

The Microsoft MVP Guide to Exchange Availability

10 Essential Rules that Will Save Your Job

Paul Robichaux, Microsoft Exchange MVP
Chris Scharff, Microsoft Exchange MVP
Ben Winzenz, Microsoft Exchange MVP

Brought to you by MessageOne™

MessageOne's Emergency Mail System™ (EMS™) provides guaranteed email continuity. When your Exchange servers become unavailable, EMS allows users to continue to send and receive email through a web browser or via a BlackBerry® wireless device without interruption. Today, more than 700 CIOs at companies including DaimlerChrysler, Time Warner, and Marriott depend on MessageOne to ensure that email is always available – no matter what. Learn more at www.messageone.com/mvp.

Introduction

It's a very bad day when Microsoft Exchange goes down.

Unfortunately, achieving high availability with Exchange can be a daunting task: a wide variety of software, hardware, directory, storage, network, and datacenter problems are always lurking. Each one has the potential to bring email down.

MessageOne has seen many causes of downtime: an idiot with a backhoe cutting the fiber line, an executive emailing his 7 GB ripped video of a Grateful Dead DVD, termites in the data center, a night visitor accidentally shutting down power – not to mention the mundane failures caused by human error, technical problems, and natural disasters.

This pocket guide provides 10 essential rules that will help you ensure that email is always available, no matter what. It was written by three Microsoft Exchange MVP's to help Exchange Administrators avoid many of the pitfalls that can lead to painful downtime.

Rule No.

01

**Simplify,
Simplify,
Simplify.**

01 Simplify, Simplify, Simplify.

Highly complex availability solutions create new risks that increase their cost and value. Aircraft engineers have known this rule for a long time: extra bells and whistles add weight and cost and sap agility, performance, and maneuverability.

The same is true for your availability solution design.

Instead of larding up your infrastructure with complexity, search for solutions that reduce the number of failure points by removing unnecessary components, consolidating functions where it makes sense to do so, eliminating processes that you don't need, and streamlining whatever you keep.

The Zen masters teach that you can only reach Nirvana by letting go of your possessions; to reach high availability nirvana, you must simplify in exactly the same way.

Rule No.

02

**Know Thy
Enemies**

02 Know Thy Enemies

GI Joe's motto is "*Knowing is half the battle.*"

That's as true for Exchange availability as it is for plastic action figures.

Your efforts to build a highly available Exchange system depend on knowing what failure points exist in your design and what you can do about them. Some of these failure points will be outside your control, like security flaws in the software you run or the quality of your local utility company's electrical service. Most of these lurking enemies, though, are yours to command – and destroy!

First, you have to know where your infrastructure is vulnerable; then you have to have the training and knowledge to know how to best fix those vulnerabilities without violating Rule #1. For example, understand the history of your failures and what caused them – were they SAN-related, related to a specific upgrade process, or something else?

Rule No.

03

**Is that a Tool
or a Weapon?**

03 Is that a Tool or a Weapon?

George Washington said that government, “*like fire, is a dangerous servant and a terrible master.*”

So it is with the Exchange maintenance tools we depend on to fix things when they go wrong. *Eseutil* and *isinteg* (and lesser-known tools available from Microsoft support that you may have heard of) are wonderfully useful in the right circumstances – but in untrained hands, or when used for the wrong reasons, they can irreparably damage your data.

Know what these tools are for, how to use them, and when *not* to use them. Don't experiment with these tools on your production servers (that's what Virtual PC is for), and don't plan on running them as part of your normal maintenance routines. If you get into a situation where running these tools seems like a good idea, stop and think – and consider calling Microsoft's PSS if you're not 100% sure that you're choosing the right tool for the job.

Rule No.

04

**Clusters, Not
Cluster Bombs**

04 Clusters, Not Cluster Bombs

Clusters are like nuclear weapons: they're expensive, they require lots of maintenance, and they don't solve the problems most people think that they do. They're both devastating if improperly used or secured. Despite this, they are much sought-after.

If you're considering using clusters, or if you've already got them deployed, ask yourself whether your cluster implementation actually delivers the benefits you want. Clusters are great at protecting against single points of hardware failure, and they make rolling upgrades of the operating system easy. They can also be used to provide higher availability than standalone systems *when properly designed and used with appropriate storage systems*.

