



## Five Considerations for Choosing a Microsoft Exchange Continuity Solution

Software Business Division

---

How long can you afford your email server to go down? Five minutes? Ten minutes? One hour? Email communication is critical to today's business. Email system continuity, high availability (HA) or disaster recovery (DR) is an issue for any business, regardless of its size; after all, if communication halts or the data lost, critical business operations and revenue streams could be disrupted.

### Introduction

The Microsoft® Exchange server continues to dominate the corporate messaging market. For most businesses, the Microsoft Exchange system handles all of a company's email needs. As a critical service to business success, email reliability and recovery are even more vital than ever.

With so many businesses running on Microsoft Exchange, its availability and recovery capabilities are a concern to any company's system administrator.

Given the variety of available technologies and products with numerous features and cost differences, it can be confusing and time consuming to evaluate and select the right solution to ensure continuity of critical Microsoft Exchange systems in your organization.

This guide discusses five areas to consider when evaluating the right solution for your business.

■■■ Finding the optimal email system continuity solution is more than just meeting functional and performance needs. It is also important to consider the hidden complexities and costs associated with any solution.

## Five Considerations

1. Usability and Manageability
2. Application and Data Recovery Performance
3. Unplanned and Planned Downtime Mitigation
4. Hidden Solution Costs
5. Deployment Options

### 1. Usability and Manageability

Most organizations, especially small and medium enterprises (SME) and enterprise remote offices and branch offices (ROBO), have limited IT resources and need solutions that are easy to deploy and simple to manage.

Often, email system continuity solutions require the integration of multiple products in order to provide full protection and recovery of applications and data. Such solutions many times require the administrator to use multiple tools with little or no integration. This increases the complexity of the solution that could result in lower productivity.

#### Consider this...

*How many tools or management consoles are required to monitor the health and status of your overall system (e.g. application and data)? Are they easily accessible from a Web browser or from a client system located on the network without a separate installation? Solutions that require multiple management consoles and tools or provide remote monitoring and configuration capabilities are more complex to use and can result in lower productivity and effectiveness.*

*Does the solution require the integration of multiple products to provide both application and data protection and recovery? Integration of multiple products, even from the same vendor, can be very complex and time consuming since the products are likely developed by different development groups. These solutions can also be less reliable due to the intricate dependencies between application and data protection under a wide ranging of system failure conditions*

### 2. Application and Data Recovery Performance

A critical email system is constantly dodging bullets and avoiding traps, but eventually its luck will run out and the system will go down – and when it fails, unplanned outages average almost an entire business day, with over 25% of outages lasting more than two days.

The ideal methodology for Microsoft Exchange system outage mitigation comes in the form of a system continuity solution. Some “dial-tone” recovery solutions will only provide a substitute email server to enable sending and receiving of new email messages without access to any previously saved messages, contacts, or calendar items. Some are solutions that rely on traditional data backup products and technologies that can lose hours or even days of data in the event of a Microsoft Exchange system failure. The best solutions provide real-time synchronous data mirroring so all critical email data can be recovered on a standby system without loss.

In terms of recovery time, some solutions require manual recovery procedures that can take hours or days to bring a functional system online with recovered data. Such solutions are generally ill-suited for business critical systems and may not meet relevant regulatory compliance requirements. For these situations, solutions need to provide fast and automated recovery with little or no data loss.

**Consider this...**

*How quickly does the solution recover both the Microsoft Exchange application and data? Are you down for 2 minutes or 2 hours? How much is that costing your company in time, resources, lost revenue and productivity? Are you looking for a continuity solution to provide near-instant system recovery, minimizing email communication interruption and preventing critical loss of email, contacts and calendar data?*

*Does the solution provide fast and automated recovery against all major failures that can occur in the hardware, software, network or site? If your organization is located at a single location with only onsite users, then fast recovery against hardware and software failures isn't a primary concern. However, if your Microsoft Exchange system serves many mobile or remote users, then you should consider a solution that can also provide fast recovery across geographical sites. Such capability is also critical if your site is prone to natural disasters or is at risk of attack or sabotage.*

