TECHNICAL PAPER

Clustering Strategies for MailSite SP

Version 11

A MailSite Technical Paper

November 2026

© 2026 Rockliffe Systems, Inc. All rights reserved. MailSite is a registered trademark of Rockliffe Systems, Inc. All other trademarks are the property of their respective owners.

Contents

1 Introduction 2
2 Basic Clustering 3
2.1 Message Flow 3
2.2 Benefits and Disadvantages 3
2.3 Installation and Configuration 3
2.4 Monitoring 4
2.5 Backup 4
2.6 Adding Capacity 5
2.7 Failure Scenarios 5
3 Standard Clustering 6
3.1 Message Flow 6
3.2 Benefits and Disadvantages 6
3.3 Installation and Configuration 6
3.4 Monitoring 7
3.5 Backup 7
3.6 Adding Capacity 7
3.7 Failure Scenarios 7
4 Advanced Clustering 9
4.1 Message Flow 9
4.2 Benefits and Disadvantages 10
4.3 Installation and Configuration 10
4.4 Monitoring 10
4.5 Backup 10
4.6 Adding Capacity 11
4.7 Failure Scenarios 11
5 Using ETRN with MailSite SP 12
6 Additional Assistance 13

© 2026 Rockliffe Systems, Inc. · www.mailsite.com

1 Introduction

This paper presents three strategies for deploying MailSite SP 11 in a clustered environment. It describes the advantages and limitations of each strategy and gives the steps for setting up MailSite in each one.

The right clustering method and network design depend on the needs of each site. Treat these strategies as a guideline, not as sizing advice.

In every configuration in this paper, MailSite runs on standard Windows Server. It does not need a clustered version of Windows.

A MailSite 11 cluster is two or more Windows servers that serve the same domains and mailboxes. Every server runs the complete set of MailSite services: SMTP, POP, IMAP, ExpressPro webmail, the Console, Exchange ActiveSync, Exchange Web Services (EWS) and MAPI over HTTP for Classic Outlook. MailSite serves the web and Exchange protocols itself, so there is no IIS to install or configure.

All servers keep their mail and their settings in one shared mail store on a file server. MailSite 11 keeps its configuration in SQLite databases inside that mail store, so there is no SQL Server database to set up. A change made in the Console applies to every server. Each server keeps only a few things of its own: its license key, its log directory, its mail spool and its certificates.

Many sites run the MailSite servers as virtual machines. That makes it easy to add a server or to take a broken one out of service. In this paper a MailSite server can be a virtual or a physical machine. The file server that holds the mail store is usually a dedicated, well-protected system, because every MailSite server depends on it.

© 2026 Rockliffe Systems, Inc. · www.mailsite.com

2 Basic Clustering

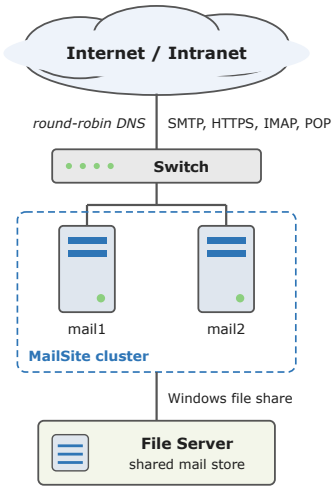
The simplest MailSite 11 cluster has three Windows servers:

- Two MailSite servers, each running all of the MailSite services.
- One file server holding the shared mail store.

In this configuration mail can arrive at either MailSite server, and both deliver messages to the mail store on the file server. Likewise, any POP, IMAP, ExpressPro, ActiveSync, EWS or Outlook connection can reach either server, and either server can open any mailbox.

Round-robin DNS spreads mail and client connections between the two servers. Fail-over is not automatic: DNS does not notice a failed server, so you change DNS by hand to send everyone to the surviving server.

The MailSite servers reach the mail store through a Windows file share.



2.1 Message Flow

Mail enters the cluster from the internet or the local network over SMTP, at either MailSite server. That server keeps each message in its own spool directory until it is delivered. It then relays the message to a remote domain over SMTP or delivers it to a mailbox in the shared mail store.

People read their mail by signing in to either server over IMAP, POP, ExpressPro, ActiveSync, EWS or MAPI. The server reads their mailbox from the file server through the file share. A change made through one server, such as a message moved to another folder, reaches clients connected to the other server.

