Eliminating End User and Application Downtime

Protecting the Mobile Messaging Ecosystem

March 2010

Table of Contents

Introduction

Messaging is the lifeblood of modern business. While email, mobile messages and mobile applications are critical to business success, not enough organizations are taking the proactive means to protect them from unplanned and planned downtime. This whitepaper discusses the criticality of messaging, the impact of messaging downtime and the importance of providing continuous availability for the entire messaging ecosystem.

Keeping Workers Productive 24x7

Email is at the center of an organization's communication and collaboration strategy. It is the key to keeping the lines of communication open. Customer service, competitive tendering, internal workflow, supplier negotiations and even disaster communications are all examples of business processes dependent on email.

Senior executives and field-based employees rely on their mobile devices to help them make the right decision at the right time. It is imperative that their mobile devices keep information flowing whether they are at the airport, in the car, at an on-site meeting or during a host of other activities.

While email, mobile messaging and mobile applications are critical to business processes, they also keep end users productive well beyond standard business hours. According to a 2009 Forrester Report, sponsored by RIM, a business can benefit anywhere from $35,506 - $64,780 in increased business efficiency over three years from a single BlackBerry Smartphone. With revenue and user productivity at stake, the goal of keeping business communication flowing makes mobile messaging mission-critical.

Mobile Messaging High Availability and Disaster Recovery

Few corporate messaging systems and mobile applications work in isolation. Email systems are reliant on anti-virus systems. Completion of an intranet form likely triggers a workflow that involves email and SQL based applications.

Emails themselves reference public folder entries, documents on file systems and increasingly extended content in SharePoint deployments. The interrelated nature of corporate processes demands that all of these components be made continuously available. But, the requirement goes further.

Managing availability of interdependent components means that for performance reasons, a failover of a BlackBerry Enterprise Server, for example, to a remote disaster recovery site should also trigger a failover of the associated email server (Exchange, Domino or GroupWise) to the remote site to ensure additional performance issues are not introduced. Neverfail's wide

range of application support means the mobile ecosystem can be protected against the unexpected.

The Business Impact of Downtime

Business stops when messaging is down. Without email access, your company's productivity, reputation and revenue are at risk. When you consider remote and mobile workers, who rely heavily on mobile devices, they are simply ineffective in the event of an outage. These on-the go employees require continuous and reliable availability of mobile data and messages.

For some implementations, the impact of downtime might be limited, for others it can be significant. However, in all cases it is vital to assess the impact from an end-user perspective. Can IT staff provide 24 hour operational cover in the event of a critical application outage? Is it sufficient for a user to alert them of an issue? If immediate action is required, shouldn't application monitoring integrated with automated failover be a mandatory requirement? If a data failure will require recovery from a backup, then continuous replication should be mandatory across all messaging components.

Due to the fact that the messaging ecosystem is comprised of multiple applications and servers, if multiple technologies are used, it is highly likely there will be conflict and contention when it comes to dealing with an outage. As with many things, the more simple the approach, the less potential there will be for failure. Identifying a business process level and integrated approach to local and remote failover is important; it will provide the most cost effective solution for continuous availability.

Protecting the Messaging Ecosystem

Keeping lines of communication open is mission-critical to all types of organizations. Nothing less than continuous availability is acceptable for messaging. This means protecting the end-to-end infrastructure 24x7. As discussed earlier, messaging does not rely on the email application alone, but also on many different components such as anti-virus, anti-spam, mobile email servers and associated SQL databases. They are also part of an extended ecosystem that is used to ultimately deliver the business service.

The result is that protection of the email infrastructure against downtime needs to be complemented by protection of the SQL, ActiveSync and BlackBerry Enterprise Servers as well. This is the only way the end-user experience can be fully protected.

Messaging Continuous Availability

The ultimate goal should be to isolate users from the impact of messaging downtime. When applications are critical, organizations need to think in terms of "no business downtime". For

business critical systems, this means continuous availability is necessary. When dealing with less critical systems, data protection or pure disaster recovery strategies may be sufficient.