*How much email data can you afford to lose? Ten minutes...30 minutes...2 hours? If you have a very low data loss tolerance, then you should consider a solution that provides synchronous data mirroring. By replicating critical data to the standby server in real-time, synchronous data mirroring ensures that the live server and backup server always match, virtually guaranteeing full recoverability and zero data loss.*

However, the network infrastructure required for synchronous mirroring is generally more costly, so it may not be justified for all Microsoft Exchange data protection. In many organizations, low data loss tolerance only applies to certain users or groups (e.g. executives, legal department, etc.). In these situations, you should look for a solution that can provide both synchronous and asynchronous mirroring to address the different Microsoft Exchange user data and to realize optimized balance between low data loss and low cost of ownership.

### 3. Unplanned and Planned Downtime Mitigation

Critical email systems can become unavailable for many reasons, but there are generally two types of scenarios: unplanned and planned.

Unplanned downtime is caused by unexpected failures, including hardware component failures, application and OS failures, damaged hardware from power surges, and natural disasters, network problems and site failures.

Planned downtime is typically caused by planned hardware and software maintenance tasks in order keep an email system healthy. Other causes include network infrastructure

maintenance, system testing, equipment moves and power grid maintenance.

Many email continuity solutions only detect certain types of failures or do not provide fully automated recovery in case of unexpected failures. While some email continuity solutions provide adequate recovery for unplanned downtime mitigation; they provide little support for fast restoration to the original operating condition after the primary server is replaced or repaired. This can make system restoration a long and difficult process and all but unusable for planned downtime mitigation.

**Consider this...**

*Does the solution provide fast detection and recovery against all major system failures?*

*Does it detect hardware, software network and site failures? A comprehensive solution should address all potential failures relevant to your situation.*

*Does the solution support automated recovery without requiring manual reconfiguration on the Microsoft Exchange servers, network switches or routers, or Microsoft Outlook client application? A solution that requires any manual reconfiguration may do little to reduce unplanned downtime in case of unexpected failures.*

*Is planned downtime a significant portion of the total downtime of your system? Do you have to deal with the complex logistics and inconvenience associated with off-hour maintenance for planned Microsoft Exchange or OS patch installation?*

For planned downtime mitigation you should consider not only whether a solution supports fast recovery, but also fast restoration. *Does the solution provide a fast and easy way to move applications and data access between servers? Does it support rolling upgrades of hardware and software? Does it provide incremental data resynchronization to enable fast restoration? Does it allow a replaced or repaired primary server to be on the same network as the standby server simultaneously for easy restoration?* If the solution cannot perform all of these functions, it may not meet your planned downtime mitigation needs.

A practical planned downtime mitigation solution should enable you to quickly migrate active applications and data workloads from one server to another prior to the start of maintenance activities, and then quickly restore the normal operating configuration after the completion of maintenance activities. This type of solution can drastically reduce planned system downtime and associated business service disruption and productivity loss.

#### **4. Hidden Solution Costs**

Finding the optimal email system continuity solution is more than just meeting functional and performance needs. It is also important to consider the hidden complexities and costs associated with any solution.

Some solutions may require a major OS and Microsoft Exchange upgrade to a higher cost Enterprise Edition. This significantly increases the solution cost in additional software license fees, and deployments, and migration time.

There are other solutions that require the integration of multiple products to provide protection and recovery for applications and data. These have higher costs due to longer and more complex deployment and higher ongoing operational costs due to usage of multiple non-integrated tools.

Lastly, there are solutions that have high hidden costs because they require additional server or storage hardware resources.

**Consider this...**

*Does the solution support Standard and Enterprise editions of OS and Microsoft Exchange?*

If you are in an SME or ROBO environment, then support for both may be especially important. It is also something to consider as your organization and email system grows.

*Are you looking for a solution to provide integrated application and data protection and recovery? Solutions that require the integration of multiple products are typically less robust due to separate development and quality assurance processes, even within the same company.*

*Does the solution require external storage arrays or proprietary storage systems from specific vendors? Does it require additional servers for management or operational support? Such requirements can drastically increase the solution cost and should not be overlooked.*

## 5. Deployment Options

Microsoft Exchange system deployment can be varied greatly even within a single organization. Systems may differ by location, network infrastructure, server and storage hardware. A solution that can not support a broad range of deployment scenarios may be costly to maintain or replace as your organization evolves.