To get the most out of your clusters, carefully study Microsoft's recommendations for cluster design and sizing; buy only hardware that appears as "cluster-certified" on Microsoft's hardware compatibility list, and gain experience with cluster management and setup by using Virtual PC or VMware before you take the big plunge.

Rule No.

05

**Take Care of
Your Spare to
Avoid a Scare**

05 Take Care of Your Spare to Avoid a Scare

You probably wouldn't drive your car across the country without a spare tire.

Likewise, you probably shouldn't operate your Exchange servers without a good backup and recovery plan. Backups are your last-ditch safety net; they can save your data when the protective mechanisms built into Exchange and your server hardware have failed you. However, it pays to be sure that your safety net doesn't have any holes in it. You, and everyone else on your messaging team, should be intimately familiar with how your backup procedures work. Everyone on the team should be able to do a restore, on demand, of anything from a single mailbox up to an entire server (including the operating system). The best way to develop this level of skill is to practice—a lot. Doing so will build your confidence level *and* your skill.

Apart from the question of whether your backups and restores *work* is the question of whether they meet your business needs. Be sure that your restore processes—including media retrieval, the actual restore, and any post-restore operations—can be completed during the amount of time you've specified as your recovery time objective (RTO). Also, you need to ensure that your backup captures all the data you need for a complete restoration—don't forget Active Directory, the Windows Certificate Services certificate authority, your anti-spam filters, and any other data that you'd need to completely reconstitute your Exchange operations.

Rule No.

06

**Know the
Difference
between HA,
DR and BC**

06 Know the Difference between HA, DR and BC

Modern messaging operations impose two requirements: protect your data (and be able to recover it) and minimize downtime. They're related, but not identical, and they have different requirements that you must know and meet:

- **Disaster Recovery (DR)** is being able to come back from a failure, whether large or small. DR may involve restoring from conventional backups, moving work to another node in a cluster, or shifting operations to an alternate location. For example, if your server explodes because someone spilled a diet Coke in it, and you restore it, that's DR.
- **High availability (HA)** is being able to *avoid* failures in the first place. RAID, clustering, and redundant power supplies all provide elements of HA capability. If your server explodes, and no one notices because its work automatically moves to another cluster node, that's HA.
- **Business continuity (BC)** is being able to keep with some (possibly degraded) degree of functionality while a disaster recovery is taking place. If your server explodes and you switch messaging operations over to your remote data center or a hosted service while you're repairing it, that's BC.

DR is something basic that every organization must implement to some degree, even if it's only the "spare tire" level. **HA** is something that most organizations choose to implement at some level; **BC** is usually what those organizations are trying to achieve.

Rule No.

07

**Monitor,
Monitor,
Monitor.**

07 Monitor, Monitor, Monitor.

If a tree falls in the forest, does anyone hear it? I don't know. I *do* know that if your server falls over, you're going to hear about it when users start calling your help desk—or you—to complain. Before that happens, you should take advantage of the monitoring tools built into Windows and Exchange to keep tabs on your servers' performance, health, and behavior.

Windows' basic performance monitoring tools will tell you when resource usage goes outside of preset limits, and these indications can give you valuable advance warning of problems. If you can't measure your systems' performance or availability, you can't manage to improve it. Watch message flow, resource usage, and uptime to figure out where potential weak spots are. If you depend on non-Exchange servers for message hygiene or filtering, keep an eye on them, too, to make sure that you get early warning of problems with inbound or outbound message flow.

For large or complex networks, the money you spend on a solid monitoring package like Microsoft Operations Manager or HP OpenView will be money well-spent because you'll be able to get timely notifications of queue buildups, unexpected changes in disk space usage, and other conditions that can lead to Exchange problems if not corrected in a timely manner.

Rule No.

08

**Ruthlessly
Drive Out
SPOFs**

08 Ruthlessly Drive Out SPOFs

Writer and explorer Antoine de Saint-Exupery nailed this rule: *“You know you’ve achieved perfection in design, not when you have nothing more to add, but when you have nothing more to take away.”*

As you design your Exchange system, you should ruthlessly identify and remove every individual single point of failure (SPOF) that you can find. You may find SPOFs in your physical infrastructure, your Exchange design, your DNS or Active Directory configuration, your processes, or even your people. (after all, if you have even one irreplaceable person on your team, what happens when they’re not available?)