If the priority is to protect data and provide a mechanism for recovering the entire messaging ecosystem then learning all the ins and outs of content recovery, backup/restore, clustering, mirroring, log shipping and other tools may be a suitable approach if sufficient resources are available.

This process will consume a great deal of time, requiring scripting and using the command line interface while not overlooking a single piece that could turn out to be critical for the entire operation to work. Significant ongoing maintenance and validation will be required to deal with new configuration details. If a pro-active approach to downtime is required, some sort of monitoring tool is recommended.

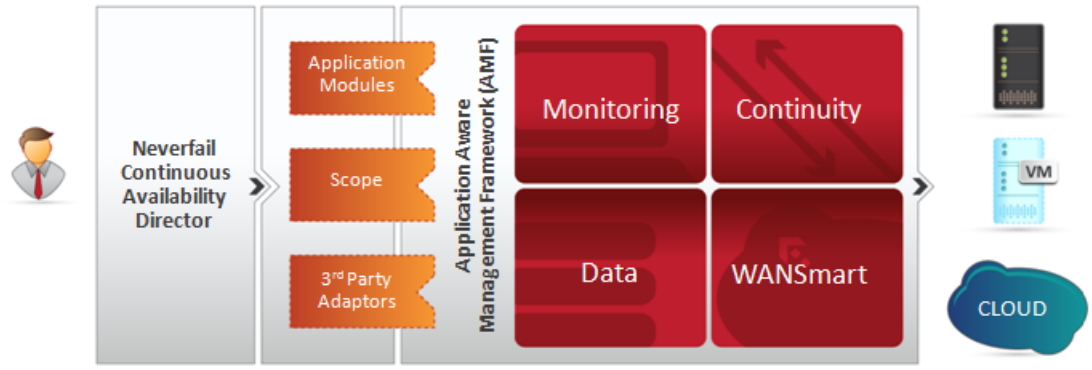
Backups, versioning, clustering, network load balancing, database mirroring and log shipping are all important tools to protect the business from messaging failure; however, this approach alone will result in business disruption which can result in days of downtime while the ecosystem is rebuilt from scratch.

Continuous availability can only really be achieved by addressing potential outages at all levels. Outages can be unplanned database failures or planned interruptions to perform system maintenance. These outages may affect individual servers as well as whole messaging ecosystems and depending on their nature may require local or remote failover. As a result, the deployment architecture must be designed to deal with all eventualities.

For companies in which messaging downtime cannot be tolerated, the only option is a continuous availability solution that delivers integrated high availability and disaster recovery as a complete solution to protect the entire messaging infrastructure.

Neverfail Solutions for Mobile Messaging Environments

The key to providing protection for the entire messaging ecosystem lies in the Neverfail Continuous Availability Suite. This is a complete solution designed to deliver continuous availability for business critical applications, such as email and mobile messaging.



To eliminate user and application downtime, the Neverfail solution is architected from the ground up to protect data through continuous replication. It monitors the health and state of applications and enables automated failover or manual switchover to additional local and/or remote servers. This provides a business centric, continuous availability solution for the messaging environment. As part of the approach, the Neverfail software maintains a second, complete, consistent and up-to-date copy of all messaging components and configuration data. This is more than just a copy of the data. Neverfail provides a "ready-to-go" clone of the components, including any configuration changes that may have been applied since the database, index and application servers were first installed.

To guard against configuration creep, Neverfail's Application Management Framework provides automatic and ongoing discovery of all data associated with the protected applications, including related registry changes, and automatically adjusts the replication schema accordingly. This means there is no need to manually specify existing and additional application data locations to be protected.

Taking things further, the Application Management Framework then uses out-of-the-box policies to control monitoring of the components in a messaging environment, with the option to alert IT staff to potential issues and execute tasks according to pre-defined rules. These policies, rules and tasks provide complete protection for all messaging components, and can be further configured through a unique point-and-click interface, without the need to create complex scripts.

In short, Neverfail ensures the application is immediately fully functional and available in the event of an automated failover or a simple "one-click" manual switchover.