2.2 Benefits and Disadvantages

The benefits of this configuration are simplicity and cost. No load balancer is needed and the setup is short. Both servers read the same configuration, so a security setting or any other change is made once. Monitoring is simple because there are few servers.

The disadvantages are limited fault tolerance and limited growth. Round-robin DNS keeps sending some clients to a failed server until you change it. The file server is a single point of failure: if it stops, neither MailSite server can reach mail.

2.3 Installation and Configuration

To set up this cluster, follow these steps. The MailSite 11 Administrator Guide gives the details of each step.

1. On the file server, create a folder for the mail store and share it. Because the mail store is disk-intensive, put it on a fast, reliable volume. Use a file server that fully supports Windows

file sharing and file locking: the MailSite servers rely on file locks so that two servers never change the same data at once.
2. Create a Windows user for the MailSite services. In a Windows domain, use a domain account. Give it full control of the mail store folder and access to the MailSite program folder on each server.
3. Install MailSite on the first MailSite server with the MailSite installer (the PowerShell installation command or MailSite Setup). Run the services as the Windows user from step 2. Make sure the mail store, which also holds the configuration, is on the shared folder.
4. Open the Console and create your domains. Set each domain's mailbox root directory and mail list root directory to network (UNC) paths under the shared folder, for example `\\data\mailstore\domain1.com`.
5. Create the mailboxes.
6. On the second server, install the same MailSite release as the same Windows user. Then join it to the installation with `msdbma.exe join`, giving it its own license key (see "Adding a server" in the Administrator Guide). The installers do not do this step.
7. Give the second server the certificates its clients need (see Transport Layer Security below), then add it to DNS.

You can manage the cluster from the MailSite Console on any computer, or from the Console in a web browser.

2.4 Monitoring

Watch processor and memory use on both MailSite servers. High processor use can mean a lot of incoming mail or many people using webmail or Outlook at once. Task Manager shows which MailSite service is responsible, for example SMTPRA for incoming mail, IMAP4A for IMAP or HTTPMA for the web.

In the Console, Server, Services shows each service's status and its log. Watch the queue age, mailbox growth and certificate expiry. If processor or memory use stays high, add another MailSite server.

Watch the free space on the file server so that its disks never fill up.

2.5 Backup

- Back up the whole mail store, including the configuration and mailbox databases inside it, as one consistent copy. The message files alone cannot rebuild database-only data such as Outlook items, flags and synchronization state.
- For an offline backup, stop MailSite on every server that shares the mail store before you copy it.
- Back up the spool directory of each MailSite server every day, so that mail in transit can be restored after a failure.
- Back up each server's certificate files.
- Archive the log files of each server every week.
- Test a restore on an isolated server before you rely on the backup.

© 2026 Rockliffe Systems, Inc. · www.mailsite.com

2.6 Adding Capacity

To add mail processing capacity, add a third MailSite server. Install the same MailSite release, join it to the installation and give it its certificates, as in the steps above. Once it is tested and working, add it to the round-robin DNS.

For more storage, add disks to the file server and extend the volume that holds the mail store. If the file server cannot take more disks, bring a larger file server online and move the mail store, or the mailboxes of some domains, to it. When you move a domain's mailboxes, update that domain's mailbox root directory in the Console.

2.7 Failure Scenarios

- **If the switch fails:** all mail service stops until the switch is replaced.
- **If a MailSite service fails on one server:** clients that DNS sends to that server cannot use that service. Point DNS at the working server, repair the service, then restore round-robin DNS.
- **If a MailSite server fails:** clients that DNS sends to it cannot use any mail service. Point DNS at the working server. Repair the failed server, or install MailSite on a replacement and join it to the installation. Mail waiting in the failed server's spool is delivered once that server is back with the same spool directory, so repair it rather than discard it.
- **If the file server fails:** no mail service is available and the MailSite servers cannot deliver mail. Restore the file server as quickly as possible, or replace it and restore the mail store from backup.