**Consider this...**

*Does the solution support multiple Microsoft Exchange servers sharing an external storage system? Does it support a standalone server with only internal disk storage? A solution that only supports external storage systems may not be suitable for ROBO environments.*

*Does the solution support synchronous real-time data mirroring for maximum data protection in high-speed network environments? Does it support asynchronous best-effort data mirroring for less critical data over low bandwidth and long latency WAN links across hundreds or even thousands of miles? Does it allow an easy change between synchronous and asynchronous data mirroring modes? A solution that supports only asynchronous data mirroring can mean a lower performance and protection level for critical data even in a high-speed network. Conversely, solutions that support only synchronous data mirroring will require higher cost network infrastructure, even when the benefits do not justify the cost.*

## Summary

This guide is a tool to help you consider the pros and cons of the variety of available

technologies and products out there. Below is a worksheet that can help you decide what is best for your environment and to meet your requirements, so you can select the right solution to ensure continuity for the critical Microsoft Exchange systems in your organization.

Considerations	NEC ExpressCluster	Conventional HA Clustering Solutions	Conventional Server Replication Solutions	Another Solution
<b>1. Usability and Manageability</b>	<ul style="list-style-type: none"> <li>Unified application and data protection, and recovery management</li> <li>Pure Web console</li> </ul>	<ul style="list-style-type: none"> <li>No data protection monitoring or management</li> <li>Fat GUI management console</li> </ul>	<ul style="list-style-type: none"> <li>No individual application resource protection and recovery</li> <li>Fat GUI management console</li> </ul>	
<b>2. Application and Data Recovery Performance</b>	<ul style="list-style-type: none"> <li>Fast automated application and data recovery</li> <li>Sync mirroring for no data loss</li> </ul>	<ul style="list-style-type: none"> <li>Good application recovery performance</li> <li>Limited or no data protection and application protection.</li> </ul>	<ul style="list-style-type: none"> <li>Asynchronous mirroring only</li> <li>Whole server recovery only</li> </ul>	
<b>3. Unplanned and Planned Downtime Mitigation</b>	<ul style="list-style-type: none"> <li>Robust failure detection and recovery</li> <li>Easy workload migration and system restoration</li> </ul>	<ul style="list-style-type: none"> <li>Primitive failure detection</li> <li>No recovery against storage system failures</li> <li>Limited planned downtime mitigation</li> </ul>	<ul style="list-style-type: none"> <li>No recovery against individual application failures</li> <li>Complex manual system restoration required</li> </ul>	
<b>4. Hidden Solution Costs</b>	<ul style="list-style-type: none"> <li>Standard and Enterprise OS and Microsoft Exchange support</li> <li>Internal and external storage support</li> </ul>	<ul style="list-style-type: none"> <li>Enterprise OS and Microsoft Exchange required</li> <li>External storage required</li> <li>Extra support server required in some cases</li> </ul>	<ul style="list-style-type: none"> <li>Enterprise OS and Microsoft Exchange required in some cases</li> <li>Dedicated idle standby server required</li> </ul>	
<b>5. Deployment Options</b>	<ul style="list-style-type: none"> <li>Mirrored or shared storage support</li> <li>LAN or WAN support</li> </ul>	<ul style="list-style-type: none"> <li>Limited asynchronous data replication support only</li> <li>Limited WAN support</li> </ul>	<ul style="list-style-type: none"> <li>No shared storage support</li> <li>Limited LAN performance</li> </ul>	

**NEC CORPORATION**  
**IT Platform Global Business Development Division**  
 1-10, Nisshin-cho, Fuchu  
 Tokyo 183-8501, Japan

Email: [info@expresscluster.jp.nec.com](mailto:info@expresscluster.jp.nec.com)  
 Web: [www.nec.com/expresscluster](http://www.nec.com/expresscluster)

© 2008 NEC Corporation. All rights reserved. Specifications subject to change without notice. NEC is a registered trademark and Empowered by Innovation is a trademark of NEC Corporation. All other trademarks are the property of their respective owners.