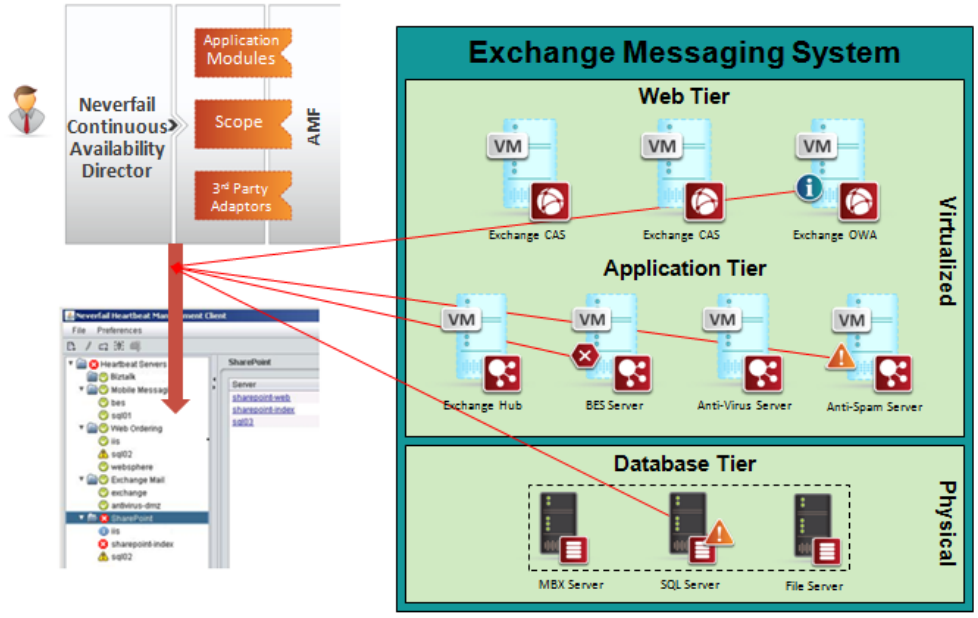
Managing Full-Ecosystem Failover with Neverfail

As messaging environments increase in size and complexity it becomes important to make the entire ecosystem resilient to deliver both high availability and disaster recovery. Application resiliency cannot be achieved by making individual servers redundant. It requires a more holistic approach that protects email together with related applications such as SQL and mobile messaging servers.

There are a number of fundamental requirements for full ecosystem failover. Most important is a consistency of technology used. The potential for things to go wrong is directly influenced by the number of different technologies. Each technology requires separate administration, different policies and IT admin staff to learn different ways of managing the technology. Equally important is having a central point of management which gives an integrated view of availability, and enables a single point of control.

To deal with the level of complexity required, Neverfail has a unique approach in which the Neverfail Continuous Availability suite can be used to protect each individual component while at the same time providing a view of the entire messaging environment. This gives IT staff the ability to manage the failover configuration, activities and state from a single technology set.

In addition to protecting each component within the ecosystem, Neverfail includes a central management console – The Neverfail Continuous Availability Director. This unique interface provides an enterprise-wide, business-centric view of critical applications and IT services. It has a flexible approach which allows logical grouping of application, database, messaging and other servers. The grouping provides a way of visualizing interdependencies across servers and gives a central console where events, alerts and the overall health can be viewed.



In The logical grouping provides a very convenient way of visualizing and managing your messaging infrastructure. If there are any issues with email, mobile messaging or other server, alerts can also be routed to the Availability Director so that the extended ecosystem can be managed.