© 2026 Rockliffe Systems, Inc. · www.mailsite.com

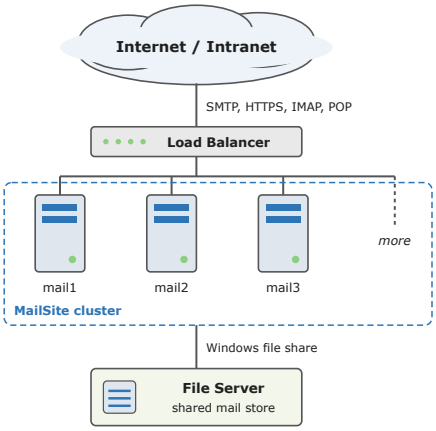
3 Standard Clustering

The standard MailSite 11 cluster has these parts:

- Three or more MailSite servers, each running all of the MailSite services.
- One file server holding the shared mail store.
- One load balancer.

Mail can arrive at any MailSite server, and all of them deliver to the mail store on the file server. Any client connection, whether IMAP, POP, ExpressPro, ActiveSync, EWS or Outlook, can reach any server.

Fail-over is automatic. If a server fails, the load balancer stops sending it new connections. Clients that were connected to it reconnect to the other servers and carry on.



3.1 Message Flow

Mail enters the cluster from the internet or the local network over SMTP. The load balancer passes each connection to one of the MailSite servers. That server keeps the message in its own spool directory, then relays it to a remote domain over SMTP or delivers it to a mailbox in the shared mail store.

People sign in through the load balancer to any MailSite server, with IMAP, POP, ExpressPro, ActiveSync, EWS or Outlook. The server reads their mailbox from the file server. MailSite does a mailbox's background work, such as indexing new mail, on the server its clients are using. When a server stops, the others take over its share of that work.

3.2 Benefits and Disadvantages

The benefits of this configuration are better fault tolerance, better performance and room to grow. Administration stays simple: all servers share one configuration, so a change made once applies to every server. The load balancer moves connections away from a failed or busy server.

The disadvantages are that the file server and the load balancer are still single points of failure. Every server runs every service, so heavy use of one service, such as many IMAP connections, can slow the others on the same server. More servers also mean more cost and more to manage.

3.3 Installation and Configuration

Follow the steps for Basic Clustering, with these changes:

1. Prepare the file server, the shared mail store folder and the Windows user for the MailSite services as before.

2. Install MailSite on the first server, create the domains with mailbox and mail list root directories under the shared folder, and create the mailboxes.
3. On each further server, install the same MailSite release as the same Windows user and join it to the installation with `msdbma.exe join`.
4. Check each server's mail spool directory in the Console under Server, Directories. Each server keeps its own spool; a local folder such as `C:\Program Files\MailSite\SPOOL` is a good choice.
5. Give every server the certificates its clients need.
6. Add every server to the load balancer, for SMTP, the client mail ports and HTTPS.

> **Publishing behind a load balancer.** Outlook can sign in with NTLM over MAPI, EWS and Autodiscover when you turn that on. MailSite does not offer NTLM to a request that says it came through a proxy. If your load balancer reuses connections between clients, use Basic or OAuth sign-in for Outlook, or publish MailSite directly.

3.4 Monitoring

Watch processor and memory use on every MailSite server. If one server is busier than the others, check the load balancer's distribution. Task Manager shows which MailSite service uses the most, and the Console shows each service's status and log. If use stays high across the servers, add another server.

Watch the free space and response time of the file server, the queue age and certificate expiry.

3.5 Backup

- Back up the whole mail store, including the configuration and mailbox databases inside it, as one consistent copy.
- For an offline backup, stop MailSite on every server that shares the mail store before you copy it.
- Back up the spool directory and the certificate files of each MailSite server every day.
- Archive the log files of each server every week.
- Test a restore on an isolated server.

3.6 Adding Capacity

To add mail processing capacity, deploy another MailSite server. Install the same release, join it to the installation, give it its certificates and test it. Then add it to the load balancer. A new server handles every protocol, so the same step adds capacity for webmail, phones and Outlook as well as for mail delivery.

For more storage, add disks to the file server and extend the volume that holds the mail store. If the file server cannot take more disks, bring a larger file server online and move the mail store, or the mailboxes of some domains, to it. Update the mailbox root directory of each domain you move.