The first step to implementing this rule is to identify any area where you have potential SPOFs (which we define loosely as any single service, server, or component whose failure can interrupt your messaging operations). Next, rank the SPOFs twice: once according to their potential for failure and once according to the cost of fixing them. Use these rankings to decide what to fix first according to your operational requirements and budget requirements. Finally, fix things (at all times being sure to remember Rule #1!).

Rule No.

09

| D2D N-O-W

It's cheap and easy. No, not vending-machine dinners—disk-to-disk backup.

The fastest way to back up Exchange data is to use a disk as the target medium; this gives you much faster backups—and thus quicker recoveries—than using tapes, at a per-gigabyte cost that compares favorably with many tape-based solutions. You can take one (or more, space permitting) disk-to-disk backups, then selectively write them to tape when it's convenient. This hybrid approach gives you fast backups, low overhead, and quick recoverability, plus long-term archival and storage.

You don't need any additional software to do this, because Windows' built-in *ntbackup* utility can make disk-to-disk backups of Exchange right out of the box. Third-party backup utilities add more flexible scheduling and a wider range of backup options, but because the bundled tools give you a cheap way to get started, you should start investigating how disk-to-disk technology can improve your backup and recovery processes.

Rule No.

10

**Don't Trade
Performance
for Availability**

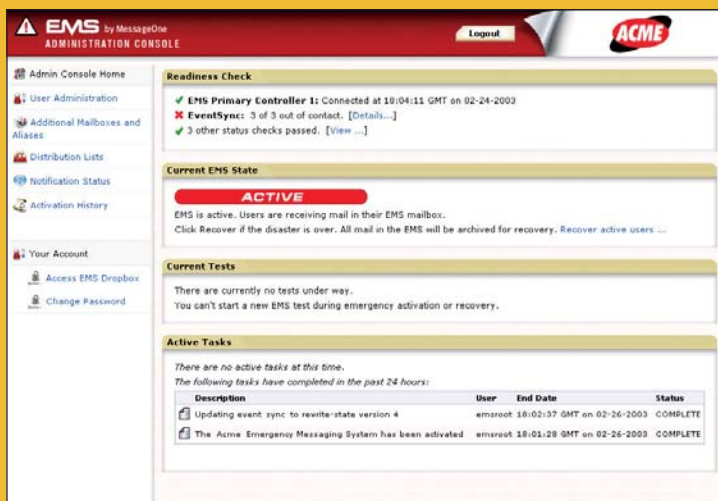
10 Don't Trade Performance for Availability

Life is all about tradeoffs; the more successful you are at making the *right* tradeoffs, the better off you're likely to be.

This is true for your Exchange design too—picking the right combination of hardware, software, and design elements makes it possible for you to have your cake and eat it too.

The type of RAID system you use, the number of physical disks you use, and the number and size of your database and storage groups—these factors have a huge influence on the balance between performance and availability in your system. For the best mix, choose a RAID level that's appropriate for your recovery needs (RAID-1 + 0 is generally best, but RAID-5 is workable in many environments) and back it with the right number of physical disks to give you an adequate number of I/O operations per second (IOPS).

When you combine the right design principles with good monitoring and solid backup, you'll find that your performance and availability both rise to meet your expectations.



EMS by MessageOne
ADMINISTRATION CONSOLE

Logout 

Admin Console Home

- User Administration
- Additional Mailboxes and Aliases
- Distribution Lists
- Notification Status
- Activation History

Your Account

- Access EMS Dropbox
- Change Password

Readiness Check

- ✓ **EMS Primary Controller 1:** Connected at 18:04:11 GMT on 02-24-2003
- ✗ **EventSync:** 3 of 3 out of contact. [Details...]
- ✓ 3 other status checks passed. [View ...]

Current EMS State

ACTIVE

EMS is active. Users are receiving mail in their EMS mailbox.
Click Recover if the disaster is over. All mail in the EMS will be archived for recovery. Recover active users ...

Current Tests

There are currently no tests under way.
You can't start a new EMS test during emergency activation or recovery.