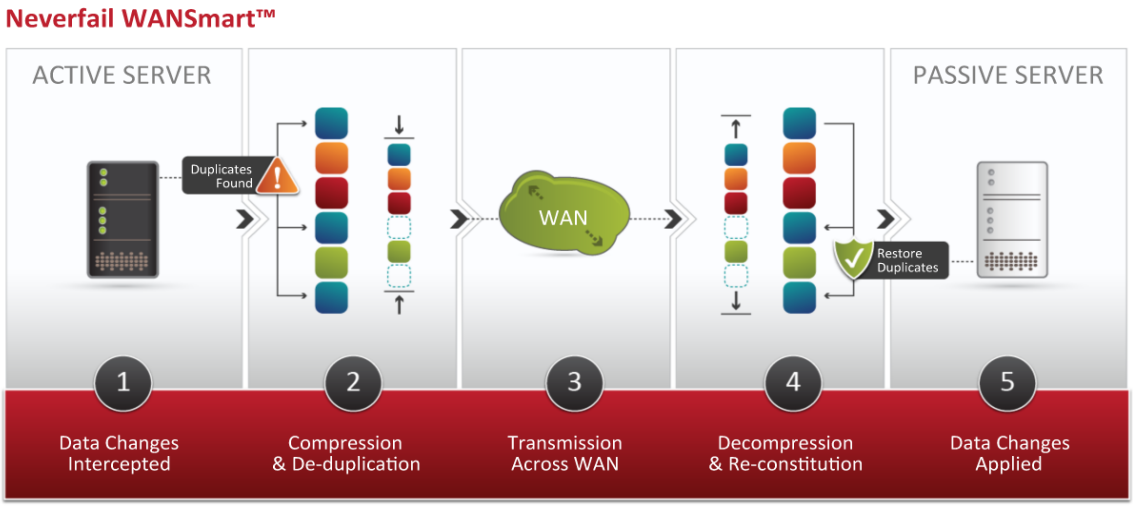
Optimized for Local and Remote Deployments

Traditional solutions for high availability and disaster recovery have restricted the level of protection against outages. Very restrictive requirements for network latency and bandwidth have been a significant barrier to stretching messaging protection to remote sites in order to guard against events such as power failures, floods and other site-wide issues.

Until now, the result has been a compromise. Even where high availability tools, such as clustering, have been deployed locally, the impact of a power outage or local storage failure has resulted in significant downtime because legacy disaster recovery approaches have been unable to meet the required service levels. The Neverfail Continuous Availability solution includes patent-pending technology which allows cost-effective deployment of a multi-tiered solution for continuous availability. At the heart of this is Neverfail WANSmart™.

Neverfail WANSmart provides patent-pending de-duplication based WAN optimization through a software component in the suite. It frees implementations from bandwidth and latency constraints which would otherwise prohibit the protection of individual messaging components.

WAN—and making their deployment feasible.



Neverfail WANSmart can be used to reduce the bandwidth costs associated with implementing a stretched high availability architecture where primary and secondary servers are deployed across a WAN. In addition, WANSmart can be used as an integral part of a multi-tier architecture where high availability is integrated with disaster recovery using Neverfail Tertiary™.

Neverfail Tertiary allows three servers to be used to provide high availability and disaster recovery in one solution controlled by the Continuous Availability Director. This model entails Neverfail software maintaining local and remote clones of the application, database and other servers.

Neverfail Customer Experience

Numerous organizations have selected Neverfail to provide continuous availability for their messaging environment. One example is DB Schenker Rail (UK) Ltd, the UK's largest rail freight haulier, employing almost 4,000 people and operating hundreds of freight trains every day.

For DB Schenker Rail, BlackBerry smartphones have become an essential tool for the mobile workforce. With more than 300 BlackBerry users, they required a solution to ensure the mobile workforce would have continuous access to their BlackBerry smartphones and associated applications. In order to achieve an end-to-end, resilient messaging infrastructure, DB Schenker Rail needed to find a continuous availability solution that, in addition to protecting the BES itself, would also protect the associated Exchange and SQL Servers so that the actual applications accessed via their BlackBerry smartphones would also remain available 24x7.

DB Schenker Rail selected Neverfail to protect their Exchange, SQL and BlackBerry Enterprise Servers because with Neverfail, they have a solution that provides seamless failover, flexibility, reliability and continuous end-user availability.

In Summary

Neverfail is unique because it's the only continuous availability solution can proactively manages the availability of the entire messaging ecosystem. It protects critical applications against physical server hardware, network infrastructure and operating system and application failures. If a problem occurs Neverfail can take a variety of pre- emptive, corrective actions including application failover.

The net result is the elimination of end-user downtime and continuous availability for the mobile messaging ecosystem.

www.neverfailgroup.com