard interfaces, similar to those used in business portal applications, should be used to display the current system statuses. This type of interface means that non-skilled staff can interpret the status of the environment, where a simple amber or red light beside a service indicates a potential problem. At that point, skilled staff can be called in to investigate. The advantages to this approach are obvious:

- 1st level helpdesk staff can monitor a dashboard constantly, informing skilled staff of a potential issue only when needed. Skilled staff can be called upon only when needed.
- The expensive skill set of the technical staff is resourced onto appropriate high-value tasks.
- Management has an instant snapshot of the state of the environment.

Managed services , and software as a service offerings are finally infusing its way into the common marketplace for companies of any size. Hosted hardware and services are a worthy consideration for companies planning ways to reduce their overall IT costs. Moving to a service-based architecture or full managed service-based architecture should not reduce your monitoring demands, however. In fact, it should reinforce your requirement to monitor your services which are now in the hands of a supplier.

A typical managed-service agreement includes the requirement that the supplier monitors all services and reports back to the customer. In the case of downtime, the supplier is responsible for the problem resolution. Unfortunately, downtime is downtime regardless of where the system is hosted, and this inevitably has an impact on the business. Monitoring these services, regardless of where they are hosted, permits the IT staff to constantly have an understanding of the current situation. It also reduces the time it takes for the organization to react to the outage, possibly even to the point where the business catches the outage before the supplier informs the business. No service company will ever know your business as well as you do. What is deemed critical in your environment can vary from quarter to quarter, month to month, or even day to day. Relinquishing all monitoring to the supplier adds another level of business risk, and could be dangerous to the profit or even the existence of the company.

What to monitor

Every environment is different, each with their own configurations and business classifications of critical systems. That being said, there are generic statistics that should be monitored regardless of product or version:

Service availability

Be it Lotus Domino, Microsoft Exchange, Blackberry Enterprise Server or any other product, monitoring software should ensure that the services are running and available.. If any server or service becomes unavailable, it needs to be flagged on a dashboard so that it proactively informs the support desk that there is a serious issue.

Delayed or pending email

Email is the backbone of communication in the business. Your monitoring software should be able to identify any delay or failure in mail routing on a timely basis.

Communication

Applications in the business typically uses data pulled from many sources. This information is gathered via replication, XML data integration, web services, ODBC, or many other methods. In order for this service to function correctly, the servers must be able to communicate with the sources necessary to obtain the data. Ensuring that server-to-server communication is available and functioning is an absolute must.

Conclusion

You may not have had any system outages recently, but it *will* happen at some point. Hopefully this whitepaper has convinced you that system monitoring is not an option that you can afford to ignore. The money spent up-front to acquire and install a robust monitoring system will pay off for your business, both in increased uptime, decreased outages, and IT staff that can be building new systems to allow you to better compete with your competitors.

About Paul Mooney

Paul Mooney is Senior Technical Architect for Bluewave Technology (www.bluewave.ie). Between Bluewave and it's sister company BE Systems (www.besystems.eu), they offer a vast array of IBM Lotus Domino development and administration skills, servicing Europe, the Middle East, and Asia. Paul is a 12 year veteran of Domino and related IBM Lotus products, and is a frequent speaker at IBM and Lotus events around the world. His blog site (www.pmooney.net) contains many infrastructure-related tricks, tips and articles covering IBM, Domino, Blackberry, iPhone and any other technology that catches his interest.