3.7 Failure Scenarios

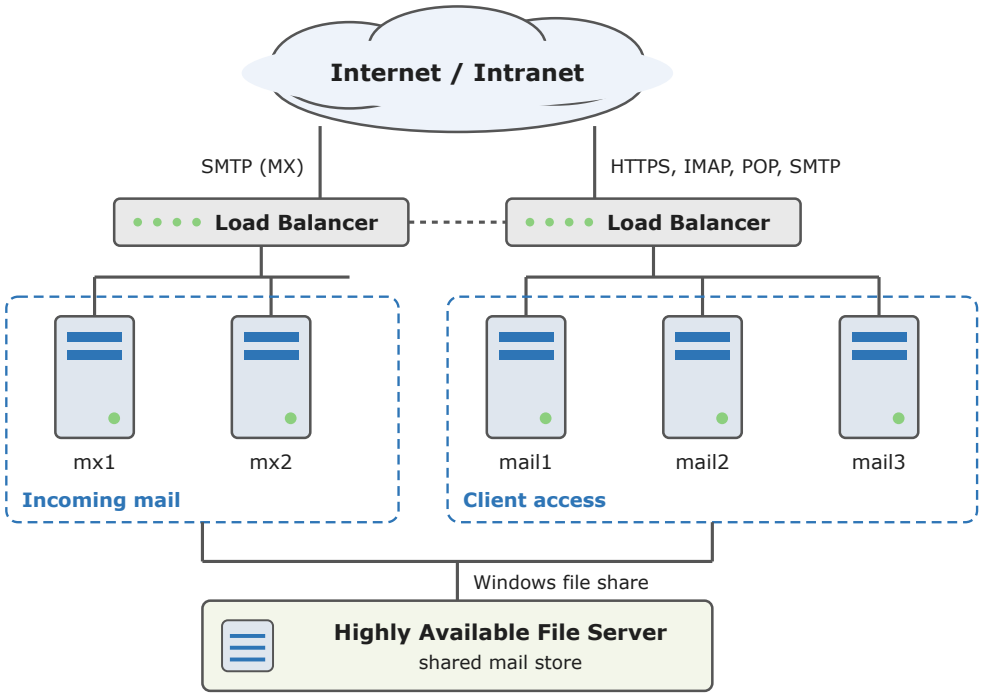
- **If the load balancer fails:** all mail service stops until it is replaced.

- **If a MailSite service fails on one server:** the load balancer sends that service's connections to the other servers. People who were connected may have to reconnect. When the service is back, the load balancer includes it again.
- **If a MailSite server fails:** the load balancer sends all connections to the remaining servers. People who were connected may have to reconnect. Repair the server, or install MailSite on a replacement and join it to the installation. Mail in the failed server's spool waits there until that server is back with the same name and spool directory; the other servers do not take it over.
- **If the file server fails:** no mail service is available and the MailSite servers cannot deliver mail. Restore it as quickly as possible, or replace it and restore the mail store from backup.

4 Advanced Clustering

The advanced MailSite 11 cluster gives each group of servers its own job. Every server is still a complete MailSite installation that shares the one configuration; the groups differ only in the traffic sent to them:

- Two or more MailSite servers that receive mail from the internet (mx1, mx2…). The domains' MX records point at them.
- Two or more MailSite servers for client access (mail1, mail2…). People's apps connect to them for IMAP, POP, sending mail over SMTP, ExpressPro, ActiveSync, EWS and Outlook.
- A highly available file server holding the shared mail store.
- Two load balancers, so that one can take over from the other.



4.1 Message Flow

Mail from the internet arrives through the load balancers at the incoming mail servers (mx1…). Each one keeps the message in its own spool directory and delivers it to the recipient's mailbox in the shared mail store. Replies and non-delivery reports that these servers create are sent from the same servers.

Mail that people send is received by the client access servers (mail1…). If it is for a local mailbox, it is delivered to the mail store. If it is for another domain, that server relays it over SMTP.

People read their mail by signing in to any client access server, with IMAP, POP, ExpressPro, ActiveSync, EWS or Outlook. The servers read the mailboxes from the file server.

4.2 Benefits and Disadvantages

The benefits of this configuration are the best performance, room to grow and fault tolerance. Spam floods and attacks from the internet reach only the incoming mail servers, so they do not slow down people's mail. Problems are easier to find, because each group does one job. Redundant load balancers and a highly available file server remove most single points of failure.

The disadvantages are the cost of more servers and a more complex setup. The file server must be designed for high availability; if the mail store is unavailable, no server can reach mail.