Active Tasks

There are no active tasks at this time.
The following tasks have completed in the past 24 hours:

Description	User	End Date	Status
Updating event sync to rewrite-state version 4	amsroot	18:02:37 GMT on 02-26-2003	COMPLETE
The Acme Emergency Messaging System has been activated	amsroot	18:01:28 GMT on 02-26-2003	COMPLETE

MessageOne's Emergency Mail System provides guaranteed email continuity. When your Exchange servers become unavailable, EMS allows users to continue to send and receive email through a web browser or via a Blackberry wireless device without interruption.

MessageOne EMS: Guaranteed Exchange Availability

No matter what may happen to your physical facilities, data centers, servers, software, network connectivity, or IT staff, MessageOne's Emergency Mail System (EMS) guarantees that email will always be up and running.

EMS is a Linux-based standby email system that is automatically synchronized with your primary email environment. In the event of an emergency or planned outage, EMS can quickly be activated over the Web or by phone. In less than minute, selected email users will have direct access to a fully functional Web-based email account that allows users to send and receive email from their standard email address. The standby account includes all of the key features of the primary email system including contact lists, calendar appointments, distribution lists, and important historical email.

Today, millions of users depend on EMS at more than 700 companies to ensure that email is always available. EMS is the only affordable solution to address the shortfalls of tape backup and traditional mirroring and replication solutions. It is easy to use, inexpensive, and can be installed in a few hours.

The bottom line: EMS provides guaranteed email continuity – no matter what.

EMS includes the following features:

- **Guaranteed 60-Second Email Continuity** – Activate in less than 60 seconds to provide any employee with full email & BlackBerry access during an email outage. EMS ensures that email never bounces and that email system outages are never evident to the outside world.

- **Emergency Access to Historical Email** – EMS intelligently synchronizes historical email to your standby email system based on your organization's needs. For example, you can provide executives with a full email history, managers with the last five days of email, and other employees with no email history at all in their EMS inbox.
- **Automated Synchronization** – Automatically synchronizes corporate directories, user accounts, contacts, calendars, and distribution lists to secure SunGard & IBM data centers.
- **Designed for Immunity** – Linux-based system provides immunity from viruses and database corruption that may cause downtime in the primary Exchange environment.
- **Quick Recovery** – After an outage, EMS automatically moves all sent and received email back to the primary system in one step, with all forensic information intact.

Learn More

Learn why leading companies depend on MessageOne's Emergency Mail System to ensure that email is always available. Visit www.messageone.com/mvp or call **888-367-0777** for white papers, product information, or to request a web-based demo.

About the Authors

Paul Robichaux

Paul Robichaux is a principal engineer for 3sharp. A well-known corporate messaging expert, Paul is an MCSE and a Microsoft Exchange MVP. He is the author of several books, including *The Exchange Server Cookbook* (O'Reilly and Associates), and creator of the <http://www.exchangefaq.org> Web site.

Chris Scharff

Chris Scharff is a Senior Systems and Sales Engineer at MessageOne. Chris, a MCSE and a Microsoft Exchange MVP, serves as the technical/reviews Editor and Columnist at Microsoft Exchange & Outlook Magazine and has contributed to a number of best-selling reference titles on Microsoft Exchange including the ever popular Nutshell and Pocket Consultant Guides. Chris holds a Bachelor's degree from Iowa State University.

Ben Winzenz

Ben Winzenz is a Senior Systems and Sales Engineer at MessageOne and a Microsoft Exchange MVP. Ben holds a Bachelor's degree from Brigham Young University.

For Further Reading...

Visit **www.messageone.com/mvp** for direct access to our Microsoft MVP product resources including:

- **“Avoid Exchange Availability Pitfalls”** – A whitepaper by WindowsITPro author Ed Roth that describes the most common Exchange problems and pitfalls.
- **“Why Email Fails”** – A whitepaper analyzing real world Microsoft Exchange failure data.
- **“Building the Business Case for High Availability Email”** – A thorough analysis of the economic and business drivers for high availability exchange architectures.
- **“The Paradox of High Availability”** – A webinar featuring Gartner, Inc. analyst Donna Scott discussing the pros and cons of various approaches to high availability for Exchange and other Windows applications.
- **Direct access to EMS product information.**

Visit **www.messageone.com/mvp** today!

MessageOne™

www.messageone.com/mvp
1-888-367-0777

MessageOne, Inc.
11044 Research Blvd.
Building C, Fifth Floor,
Austin, TX 78759