4.3 Installation and Configuration

1. Set up a highly available file server and share a folder for the mail store. It must fully support Windows file sharing and file locking.
2. Create a Windows domain user for the MailSite services, with full control of the mail store folder and access to the MailSite program folder.
3. Install MailSite on the first server, create the domains with mailbox and mail list root directories under the shared folder, and create the mailboxes.
4. Install the same MailSite release on every other server as the same Windows user, and join each one to the installation with `msdbma.exe join`.
5. Check each server's mail spool directory in the Console under Server, Directories.
6. Give every server the certificates for the host names that reach it.
7. Configure the load balancers: send SMTP for the MX host names to the incoming mail servers, and the client host names (SMTP submission, IMAP, POP and HTTPS) to the client access servers.
8. Set the security settings for the internet-facing traffic with the Console: relay restrictions, Brute Force Attack Protection (BFAP), anti-spam and anti-virus. These settings are shared by every server.

4.4 Monitoring

Because each group does one job, it is easy to see what uses the resources. Watch processor and memory use on the incoming mail servers to follow the level of incoming mail, including spam and attacks. Watch the client access servers for the number of people connected. If one group stays busy, add a server to that group.

Watch the free space and response time of the file server, the queue age on every server and certificate expiry.

4.5 Backup

- Back up the whole mail store, including the configuration and mailbox databases inside it, as one consistent copy.
- For an offline backup, stop MailSite on every server that shares the mail store before you copy it.
- Back up the spool directory and the certificate files of each MailSite server every day.
- Archive the log files of each server every week.
- Test a restore on an isolated server.

© 2026 Rockliffe Systems, Inc. · www.mailsite.com

4.6 Adding Capacity

To add capacity, deploy another MailSite server in the group that needs it. Install the same release, join it to the installation, give it its certificates and test it. Then add it to that group on the load balancers.

For more storage, add disks to the file server and extend the volume that holds the mail store, or move the mailboxes of some domains to a larger file server and update those domains' mailbox root directories.

4.7 Failure Scenarios

- **If a load balancer fails:** the other load balancer handles all traffic.
- **If a MailSite service fails on one server:** the load balancers send that service's connections to the other servers in the group. People who were connected may have to reconnect.
- **If an incoming mail server fails:** the load balancers send incoming mail to the other incoming mail servers. Sending servers keep messages that were in transit and send them again. No client connections are affected. Mail in the failed server's spool waits there until it is back, so repair it rather than discard it.
- **If a client access server fails:** the load balancers send client connections to the other client access servers. People who were connected may have to reconnect. No incoming mail is lost. Repair the server, or install MailSite on a replacement and join it to the installation.
- **If the file server fails:** no mail service is available until the mail store is back. Design the file server so that it can fail over by itself, and restore the mail store from backup if it cannot be recovered.

© 2026 Rockliffe Systems, Inc. · www.mailsite.com

5 Using ETRN with MailSite SP

ETRN (Extended Turn) is an SMTP command that asks another mail server to start sending the mail it holds for a domain. It is used for "store and forward" service, where a server keeps mail for a site that connects to the internet only some of the time.

MailSite 11 still answers ETRN, and the MSSTART utility sends it. A cluster is not a good place for a store and forward service, however. Each MailSite server keeps its own mail spool, so mail held for a domain can sit on any of the servers, and an ETRN request reaches only one of them.

MailSite SP is designed for large-scale mailbox hosting. If you also need to provide ETRN service, run it on a separate MailSite server outside the cluster.

6 Additional Assistance

Every hosting environment is different. For more about how a cluster works, read the Configuration Storage, Backup and Upgrade sections of the MailSite 11 Administrator Guide, the sample environments in “MailSite SP Sample Clustered Environments” and the “MailSite TLS Configuration Guide”.

Plan upgrades as a short outage for the whole cluster. All servers of a cluster run the same MailSite release, and most releases change how the services talk to each other, so a server refuses to work with one from another release. For such a release, stop MailSite on every server, upgrade them all with the installer, then start them again. The release notes say which releases this applies to. Install the whole package on each server; do not replace single services.

Each server loads its certificates from its own certificate folder. When MailSite requests or renews a certificate automatically, the new files are written on the server that made the request. Copy them to the other servers so that every server presents a valid certificate.

If you need help planning a MailSite SP cluster, contact Rockliffe at sales@mailsite.com with your mailbox count and availability needs.